(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 596 308**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.10.2006 PCT/IB2006/002742**

(87) Fecha y número de publicación internacional: **12.04.2007 WO07039806**

(96) Fecha de presentación y número de la solicitud europea: **03.10.2006 E 06808930 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.07.2016 EP 1997291**

(54) Título: **Método y disposición para autenticación segura**

(30) Prioridad:

03.10.2005 NO 20054549

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.01.2017

(73) Titular/es:

ALLCLEAR ID, INC. (100.0%)
823 Congress Ave, Suite 300
Austin, TX 78701, US

(72) Inventor/es:

TAUGBOL, PETTER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y disposición para autenticación segura

Campo de la invención

La presente invención se refiere al campo de la autenticación de usuarios en un entorno electrónico y, más en particular, a una disposición y un método para utilizar un terminal de datos personal de uso general como factor de autenticación segura de usuario.

Antecedentes de la invención

Los proveedores de servicios a través de canales electrónicos se enfrentan al reto de autenticar a los usuarios de sus servicios. La capacidad de proporcionar autenticación segura de usuarios es necesaria para muchos servicios electrónicos.

Los proveedores de servicios que requieren autenticación fuerte de usuario a menudo crean uno o varios factores de autenticación para un usuario, que el proveedor de servicios puede utilizar más tarde para autenticar al usuario. Si se crean varios factores de autenticación para el usuario y se le pide al usuario que proporcione todos los factores de autenticación en un incidente de autenticación, se reduce considerablemente el riesgo de incidentes falsos. Si, además, los factores de autenticación tienen diferente naturaleza, y cada uno proporciona una identificación única del usuario, y los datos de autenticación producidos son secretos para quienes no sean el usuario o el proveedor de servicios, la solución de autenticación se convierte en lo que se conoce en la técnica como una solución de autenticación multifactor fuerte.

Los factores de autenticación comúnmente utilizados son un factor de conocimiento ("algo que sabes", por ejemplo una contraseña o un código PIN) y un factor de posesión ("algo que tienes", por ejemplo un generador electrónico de contraseña de un solo uso, un cliente (en la acepción informática) de seguridad con claves de cifrado privadas almacenadas en la memoria de un ordenador o en una tarjeta de chip, listas impresas de códigos de acceso de un solo uso, *etc*.). Además, a veces se utilizan datos biométricos ("algo que eres", por ejemplo representaciones digitales de una huella digital o escaneo del iris) como factor de autenticación.

Los factores de posesión tienen a menudo naturaleza física, como las tarjetas de chip, calculadores de contraseñas o testigos (en inglés, "token"), o tarjetas desechables. La emisión de factores físicos de posesión representa a menudo un coste importante para los proveedores de servicios, y a menudo es visto como un inconveniente por los usuarios. Por tanto, puede ser de interés para proveedores de servicios y usuarios utilizar como factor de posesión segura un terminal de datos personal comúnmente disponible, ya en poder del usuario. Los ejemplos de terminales personales que pueden ser atractivos para el uso como factores de posesión son los teléfonos móviles, ordenadores portátiles, ordenadores de mano como las PDA y los teléfonos inteligentes, y terminales de entretenimiento personal.

Se conocen diversos métodos en los que se utilizan terminales personales de datos para autenticación de usuarios.

Un método conocido es aquel en que un proveedor de servicios registra los números de abonado móvil de los usuarios y, en un proceso de autenticación, distribuye un secreto compartido al terminal móvil del usuario, pidiendo al usuario que devuelva, por otro canal electrónico, el secreto compartido. Las debilidades de este método residen en que el emisor (el proveedor de servicios) no puede verificar la identidad de la parte receptora (el usuario), en que el secreto compartido se genera en un servidor y por lo tanto no existe referencia a un factor de posesión en la respuesta de autenticación, y en que el dispositivo móvil se utiliza exclusivamente como un terminal de comunicación. Por último, no se considera al terminal móvil un ambiente seguro para contener secretos compartidos; por ejemplo, los secretos compartidos pueden ser divulgados a la red o bien ser leídos por un tercero, o redistribuidos a un tercero, desde el terminal móvil.

El documento US 2003/0204726 A1 proporciona un método de este tipo en el cual se distribuye el secreto compartido, o respuesta de autenticación, en formato cifrado a un terminal móvil. A continuación se transfiere desde el terminal móvil a un cliente la respuesta de autenticación cifrada, el cliente conserva la clave de cifrado y, por tanto, el cliente puede descifrar la respuesta de autenticación. En el documento US 2003/0204726 A1 se distribuye una clave de cifrado entre el cliente y el servidor en cada incidente de autenticación. Un método en el que no se transmitiese la clave de cifrado en cada incidente de autenticación constituiría un método con seguridad mejorada.

Otro método implica la implementación de un elemento de seguridad (por ejemplo un cliente 3DES o un cliente PKI) en una memoria de terminal de datos personal, donde el elemento de seguridad contiene datos sensibles de usuario. En este método, el factor de posesión son los datos sensibles de usuario, por ejemplo claves de cifrado privadas. Se puede cifrar el elemento de seguridad mediante un factor de conocimiento (un PIN o una contraseña). Un problema de este método es que se puede copiar el elemento de seguridad y los datos sensibles de usuario pueden ser revelados, por ejemplo, mediante un ataque de prueba y error sobre el factor de conocimiento. Se pueden generar copias de los datos sensibles de usuario, reduciendo con ello la fiabilidad de este método como factor de posesión segura.

Los terminales móviles de la norma GSM y otros tienen instalados una tarjeta de chip, denominada tarjeta SIM, en la cual los operadores de telefonía móvil almacenan datos de autenticación de abonado a móvil y otros datos de red. La tarjeta SIM es un testigo de *hardware* resistente a la manipulación y es un recipiente de almacenamiento seguro para elementos de seguridad. Por lo tanto, la tarjeta SIM es un factor de posesión segura en un terminal móvil. Las limitaciones del uso de la tarjeta SIM como factor de posesión para los proveedores de servicios residen en que la tarjeta SIM no es una plataforma abierta, y el acceso a la tarjeta SIM requiere acuerdos con los operadores de telefonía móvil. El abrir la SIM a otros proveedores de servicios puede exponer la SIM a nuevas amenazas a la seguridad, y/o es costoso para los proveedores de servicios satisfacer los requisitos de seguridad de los operadores de telefonía móvil, para que se les permita el acceso a la SIM. La tarjeta SIM ofrece una capacidad de memoria limitada y una complicada gestión del aprovisionamiento y del ciclo de vida. Por ejemplo, el tiempo de vida de un elemento de seguridad basado en SIM, creado por un proveedor de servicios, concluirá cuando el operador de telefonía móvil o el abonado cambien la SIM.

El código IMEI es un ejemplo de código que es único, está asociado con el terminal personal y reside en el terminal personal. Otros ejemplos de tales códigos son un MAC, un número de procesador, un código electrónico de producto (EPC, por sus siglas en inglés) o un número de serie de SIM (SSN, por sus siglas en inglés). Pero, aunque estos códigos son únicos, están asociados con el terminal personal y residen en el terminal personal, no son secretos y pueden ser leídos y copiados a otros entornos. Si se utilizan estos códigos como única representación de un factor de posesión por un usuario, pueden ser utilizados para producir falsos incidentes por intrusos expertos que hayan obtenido copias de los códigos. En la solicitud de patente NO 20050152 se describe un método de este tipo, en el cual, por medio de un dispositivo de usuario programable donde se ha almacenado previamente un identificador de equipo que identifica de manera única el dispositivo de usuario, y utilizando el identificador de equipo como representación del factor de posesión en una autenticación de usuario, se genera un código de seguridad reproducible para autenticación del usuario.

En el documento WO 01/31840 A1 se describe un método para utilizar terminales móviles para autenticación de usuarios, en el cual se utiliza el IMEI de un terminal móvil como representación del elemento físico, o factor de posesión, en la solución de autenticación. El método del documento WO 01/31840 A1 no incluye métodos para protección contra las amenazas de producir falsos incidentes basándose en copias de los códigos que son únicos, están asociados al terminal personal y residen en el terminal personal, ni se describe ningún método de control de la autenticidad del creador y el receptor de la disposición, a fin de proteger aún más el método frente a ataques maliciosos. El método se basa en el almacenamiento y el uso de datos para autenticación de usuario en el extremo receptor, lo que añade así el riesgo adicional de exponer a los intrusos los datos para autenticación de usuario. Por último, el método se basa en el uso del tiempo como único elemento no revelado en el cálculo de los datos para autenticación de usuario (la contraseña de un solo uso), siendo el tiempo una variable que es relativamente fácil de determinar, y donde no hay soluciones conocidas para sincronizar el reloj de un terminal de teléfono móvil con otros sistemas, lo que dificulta producir una variable larga e impredecible basada en el tiempo, en una disposición de autenticación de usuario en un terminal móvil.

Los documentos US 2003/0236981 y US 2004/0030906 describen un método en el cual se utiliza un código que es único, está asociado con el terminal personal y reside en el terminal personal, el IMEI de un terminal móvil, para proteger un terminal de datos personal contra ataques maliciosos. Este método no utiliza un terminal de datos personal en un procedimiento para producir una autenticación de usuario destinada a un proveedor de servicios, ni tiene en cuenta este método las amenazas, mencionadas más arriba, de utilizar el IMEI como única referencia para un factor de posesión segura.

En el documento US 2005/0187882 se describe una invención para utilizar el terminal móvil en servicios de pago electrónico dentro de un entorno con comunicaciones de corto alcance (RFID), donde se crea para el usuario un testigo separado, destinado a la autenticación del usuario. La utilización de un terminal móvil como factor de posesión segura podría permitir a un proveedor de servicios producir datos para autenticación de usuario desde una disposición en el propio terminal móvil, eliminando así la necesidad de crear para el usuario un testigo físico independiente, como se describe en el documento US 2005/0187882. El hecho de evitar el uso de un testigo físico es importante para el usuario que se abona a varios servicios de un proveedor de servicios o bien se abona a servicios de varios proveedores de servicios.

Existen varios métodos para utilizar un terminal de datos personal comúnmente disponible como factor de posesión para autenticación de usuarios. En distintos tipos de terminales personales de datos existen códigos que son únicos, están asociados con el terminal personal y residen en el terminal personal. Sin embargo, estos códigos no son secretos y pueden ser leídos y copiados a otros entornos. Si se utilizan estos códigos como única representación de un factor de posesión por un usuario, intrusos expertos, que hayan obtenido copias de los códigos, los pueden utilizar para producir falsos incidentes

Además, el uso de los códigos antes mencionados como única representación de un factor de posesión por un usuario no va a producir un factor de posesión que sea único si el factor de posesión lo utilizan varios proveedores de servicios. El proveedor de servicios no puede saber si el mismo factor de posesión es o no reutilizado por otros proveedores de servicios. Mejorará la confianza en el factor de posesión el hecho de que el proveedor de servicios sepa que los datos para autenticación de usuario (por ejemplo, un código de usuario) producidos a partir del factor

de posesión son válidos solamente para un registro de usuario, y que no se utilizan los mismos datos para autenticación de usuario en ningún otro registro ante proveedores de servicios.

Un problema adicional que se identificado en el uso, como factor de posesión, de códigos que son únicos, están asociados con el terminal personal y residen en el terminal personal, es que el proveedor de servicios debe estar seguro de que el código se lee del terminal personal real, y no de otro entorno

En el documento JP 2003410949 se describen un sistema y método que generan códigos únicos y muestran el código en el terminal móvil, por ejemplo, en forma de una imagen. Se utiliza después este código para acceder a un servicio, como una retirada de dinero o un pago. Además de requerir una interacción adicional del usuario, el método presenta la debilidad de que puede revelarse inintencionadamente el código en la pantalla. Además, este método no tiene un procedimiento de registro con cada proveedor de servicios, por lo que la verificación inicial de la identidad del usuario se deja a un procedimiento común para todos y no al estándar de seguridad elegido por cada proveedor, como puede ser el registrar al cliente solamente si el terminal móvil y el usuario están presentes en las instalaciones del proveedor.

El documento GB 2337908 describe un método donde se emite un localizador (en inglés, "pager") de tarjeta de PC con una contraseña de un solo uso generada por el anfitrión y una tabla de cifrado, y donde un usuario se autentica mediante el cifrado de la información de autenticación con una clave de cifrado de la tabla de cifrado. Este método se basa en emitir una nueva contraseña de un solo uso para cada nueva autenticación, y almacena la lista de cifrado en el localizador de tarjeta del PC. Por tanto, el método se expone a amenazas de copia de la tabla de cifrado y de asegurar la distribución de contraseñas de un solo uso. Además, el método no genera un código de usuario reproducible, que se pueda utilizar muchas veces como elemento de posesión para la identificación del usuario y que pueda utilizarse para propósitos de autenticación, firma y cifrado.

Para crear un factor de posesión segura desde un terminal personal comúnmente disponible, terminal personal que contiene uno o varios códigos que son únicos, están asociados con el terminal personal y residen en el terminal personal, una disposición asociada con el terminal personal debe asegurar que:

- no se pueda reproducir o copiar el factor de posesión;
- el factor de posesión sea único para el proveedor de servicios, de manera que el proveedor de servicios pueda reconocer un factor de posesión único creado para un usuario a partir de un incidente específico de registro;
- se utilice realmente el terminal personal en la producción del factor de posesión.

Sumario de la invención

El objeto de la presente invención es un método y una disposición para utilizar un terminal de datos personal comúnmente disponible como factor de posesión segura y fiable para autenticación de usuarios. Las características definidas en las reivindicaciones independientes adjuntas caracterizan este método y esta disposición.

Así, la presente invención se refiere a un método para transferencia segura de datos, por ejemplo autenticación o cifrado de datos, entre dos interlocutores, un usuario y un segundo interlocutor, comprendiendo dicho método al menos uno de los siguientes: una primera sesión para generar un factor de autenticación/código de usuario único, reproducible y nuevo, adaptado para autenticación de usuario; una segunda sesión para registrar el o los factores de autenticación de usuario/códigos de usuario en el segundo interlocutor; y una tercera sesión para asegurar la autenticación del usuario o cifrar datos entre los dos interlocutores de la transferencia de datos, estando el usuario registrado en el segundo interlocutor y siendo el segundo interlocutor un proveedor de servicios, donde el usuario al menos utiliza un terminal personal que comprende al menos una unidad central de procesamiento, medios de comunicación y al menos un cliente almacenado en un medio de almacenamiento o bien almacenado parcialmente en el medio de almacenamiento adaptado para autenticación de usuario, donde el al menos un cliente incluye capacidad para generar y almacenar números aleatorios, donde la primera sesión comprende al menos los pasos de:

- el al menos un cliente genera un número aleatorio, utilizando una capacidad de generación presente en el al menos un cliente;
- el al menos un cliente almacena el número aleatorio en el al menos un cliente y etiqueta como referencia de cliente el número aleatorio almacenado;
- el al menos un cliente obtiene un código que es único, está asociado con el terminal personal y reside en el terminal personal, y el al menos un cliente obtiene la referencia de cliente, y;
- el al menos un cliente utiliza uno o varios algoritmos de cálculo almacenados en el al menos un cliente, donde una representación del código es única para el terminal personal, y;
- se introduce la referencia de cliente en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa la posesión del terminal personal por el usuario.

Es otro objeto de la invención combinar el factor de posesión, o código de usuario, producido según el método de la presente invención, con un factor de conocimiento del usuario, un código de acceso, con el fin de proporcionar una autenticación de usuario mediante dos factores.

Es otro objeto de la presente invención proporcionar un método para autenticación de usuarios, en el cual se intercambian los datos de autenticación entre el usuario y el proveedor de servicios a través de dos canales de comunicación separados.

Otro objeto de la invención se concreta en que el al menos un cliente reside en parte en el terminal personal y en parte en un servidor intermediario (en inglés, "proxy").

Es otro objeto de la invención proporcionar un método para autenticación de usuarios y firma por usuarios, en el cual un segundo interlocutor ha almacenado en una carpeta de usuario un nombre de usuario y uno o varios códigos de usuario del usuario, y tiene acceso a los mismos uno o varios algoritmos de cálculo que un terminal personal del usuario, y tiene acceso a un elemento de información, y existe al menos un canal de comunicación entre el terminal personal y el segundo interlocutor. En al menos un cliente se introduce un elemento de información en el terminal personal, produciendo el al menos un cliente el código de usuario, introduciendo el mencionado código de usuario y el elemento de información en uno o varios algoritmos de cálculo, que producen una salida, un elemento firmado. Se remite el nombre de usuario desde el usuario hacia el segundo interlocutor, y se remite el elemento firmado hacia el segundo interlocutor. El segundo interlocutor introduce el código de usuario almacenado en la carpeta de usuario y el elemento de información en los uno o varios algoritmos de cálculo, que producen una salida, el elemento firmado. El segundo interlocutor compara el elemento firmado generado como salida desde los uno o varios algoritmos de cálculo y el elemento firmado remitido desde el usuario y, si los dos elementos son iguales, la autenticación del usuario es satisfactoria.

Es otro objeto más de la presente invención proporcionar una disposición para autenticación segura de usuario entre dos interlocutores, donde el primer interlocutor es un usuario que al menos utiliza un terminal personal que comprende al menos una unidad central de procesamiento, medios de comunicación y medios de almacenamiento adaptados para almacenar uno o varios clientes o bien adaptados para almacenar parcialmente uno o varios clientes adaptados para autenticación de usuario, donde el segundo interlocutor es un proveedor de servicios, donde los uno o varios clientes al menos comprenden:

- uno o varios algoritmos de cálculo;
- parámetros de entrada procedentes de un código que es único, está asociado con el terminal personal y reside en el terminal personal, por ejemplo un número IMEI, un MAC, un número de procesador, un código electrónico de producto (EPC) o un número de serie de SIM (SSN);
- medios adaptados para generar y almacenar números aleatorios en los uno o varios clientes;
- medios adaptados para identificarse a sí mismos con el segundo interlocutor y para identificar al segundo interlocutor, y
- medios para comunicación segura con un servidor.

Estos y otros objetivos se consiguen según un método y una disposición como se reivindican en las reivindicaciones de patente adjuntas.

Breve descripción de los dibujos

Con el fin de hacer la invención más fácilmente comprensible, la siguiente descripción se referirá a los dibujos adjuntos, en los cuales:

Las Figuras 1A y 1B muestran la disposición de la presente invención en un terminal personal y una disposición de la invención utilizando un servidor intermediario.

La Figura 2 muestra la secuencia de la generación de un código de usuario en una sesión de registro.

La Figura 3 muestra la secuencia de la producción de un elemento firmado en un terminal personal, para autenticación del usuario, y de la verificación del elemento firmado por el proveedor de servicios.

La Figura 4 muestra una realización con dos canales según la presente invención.

Descripción detallada de la invención

En lo que sigue, se describirá la presente invención haciendo referencia a los dibujos y por medio de realizaciones preferidas.

Además, para facilitar la comprensión y la legibilidad de la presente descripción, se describirá el método en tres

sesiones. Una primera sesión describe el método para generar un factor de autenticación/código de usuario único y nuevo, adaptado para autenticación de usuario, una segunda sesión describe el método para registrar el o los factores de autenticación/códigos de usuario en el segundo interlocutor y una tercera sesión para asegurar la autenticación de usuario entre los dos interlocutores de la transferencia de datos. De ahí que la primera sesión puede ser una sesión de primera vez para generar factores de autenticación/códigos de usuario únicos y nuevos en un terminal personal de usuario. En consecuencia, la segunda sesión será la sesión de registro, en la cual se utilizan los "códigos" de la primera sesión para un registro "por primera vez" en un proveedor de servicios. La sesión tercera y final describe una sesión de autenticación que se puede utilizar varias veces, es decir, cada vez que un usuario ha completado la primera y la segunda sesiones y quiere establecer la transferencia segura de datos entre dos interlocutores; este suele ser el caso de las transacciones que un abonado tiene con su proveedor de servicios una vez que se ha provisionado el servicio. Son posibles otras varias realizaciones alternativas de cada tipo de sesión, dado que son posibles diferentes enfoques para producir códigos de usuario dentro del alcance de la presente invención, por ejemplo con o sin uso de códigos de acceso.

Haciendo referencia a la Figura 1A, una primera realización preferida describe una disposición para autenticación segura de usuario entre dos interlocutores, donde el primer interlocutor es un usuario que utiliza un terminal personal 100 que comprende al menos una unidad central de procesamiento101, medios de comunicación102, y medios de almacenamiento 103 adaptados para almacenar uno o varios clientes o bien adaptados para almacenar parcialmente uno o varios clientes adaptados para autenticación 104 de usuario, donde los uno o varios clientes comprenden:

- uno o varios algoritmos de cálculo 105;
- parámetros de entrada procedentes de un código que es único 106, está asociado con el terminal personal y reside en el terminal personal 100, por ejemplo un número IMEI, un MAC, un número de procesador, un código electrónico de producto (EPC) o un número de serie de SIM (SSN);
- medios adaptados para generar y almacenar números aleatorios en los uno o varios clientes 107;
- medios adaptados para identificarse a sí mismos con el segundo interlocutor y para identificar al segundo interlocutor 108;
- medios para comunicación segura con un servidor 102.

El terminal personal podría ser uno de los siguientes: un teléfono móvil, una PDA o un ordenador de mano que comprenda medios de comunicación, un terminal de entretenimiento informático que comprenda medios de comunicación o un ordenador portátil que comprenda medios de comunicación. El terminal personal está adaptado para descargar los uno o varios clientes utilizando medios de comunicación inalámbricos o cableados.

El segundo interlocutor es un proveedor de servicios.

Primera realización de la presente invención.

En una primera realización de la invención se registran (segunda sesión) uno o varios códigos de usuario generados por la disposición, en calidad de uno o varios factores de autenticación de un usuario en un proveedor de servicios. El proveedor de servicios realizará el registro conforme a sus políticas de seguridad establecidas. El procedimiento de registro podría incluir la distribución de secretos compartidos, y el procedimiento de registro podría consistir en procedimientos con conexión (en inglés, "online") o sin conexión (en inglés, "offline"), o combinaciones de los mismos.

El procedimiento de registro incluye el intercambio de datos entre el usuario y el proveedor de servicios. Los datos producidos en la sesión de registro, es decir, los códigos de usuario, serán utilizados más tarde para la autenticación del usuario. Los códigos de usuario podrían representar solamente un factor de posesión del usuario o bien representar un factor de posesión del usuario y también un factor de conocimiento. Una sesión de registro (segunda sesión) podría incluir la emisión de un código de usuario basado solamente en el factor de la posesión y/o un código de usuario basado en el factor de la posesión y también en el factor de conocimiento.

Haciendo referencia a la Figura 2, una sesión de registro en la cual el usuario tiene acceso a una disposición según la presente invención y el proveedor de servicios ha autenticado al usuario conforme a su política de seguridad establecida, puede comprender al menos los pasos de

- el al menos un cliente genera un número aleatorio, utilizando una capacidad de generación presente en el al menos un cliente 201,
- el al menos un cliente almacena el número aleatorio en el al menos un cliente y etiqueta como referencia de cliente el número aleatorio almacenado 202,
- el al menos un cliente obtiene un código que es único, está asociado con el terminal personal y reside en el terminal personal 203, y el al menos un cliente obtiene la referencia de cliente, y opcionalmente pide al usuario

que introduzca un código de acceso en el terminal personal, y

- el al menos un cliente utiliza uno o varios algoritmos de cálculo almacenados en el al menos un cliente, donde una representación del código es única para el terminal personal, y

- se introduce la referencia de cliente en los uno o varios algoritmos de cálculo, que producen una salida 204, un código de usuario que representa la posesión del terminal personal por el usuario y, si el usuario ha introducido un código de acceso en el terminal personal,

- introducir adicionalmente el código de acceso en el algoritmo de cálculo, que produce una salida 204, un código de usuario que representa la posesión del terminal personal por el usuario y el conocimiento del código de acceso,

- el segundo interlocutor pide al usuario que registre el código de usuario en un dato de usuario en el segundo interlocutor,

- el al menos un cliente proporciona al segundo interlocutor información de autenticidad de los uno o varios clientes 205, y

- un paso de finalización en el cual se remite hacia el segundo interlocutor dicho código de usuario 206 y se almacena como parte de los datos de usuario asociados con el usuario en el segundo interlocutor.

Se genera una referencia de cliente en cada sesión de registro, basada en una capacidad de generación de números aleatorios o pseudoaleatorios presente en los uno o varios clientes.

La referencia de cliente:

- se almacena en el uno o varios clientes donde se ha generado,

- nunca se copia ni se remite desde el uno o varios clientes donde se ha generado,

- nunca se muestra ni se expone en el terminal personal,

- solamente se utiliza para calcular el código de usuario,

- no es conocida por el proveedor de servicios.

El código generado por el usuario es único para la sesión de registro (segunda sesión), porque se basa en una entrada de número aleatorio. El código de usuario sólo puede reproducirse con la copia específica de los uno o varios clientes en donde se almacena la referencia de cliente.

En sesiones de registro en las que se calcula el código de usuario a partir de la utilización del código de acceso como una de las entradas, se puede almacenar la referencia de cliente cifrada mediante el código de acceso.

Se puede utilizar la invención para registrar códigos de usuario en más de un proveedor de servicios.

Los uno o varios clientes pueden almacenar múltiples referencias de cliente y pueden permitir que un usuario registre diferentes códigos de acceso para cada registro. El método asegurará que los uno o varios códigos de usuario generados en cada sesión de registro sean diferentes para cada sesión de registro.

Una vez que ha acabado la sesión de registro (segunda sesión) y se han generado y registrado en un proveedor de servicios uno o varios códigos de usuario, un proveedor de servicios puede utilizar los uno o varios códigos de usuario para realizar servicios de seguridad con el usuario.

Al ejecutar los servicios de seguridad, por ejemplo una solicitud de autenticación, es decir, la tercera sesión, el usuario generará en el terminal personal el mismo código de usuario que se generó en el registro, y el proveedor de servicios verificará la autenticación del usuario mediante la comparación del código de usuario almacenado en el registro con el código de usuario generado por la solicitud de autenticación.

Cuando el usuario recibe una solicitud de autenticación en el terminal personal (100), la sesión de autenticación comprende al menos los pasos de:

- el al menos un cliente obtiene un código que es único, está asociado con el terminal personal y reside en el terminal personal, y el al menos un cliente obtiene la referencia de cliente, y opcionalmente pide al usuario que introduzca un código de acceso en el terminal personal, y

- el al menos un cliente utiliza uno o varios algoritmos de cálculo almacenados en el al menos un cliente, donde una representación del código es única para el terminal personal, y

- se introduce la referencia de cliente en los uno o varios algoritmos de cálculo, que producen una salida, un

código de usuario que representa la posesión del terminal personal por el usuario y, si el usuario ha introducido un código de acceso en el terminal personal, adicionalmente introducir el código de acceso en el algoritmo de cálculo, que produce una salida, es decir, un código de usuario que representa la posesión del terminal personal por el usuario y el conocimiento del código de acceso,

- el al menos un cliente proporciona al segundo interlocutor información de autenticidad de los uno o varios clientes, y

- un paso de finalización en el cual se remite hacia el segundo interlocutor la salida de los uno o varios algoritmos de cálculo en el terminal personal.

Segunda realización de la presente invención.

En una segunda realización de la invención en la que no se utilizan medios de comunicación de un terminal personal en la comunicación entre un usuario y un proveedor de servicios (segundo interlocutor), el usuario puede leer un código de usuario en la pantalla de visualización del terminal personal e introducir el código de usuario en un segundo terminal, con el cual el usuario se comunica con el proveedor de servicios. En esta realización, el proveedor de servicios no requerirá control de autenticidad de uno o varios clientes, o incluso podría no ser consciente del uso por los uno o varios clientes. Se puede aplicar el uso sin conexión cuando los proveedores de servicios tienen requisitos menos estrictos en materia de seguridad y el usuario quiere asegurarse de que la contraseña del usuario, o secreto de usuario, es distinta en cada proveedor de servicios.

Tercera realización de la presente invención.

En una tercera realización según la presente invención, uno o varios clientes pueden estar instalados en parte en un servidor intermediario y en parte en un terminal personal. Un servidor intermediario es un servicio que permite al al menos un cliente realizar una conexión de red indirecta con el proveedor de servicios.

Haciendo referencia a la Figura 1B, en esta realización se ejecutan en el terminal personal 100 un conjunto limitado de funciones, y el resto se ejecuta en el servidor intermediario 109. La parte de terminal personal de la disposición incluirá control de autenticidad 108, mientras que en el servidor intermediario se almacenan la capacidad de generación de números aleatorios 107 y uno o varios algoritmos de cálculo 105. El servidor intermediario puede trabajar en un entorno seguro y de confianza.

Las ventajas de esta realización son dos:

- la introducción de datos requerida para producir el código de usuario se distribuye en dos lugares, lo que hace más difícil que un intruso acceda a los dos;

- reduce el tamaño y la complejidad del al menos un cliente presente en el terminal personal, mejorando así la flexibilidad y el rendimiento de la disposición, incluidas implementaciones en las cuales se descarga el cliente en el terminal personal una vez por sesión.

En esta realización, el servidor intermediario comprenderá al menos:

- medios para recibir parámetros de entrada procedentes de los uno o varios clientes presentes en el terminal personal,

- uno o varios algoritmos de cálculo 105,

- medios adaptados para generar y almacenar números aleatorios en los uno o varios clientes 107,

- medios adaptados para identificarse a sí mismos con los uno o varios clientes presentes en el terminal personal y para identificar a los uno o varios clientes presentes en el terminal personal 110,

- medios adaptados para identificarse a sí mismos con el segundo interlocutor y para identificar al segundo interlocutor,

- medios para comunicación segura con un servidor 111.

En esta realización, la primera, segunda y tercera sesiones comprenden en el terminal personal (100) al menos los pasos de:

- proporcionar al servidor intermediario 109 información de autenticidad 108 del al menos un cliente, y

- el al menos un cliente obtiene un código que es único, está asociado con el terminal personal 100 y reside en el terminal personal 100, remitiendo dicho código hacia el servidor intermediario 109 y, si se ha solicitado al usuario que introduzca un código de acceso, se remite dicho código de acceso hacia el servidor intermediario.

En esta realización, la primera sesión en el servidor intermediario comprende al menos los pasos de:

- el al menos un cliente presente en el servidor intermediario 109 recibe desde el al menos un cliente presente en el terminal personal 100 el código 106 que es único, está asociado con el terminal personal 100 y reside en el terminal personal 100, y el código de acceso, si se le solicita al usuario que introduzca un código de acceso en el terminal personal,

- el al menos un cliente presente en el servidor intermediario genera un número aleatorio, utilizando una capacidad de generación presente en el al menos un cliente 107,

- el al menos un cliente almacena el número aleatorio en el al menos un cliente y etiqueta como referencia de cliente el número aleatorio almacenado,

- el al menos un cliente utiliza uno o varios algoritmos de cálculo 105 almacenados en el al menos un cliente presente en el servidor intermediario 109, donde se introducen una representación del código que es única para el terminal personal, y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa para el proveedor de servicios la posesión del terminal personal por el usuario y, si el usuario ha introducido un código de acceso en el terminal personal,

- adicionalmente, introducir el código de acceso en el algoritmo de cálculo, que produce una salida, un código de usuario que representa la posesión del terminal personal por el usuario y el conocimiento del código de acceso.

Como se comprenderá fácilmente, la distribución de tareas entre el terminal personal y el servidor intermediario puede variar. Por ejemplo, se puede generar el número aleatorio en el terminal personal y transmitirlo al servidor intermediario.

En esta realización, la segunda sesión en el servidor intermediario comprende al menos los pasos de:

- el segundo interlocutor pide al usuario que registre el código de usuario en unos datos de usuario en el segundo interlocutor,

- el al menos un cliente presente en el servidor intermediario proporciona al segundo interlocutor información de autenticidad 110 del al menos un cliente, y

- un paso de finalización en el cual se remite hacia el segundo interlocutor el mencionado código de usuario y se almacena como parte de los datos de usuario asociados con el usuario en el segundo interlocutor.

En esta realización, la tercera sesión en el servidor intermediario comprende al menos los pasos de:

- recibir desde el al menos un cliente presente en el terminal personal el código 106 que es único, está asociado con el terminal personal y reside en el terminal personal, y el código de acceso, si se le solicita al usuario que introduzca un código de acceso,

- el al menos un cliente presente en el servidor intermediario obtiene una referencia de cliente, generada en la primera sesión entre el usuario y el segundo interlocutor, y

- el uso de uno o varios algoritmos de cálculo 105 almacenados en el al menos un cliente presente en el servidor intermediario, donde se introducen una representación del código que es única para el terminal personal, y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa para el proveedor de servicios la posesión del terminal personal por el usuario y, si el usuario ha introducido un código de acceso en el terminal personal,

- introducir adicionalmente el código de acceso en el algoritmo de cálculo, que produce una salida, un código de usuario que representa la posesión del terminal personal por el usuario y el conocimiento del código de acceso,

- el al menos un cliente presente en el servidor intermediario 109 proporciona al segundo interlocutor información de autenticidad 110 de los uno o varios clientes, y

- un paso de finalización en el cual se remite hacia el segundo interlocutor la salida de los uno o varios algoritmos de cálculo del al menos un cliente presente en el servidor intermediario.

Cuarta realización de la presente invención.

Una cuarta realización de la invención describe un método de autenticación y firma en el cual un usuario se autentica a sí mismo con un proveedor de servicios (segundo interlocutor) realizando en uno o varios clientes un cálculo en el cual un código de usuario es un elemento de entrada y otro elemento de entrada es un elemento de información generado para el incidente de autenticación o incidente de firma. La salida de los uno o varios algoritmos de cálculo es un elemento firmado, donde el proveedor de servicios puede analizar el elemento firmado para comprobar la autenticación del usuario o la firma del usuario. Para la autenticación, también se denomina al elemento de información un desafío, una variable o una semilla (en inglés, "nonce"), y al elemento firmado también se le denomina "contraseña de un solo uso" (OTP, por sus siglas en inglés).

Para la autenticación de usuario se puede utilizar un código de usuario que represente la posesión del terminal personal por el usuario. Tanto para la autenticación como para la firma se puede utilizar un código de usuario que represente la posesión del terminal personal por el usuario y el conocimiento del código de acceso. Haciendo referencia a la Figura 3, esta realización puede utilizar una secuencia que comprende al menos los pasos de:

- se pone a disposición un elemento de información en el terminal personal 301. El elemento de información lo puede generar un proveedor de servicios o un tercero, se puede generar en el terminal personal o bien ser introducido por el usuario,
- el al menos un cliente produce dicho código de usuario en el al menos un cliente 302 e
- introduce dicho código de usuario y el elemento de información en los uno o varios algoritmos de cálculo, produciendo una salida, el elemento firmado 303.
- el segundo interlocutor ha almacenado en una carpeta de usuario el nombre de usuario y uno o varios códigos de usuario del usuario, y tiene acceso a los mismos uno o varios algoritmos de cálculo que el terminal personal del usuario. El proveedor de servicios tiene acceso al elemento de información, y existe al menos un canal de comunicación entre el terminal personal y el segundo interlocutor

la sesión comprende adicionalmente el paso de:

- se remite el nombre de usuario desde el usuario hacia el segundo interlocutor 304,
- se remite el elemento firmado hacia el segundo interlocutor 304,
- el segundo interlocutor introduce el código de usuario almacenado en la carpeta de usuario y el elemento de información en los uno o varios algoritmos de cálculo, que producen una salida 305, el elemento firmado
- el segundo interlocutor compara el elemento firmado producido como salida desde los uno o varios algoritmos de cálculo y el elemento firmado remitido desde el usuario 306 y, si los dos elementos son iguales, la autenticación del usuario es satisfactoria.

Quinta realización de la presente invención, que describe alternativas mediante el uso de dos canales.

Haciendo referencia a la Figura 4, se describe una quinta realización de la presente invención en la cual un usuario puede comunicarse con un proveedor de servicios (segundo interlocutor) a través de dos canales de comunicación separados, donde el primer canal, el canal 1 404, se establece entre el terminal personal 401 y el proveedor de servicios 403, y el segundo canal, canal 2 405, se establece entre un segundo terminal 402 al que pueden acceder el usuario y el proveedor de servicios. El segundo terminal puede utilizarse para la comunicación unidireccional o bidireccional.

Mediante el uso de una comunicación por dos canales entre el usuario y el proveedor de servicios, se consiguen diferentes realizaciones de la autenticación de usuario y la firma.

En una alternativa, se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 405, se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 2 405 y se remite el elemento firmado desde el primer interlocutor hacia el segundo interlocutor a través del canal 1 404.

En otra alternativa de la quinta realización, se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 405, se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 1 404 y se remite el elemento firmado desde el usuario hacia el segundo interlocutor a través del canal 1 404.

En otra alternativa más de la quinta realización, se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 405, se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 1 404 y se remite el elemento firmado desde el usuario hacia el segundo interlocutor a través del canal 2 405.

Sexta realización de la presente invención.

La sexta realización de la presente invención se puede utilizar para proveedores de servicios (segundos interlocutores) que creen para un usuario uno o varios elementos de información a los que solamente va a poder acceder el usuario. Una credencial electrónica o un monedero electrónico son ejemplos de tales elementos de información. En esta realización no es necesario intercambiar el código de usuario desde el usuario hacia al proveedor de servicios.

La invención (con uno o varios clientes) puede utilizarse para proteger el elemento de información y para asegurar que el elemento de información solamente sea accesible para el usuario. En tales casos, se utiliza el código de

usuario como clave de cifrado para el mencionado elemento de información.

La emisión de un elemento de información que solamente sea accesible para el usuario puede comprender al menos los pasos descritos en la presente memoria, donde el usuario tiene acceso a una disposición de la invención, y el proveedor de servicios ha autenticado al usuario conforme a su política de seguridad establecida.

- el al menos un cliente genera un número aleatorio, utilizando una capacidad de generación presente en al menos un cliente,
- el al menos un cliente almacena el número aleatorio en el al menos un cliente y etiqueta como referencia de cliente el número aleatorio almacenado,
- el al menos un cliente obtiene un código que es único, está asociado con el terminal personal y reside en el terminal personal, y
- el al menos un cliente obtiene la referencia de cliente, y opcionalmente pide al usuario que introduzca un código de acceso en el terminal personal, y
- el al menos un cliente utiliza uno o varios algoritmos de cálculo almacenados en el al menos un cliente, donde una representación del código es única para el terminal personal, y
- se introduce la referencia de cliente en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa la posesión del terminal personal por el usuario y, si el usuario ha introducido un código de acceso en el terminal personal,
- introducir adicionalmente el código de acceso en el algoritmo de cálculo, que produce una salida, un código de usuario que representa la posesión del terminal personal por el usuario y el conocimiento del código de acceso,
- se pone a disposición del usuario, en el terminal personal, un elemento de información,
- se cifra el elemento de información con el código de usuario como clave de cifrado y se almacena en un entorno accesible para el usuario el elemento de información cifrado.

Séptima realización de la presente invención.

Una séptima realización según la presente invención describe el cifrado y descifrado de al menos un elemento de información. En esta realización, un proveedor de servicios ha registrado uno o varios códigos de usuario de un usuario en una carpeta de cliente, el elemento a cifrar/descifrar es al menos un elemento de información, se utiliza un código de usuario como clave de cifrado y el algoritmo de cifrado utilizado es un algoritmo de dos vías.

El método según la invención para la séptima realización puede comprender al menos los pasos de:

- se pone a disposición en el terminal personal el elemento de información a cifrar/descifrar,
- el usuario activa una función de cifrado en los uno o varios clientes,
- uno o varios clientes generan el mencionado código de usuario,
- los uno o varios clientes cifran/descifran el elemento de información utilizando el código de usuario como clave de cifrado.

En el proveedor de servicios, la secuencia según la séptima realización de la presente invención puede ser como la siguiente:

- se identifica el elemento de información a cifrar/descifrar,
- el proveedor de servicios encuentra el código de usuario del usuario en la carpeta de abonado del usuario,
- el proveedor de servicios cifra/descifra el elemento de información utilizando el código de usuario como clave de cifrado.

Se puede intercambiar de forma segura entre un proveedor de servicios y un usuario un elemento de información cifrado. Un proveedor de servicios puede utilizar este método para la distribución segura de elementos de información (personal) hacia un usuario; son ejemplos de ello los billetes electrónicos, credenciales electrónicas, monederos electrónicos, registros de datos personales tales como información sobre la salud del usuario, una receta médica y similares.

Un proveedor de servicios, donde se ha registrado el usuario, tiene un elemento de información que debe ser distribuido de forma segura hacia el usuario.

- el proveedor de servicios envía un elemento de información cifrado al usuario, o pone a disposición del usuario el elemento de información cifrado,
- en el terminal personal, el usuario genera un código de usuario,
- el usuario descifra el elemento de información cifrado, utilizando el código de usuario como clave de descifrado,
- el usuario tiene acceso al elemento de información.

Un usuario puede utilizar el código de usuario como clave de cifrado para proteger elementos de información sensibles o secretos. También se puede utilizar el método para que un usuario firme elementos de información, pudiendo verificar la firma el proveedor de servicios.

Octava realización de la presente invención.

En una realización adicional, se puede utilizar la invención para simplificar el proceso de actualizar los datos de autenticación cuando un usuario cambia un terminal personal. Esta realización requiere que el terminal personal tenga más de un código que sea único, esté asociado con el terminal personal y resida en el terminal personal, y que se reutilice al menos uno de estos dichos códigos en el nuevo terminal personal. Los teléfonos móviles de las normas GSM o UMTS, donde se puede reutilizar la tarjeta SIM en un nuevo terminal, son ejemplos de terminales personales que contienen más de un código que sea único, esté asociado con el terminal personal y resida en el terminal personal.

En el proceso de cambio, se puede utilizar el método de la invención para producir una salida, una clave de cambio, desde uno o varios algoritmos de cálculo en donde uno de los elementos de entrada es el código que es único, está asociado con el terminal personal y reside en el terminal personal del elemento que se va a reutilizar, y el otro elemento de entrada podría ser un código de acceso de usuario. Además, dicha clave de cambio podría constituir una entrada, junto con el código de usuario, para los uno o varios algoritmos de cálculo, que producirían una salida que es un elemento firmado. Dicho elemento firmado asocia al usuario con la clave de cambio.

Después, en el nuevo terminal personal, se puede utilizar el método de la invención para generar la clave de cambio, a partir de los uno o varios algoritmos de cálculo en donde uno de los elementos de entrada es el código que es único, está asociado con el terminal personal y reside en el terminal personal del elemento reutilizado, y el otro elemento de entrada puede ser un código de acceso de usuario.

El proveedor de servicios puede utilizar la clave de cambio producida en el nuevo terminal para autenticar al usuario en el nuevo terminal personal. Después, si se desea, el usuario y el proveedor de servicios pueden pasar por el proceso de generar y registrar un nuevo código de usuario, con el método de la invención, en el nuevo terminal personal.

Abreviaturas

3DES	Estándar de triple cifrado digital
EPC	Código electrónico de producto
GSM	Sistema global para comunicaciones móviles
ID	credencial, identificación
IMEI	Identificación internacional de equipo móvil
MAC	control de acceso al medio
OTP	contraseña de un solo uso
PDA	agenda personal electrónica
PIN	número de identificación personal
PKI	infraestructura de clave pública
RFID	identificación por radiofrecuencia
SIM	módulo de identificación de abonado
SSN	número de serie de SIM
UMTS	Sistema universal de telecomunicaciones móviles

REIVINDICACIONES

1. Un método para transferencia segura de datos entre dos interlocutores, un usuario y un segundo interlocutor, que comprende:

- al menos un cliente almacenado en un medio de almacenamiento (103) o bien parcialmente almacenado en el medio de almacenamiento (103) adaptado para autenticación de usuario (104), y donde el al menos un cliente incluye capacidad para generar y almacenar números aleatorios;

- una primera sesión para generar un factor de autenticación/código de usuario único y nuevo adaptado para autenticación de usuario, donde la primera sesión comprende al menos los pasos de:

B.1) el al menos un cliente genera un número aleatorio (107), utilizando una capacidad de generación presente en el al menos un cliente,

C1) el al menos un cliente almacena el número aleatorio en el al menos un cliente y etiqueta como referencia de cliente el número aleatorio almacenado,

D.1) el al menos un cliente obtiene un código que es único, está asociado con un terminal personal (100) del usuario y reside en el terminal personal (100), y el al menos un cliente obtiene la referencia de cliente, la primera sesión comprende además los pasos adicionales de pedir al usuario que introduzca un código de acceso en el terminal personal (100), y

E.1) el al menos un cliente utiliza uno o varios algoritmos de cálculo (105) almacenados en el al menos un cliente, donde se introducen una representación del código que es única para el terminal personal (100), y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario, la primera sesión comprende además el paso adicional de introducir el código de acceso en el algoritmo de cálculo (105), que produce una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario y el conocimiento del código de acceso

- una segunda sesión para registrar el o los factores de autenticación de usuario/códigos de usuario en el segundo interlocutor, el segundo interlocutor comprende al menos los pasos de:

A.2) el segundo interlocutor pide al usuario que registre el código de usuario en unos datos de usuario en el segundo interlocutor,

B.2) proporcionar al segundo interlocutor información de autenticidad de los uno o varios clientes (205), y

C.2) un paso de finalización en el cual se remite hacia el segundo interlocutor el mencionado código de usuario (206) y se almacena como parte de los datos de usuario asociados con el usuario en el segundo interlocutor y

- una tercera sesión para asegurar la autenticación de usuario entre los dos interlocutores de la transferencia de datos, estando el usuario registrado en el segundo interlocutor y siendo el segundo interlocutor un proveedor de servicios, donde el usuario al menos utiliza el terminal personal (100) que comprende al menos una unidad central de procesamiento (101), medios de comunicación (102) y el al menos un cliente.

2. Un método según la reivindicación 1, caracterizado por que la tercera sesión comprende al menos los pasos de:

B.3) el al menos un cliente obtiene un código que es único, está asociado con el terminal personal (100) y reside en el terminal personal (100),

C.3) el al menos un cliente obtiene una referencia de cliente, generada en una sesión de registro entre el primer interlocutor y el segundo, y

D.3) utiliza uno o varios algoritmos de cálculo almacenados en el al menos un cliente, donde se introducen una representación del código que es única para el terminal personal (100), y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa para el proveedor de servicios la posesión del terminal personal (100) por el usuario.

3. Un método según la reivindicación 2, caracterizado por que la tercera sesión comprende además al menos un paso introductorio de:

A.3) proporcionar al segundo interlocutor información de autenticidad de los uno o varios clientes; y

E.3) un paso de finalización en el cual se remite hacia el segundo interlocutor la salida de los uno o varios algoritmos de cálculo del terminal personal (100).

4. Un método según la reivindicación 2, caracterizado por que el paso D.3) comprende los pasos adicionales de:

el primer interlocutor introduce un código de acceso en el terminal personal (100); se utiliza dicho código de acceso

como entrada adicional en el algoritmo de cálculo, que produce una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario y el conocimiento del código de acceso.

5. Un método según cualquiera de las reivindicaciones 1-4, caracterizado por que el al menos un cliente reside en parte en el terminal personal (100) y en parte en un servidor intermediario (109).

6. Un método según la reivindicación 5, caracterizado por que la primera, segunda y tercera sesiones comprenden en el terminal personal (100) al menos los pasos de:

A.4) proporcionar al servidor intermediario (109) información de autenticidad del al menos un cliente, y

B.4) el al menos un cliente obtiene un código que es único, está asociado con el terminal personal (100) y reside en el terminal personal (100), y remite dicho código hacia el servidor intermediario (109).

7. Un método según la reivindicación 6, caracterizado por que el paso B.4) comprende los pasos adicionales de: el usuario introduce un código de acceso en el terminal personal (100), se remite dicho código de acceso hacia el servidor intermediario (109).

8. Un método según la reivindicación 5, caracterizado por que la primera, segunda y tercera sesiones comprenden en el servidor intermediario al menos los pasos de:

A.5) recibir desde el al menos un cliente presente en el terminal personal (100) el código que es único, está asociado con el terminal personal (100) y reside en el terminal personal (100),

B.5) el al menos un cliente presente en el servidor intermediario (109) obtiene una referencia de cliente, generada en la primera sesión, y

C.5) utilizar uno o varios algoritmos de cálculo almacenados en el al menos un cliente presente en el servidor intermediario (109), donde se introducen una representación del código que es única para el terminal personal (100), y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa para el proveedor de servicios la posesión del terminal personal (100) por el usuario.

9. Un método según la reivindicación 8, caracterizado por que el paso B.5) comprende el paso adicional de recibir desde el al menos un cliente presente en el terminal personal (100) un código de acceso, y el paso C.5) comprende el paso adicional de utilizar dicho código de acceso como entrada adicional en el algoritmo de cálculo, que produce una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario y el conocimiento del código de acceso.

10. Un método según cualquiera de las reivindicaciones 1 y 2-9, caracterizado por que la tercera sesión comprende al menos los pasos de:

A.6) introducir un elemento de información (301) en el terminal personal (100)

B.6) producir el mencionado código de usuario (302) en el al menos un cliente

C.6) introducir el mencionado código de usuario y el elemento de información en los uno o varios algoritmos de cálculo, que producen una salida (303), el elemento firmado.

11. Un método según la reivindicación 10, caracterizado porque si el segundo interlocutor ha almacenado en una carpeta de usuario el nombre de usuario y uno o varios códigos de usuario del usuario, y tiene acceso a los mismos uno o varios algoritmos de cálculo que los uno o varios clientes presentes en el intermediario (109) o en el terminal personal (100) del usuario, y tiene acceso al elemento de información, y existe al menos un canal de comunicación entre el terminal personal (100) y el segundo interlocutor, entonces la tercera sesión comprende además al menos el paso de:

D.6) se remite el nombre de usuario (304) desde el usuario hacia el segundo interlocutor,

E.6) se remite el elemento firmado (304) hacia el segundo interlocutor,

F.6) el segundo interlocutor introduce el código de usuario almacenado en la carpeta de usuario y el elemento de información en los uno o varios algoritmos de cálculo, que producen una salida (305), el elemento firmado

G.6) el segundo interlocutor compara (306) el elemento firmado producido como salida de los uno o varios algoritmos de cálculo y el elemento firmado remitido desde el usuario y, si los dos elementos son iguales, se autentica al usuario.

12. Un método según las reivindicaciones 10 y 11, caracterizado por que establece para la segunda y tercera sesiones una comunicación de dos canales entre el primer interlocutor y el segundo, donde el primer canal, canal 1 (404), se establece entre el terminal personal (100) y el segundo interlocutor, el segundo canal, canal 2 (405), se establece entre un segundo terminal accesible para el primer interlocutor y el segundo interlocutor.

13. Un método según la reivindicación 12, caracterizado por que se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 (405), se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 2 (405) y se remite el elemento firmado desde el primer interlocutor hacia el segundo interlocutor a través del canal 1 (404).

14. Un método según la reivindicación 12, caracterizado por que se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 (405), se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 1 (404) y se remite el elemento firmado desde el usuario hacia el segundo interlocutor a través del canal 1 (404).

15. Un método según la reivindicación 12, caracterizado por que se remite el nombre de usuario desde el usuario hacia el segundo interlocutor a través del canal 2 (405), se remite el elemento de información desde el segundo interlocutor hacia el usuario a través del canal 1 (404) y se remite el elemento firmado desde el usuario hacia el segundo interlocutor a través del canal 2 (405).

16. Un método según cualquiera de las reivindicaciones precedentes, caracterizado por que se utiliza un número IMEI, un MAC, un número de procesador, un código electrónico de producto (EPC) o un número de serie de SIM (SSN), como código que es único, está asociado con el terminal personal (100) y reside en el terminal personal (100).

17. Un método según cualquiera de las reivindicaciones precedentes, caracterizado por que el usuario utiliza como código de acceso cualquier entrada de usuario en el terminal personal (100), por ejemplo caracteres alfanuméricos y numéricos, representación de la voz o datos biométricos.

18. Una disposición para autenticación segura de usuario (104) entre dos interlocutores, donde el primer interlocutor es un usuario que al menos utiliza un terminal personal (100) que comprende al menos una unidad central de procesamiento (101), medios de comunicación (102) y medios de almacenamiento (103) adaptados para almacenar uno o varios clientes o bien adaptados para almacenar parcialmente uno o varios clientes adaptados para autenticación de usuario (104), donde el segundo interlocutor es un proveedor de servicios, caracterizado por que los uno o varios clientes comprenden al menos:

- uno o varios algoritmos de cálculo (105), almacenados en el al menos un cliente, donde se introducen una representación del código que es única para el terminal personal (100), y la referencia de cliente, en los uno o varios algoritmos de cálculo, que producen una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario, la primera sesión comprende además el paso adicional de introducir el código de acceso en el algoritmo de cálculo (105), que produce una salida, un código de usuario que representa la posesión del terminal personal (100) por el usuario y el conocimiento del código de acceso

- parámetros de entrada procedentes de un código que es único (106), está asociado con el terminal personal (100) y reside en el terminal personal (100), siendo el código un número IMEI, un MAC, un número de procesador, un código electrónico de producto (EPC) o un número de serie SIM (SSN),

- medios adaptados para generar y almacenar números aleatorios (107) en los uno o varios clientes, medios adaptados para identificarse a sí mismos con el segundo interlocutor y para identificar al segundo interlocutor (108), y

- medios para comunicación segura con un servidor (102).

19. Una disposición según la reivindicación 18, caracterizada por que la disposición comprende además parámetros de entrada procedentes del usuario, por ejemplo caracteres alfanuméricos y numéricos, representación de la voz o datos biométricos.

20. Una disposición según la reivindicación 18, caracterizada por que la disposición comprende además un segundo terminal para comunicación unidireccional o bidireccional entre el usuario y el segundo interlocutor.

21. Una disposición según cualquiera de las reivindicaciones 18 a 20, caracterizada por que comprende además un servidor intermediario que comprende al menos:

- medios para recibir parámetros de entrada procedentes de los uno o varios clientes presentes en el terminal personal (100), uno o varios algoritmos de cálculo (105), medios adaptados para generar y almacenar números aleatorios (107) en los uno o varios clientes,

- medios (110) adaptados para identificarse a sí mismos con los uno o varios clientes presentes en el terminal personal (100) y para identificar a los uno o varios clientes presentes en el terminal personal (100),

- medios adaptados para identificarse a sí mismos con el segundo interlocutor y para identificar al segundo interlocutor,

- medios para comunicación segura con un servidor (111).

22. Una disposición según cualquiera de las reivindicaciones 18 a 20, caracterizada por que el terminal personal (100) es uno de los siguientes: un teléfono móvil tal como un teléfono GSM o UMTS, una PDA que comprende medios de comunicación (102), un terminal de entretenimiento informático que comprende medios de comunicación (102) o un ordenador portátil que comprende medios de comunicación (102).

23. Una disposición según cualquiera de las reivindicaciones 18 - 20, caracterizada por que el terminal personal (100) está adaptado para descargar los uno o varios clientes utilizando medios de comunicación inalámbricos o cableados (102).

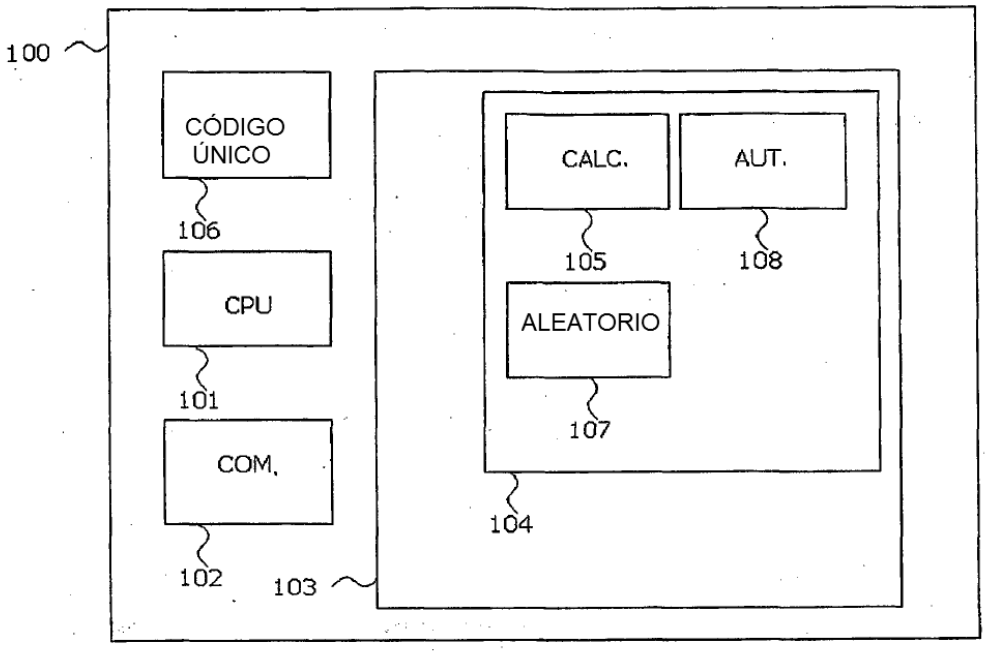
100
CÓDIGO ÚNICO
106
CPU
101
COM.
102
103
CALC.
AUT.
105
108
ALEATORIO
107
104

FIG.1A

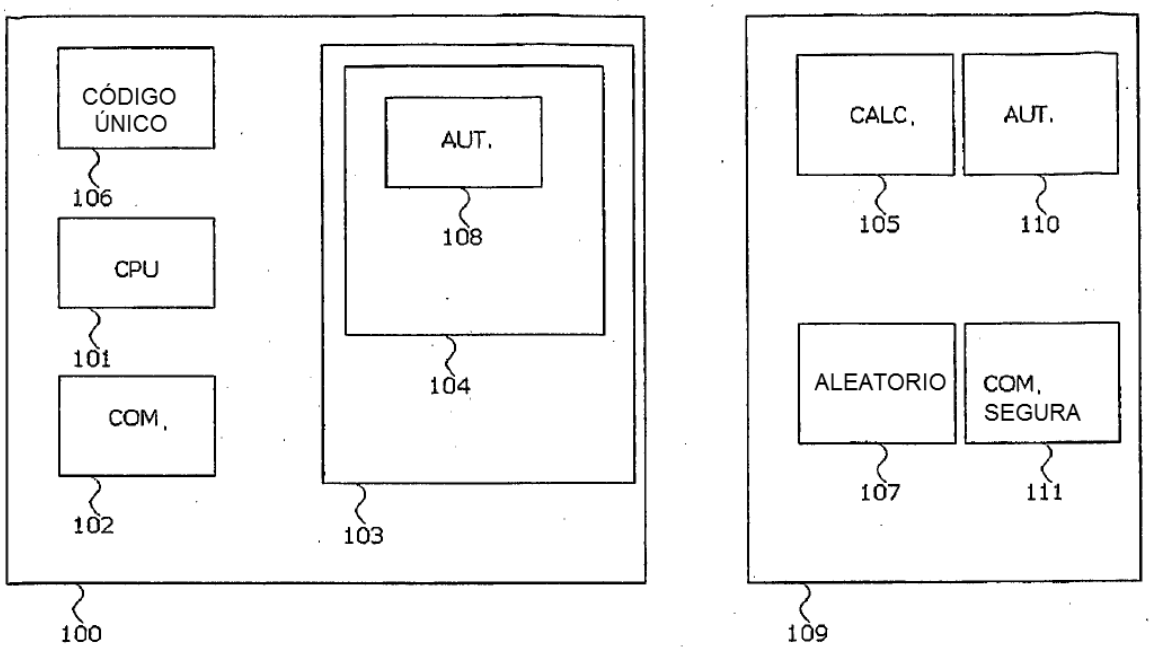
CÓDIGO ÚNICO
106
CPU
101
COM.
102
AUT.
108
104
103
100
CALC.
AUT.
105
110
ALEATORIO
COM. SEGURA
107
111
109

FIG.1B

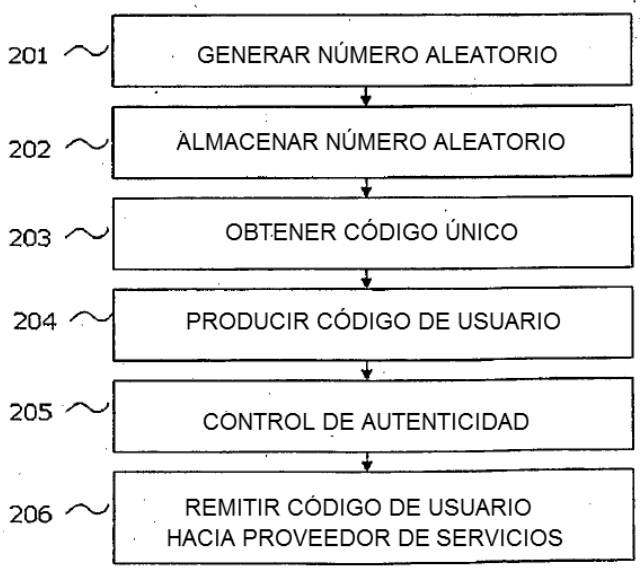
201
GENERAR NÚMERO ALEATORIO
202
ALMACENAR NÚMERO ALEATORIO
203
OBTENER CÓDIGO ÚNICO
204
PRODUCIR CÓDIGO DE USUARIO
205
CONTROL DE AUTENTICIDAD
206
REMITIR CÓDIGO DE USUARIO HACIA PROVEEDOR DE SERVICIOS

FIG.2

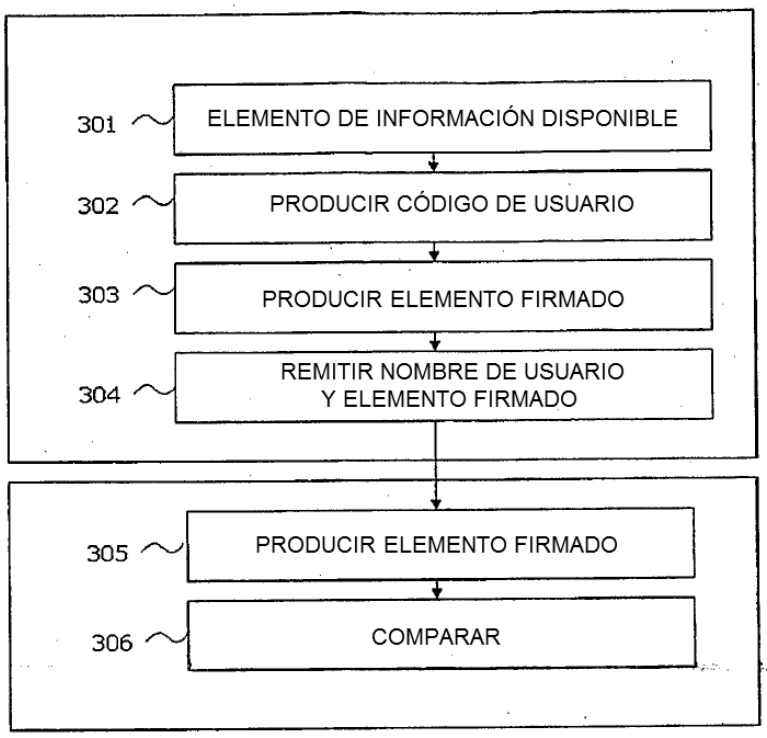
301
ELEMENTO DE INFORMACIÓN DISPONIBLE
302
PRODUCIR CÓDIGO DE USUARIO
303
PRODUCIR ELEMENTO FIRMADO
304
REMITIR NOMBRE DE USUARIO
Y ELEMENTO FIRMADO
305
PRODUCIR ELEMENTO FIRMADO
306
COMPARAR

FIG.3

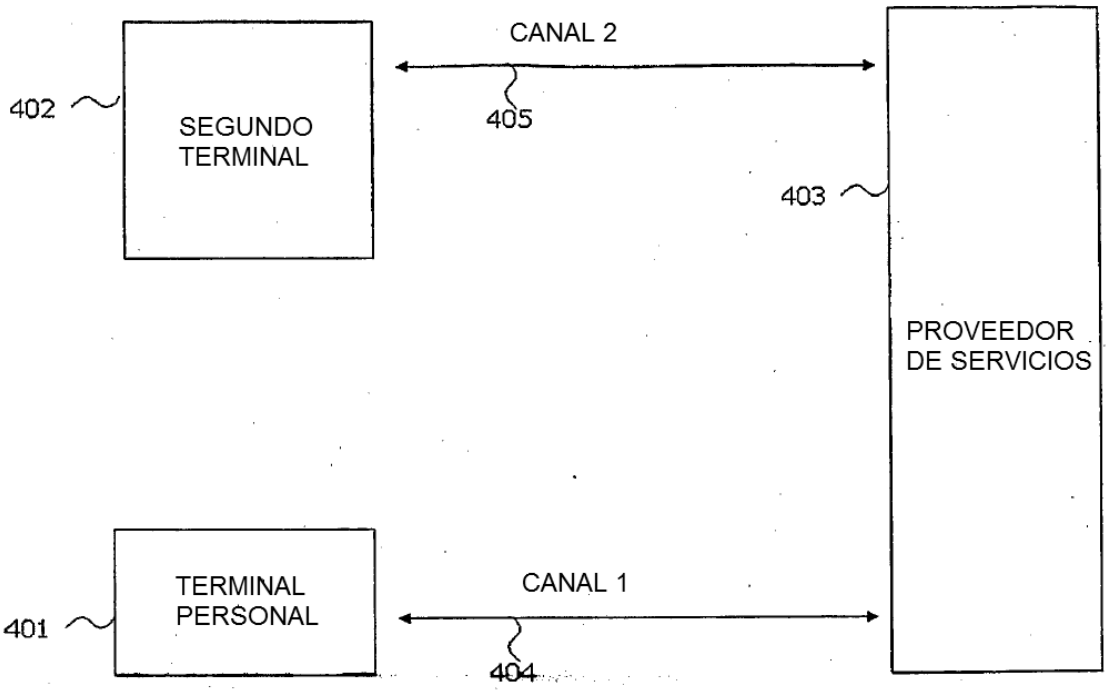
CANAL 2
402
SEGUNDO TERMINAL
405
403
PROVEEDOR DE SERVICIOS
TERMINAL PERSONAL
CANAL 1
401
404

FIG. 4