(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 575 356**

(51) Int. CI.:

G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.07.2004 E 04743579 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.03.2016 EP 1671198**

(54) Título: **Facilitar y autenticar transacciones**

(30) Prioridad:

09.10.2003 GB 0323693
10.10.2003 GB 0323836

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.06.2016

(73) Titular/es:

VODAFONE GROUP PLC (100.0%)
VODAFONE HOUSE THE CONNECTION
NEWBURY, BERKSHIRE RG14 2FN, GB

(72) Inventor/es:

JEAL, DAVID;
MUDIE, GEORGE, STRONACH y
DEBNEY, CHARLES, WILLIAM

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Facilitar y autenticar transacciones

Antecedentes de la invención

La invención se refiere a la facilitación y autenticación de transacciones. En las realizaciones de la invención, a ser descritas más adelante en más detalle a modo de ejemplo solamente, se facilitan y autentican transacciones entre un aparato de proceso de datos (tal como un ordenador personal) o un usuario del mismo y una tercera parte (posiblemente remota) y tal facilitación y autenticación también puede implicar la facilitación y autenticación de un pago o transferencia de datos a ser hecha por o en nombre del usuario a la tercera parte.

Compendio de la invención

La invención se define por las reivindicaciones adjuntas.

Según un aspecto de la invención, se proporciona un método para llevar a cabo un proceso de autenticación para autenticar una transacción con un aparato de proceso de datos, en el que al menos durante el proceso de autenticación el aparato de proceso de datos ha asociado operativamente con él uno seleccionado de una pluralidad de medios de almacenamiento de autenticación cada uno para almacenar información de autenticación predeterminada, los medios de almacenamiento de autenticación que son registrables con un sistema común y que incluyen el paso de llevar a cabo el proceso de autenticación a través de un enlace de comunicaciones con ese sistema, el proceso de autenticación que se lleva a cabo mediante medios de autenticación incorporados en el sistema y que implican el uso de la información de autenticación predeterminada almacenada por el seleccionado de los medios de almacenamiento de autenticación.

Según otro aspecto de la invención, se proporciona un aparato de proceso de datos en combinación con uno seleccionado de una pluralidad de medios de almacenamiento de autenticación cada uno para almacenar información de autenticación predeterminada relativa a llevar a cabo un proceso de autenticación para autenticar una transacción con el aparato de proceso de datos, los medios de almacenamiento de autenticación todos que son registrables con un sistema común, los medios de almacenamiento de autenticación cuando se asocian operativamente con el aparato de proceso de datos que es operativo para llevar a cabo el proceso de autenticación a través de un enlace de comunicaciones con ese sistema, el proceso de autenticación que se lleva a cabo mediante medios de autenticación incorporados en el sistema y que implican el uso de la información de autenticación predeterminada almacenada por el seleccionado de los medios de almacenamiento de autenticación.

Según otro aspecto de la invención, se proporciona un dispositivo para acoplarse a un aparato de proceso de datos para permitir un proceso de autenticación que implica el uso de medios de autenticación separados, el dispositivo que se configura para proporcionar una pluralidad de registros de información de autenticación activables separadamente para uso en el proceso de autenticación, los registros de información de autenticación que se registran con un sistema que incluye los medios de autenticación, el dispositivo que es sensible a un mensaje de entrada para derivar una respuesta dependiente del mensaje de entrada y del registro de información de autenticación activado para permitir a los medios de autenticación llevar a cabo el proceso de autenticación a través de un enlace de comunicación con los medios de autenticación en el citado sistema por el cual autenticar una transacción.

Según otro aspecto de la invención, se proporciona un sistema de autenticación para autenticar transacciones de usuarios registrados con ese sistema para permitir una transacción con otro sistema a ser autenticado, el sistema de autenticación que incluye medios de autenticación para enviar un mensaje de autenticación en respuesta a una petición de autenticación de un abonado y para recibir y analizar una respuesta a la misma para determinar si la respuesta recibida corresponde a una respuesta esperada para autenticar la identidad del usuario; y medios de generación de un testigo de seguridad para generar un testigo de seguridad para uso en la realización de una transacción con el otro sistema.

Según otro aspecto de la invención, se proporciona un sistema para almacenar datos de usuario para uso en la realización de transacciones con una pluralidad de proveedores de servicios, en donde para cada usuario se almacena una pluralidad de registros de datos para uso cuando se realizan transacciones con proveedores de servicios respectivos y en donde solamente un registro de datos pertinente a un proveedor de servicios particular se pone a disposición en respuesta a una petición en nombre de ese proveedor de servicios.

Según otro aspecto de la invención, se proporciona un paquete de datos para uso en autenticar y realizar una transacción entre un cliente y un proveedor de productos o servicios, el paquete de datos que incluye datos indicativos de la identidad del proveedor de productos o servicios de manera que el paquete de datos es utilizable solamente para autenticar y realizar una transacción con ese proveedor de productos o servicios.

Según otro aspecto de la invención, se proporciona un método de facilitación de transacciones entre una pluralidad de usuarios registrados con un sistema de autenticación y una pluralidad de proveedores de productos o servicios, el método que incluye:

dotar a cada usuario con medios de almacenamiento de autenticación que almacenan información de autenticación predeterminada, cada medio de almacenamiento de autenticación que es acoplable a un aparato de proceso de datos para intercambio de datos con el mismo;

generar en respuesta a una petición, hecha usando el aparato de proceso de datos, desde un usuario a un proveedor de productos o servicios un paquete de datos de petición de transacción que incluye datos indicativos de la identidad del usuario y la identidad del proveedor de productos o servicios;

transmitir el paquete de datos de petición de transacción al sistema de autenticación a través del aparato de proceso de datos;

analizar en el sistema de autenticación el paquete de datos de petición de transacción y extraer del mismo la identidad del usuario;

transmitir desde el sistema de autenticación una señal de petición de autenticación a los medios de almacenamiento de autenticación de usuario a través del aparato de proceso de datos;

recibir a través del aparato de proceso de datos una respuesta de los medios de almacenamiento de autenticación de usuario en el sistema de autenticación;

analizar dicha respuesta en el sistema de autenticación para determinar si dicha respuesta corresponde a una respuesta esperada con referencia al conocimiento de dicha información de autenticación predeterminada para ese usuario;

generar un testigo de autenticación y proporcionar éste al proveedor de productos o servicios a través del aparato de proceso de datos, el testigo de autenticación que indica al proveedor de productos y servicios que el usuario está autenticado por el sistema de autenticación.

Breve descripción de los dibujos

Un método según la invención de facilitación y autenticación de transacciones que implica un aparato de proceso de datos tal como un ordenador personal y dispositivos para conexión a un aparato de proceso de datos (tal como un ordenador personal) que encarnan la invención, se describirá ahora, a modo de ejemplo solamente, con referencia a los dibujos esquemáticos anexos en los que:

La Figura 1 es un diagrama de bloques para explicar la operación del método en relación con el aparato de proceso de datos;

La Figura 2 es un diagrama de flujo para uso en la comprensión del diagrama de bloques de la Figura 1;

La Figura 3 es un diagrama de bloques que corresponde a la Figura 1 en el que se usa un “dispositivo de protección” según la invención;

La Figura 4 es una vista en perspectiva de una configuración de un dispositivo de protección;

La Figura 5 muestra un alzado lateral de una configuración adicional del dispositivo de protección;

La Figura 6 muestra un diagrama de bloques para explicar la operación de un método de autenticación de una transacción que usa un aparato de proceso de datos;

Las Figuras 7A, 7B y 7C son un diagrama de flujo para uso en la comprensión del proceso de autenticación llevado a cabo por el aparato de proceso de datos de la Figura 6;

La Figura 8A muestra una vista frontal de una tercera configuración de un dispositivo de protección;

La Figura 8B muestra una vista lateral del dispositivo de protección de la Figura 8A;

La Figura 8C muestra una vista en sección transversal tomada a lo largo de la línea x-x de la Figura 8B pero con el conector del dispositivo de protección extendido;

La Figura 8D muestra una vista lateral que corresponde a la Figura 8B pero con el conector del dispositivo de protección extendido;

La Figura 9A muestra una vista frontal de una cuarta configuración de un dispositivo de protección;

La Figura 9B muestra una vista lateral del dispositivo de protección de la Figura 9A;

La Figura 9C muestra una vista frontal que corresponde a la Figura 9A pero con el conector del dispositivo de protección extendido;

La Figura 9D muestra una vista lateral que corresponde a la Figura 9B pero con el conector del dispositivo de protección extendido;

La Figura 10A muestra una vista frontal de una quinta configuración de un dispositivo de protección;

La Figura 10B muestra una vista lateral del dispositivo de protección de la Figura 10A;

La Figura 10C muestra una vista frontal que corresponde a la Figura 10A pero con el conector del dispositivo de protección extendido;

La Figura 10D muestra una vista lateral que corresponde a la Figura 10B pero con el conector del dispositivo de protección extendido;

La Figura 11A muestra una vista frontal de una sexta configuración de un dispositivo de protección;

La Figura 11B muestra una vista lateral del dispositivo de protección de la Figura 11A; y

La Figura 11C muestra cómo el conector eléctrico emerge de la carcasa del dispositivo de protección.

En las figuras elementos iguales se designan generalmente con los mismos números de referencia.

Modos de llevar a cabo la invención

Existen muchos casos cuando una transacción que implica el uso de un aparato de proceso de datos requiere autenticación. Por ejemplo, el aparato de proceso de datos se puede requerir que lleve a cabo una transacción, tal como el intercambio de información, con una tercera parte, tal como una tercera parte remota con la cual la comunicación se debe hacer sobre un enlace de telecomunicaciones (incluyendo a través de Internet). La tercera parte puede requerir que el aparato de proceso de datos o el usuario del mismo, por el momento, se autentique a satisfacción de la tercera parte antes de que tenga lugar la transacción.

Como se expuso, la transacción puede implicar meramente el intercambio de información. Por ejemplo, el usuario del aparato de proceso de datos puede simplemente necesitar ser autenticado a fin de descargar información desde la tercera parte. Tal información puede ser información mantenida por la tercera parte en nombre del usuario del aparato de proceso de datos (por ejemplo, información relativa a la cuenta bancaria del usuario). En su lugar, la información pudiera ser información mantenida en otro aparato de proceso de datos, tal como una red de datos que pertenece a una organización o entidad comercial con la cual está conectado el usuario o por la cual está empleado el usuario, facilitando de esta manera acceso a esa red por el usuario cuando el usuario está viajando. Otra transacción posible puede implicar la descarga por el aparato de proceso de datos de software desde la ubicación remota.

Además, la transacción puede requerir que un pago sea hecho por el usuario a fin de permitir que la transacción tenga lugar, tal como un pago a la tercera parte a cambio de la información proporcionada. Claramente, cuando está implicado tal pago, es importante que el usuario se autentique a satisfacción de la tercera parte y que el pago se haga de una manera simple y segura.

Aunque la discusión precedente se ha referido a un “usuario” del aparato de proceso de datos, algunas, por lo menos, de las transacciones descritas anteriormente pueden no implicar de hecho ningún usuario humano: se puede requerir que el aparato de proceso de datos opere automáticamente (por ejemplo, operando intermitentemente en un papel de recogida de información o monitorización y notificando los resultados a una tercera parte). En tales casos, puede ser necesario alternativa o adicionalmente para el aparato de proceso de datos autentificarse por sí mismo a satisfacción de la tercera parte.

El aparato de proceso de datos se dota con o asocia con, medios (medios de almacenamiento de autenticación) para almacenar información de autenticación predeterminada para autenticar ese aparato o un usuario particular del mismo. En una realización, los medios para almacenar la información predeterminada son desmontables y se pueden tomar de esta manera por el usuario e insertar en cualquier aparato de proceso de datos (u ordenador) que esté adaptado para recibirlos, para permitir a ese usuario ser autenticado con respecto a una transacción a ser llevada a cabo por ese usuario con ese ordenador. Ventajosamente, en tal caso los medios para almacenar la información predeterminada están en forma de una tarjeta inteligente.

En un ejemplo más específico, la tarjeta inteligente es un Módulo de Identidad de Abonado o SIM del tipo usado en y para autenticar el uso de aparatos de teléfono en una red de telecomunicaciones móvil o celular - tal como una red GSM (Grupo Móvil Especial) o 3G (Tercera Generación). Tal red almacenará detalles de los SIM de sus usuarios (abonados). En operación de la red, un aparato de teléfono de usuario se autentica (por ejemplo, cuando el usuario activa el aparato de teléfono en la red con vistas a hacer o recibir llamadas) por la red enviando un desafío al aparato de teléfono que incorpora ese SIM, en respuesta al cual el SIM calcula una respuesta (dependiente de la información predeterminada mantenida en el SIM – típicamente un algoritmo de autenticación y una clave única Ki) y la transmite de vuelta a la red que la comprueba contra su propia información para ese usuario o abonado a fin de completar el proceso de autenticación. Del mismo modo, por lo tanto, el SIM se puede usar en o en asociación con

el aparato de proceso de datos u ordenador de manera que se puede llevar a cabo la misma forma de proceso de autenticación. En un caso, donde el SIM es el SIM de un abonado a una red de telecomunicaciones celular particular, el proceso de autenticación se puede llevar a cabo por esa red.

Se debería señalar que el proceso de autenticación que se describe no autentica necesariamente la identidad humana del usuario. Por ejemplo, las redes de telecomunicación celular tienen abonados de prepago que son titulares de SIM a cambio de prepago permitiéndoles hacer llamadas en la red. No obstante, la identidad de tales abonados de prepago no se conoce (o no se conoce necesariamente) por las redes. Sin embargo, tal usuario no puede hacer uso de la red hasta que la red ha autenticado que el SIM de usuario – es decir, ha confirmado que tal usuario es un usuario particular que tiene una cuenta de prepago particular con la red. Los SIM de tales usuarios o abonados de prepago se podrían usar igualmente bien (de la manera descrita) en o en asociación con un aparato de proceso de datos u ordenadores, para los propósitos de autenticar ese usuario.

El SIM no necesita tomar la forma de una tarjeta inteligente física (y desmontable) sino que en su lugar se puede simular estando embebido en el aparato de proceso de datos u ordenador en forma de software o representado como un chip por ejemplo.

Puede ser deseable ser capaz de cambiar la información de autenticación en el SIM (o SIM simulado) para tener en cuenta las circunstancias cambiadas. Por ejemplo, el SIM puede ser un SIM registrado con una red de telecomunicaciones celular particular – una red aplicable al país o región donde el aparato de proceso de datos u ordenador va a ser usado. No obstante, pueden surgir circunstancias (por ejemplo, el aparato o el ordenador se mueve físicamente a un país o región diferente) en las cuales es deseable o necesario volver a registrar el SIM con una red de telecomunicaciones celular diferente. Formas en que esto se puede hacer se describen en nuestras solicitudes de patente del Reino Unido en tramitación Nº 0118406.8, 0122712.3 y 0130790.9 y en nuestras solicitudes PCT Nº GB02/003265, GB02/003260 y GB02/003252 correspondientes. Como se describe en las mismas en más detalle, un SIM (y de esta manera también un SIM simulado) se puede dotar inicialmente con información de autenticación (y otra) con relación a cada una de una pluralidad de redes, la información respectiva a las diferentes redes que es activable selectivamente.

No es necesario, no obstante, para los usuarios estar abonados a una red de telecomunicaciones. En su lugar, podrían ser abonados registrados con algún otro sistema centralizado que podría llevar a cabo entonces el proceso de autenticación del mismo modo que en una red de telecomunicaciones. En tal caso, el registro de un SIM (o SIM simulado) se podría transferir desde un sistema centralizado tal a otro de la misma manera que se describió anteriormente.

Como se describió anteriormente, un objetivo del proceso de autenticación es facilitar una transacción entre el aparato de proceso de datos u ordenador y una tercera parte. Donde el proceso de autenticación se lleva a cabo por una red de telecomunicaciones o por algún otro sistema, al que el usuario del SIM está abonado, la terminación satisfactoria del proceso de autenticación entonces se comunicaría por esa red o sistema a la tercera parte – para permitir avanzar a la transacción.

Para muchas transacciones del tipo descrito, puede estar implicado un pago por el usuario a la tercera parte. Una disposición como se describió anteriormente, en la que el proceso de autenticación se lleva a cabo por una red de telecomunicaciones u otro sistema centralizado al cual está abonado el usuario facilita ventajosamente la realización de tales pagos y es particularmente ventajosa donde (como puede ser el caso a menudo) el pago es de una cantidad pequeña (por ejemplo, un pago a cambio de la recepción de información – por ejemplo, información meteorológica o de tráfico o para uso temporal de software específico); en tal caso, el pago se puede adeudar a la cuenta del abonado mantenida por la red de telecomunicaciones u otro sistema centralizado – y entonces, por supuesto, pasado a la tercera parte, quizás después de la deducción de un cargo de tramitación.

El diagrama de bloques de la Figura 1 ilustra esquemáticamente una forma de operar el método descrito anteriormente.

Se muestra un ordenador personal o PC 10 basado en Windows (‘Windows’ es una marca registrada). El PC 10 está adaptado para recibir un SIM mostrado esquemáticamente en 12. El SIM se puede equipar de manera desmontable al PC, para uso en identificar un usuario (es decir, el titular del SIM) o se puede fijar dentro del PC (para identificar el PC en sí mismo). El PC 10 incorpora software de gestión de transacción 14 que interactúa con y controla algunas de las funciones del SIM.

Aunque se ha descrito una disposición donde el PC 10 se adapta a recibir un SIM, se debería apreciar que se podría usar una tarjeta inteligente distinta de un SIM y ésta está de acuerdo con la invención. Además, en lugar del SIM (o tarjeta inteligente) que se recibe por el PC – siendo equipado de manera desmontable al PC o fijado dentro del PC – el SIM (o tarjeta inteligente) se podría asociar con el PC de cualquier forma que permita comunicación entre el SIM (o tarjeta inteligente) y el PC 10. Por ejemplo, el SIM (o tarjeta inteligente) se podría dotar con un “dispositivo de protección” (ejemplos del cual se describen en lo sucesivo en detalle) que permite comunicación cableada o inalámbrica con el PC 10. Preferiblemente, la comunicación entre el SIM (o tarjeta inteligente) y el PC 10 es segura. Las comunicaciones se pueden cifrar o se puede emplear cualquier otro medio para comunicación segura.

También mostrada en la Figura 1 está una red de telefonía celular 16, tal como la red de Vodafone (marca registrada) y se supone que el SIM 12 se registra con la red 16.

La operación del sistema mostrado en la Figura 1 se explicará en relación al diagrama de flujo de la Figura 2.

En el paso A, el usuario del PC 10 solicita el uso de una aplicación particular 17 en el PC. Por ejemplo, el usuario pudiera desear ver páginas web que contienen información especializada que están cifradas y, de esta manera, no disponibles de manera general. A fin de hacer esto, el usuario solicita una "clave de sesión" – es decir, por ejemplo, permiso para llevar a cabo una transacción que implica uso por tiempo limitado de la aplicación particular. La petición de la clave de sesión se dirige al gestor de transacción 14. El gestor de transacción 14 entonces, transmite información de identificación derivada del SIM 12 (un mensaje "estoy aquí") a la parte de servicios de seguridad 18 de la red 16 (paso B). En respuesta al mensaje "estoy aquí", la red transmite un desafío aleatorio (paso C) al gestor de transacción 14, este desafío que se basa en información conocida para la red acerca del SIM 12.

La flecha doble punta 19 en la Figura 1 indica esquemáticamente la comunicación de datos de dos vías entre el PC 10 y la red 16. Esta comunicación de datos puede ser sobre cualquier medio de comunicación adecuado. Por ejemplo, el medio de comunicación puede ser una red de telefonía fija (tal como PSTN) o una red inalámbrica. Por ejemplo, la red inalámbrica puede ser la misma que la red 16 que proporciona servicios de seguridad 18 o puede ser otra red. La comunicación de datos se puede realizar a través de Internet. La comunicación de datos es preferible de una forma que sea segura y cifrada.

En el paso D, el gestor de transacción 14 transmite una respuesta desde el SIM 12 al desafío proporcionando una respuesta derivada del desafío y la clave mantenida en el SIM. La respuesta se comprueba por la parte de servicios de seguridad 18 de la red 16. Suponiendo que la respuesta es satisfactoria, la parte de servicios de seguridad 18 autentica el usuario y confirma esto al gestor de transacción 14 (paso E) – posiblemente proporcionando un Testigo de Seguridad poblado. Al mismo tiempo, la parte de servicios de seguridad 18 en la red transmite la clave de sesión (paso F) a la parte de servicios de aplicaciones 22 de la red 16.

El gestor de transacción 14 también transmite la clave de sesión a la aplicación 17 (paso G).

En la realización descrita, el gestor de transacción facilita la transferencia de datos a y desde el SIM 12. No hay requisito para que el gestor de transacción sea capaz de comprender o interpretar estos datos. La función del gestor de transacción en la realización que se describe es actuar como un conducto para los datos que se pasan a y desde el SIM 12.

El usuario ahora puede hacer la petición de la aplicación particular (paso H), acompañando esta petición de aplicación con la clave de sesión recibida en el paso G. La petición de aplicación del paso H se transmite a una parte de servicios de aplicaciones 22 que puede ser parte de la red 16 (como se muestra) o puede estar separada y controlada por una tercera parte. En el paso I la parte de servicios de aplicaciones compara la clave de sesión recibida con la petición de aplicación (paso H) con la clave de sesión recibida en el paso F. Suponiendo que el resultado de esta comprobación es satisfactorio, la parte de servicios de aplicaciones 22 ahora transmite la aceptación de la petición de aplicación (paso J) al PC 10 y ahora avanza la petición. La clave de sesión puede permitir un uso de tiempo limitado del servidor de aplicaciones 22, un uso único o un uso infinito – dependiendo de las circunstancias. La red ahora puede adeudar la cuenta del usuario con un cargo por la sesión. Puede haber un enlace de comunicación entre la parte de servicios de aplicaciones 22 y la parte de servicios de seguridad 18 para permitir intercambio de datos entre aquellas partes – por ejemplo permitir a la parte de servicios de seguridad 18 disponer que la cuenta del usuario con la red 16 sea adeudada.

Lo precedente es por supuesto meramente un simple ejemplo de una implementación de lo que se ha descrito.

En una disposición alternativa, un portador de datos se puede dotar con medios para almacenar información predeterminada tal como en una de las formas descritas anteriormente – es decir, un SIM o (más probablemente) software que simula un SIM. El SIM simulado se asocia con datos almacenados en el portador de datos. El portador de datos puede ser, por ejemplo, un DVD o CD ROM o algún otro portador de datos similar y los datos en los mismos pueden ser software o un conjunto de software.

El SIM simulado se puede usar para identificar y autenticar los datos (tales como el software) en el portador de datos. El SIM simulado se registrará con una red de telecomunicaciones o algún otro sistema centralizado, de la misma manera que se describió anteriormente. Cuando el portador de datos se coloca en un aparato de proceso de datos tal como un ordenador, para uso en el mismo, el SIM se usaría para identificar y autenticar el portador de datos y los datos almacenados en el mismo y (por ejemplo) entonces podría permitir al software ser descargado para uso en el ordenador. De este modo, el SIM se podría usar posteriormente para bloquear un uso adicional del software (por ejemplo, en otro ordenador) o para permitir a los datos ser usados solamente durante un número predeterminado de veces (ya sea en el mismo o en un ordenador diferente). Si, por ejemplo, el portador de datos (con su SIM) se coloca en un ordenador que también ha recibido un SIM de usuario particular entonces (a) el SIM en el portador de datos se puede usar para identificar y autenticar el software y (b) el SIM en o asociado con el ordenador se puede usar para autenticar al usuario y se podría usar posteriormente para permitir que un cargo sea adeudado a ese usuario como pago por uso del software.

Los datos almacenados en el portador de datos con el SIM, por ejemplo, pueden ser datos cifrados. Esos datos cifrados solamente se pueden cifrar usando información proporcionada por el SIM en el portador de datos. De este modo, el SIM en el portador de datos puede controlar el uso de los datos almacenados en el portador de datos. Por ejemplo, el portador de datos se puede vender con una licencia particular dando a un usuario derechos restringidos para usar los datos en el portador de datos. Se puede permitir al usuario usar los datos durante un periodo de tiempo predeterminado o durante un número de veces predeterminado. Cada vez que se usan los datos se descifran usando datos almacenados en el SIM. Se mantiene un registro en el SIM (o cualquier otro lugar) del número de veces que se descifran los datos. Cuando el número de veces que se han descifrado los datos iguala el número de veces proporcionadas en la licencia vendida con el portador de datos, el SIM evita un uso adicional de los datos no descifrando los datos. Si los datos se dotan con una licencia que dura hasta el tiempo predeterminado, cada vez que el SIM descifra los datos, el SIM comprobará que el tiempo actual (con referencia a un reloj adecuado proporcionado, por ejemplo, en el SIM, en el PC 10 o con referencia a la red 16) de manera que el descifrado de los datos se realiza solamente hasta el tiempo especificado en la licencia vendida con el portador de datos.

Aunque se describió anteriormente un SIM simulado, se prefiere ahora que el SIM se implemente en hardware debido a esto es más seguro. Los datos de autenticación secretos en un SIM hardware son inaccesible a personas no autorizadas.

En lugar del PC 10 que se adapta para recibir un SIM 12 o un portador de datos que se modifica para incorporar un SIM o software que simula un SIM, un dispositivo separado o “dispositivo de protección” 30 se puede proporcionar para recibir el SIM 12 o para incorporar software que simula el SIM 12.

La Figura 3 muestra un dispositivo de protección 30 que permite datos para autenticar una transacción (o para cualquier otro propósito adecuado) a ser pasados entre el dispositivo de protección 30 y el PC 10 y de manera hacia delante a/desde la red 16.

El dispositivo de protección 30 comprende un alojamiento 32 que tiene una ranura para recibir un SIM 12. El alojamiento 32 se puede hacer de cualquier material adecuado. Preferiblemente, este material es un aislante eléctricamente. Por ejemplo, el alojamiento puede comprender resina o plásticos activados por láser.

Se proporcionan conectores adecuados (no mostrados) dentro del alojamiento 32 para permitir intercambio electrónico de datos entre el SIM 12 y el dispositivo de protección 30. El dispositivo de protección 30 además comprende un conector adecuado 34 para permitir conexión para propósitos de comunicación de datos al PC 10. Por ejemplo, el conector podría ser un conector USB, un conector Firewire 1394 o cualquier otro conector adecuado. Por supuesto, se pueden proporcionar diferentes configuraciones del dispositivo de protección. Por ejemplo, el SIM 12 se puede acomodar completamente dentro del dispositivo de protección 30 y puede ser desmontable del dispositivo de protección 30 abriendo el alojamiento 32 o el SIM 12 se puede sellar o encapsular permanentemente dentro de la carcasa del dispositivo de protección 32. Si se proporciona esta última disposición, un usuario del sistema de telecomunicación se puede dotar con un primer SIM para uso, por ejemplo, en su aparato de teléfono móvil y se puede dotar con un dispositivo de protección 30 que aloja un SIM separado que se usa para realizar transacciones a través del PC 10. Si se desea, la red de telecomunicaciones incluirá un registro que indica que el SIM dentro del aparato de teléfono móvil del usuario y el SIM dentro del dispositivo de protección del usuario se poseen comúnmente y esta información se puede usar para dotar convenientemente al usuario con una única cuenta de cargos incurridos con respecto al uso de ambos SIM.

El dispositivo de protección 30 se dota con un controlador de interfaz de dispositivo de protección 36 que controla la comunicación con el PC 10. Todas las comunicaciones desde el PC 10 se encaminan a través del controlador de interfaz de dispositivo de protección 36 y los datos almacenados en el SIM 12 no se pueden acceder de manera distinta de usando el controlador de interfaz de dispositivo de protección 36. Un controlador de interfaz de PC 38 correspondiente se proporciona para el PC 10. El controlador de interfaz de PC 38, por ejemplo, puede comprender una serie de comandos en forma de un programa de ordenador que se carga en y ejecuta por el PC 10. El controlador de interfaz de PC 38, por ejemplo, se puede proporcionar por o bajo el control de la red 16. El controlador de interfaz de PC 38 por lo tanto será “de confianza” en la red 16 y se configurará para permitir solamente acceso al dispositivo de protección 30 y consecuentemente el SIM 12 de una manera aprobada que no permitirá que la información de seguridad presente en el SIM 12 sea comprometida.

Para evitar o reducir, la probabilidad de que el controlador de interfaz de PC 38 sea sustituido o puenteado por un controlador alternativo, lo que podría comprometer la seguridad de los datos en el SIM 12, el controlador de interfaz de PC 38 y el controlador de interfaz de dispositivo de protección 36 se dotan con claves secretas compartidas 40, 42 respectivas. Cada comunicación desde el controlador de interfaz de PC 38 al dispositivo de protección 30 se cifra usando la clave secreta compartida 40. Todas las comunicaciones desde el PC 10 al dispositivo de protección 30 se reciben por el controlador de interfaz de dispositivo de protección 36. El controlador de interfaz de dispositivo de protección 36 comprende medios de procesamiento para descifrar las comunicaciones recibidas usando su clave secreta 42. Para mejorar la seguridad, el controlador de interfaz de dispositivo de protección 36 evitará todas las comunicaciones distintas de la cifrada usando la clave secreta compartida 40 de los datos de envío o los datos de recepción desde el SIM 12.

Por lo tanto, el controlador de interfaz de PC 38 controla y supervisa el acceso al dispositivo de protección 30 y el SIM 12 para reducir la probabilidad de que los datos almacenados en el SIM 12 sean comprometidos por intentos no autorizados de acceder al SIM 12.

A condición de que una petición de acceso a datos en el SIM 12 se apruebe por el controlador de interfaz de PC (según, por ejemplo, criterios fijados por la red 16) y por lo tanto se comunique al controlador de interfaz de dispositivo de protección 36 con la clave apropiada 40, una transacción se puede autenticar usando el SIM 12 de la manera descrita en relación con las Figuras 1 y 2.

Aunque la provisión de claves secretas compartidas 40, 42 es ventajosa, se debería apreciar que la provisión de claves secretas compartidas 40, 42 no es esencial para la invención.

En una disposición alternativa el controlador de interfaz de PC 38 no se dota con una clave secreta particular 40. No obstante, el controlador de interfaz de dispositivo de protección 36 se dota con una clave 42. Cuando el dispositivo de protección 30 se acopla con el PC 10 el controlador de interfaz de PC 38 detecta que el controlador de interfaz de dispositivo de protección se dota con una clave 42. El controlador de interfaz de PC 38 entonces puede obtener de la red 16 a través del enlace de comunicación 19 una clave que permitirá intercambio de datos entre el controlador de interfaz de PC 13 y el controlador de interfaz de dispositivo de protección 36 cifrado usando la clave 42. Por ejemplo, la clave 42 del controlador de interfaz de dispositivo de protección 36 puede ser una clave privada y la clave 40 proporcionada al controlador de interfaz de PC por la red 16 puede ser una clave pública – las dos claves que son un par de claves pública-privada. Las claves proporcionadas por la red 16 no se proporcionan preferiblemente bajo petición por ninguna aplicación. Por ejemplo, la red 16 se puede configurar para proporcionar solamente estas claves a un controlador de interfaz de PC de confianza y/o después de algún proceso de autenticación.

Alternativamente, la transferencia de datos entre el controlador de interfaz de dispositivo de protección 36 y el controlador de interfaz de PC 38 puede no estar cifrada o puede estar cifrada de una forma que es común a muchos controladores de interfaz de dispositivo de protección y controladores de interfaz de PC proporcionados en diferentes equipos, lo cual tiene la ventaja de permitir al dispositivo de protección 30 ser usado con una multiplicidad de diferentes PC.

Como una medida de seguridad añadida, se pueden cifrar las comunicaciones entre el controlador de interfaz de PC 38 y el gestor de transacción 14. Por ejemplo, esas partes pueden tener cada una clave secreta compartida y las comunicaciones entre ellas se pueden cifrar usando la clave secreta compartida.

Una realización adicional para la presente invención se describirá en relación a la Figura 4. Según la Figura 4, el dispositivo de protección 30 tiene el SIM 12 acomodado completamente dentro de su alojamiento 32 y el SIM, por lo tanto, no se puede ver en la Figura. El dispositivo de protección 30 tiene un conector 34 para conexión al PC 10 de una manera similar a la realización de la Figura 3. En el extremo opuesto de la carcasa 32 se puede proporcionar un conector de bucle opcional 44 para proporcionar un medio conveniente para transportar el dispositivo de protección 30 uniéndolo al llavero de un usuario.

Una cara del alojamiento 32 tiene una variedad de pulsadores 46 montados sobre la misma, diez de los cuales tienen números respectivos desde 0 a 9 mostrados sobre los mismos. En esta realización, el dispositivo de protección 30 incluye medios (tales como software) para recibir la entrada de un número PIN desde un usuario operando los pulsadores 46 designados adecuadamente el cual se compara con el número PIN proporcionado para y almacenado en el SIM 12. Los SIM usados en la red de telecomunicaciones GSM se dotarán convencionalmente con tal PIN.

El alojamiento 32 puede proporcionar opcionalmente además un visualizador 48 para sugerir al usuario introducir su número PIN y/o para mostrar el número PIN a medida que se introduce, si se desea. Al introducir el número PIN usando los pulsadores 46, el número PIN introducido se compara con el número PIN almacenado en el SIM. Si los PIN se encuentra que coinciden, la comunicación entre el SIM y el PC 10 se permite para autenticar una o más transacciones. La comparación entre el número PIN introducido y el número PIN almacenado en el SIM 12 se realiza dentro del dispositivo de protección 30 y ni el número PIN introducido ni el número PIN almacenado en el SIM se comunican al PC 10. Esto evita o reduce la probabilidad de que los PIN llegarán a estar comprometidos por revelación a una parte autorizada.

Para permitir la entrada del PIN el dispositivo de protección 30 requiere un suministro de potencia. La potencia se puede proporcionar por el PC 10. Ventajosamente, el PIN tiene su propio suministro de potencia temporal que permite al PIN ser introducido y verificado. Posteriormente, el suministro de potencia se interrumpe y se pierden los datos del PIN. Este es un rasgo de seguridad adicional y se describe en más detalle más adelante.

La disposición de comparación de entrada de PIN de la Figura 4 se puede proporcionar además a o como una alternativa a los controladores de interfaz 36, 38 y las claves de secreto compartido 40, 42 de la disposición mostrada en la Figura 3.

Se debería apreciar que como alternativa a los pulsadores 46, se podrían proporcionar otros medios para permitir la introducción del PIN. Alternativamente, se podría autorizar al usuario para usar el SIM obteniendo alguna otra información de seguridad del usuario y comparando ésta con los datos almacenados en el SIM 12. Por ejemplo, los datos obtenidos podrían ser la huella dactilar del usuario o alguna otra característica que es improbable que vuelva a ocurrir en otra persona – por ejemplo, cualquier dato biométrico adecuado. Los detalles de la huella dactilar (u otra información) se almacenan en el SIM para comparación con los datos de entrada que representan las características.

Como un rasgo de seguridad adicional en la realización de la Figura 4, se puede proporcionar un visualizador que muestra el nombre de la aplicación u organización que solicita información desde el SIM 12. Esto permitiría al usuario monitorizar peticiones que se hacen a su SIM 12.

Si los controladores de interfaz 36, 38 respectivos y las claves de secreto compartido 40, 42 descritas en relación con la Figura 3 se usan en un sistema que también incluye la introducción del PIN y la disposición de comparación descrita en relación con la Figura 4, para proporcionar un nivel añadido de seguridad, el dispositivo de protección 30 se puede programar para mostrar el nombre de la aplicación u organización que solicita los datos desde el SIM 12 y entonces puede sugerir al usuario aprobar el suministro de datos para cada una o las seleccionadas de las aplicaciones/organizaciones introduciendo el PIN de usuario usando el teclado 46. Como alternativa a introducir un PIN se podría sugerir al usuario activar un botón “confirmar transacción” o similar.

El dispositivo de protección 30 se puede usar para facilitar transacciones con aparatos de proceso de datos distintos de los PC. Por ejemplo, un usuario que tiene una cuenta con la red 16 y que se dota con un dispositivo de protección 30 puede insertar el conector 34 en una ranura configurada adecuadamente en un parquímetro que es conectable a la red 16. El SIM 12 contenido dentro del dispositivo de protección 30 se autentica de la manera descrita anteriormente usando un gestor de transacción proporcionado dentro del parquímetro. Por este medio, el pago del aparcamiento se puede hacer deduciendo una cantidad adecuada de la cuenta del usuario con la red 16. Ventajosamente, el dispositivo de protección 30 se dotará con los pulsadores 46 y el dispositivo de protección sugerirá al usuario introducir un PIN que se compara con el PIN almacenado en el SIM de manera que el dispositivo de protección 30 no se pueda usar por una parte no autorizada. El dispositivo de protección se podría programar para permitir a los pulsadores 46, bajo control del parquímetro, permitir la entrada de datos pertinentes a la transacción – por ejemplo, la duración de tiempo durante el cual se requiere el aparcamiento.

El dispositivo de protección 30, por ejemplo, también se podría usar de una manera similar con un reproductor de DVD configurado adecuadamente para permitir que una película sea vista bajo pago de una tarifa deducida de la cuenta del usuario con la red 16. El sistema se puede disponer para permitir al dispositivo de protección 30 operar como una clave en un esquema de gestión de derechos digitales, como se describe en nuestra solicitud de patente en tramitación titulada “Data Processing” presentada en la misma fecha con la presente solicitud. El dispositivo de protección también podría permitir que productos sean adquiridos de una máquina expendedora configurada adecuadamente o entradas a ser adquiridas de una máquina de venta de entradas configurada adecuadamente. Tales máquinas incluirán un procesador de manera que las funciones que corresponden a las realizadas por el gestor de transacción 14 del PC 10 se pueden realizar por las máquinas.

En la descripción anterior se ha indicado que el SIM usado para autenticar la transacción podría tener la forma de un SIM convencional que o bien se inserta en una ranura adecuada dentro del PC 10 o bien en el dispositivo de protección 30 (si se proporciona). Éste podría ser simplemente el SIM que un abonado a una red móvil usa en su terminal móvil convencional para hacer y recibir llamadas. Alternativamente, el SIM 12 se podría embeber dentro del PC 10 o el dispositivo de protección 30 (de manera que no se puede desmontar fácilmente o no se puede desmontar en absoluto). Además alternativamente, el SIM puede no tener una forma física separada, sino que se puede simular por medio de software y/o hardware dentro del PC 10 o el dispositivo de protección 30. El SIM se podría simular o incorporar en el juego de chips del PC 10. Por ejemplo, el SIM se podría incorporar o simular dentro de la unidad central de proceso del PC 10. Tal disposición evita que el SIM (o SIM simulado) sea desmontado del PC 10 (de otra manera que no sea inutilizando el PC 10).

Si el SIM es de una forma que no es fácilmente desmontable del PC 10 o del dispositivo de protección 30, un abonado al sistema de telecomunicaciones se puede dotar con un segundo SIM para su uso, por ejemplo, en su aparato de teléfono móvil.

Si, no obstante, se usa el mismo SIM (en el PC 10 o el dispositivo de protección 30) para autenticar transacciones y para uso de la manera convencional con la red de telecomunicaciones (por ejemplo, para hacer y recibir llamadas usando un teléfono móvil), los mismos datos se pueden usar para proporcionar autenticación de transacciones como se usa para autenticar el SIM con la red de telefonía móvil cuando una llamada está siendo hecha. Alternativamente, el SIM puede tener registros separados para realizar cada tipo de autenticación. Puede haber un primer registro que contiene datos y/o algoritmos para uso en transacciones de autenticación y un segundo registro separado para uso de la manera convencional para autenticar el terminal con la red de telecomunicaciones. El primer y segundo registros pueden tener claves de autenticación respectivas, identificadores únicos a la red de telecomunicaciones y/o algoritmos de autenticación únicos.

El primer registro puede comprender en sí mismo una serie de registros separados, cada uno registrado con la red de telecomunicación, para permitir transacciones autenticadas bajo el control de los registros separados a ser reconocidos y facturados separadamente. Esto se describe ahora en más detalle en relación con la Figura 5. En la Figura 5, el dispositivo de protección 30 puede contener una pluralidad de SIM 12 o puede tener una pluralidad de SIM simulados dentro del dispositivo de protección. Alternativamente, más que una pluralidad de SIM completos que se proporcionan o simulan, una pluralidad de diferentes registros se podría almacenar en el dispositivo de protección 30. Si se proporciona una pluralidad de SIM, se proporciona una pluralidad de SIM simuladas o se proporciona una pluralidad de registros alternativos, éstos se pueden considerar como registros de datos únicos respectivos que son identificables para la red de telecomunicaciones.

Tal disposición puede ser deseable, por ejemplo, cuando un usuario o abonado desea usar su dispositivo de protección 30 en múltiples entornos. Cuando el usuario o abonado está realizando tareas para su empleador, el dispositivo de protección 30 activará el registro de datos asociado con el empleador. Las transacciones autorizadas usando ese registro de datos, donde sea adecuado, provocarán un cargo que se hace a la cuenta al empleador. Cuando el usuario o abonado no está realizando tareas para su empleador, el registro de datos personal entonces se activa. Las transacciones autenticadas usando el dispositivo de protección 30 provocarán un cargo que se deduce de la cuenta personal del usuario. Esto permite transacciones realizadas por el usuario o abonado a título personal sean separadas de las realizadas en nombre de su empleador. El modo del dispositivo de protección 30 (es decir, si el registro de datos para el empleador o los registros de datos personales se activan) se puede controlar por un conmutador de modo 50 proporcionado en el dispositivo de protección 30 o el modo se puede alterar usando software proporcionado en el gestor de transacción 14 o controlador de interfaz de PC 38 que se ejecuta en el PC 10. Cuando se dan instrucciones por el usuario, el software causaría que las señales adecuadas sean enviadas al dispositivo de protección 30 para cambiar el SIM activo, el SIM simulado y el registro de datos.

Como una medida de seguridad añadida, el dispositivo de protección puede requerir al abonado introducir un PIN (o proporcionar otros datos) a fin de activar diferentes modos del SIM (por ejemplo, un modo “empleado” o modo “personal”). Se podría requerir un PIN diferente para activar cada modo.

El dispositivo de protección 30 descrito ahora de esta manera tiene un conector físico 34 (tal como un conector USB) para permitir comunicación de datos con un PC 10. Como alternativa a un conector físico 34, se puede proporcionar un enlace inalámbrico entre el dispositivo de protección 30 y el PC 10. El intercambio de datos puede tener lugar, por ejemplo, usando técnicas de campo cercano, usando tecnología Bluetooth, mediante señalización de infrarrojos o cualquier otro medio adecuado.

En lugar de que un dispositivo de protección 30 separado sea proporcionado, un SIM de usuario se puede situar en un terminal móvil (tal como un aparato de teléfono móvil) de la forma convencional. El SIM puede autenticar transacciones con el PC 10 mediante intercambio de datos adecuado entre el terminal móvil y el PC 10. Esto se podría lograr dotando al terminal móvil con un conector físico (tal como un conector USB) para conectar el PC 10 cuando se requiere autorización de una transacción o se podría hacer por cualquiera de las técnicas inalámbricas descritas anteriormente. Preferiblemente, esta comunicación se cifra o hace segura de alguna otra forma. Si el SIM se dota con registros de datos separados para propósitos de telecomunicaciones móviles convencionales y para autorizar transacciones, puede ser posible hacer simultáneamente una llamada de teléfono, por ejemplo, con la red de telecomunicaciones y autenticar una transacción con el PC 10. El terminal móvil puede proporcionar convenientemente el enlace de comunicación entre el PC 10 y la red 16. El acoplamiento del terminal móvil al PC 10 por lo tanto en esta disposición no solamente permite autenticación de transacciones sino que también proporciona convenientemente un medio de comunicación entre el PC 10 y la red 16. En una disposición alternativa, el terminal móvil aún proporciona comunicación sobre una red de telecomunicaciones móviles, pero esta es diferente a la red 16.

El dispositivo de protección 30 también puede realizar las funciones de una tarjeta de datos convencional para uso con un PC (u otro dispositivo informático). Con esta disposición, el dispositivo de protección será de un tamaño adecuado e incluirá conectores adecuados para permitirle operar como una tarjeta de datos, además del dispositivo de protección que tiene las funciones descritas anteriormente.

Una realización mejorada adicional de una disposición para autorizar una transacción se describirá ahora con referencia a la Figura 6 y el diagrama de flujo mostrado en las Figuras 7A, 7B y 7C.

Una plataforma de cliente, tal como el PC 10, incluye un gestor de transacción 14. Un dispositivo de protección 30 que tiene un SIM 12 en el mismo se proporciona y la comunicación entre el dispositivo de protección 30 y el gestor de transacción 14 se realiza a través de la conexión 34 (que puede ser una conexión cableada o inalámbrica). En esta realización el gestor de transacción 14 incorpora el controlador de interfaz de PC 38 mostrado en la Figura 3 y, por lo tanto, el controlador de interfaz de PC no se muestra como un artículo separado en la Figura 6. De manera similar, el dispositivo de protección 30 incorpora el controlador de interfaz de dispositivo de protección mostrado en 36 en la Figura 3 y, por lo tanto, un controlador de interfaz de dispositivo de protección separado no se muestra en la Figura 6.

El PC 10, por ejemplo, puede usar el sistema operativo Windows (RTM).

Una pluralidad de aplicaciones cliente 17 se proporcionan en el PC 10, las cuales permiten al usuario obtener servicios de proveedores de servicios 22 remotos respectivos. Se debería entender que por “remoto” no se pretende implicar que deba haber una distancia geográfica particular entre el PC 10 y los proveedores de servicios 22. No obstante, generalmente los proveedores de servicios 22 se controlarán independientemente del PC 10 – aunque esto no es esencial.

En esta realización una red de telecomunicación móvil 16 proporciona servicios de red 100, tales como SMS, MMS, servicios basados en localización, etc. La red 16 también proporciona un servicio de autenticación 102 y un servicio de pago 104. No obstante, se debería entender que la red puede ser cualquier tipo de red – la invención no está restringida a redes de telecomunicación móvil. Por ejemplo, el servicio de autenticación 102 y el servicio de pago 104 se puede proporcionar en un ordenador que está enlazado con el PC 10 por una red de área local, una red de área extensa y/o Internet.

Cuando el abonado desea usar un servicio proporcionado por un proveedor de servicios 22 remoto (paso A del diagrama de flujo en la Figura 7A), el abonado acopla su SIM 12 al PC 10 insertando su dispositivo de protección 30 que contiene el SIM 12 en la ranura de conexión adecuada del PC 12 o usando un enlace inalámbrico (paso B). El abonado entonces activa en el PC 10 la aplicación cliente 17 pertinente para obtener un servicio requerido (paso C). Por ejemplo, la aplicación cliente 17 podría ser software especial proporcionado por o bajo el control de un proveedor de servicios 22 para instalación en el PC 10 del abonado. Alternativamente, una aplicación cliente 17 pudiera ser un navegador web para visitar un sitio web adecuado del proveedor de servicios 22.

Para ilustrar la operación del sistema mostrado en la Figura 6, se dará un ejemplo para un abonado que desea comprar un CD particular de un vendedor que es un proveedor de servicios 22. Usando una interfaz gráfica de usuario presente en el PC 10 el abonado lanza un software de navegador web proporcionado en el PC 10 y, a través de Internet, accede al sitio web del proveedor de servicios 22. El software de navegador web constituye la aplicación cliente 17 y permite acceder al sitio web asociado con el proveedor de servicios 22 que distribuye los CD.

La comunicación de datos entre la aplicación cliente 17 y el proveedor de servicios 22 puede ser mediante una red fija (por ejemplo, PSTN) o mediante una red inalámbrica – tal como la red 16 u otra red de telecomunicaciones móvil.

Se puede proporcionar la facilidad para el abonado de registrarse con el sitio web. Ventajosamente, los proveedores de servicios aprobados por la red 16 pueden permitir a los abonados registrar un “seudónimo” con el proveedor de servicios. El seudónimo tiene asociados con él ciertos datos que el abonado puede desear usar cuando se obtiene un servicio del proveedor de servicios. Estos datos se almacenan por la red 16. Los datos no se almacenan permanentemente por el proveedor de servicios (aunque por supuesto el proveedor de servicios mantiene una lista de seudónimos asociados con los abonados de la red 16) – por ejemplo con referencia al identificador de SIM del abonado.

El Servicio de Autenticación puede permitir a un Proveedor de Servicios almacenar datos de Seudónimo contra un SIM – con el permiso del abonado. Los datos de Seudónimo se almacenarán centralmente y se pueden distribuir al SIM mediante el suministrador de Servicios de Autenticación.

Un ejemplo de la información que la red 16 mantiene para un abonado (abonado A) se expone a continuación.

DATOS PARA EL ABONADO A

- IDENTIFICADOR(ES) DE SIM
- MSISDN(S)
- SEUDÓNIMOS
    - PARA el Proveedor de Servicios A
        - NOMBRE
        - DIRECCIÓN
        - PREFERENCIAS
        - DETALLES DE CUENTA BANCARIA
    - PARA el Proveedor de Servicios B
        - NOMBRE
        - DIRECCIÓN
        - PREFERENCIAS

- DETALLES DE CUENTA BANCARIA

- PARA el Proveedor de Servicios C
  - NOMBRE
  - DIRECCIÓN
  - PREFERENCIAS
  - DETALLES DE CUENTA BANCARIA

Así como la red 16 que almacena los datos relativos a un SIM de abonado y su MSISDN, la red 16 también incluye una lista de seudónimos que el abonado ha establecido con diversos proveedores de servicios (proveedores de servicios A, B, C,…). La información almacenada por cualquier proveedor de servicios particular puede ser diferente y dependerá de qué información pudiera requerir útilmente el proveedor de servicios desde el abonado y de la información que el abonado está dispuesto a proporcionar al proveedor de servicios. En el ejemplo mostrado, el seudónimo pudiera incluir detalles del nombre y la dirección del abonado y cualquier preferencia que puede tener relativa al servicio particular. En el ejemplo de un abonado que desea comprar un CD de un proveedor de servicios 22, ésta pudiera incluir la preferencia del abonado de un tipo particular de música, permitiendo al proveedor de servicios personalizar su servicio, quizás para ofrecer los CD del abonado relativos al tipo de música que el abonado prefiere.

Cuando el usuario accede al sitio web, el proveedor de servicios 22 hará que el abonado, como parte del procedimiento de inicio de sesión, sea estimulado, usando el navegador web, para introducir un “seudónimo” que ese abonado puede haber registrado previamente con el proveedor de servicios 22 (paso D). Si un seudónimo se ha registrado previamente por ese abonado con el proveedor de servicios 22, el abonado introduce su seudónimo y éste se envía por la aplicación cliente 17 (paso E) al proveedor de servicios 22. El proveedor de servicios 22, por medio del enlace 106 (Figura 6) entonces transmite este seudónimo al servicio de autenticación 102 de la red 16. El servicio de autenticación 102 entonces determina si el seudónimo es válido por lo que concierne a la red 16 y si se determina que es válido, la red transmite detalles almacenados por ella que están asociados con ese seudónimo al proveedor de servicios 22 (paso F).

Si no existe ningún seudónimo, el abonado entonces introduce los detalles requeridos por el proveedor de servicios 22 (tal como su nombre y dirección) - paso G.

En este punto el proveedor de servicios 22 puede sugerir al abonado preguntar si le gustaría establecer un seudónimo para uso con ese proveedor de servicios. Si el abonado desea establecer un seudónimo con ese proveedor de servicios, el proveedor de servicios entonces solicita información pertinente del abonado, tal como su nombre, dirección, detalles de preferencia de música y similares. Algo de esta información puede ser esencial para establecer un seudónimo (tal como el nombre y dirección del abonado), mientras que otros datos pueden ser opcionales (tales como las preferencias de música de abonado). Se considera ventajoso que el abonado pueda seleccionar qué información se proporciona al proveedor de servicios para uso en su seudónimo y también ventajoso que un seudónimo sea para uso con un proveedor de servicios particular solamente. Cuando se han introducido los datos para establecer el seudónimo, esta información se pasa a través del enlace 106 al servicio de autenticación 102 de la red 16. El seudónimo se almacena por el proveedor de servicios 22 pero los datos asociados con ese seudónimo no se almacenan permanentemente por el proveedor de servicios 22 (esa información se proporciona bajo petición al proveedor de servicios 22 por el servicio de autenticación 102 de la red 16).

Es importante señalar que el proveedor de servicios 22 solamente tiene acceso a datos asociados con el seudónimo particular que el abonado usa en relación con ese proveedor de servicios. Los registros separados asociados con seudónimos para otros proveedores de servicios se almacenan separadamente por la red 16. Esto es ventajoso debido a que, por ejemplo, un abonado puede estar dispuesto a que datos médicos personales estén asociados con un seudónimo que ese abonado usa cuando se obtienen servicios de su médico pero no desearía que esta información sea puesta a disposición de otros proveedores de servicios.

El abonado busca el sitio web para identificar el CD que el abonado desea comprar. Cuando se identifica el CD requerido por el abonado, el abonado hace a la aplicación cliente 17 enviar una petición de mensaje de servicio al proveedor de servicios 22 (paso H) - por ejemplo, haciendo una pulsación de ratón en un botón “comprar CD” proporcionado por el sitio web. El mensaje incluye datos que identifican el CD requerido, datos que identifican al abonado (tales como el identificador del SIM del abonado), incluyendo un campo que indica que el abonado ha instalado en su PC un gestor de transacción 14 que puede autenticar una transacción por medio del SIM 12 del abonado.

En esta etapa en la transacción, el proveedor de servicios 22 se ha dotado con ciertos detalles del abonado, que incluyen el nombre, dirección del abonado y el CD que desean ordenar. Esta información se podría proporcionar por alguien que no es realmente el abonado. Para autenticar la transacción el proveedor de servicios 22 construye un contexto de servicio S_C (paso I). El contexto de servicio es un paquete de datos que incluye los siguientes campos:

- Un identificador del proveedor de servicios 22
- El nombre del abonado (u otro identificador tal como un identificador de SIM)
- Detalles de la transacción a ser autenticada (en este caso la compra de un CD)

También se puede proporcionar por supuesto información adicional o alternativa.

El contexto de servicio S_C se envía a través de Internet a la aplicación cliente 17. La aplicación cliente 17 pasa el contexto de servicio S_C al gestor de transacción 14 (paso J). La aplicación cliente 17 puede añadir su propio identificador al contexto de servicio S_C para permitir a la red 16 determinar desde qué aplicación cliente se deriva la transacción.

El gestor de transacción 14 analiza el contexto de servicio y establece que se requiere una petición de autenticación de la transacción por la red 16. El gestor de transacción detecta si el dispositivo de protección 30 de abonado que contiene su SIM 12 está presente (paso K). Si el dispositivo de protección 30 no está presente, se sugiere al usuario poner a disposición su dispositivo de protección. El gestor de transacción 14 también puede mostrar una descripción de la transacción a ser autenticada – y el abonado se puede dotar con la opción de aprobar o desaprobar la transacción. Suponiendo que el dispositivo de protección está presente y la transacción se aprueba por el abonado, el gestor de transacción 14 entonces envía una petición al servicio de autenticación 102 de la red 16 para un testigo de seguridad S_X (paso L). La petición enviada al servicio de autenticación 102 incluye el contexto de servicio S_C. Esos datos se pueden transmitir sobre cualquier red adecuada. Los datos se pueden transmitir a través de Internet. Los datos se pueden transmitir sobre una red de telefonía fija o sobre la infraestructura móvil o celular de la red de telecomunicaciones 16.

El dispositivo de protección 30 puede incluir medios para permitir que un PIN o datos biométricos sean introducidos como se describió anteriormente en relación a la Figura 4. Si se sugiere al abonado que introduzca su PIN o proporcione otros datos, anterior a la autenticación de una transacción, esto proporciona un nivel de seguridad añadido. El gestor de transacción 14 y/o SIM 12 puede almacenar una lista de aplicaciones cliente 17 de confianza. Estas aplicaciones se pueden dotar con una clave (u otros datos de identificación). Para las aplicaciones de confianza, el gestor de transacción y el SIM se pueden configurar para aceptar la clave en lugar de requerir al abonado introducir su PIN.

Como un rasgo de seguridad adicional, el dispositivo de protección se puede dotar con una pantalla que muestra el nombre de la aplicación u organización que solicita información del SIM 12, como se describe en relación a la realización de la Figura 3 y 4. Esto permitiría al usuario monitorizar peticiones que se hacen a su SIM 12. El dispositivo de protección 30 se puede programar para mostrar el nombre de la aplicación u organización que solicita datos del SIM 12 y entonces puede sugerir al usuario aprobar el suministro de datos para cada una o las seleccionadas de las aplicaciones/organizaciones introduciendo el PIN del usuario usando un teclado o proporcionando otros datos de identificación.

El abonado a partir de entonces será autenticado por el servicio de autenticación 102 realizando una sesión de desafío y respuesta con el SIM (enviando datos a través del gestor de transacción 14) – paso M. Por ejemplo, el servicio de autenticación 102 enviará un desafío aleatorio al gestor de transacción 14, que se transmite al SIM. El SIM responde cifrando el desafío aleatorio usando tanto un algoritmo de autenticación como una clave única Ki residente dentro del SIM y asignada a ese abonado particular. La respuesta se transmite por el gestor de transacción al servicio de autenticación 102. El servicio de autenticación 102 analiza la respuesta para determinar si es la respuesta que se esperaría del SIM del abonado. Si la respuesta es como se espera, entonces el servicio de autenticación 106 emite un testigo de seguridad S_X y envía éste al gestor de transacción (paso N). El gestor de transacción 14 en sí mismo no necesita entender los datos intercambiados durante el procedimiento de desafío y respuesta – meramente actúa como un conducto para estos datos.

Como se describe en relación con la Figura 3, para evitar o reducir, la probabilidad de que el gestor de transacción 14 sea sustituido o puenteado por una aplicación alternativa, lo que podría comprometer la seguridad de los datos en el SIM 12, el gestor de transacción 14 y el controlador de interfaz de dispositivo de protección se puede dotar con claves secretas compartidas respectivas. Cada comunicación del gestor de transacción 14 al dispositivo de protección 30 entonces se cifra usando la clave secreta compartida 40. Todas las comunicaciones desde el PC 10 al dispositivo de protección 30 se reciben por el controlador de interfaz de dispositivo de protección. El controlador de interfaz de dispositivo de protección comprende medios de procesamiento para descifrar las comunicaciones recibidas usando su clave secreta. Para mejorar la seguridad, el controlador de interfaz de dispositivo de protección evitará que todas las comunicaciones distintas de las cifradas que usan la clave secreta compartida envíen datos a o reciban datos desde el SIM 12.

Por lo tanto, el gestor de transacción 14 controla y supervisa el acceso al dispositivo de protección 30 y al SIM 12 para reducir la probabilidad de que los datos almacenados en el SIM 12 estén comprometidos por intentos no autorizados de acceso al SIM 12.

No obstante, se debería apreciar que el uso de tales claves secretas compartidas no es esencial.

Si se requiere un pago para la transacción, los detalles del pago requerido se incluyen en el contexto de servicio S_C. Esta información se extrae del contexto de seguridad S_C por el servicio de autenticación 102. El servicio de autenticación 102 entonces envía un mensaje al servicio de pago 104 a través del enlace 105 que reserva fondos en la cuenta del abonado con la red 16. Es importante señalar que no se hace o autoriza, ningún pago en esta etapa. No obstante, el servicio de pago 104 es consciente de que un pago es probable que sea requerido inminentemente y se reservan los fondos adecuados en la cuenta del usuario para esa transacción.

El testigo de seguridad es un paquete de datos que incluye el Testigo de Seguridad S_X y los siguientes campos:

- identidad del abonado – tal como un identificador de SIM
- una indicación de la identidad del proveedor de servicios 22
- una indicación del servicio que se ha autenticado – en este ejemplo el pedido de un CD particular
- una indicación de la identidad del servicio de autenticación 102
- una indicación de que se debería usar el servicio de pago (si se requiere el pago)

Otros campos se pueden proporcionar adicional o alternativamente, dependiendo de las circunstancias.

El testigo de seguridad S_X se pasa a la aplicación cliente 17 (paso O).

La aplicación cliente 17 entonces pasa el testigo de seguridad al proveedor de servicios 22 (paso P).

El testigo de seguridad S_X incluye datos específicos a un abonado particular y una transacción con un particular por el proveedor de servicios 22. Numerosas transacciones se pueden manejar por la red 16, el gestor de transacción 14 y el proveedor de servicios 22 en paralelo. Éstas serán distinguibles unas de otras en virtud de los datos específicos a una transacción particular con un particular por el proveedor de servicios 22 en el testigo de seguridad S_X.

Si el testigo de seguridad S_X se intercepta a medida que pasa entre la red 16 y el gestor de transacción 14 o entre la aplicación cliente 17 y el proveedor de servicios 22, no tendrá valor para el interceptor. El testigo de seguridad S_X es específico a una transacción particular con un particular por el proveedor de servicios 22 y la provisión de un servicio a un abonado particular.

A la recepción del testigo de seguridad S_X por el proveedor de servicios 22 se analiza su contenido y, si se establece que corresponde a un contexto de servicio S_C emitido por el proveedor de servicios 22, el proveedor de servicios 22 puede asumir que la petición de servicio (pedido de un CD) se hace legítimamente por el abonado. El Proveedor de Servicios 22 podría presentar el Testigo de Seguridad S_X al Servicio de Autenticación 102 para comprobar la validez del testigo. El servicio de autenticación 102 entonces comprueba la integridad del Testigo de Seguridad S_X y valida el contenido del Testigo de Seguridad S_X. El servicio de autenticación 102 entonces envía una respuesta al proveedor de servicios 22 que indica que el Testigo de Seguridad S_X es válido. Alternativamente, el servicio de autenticación 102 puede enviar datos al proveedor de servicios 22 que permiten al proveedor de servicios 22 en sí mismo determinar la integridad y validez del Testigo de Seguridad S_X.

El proveedor de servicios 22 entonces determina si un pago necesita ser hecho (paso Q). Si no se requiere ningún pago el CD entonces se puede despachar. No obstante, si se requiere un pago, el proveedor de servicios 22 entonces genera un contexto de pago P_C que incluye los siguientes campos:

- el testigo de seguridad S_X
- la cantidad del pago requerido

Por supuesto, se pueden requerir campos nuevos o adicionales según las circunstancias.

El contexto de pago P_C se envía a la aplicación cliente 17 (paso R). La aplicación cliente pasa el contexto de pago P_C al gestor de transacción 14 (paso S).

El gestor de transacción 17 entonces envía el contexto de pago P_C al servicio de pago 104 de la red 16 (paso T). El contexto de pago P_C se analiza por el servicio de pago 106. La presencia del testigo de seguridad S_X en el contexto de pago indica al servicio de pago que ésta es una petición genuina para el pago asociado con el abonado indicado por el testigo de seguridad S_X y el servicio de pago entonces consulta la cuenta del abonado con la red 16 para determinar que el pago se puede autorizar (lo cual pudiera depender de la calificación de crédito del abonado y/o la historia de pago con la red 16 y/o el estado de su cantidad de prepago) y, si es adecuado, autoriza el pago emitiendo un testigo de pago P_X (paso U).

El gestor de transacción 14 entonces envía un testigo de pago P_X a la aplicación cliente 17 (paso V). La aplicación cliente 17 entonces envía el testigo de pago P_X al proveedor de servicios 22 (paso W). El proveedor de servicios 22 entonces usa el testigo de pago P_X para obtener el pago desde el servicio de pago 106 de la red 16 (paso X). Para

hacer esto el proveedor de servicios 22 transmite el testigo de pago P_X al servicio de pago 104 a través del enlace 108. El servicio de pago analiza el testigo de pago P_X y reconoce que éste es un testigo de pago que se ha emitido legítimamente por el servicio de pago al gestor de transacción 14 y entonces hace el ajuste adecuado a la cuenta de abonado con la red 16.

Ventajosamente, si el usuario tiene un seudónimo asociado con el proveedor de servicios 22, el proveedor de servicios 22 puede actualizar ese seudónimo sobre la base de cualquier nueva información aprendida acerca del abonado de la transacción – por ejemplo, un cambio en el gusto musical.

Las comunicaciones entre el PC 10 y la red 16 preferiblemente están cifradas, como se describió anteriormente. También es preferible para comunicaciones entre los componentes dentro del PC 10 y dentro de la red 16 que estén cifradas – por ejemplo mediante el uso de claves compartidas.

En la disposición descrita anteriormente, el abonado se autentica solamente cuando desea comprar un CD. En una disposición alternativa, el abonado se puede autenticar cuando se registra en el sitio web. El proveedor de servicios entonces tendrá un Testigo de seguridad S_X con relación a esa sesión de abonado con el sitio web. Cuando el abonado desea hacer una compra, el Testigo de Seguridad S_X se envía al servicio de autenticación 102. El servicio de autenticación 22, dependiendo del valor de la compra, por ejemplo, o bien puede validar el Testigo de Seguridad S_X o bien requerir al proveedor de servicios 22 obtener un testigo de seguridad adicional a través de la aplicación cliente 17, el gestor de transacción 14 de la manera descrita anteriormente. Cualquier dato de seudónimo relativo a ese abonado y para ese proveedor de servicios 22 se puede proporcionar al proveedor de servicios 22 tras la autenticación del abonado.

El Testigo de Seguridad S_X puede ser válido durante un periodo de tiempo limitado. El SIM se dota ventajosamente con medios para determinar con precisión el tiempo verdadero – por ejemplo con un reloj interno resistente a sabotaje, un reloj proporcionado por el PC 10 o una indicación de tiempo desde la red 16 (que será un tiempo “de confianza”).

El abonado puede obtener servicios de red 100 desde la red 16 de una manera similar a la forma en que se obtienen los servicios desde el proveedor de servicios 22. Es decir, el proveedor de servicios de red 100 emitirá un contexto de servicio S_C cuando la petición de servicio se recibe desde la aplicación cliente 17. Un testigo de seguridad S_C se obtiene desde el servicio de autenticación 102 a través del gestor de transacción 14 que sigue la autenticación usando el SIM 12. El pago por el abonado de los servicios de red se puede realizar de la manera que se describe en relación con el proveedor de servicios 22 (mediante la emisión de un contexto de pago P_C y la generación de un testigo de pago P_X).

También es posible que se proporcione un enlace directo entre un proveedor de servicios 22 remoto y el proveedor de servicios de red 100, como se indica por un enlace 107. Esto permitirá a los servicios de red ser proporcionados a un abonado por medio de una petición de servicio remoto hecha al proveedor de servicios 22.

Para los propósitos del proveedor de servicios 22 remoto que obtiene servicios desde el proveedor de servicios de red 100, el proveedor de servicios 22 remoto se dota con un identificador único para uso con el proveedor de servicios de red 100. Cuando el proveedor de servicios 22 remoto desea obtener un servicio de red desde el proveedor de servicios de red 100 en nombre de un abonado, este identificador único se transmite al proveedor de servicios de red junto con una petición para el servicio de red. El servicio de red entonces se proporciona como se requiera y se hace un cargo por el proveedor de servicios de red 100 en la cuenta del proveedor de servicios 22 con la red 16. El proveedor de servicios 22 remoto deseará típicamente hacer un cargo al abonado para uso del servicio de red pertinente (para cubrir los costes en que ha incurrido el proveedor de servicios 22 remoto y carga cualquier servicio adicional proporcionado por el proveedor de servicios 22 remoto) y el pago para este se obtendrá emitiendo un contexto de pago P_C y obteniendo un testigo de pago P_X de la manera descrita anteriormente.

Ya se ha explicado anteriormente que el gestor de transacción 14 y la aplicación cliente 17 se podrían proporcionar en un dispositivo distinto de un PC 10 – tal como en un parquímetro o una máquina expendedora o de venta de entradas.

Un ejemplo adicional del uso de este sistema se describirá ahora en relación con el alquiler de un vehículo. Un abonado a la red 16 acopla su dispositivo de protección a un PC 10 (u otro dispositivo de procesamiento) en las oficinas de la compañía de alquiler de vehículos. El PC 10 incluye el gestor de transacción 14 y una aplicación cliente 17 para proporcionar acceso al proveedor de servicios 22 de alquiler de vehículos.

Si el abonado tiene un seudónimo para uso con el proveedor de servicios 22, el abonado proporcionará éste al proveedor de servicios 22, que entonces es capaz de acceder a datos pertinentes con relación al abonado del servicio de autenticación 102 de la red 16. Si el abonado no tiene un seudónimo asociado con el proveedor de servicios 22, el abonado proporciona detalles relevantes cuando se le sugiere por el proveedor de servicios 22, tales como el nombre del abonado, la dirección, el tipo de vehículo que desea alquilar y la duración del periodo de alquiler.

El proveedor de servicios 22 entonces crea un contexto de servicio S_C adecuado y transmite éste a la aplicación cliente 17. El gestor de transacción 14 recibe el contexto de servicio S_C y pasa éste al servicio de autenticación 102 de la red 16 para buscar un testigo de seguridad S_X siguiendo la autenticación de la transición por el procedimiento de desafío y respuesta realizado entre el servicio de autenticación 102 y el SIM 12 a través del gestor de transacción 14 de la manera descrita anteriormente. Si el SIM 12 se autentica por el servicio de autenticación 102 de la red 16, un testigo de seguridad S_X se emite al gestor de transacción 14. El testigo de seguridad S_S se pasa a la aplicación cliente 17 y desde allí el proveedor de servicios 22 para autenticar la transacción.

Por medio de un enlace 105 entre el servicio de autenticación 102 y el servicio de pago 104, se pueden reservar fondos adecuados de la cuenta del abonado con la red 16. Por ejemplo, se pueden reservar fondos para cubrir los cargos de alquiler esperados y posiblemente un depósito.

Debido a que el cargo total por alquiler del coche no se puede conocer (ya que puede depender de la distancia recorrida por el abonado, la cantidad de tiempo que el abonado pasa conduciendo el vehículo y la fecha en la que el vehículo se devuelve en realidad), un contexto de pago P_C puede no ser emitido por el proveedor de servicios 22 en esta etapa.

Hasta ahora, el abonado ha autenticado la transacción con la empresa de alquiler de vehículos. La empresa de alquiler de vehículos entonces asignará un coche. Según un rasgo opcional de esta realización, el dispositivo de protección puede permitir al usuario entrar y conducir el coche – es decir, el dispositivo de protección actuará como una llave convencional para el vehículo. Esto se puede lograr dotando al vehículo con medios para autenticar el SIM en el dispositivo de protección de abonado o alternativamente se puede realizar dotando el dispositivo de protección con una ubicación de almacenamiento para almacenar información de seguridad específica a la empresa de alquiler de vehículos. Esta información de seguridad se interroga por el vehículo y si se valida permitirá el uso del vehículo.

Si el dispositivo de protección se usa o no en realidad para obtener acceso al vehículo y permitir que vehículo sea conducido, acoplando el dispositivo de protección al vehículo se puede proporcionar acceso a la red móvil 16 de la forma convencional usando un transceptor de teléfono móvil construido dentro del vehículo. El acoplamiento del dispositivo de protección al sistema de telecomunicación del vehículo es análogo a insertar el SIM de abonado en un teléfono fijo proporcionado en el vehículo. Si no hay cobertura por la red 16 en el área en que se sitúa el vehículo, las llamadas de teléfono aún se pueden hacer donde un acuerdo de itinerancia esté presente entre la red de abonado 16 y cualquier red que es operacional en la localidad del vehículo.

El acoplamiento del dispositivo de protección a los sistemas del vehículo también puede permitir a la empresa de alquiler de vehículos calcular la cantidad de tiempo que el abonado ha pasado usando el vehículo y la empresa de alquiler de vehículos puede desear cargar al usuario de esta forma.

Cuando el vehículo se devuelve a la empresa de alquiler, se calcula un cargo adecuado por el proveedor de servicios 22 de la empresa de alquiler de vehículos (posiblemente usando información de los sistemas del vehículo como se describió anteriormente) y se genera un contexto de pago P_C adecuado y se transmite a la aplicación cliente 17 presente en el PC 10 (que podría ser un PC diferente del PC 10 usado para iniciar la transacción con la empresa de alquiler de vehículos. El gestor de transacción 14 del PC 10 entonces recibe el contexto de pago P_C y obtiene del servicio de pago 104 de la red 16 un testigo de pago P_X. Éste se pasa al proveedor de servicios 22 a través del gestor de transacción 14 y la aplicación cliente 17 y el proveedor de servicios 22 entonces es capaz de recoger el pago adecuado del servicio de pago 104 de la red 16.

En un ejemplo adicional, el gestor de transacción 14 y la aplicación cliente 17 se proporcionan en un vehículo como parte del sistema de telecomunicación a bordo del vehículo. El vehículo, por ejemplo en una posición conveniente en el salpicadero, incluye un conector para recibir un dispositivo de protección 30 de abonado (aunque, por supuesto, se podría proporcionar alternativamente una conexión inalámbrica). Cuando el abonado inserta el dispositivo de protección 30, se puede obtener un acceso a servicios remotos proporcionados por proveedores de servicios 22 usando el gestor de transacción 14 y la aplicación cliente 17 de la manera descrita en relación con las Figuras 6 y 7.

Debido a que el vehículo es, por supuesto, móvil, las comunicaciones entre la aplicación cliente 17 y el proveedor de servicios 22 remoto y las comunicaciones entre el gestor de transacción 14 y el servicio de autenticación 102 y el servicio de pago 104 (o entre la aplicación cliente 17 y el servicio de red 100) se proporcionarán por un enlace inalámbrico, tal como mediante el uso de una red radio móvil o celular usando un transceptor de teléfono ya presente en el vehículo. La red usada para realizar estas comunicaciones puede ser la misma que la red 16 que proporciona los servicios de autenticación y pago 102 y 104 o puede ser una red diferente.

Al tiempo que se inserta el dispositivo de protección 30 en el conector del vehículo, el usuario también puede ser capaz de hacer y recibir llamadas de teléfono de la manera usual como si el usuario hubiera insertado su tarjeta SIM en un sistema de teléfono móvil fijo del vehículo. No obstante, debido a que el gestor de transacción 14 y la aplicación cliente 17 están presentes, el abonado también es capaz de obtener otros servicios de proveedores de servicios 22 remotos. Por ejemplo, el abonado puede desear descargar música en forma de ficheros MP3 al sistema de audio del coche u obtener información de navegación o tráfico.

El procedimiento de autenticación y pago descrito anteriormente en relación a las Figuras 6 y 7 se puede modificar desde el paso N en adelante. Cuando el servicio de autenticación 102 ha recibido el contexto de servicio Sc y ha autenticado al abonado, se hace entonces una petición al servicio de pago 104 a través del enlace 105 para reservar los fondos adecuados. Esta petición incluye el testigo de seguridad Sx – que permite al servicio de pago 104 validar la petición. El servicio de pago 104 entonces emite un testigo de pago P_x. El gestor de transacción 14 entonces pasa el testigo de pago P_x con el testigo de seguridad Sx a la aplicación cliente 17. La aplicación cliente 17 envía el testigo de pago P_x con el testigo de seguridad Sx al proveedor de servicios 22. El proveedor de servicios 22 entonces confirma la validez del testigo de pago P_x enviando éste al servicio de pago 104 a través del enlace 108 y confirma la validez del testigo de seguridad Sx enviando éste al servicio de autenticación 102 a través del enlace 106.

Como alternativa a obtener seudónimos de abonado de la manera descrita anteriormente, el Proveedor de Servicios 22 puede presentar el Testigo de Seguridad S_x al Servicio de Autenticación 102 en conjunto con una petición de cualquier seudónimo asociado con el SIM 12 y el Proveedor de Servicios 22. El Servicio de Autenticación 102 valida el testigo y devuelve el Seudónimo adecuado (o datos relacionados) al Proveedor de Servicios 22.

Para mejorar la seguridad del sistema el Proveedor de Servicios 22 se podría dotar con un Certificado (clave compartida) que se usa para codificar todas las peticiones desde el Proveedor de Servicios 22 al servicio de autenticación 102. De esta manera el Servicio de Autenticación 22 entonces puede tener un grado de confianza en quién está haciendo las peticiones para el Seudónimo o los datos de SIM asociados.

El proveedor de servicios, que está seguro que está autenticado el abonado o pago, entonces es capaz de despachar el CD al abonado.

A fin de obtener el pago el proveedor de servicios 22 puede proceder de una o dos formas.

En el primer procedimiento el proveedor de servicios 22 emite una petición de liquidación de pago enviando un paquete de datos que incluye el testigo de pago P_x (y el Testigo de Seguridad S_X) a la aplicación cliente 17. La aplicación cliente 17 pasa la petición de liquidación de pago al gestor de transacción 14, que a su vez pasa la petición de liquidación de pago (con el testigo de pago P_x) al servicio de pago 104. En este punto el servicio de pago puede dar instrucciones al servicio de autenticación 102, a través del enlace 105, para autenticar al abonado mediante datos de desafío y respuesta intercambiados con el SIM 12 (a través del gestor de transacción 14), aunque éste es un paso opcional. En cualquier caso, el servicio de pago 104 comprueba el testigo de pago P_x y el testigo de seguridad S_X (contenido en el mismo paquete) y entonces limpiará los fondos en la cuenta del abonado con la red 16. El servicio de pago 104 entonces envía un testigo de pago P_{x1} modificado al gestor de transacción 14. El gestor de transacción 14 pasa el testigo de pago P_{x1} modificado al proveedor de servicios 22 a través de la aplicación cliente 17. El proveedor de servicios 22 entonces es capaz de validar el testigo de pago mediante un enlace directo 108 con un servicio de pago 104.

Como alternativa al procedimiento descrito anteriormente, el proveedor de servicios 22 puede solicitar al servicio de pago 104 la liquidación de pago a través del enlace 108 enviando el testigo de pago P_x adecuado. El servicio de pago 104 entonces valida el testigo de pago y limpia los fondos. El servicio de pago 104 responde al proveedor de servicios 22 confirmando que se ha limpiado el pago.

Las Figuras 8 a 11 muestran ejemplos adicionales de las configuraciones del dispositivo de protección que se podrían usar en conjunto con los sistemas descritos en relación a la Figura 1 o 6 como alternativa a la primera configuración mostrada en la Figura 4 y la segunda configuración mostrada en la Figura 5.

Las Figuras 8A a 8D muestran una tercera configuración de un dispositivo de protección indicado de manera general en 250. El dispositivo de protección 250 no incluye un visualizador o pulsadores. El dispositivo de protección 50 es de sección transversal generalmente elíptica e incluye una apertura generalmente rectangular 252 formada en el extremo superior del mismo que permite a un conector eléctrico 254 de sección transversal generalmente rectangular emerger desde el mismo. La apertura 252 se cierra por un elemento de cierre 256 que tiene forma generalmente de C en sección transversal, extendiéndose desde la parte superior del dispositivo de protección 250 a lo largo de cada cara lateral 258 y pivotada alrededor de un punto de pivote montado centralmente 260. La conexión entre el elemento de cierre 256 y las paredes laterales 258 del dispositivo de protección 250 al punto de pivote 60 permite que el elemento de cierre 256 sea rotado alrededor del punto de pivote 260 como se muestra por la flecha 262.

La Figura 8C es una sección transversal tomada a lo largo de la línea X-X de la Figura 8B y muestra esquemáticamente el mecanismo por el cual el conector eléctrico 254 se puede mover entre una primera posición, mostrada en las Figuras 8A y 8B, donde el conector 54 está contenido enteramente dentro de la carcasa del dispositivo de protección 250 y la segunda posición, mostrada en las Figuras 8C y 8D, donde el conector eléctrico 254 sobresale de la carcasa del dispositivo de protección 250. El mecanismo para proporcionar este movimiento del conector eléctrico 254 comprende una cremallera 264 que se acopla al conector 254 y un piñón de cooperación 266, montado en un punto de pivote 260, los dientes del cual se acoplan a la cremallera 264. El piñón 266 se fija con respecto al elemento de cierre 256. La rotación del elemento de cierre 256 causa la rotación del piñón 266, que

causa un desplazamiento lineal de la cremallera 264 como se muestra por la flecha 268. Por supuesto, un mecanismo para soportar de manera deslizable el conector eléctrico 254 y la cremallera 264 se proporciona de una manera que se entenderá por los expertos en la técnica y no se ilustra o describe aún más aquí.

Las Figuras 9A a 9D muestran una cuarta configuración de un dispositivo de protección. Como en la tercera configuración del dispositivo de protección descrita en relación con las Figuras 8A a 8D, el conector eléctrico 254 es móvil entre una primera posición, mostrada en las Figuras 9A y 9B, donde está contenido completamente dentro de la carcasa del dispositivo de protección 270 y una segunda posición, mostrada en las Figuras 9C y 9D, donde el conector 254 se muestra extendiéndose desde la carcasa del dispositivo de protección 270. No obstante, en la tercera configuración, el movimiento lineal del conector eléctrico 254 en la dirección de la flecha 268 se proporciona rotando un mando 272 con respecto a la carcasa del dispositivo de protección 270 como se muestra por la flecha 274. La rotación del mando 272 en una primera dirección hace al conector 254 emerger desde la carcasa del dispositivo de protección 270 y la rotación en la dirección opuesta hace al conector 254 ser retraído dentro de la carcasa del dispositivo de protección 270. Se puede proporcionar cualquier mecanismo adecuado para convertir el movimiento rotativo del mando 272 en movimiento lineal del conector 254. Por ejemplo, se puede emplear un mecanismo descrito en la Patente de EE.UU. Nº 5813421 (que se incorpora en la presente memoria por referencia) para un mecanismo giratorio de barra de labios. Otros mecanismos adecuados se conocerán por los expertos en la técnica pertinente.

El dispositivo de protección 270 incluye un visualizador 248 para sugerir al usuario introducir su número de PIN y/o para mostrar el número PIN a medida que se introduce. El dispositivo de protección 270, en lugar de tener una serie de pulsadores (tales como un teclado numérico) comprende un mando de entrada de datos 276 que se monta al dispositivo de protección para rotación como se muestra por la flecha 278 y también para movimiento lineal con respecto al dispositivo de protección como se muestra por la flecha 280. Cada dígito del número PIN se introduce por el usuario agarrando el mando 276 y tirando de él en una dirección lejos de la carcasa del dispositivo de protección 270 (en la dirección de la flecha 280). Una indicación, tal como un cursor parpadeante aparece entonces en el visualizador 248 indicando que se espera el primer dígito del número PIN. El número se introduce por rotación del mando 276 (flecha 278), el número visualizado que aumenta en valor con rotación adicional del mando 276. Cuando el número requerido aparece en el visualizador 248 el usuario confirma que éste es el número que desea introducir empujando el mando 276 en la dirección opuesta a la flecha 280. Para introducir el siguiente dígito del número PIN el mando 276 se levanta de nuevo (flecha 280) y el número correcto se selecciona por rotación del mando. El número requerido se introduce devolviendo el mando 276 a su posición original moviéndolo en la dirección opuesta a la flecha 280. Este procedimiento se repite hasta que todos los dígitos del número PIN se han introducido. Cada dígito del número PIN se mostrará en el visualizador 248 a medida que se introduce.

En la realización de la Figura 9A a 9D del dispositivo de protección 270, una célula piezoeléctrica 282 se asocia con el mando 280. La célula piezoeléctrica 282 permite que sea generada potencia por el movimiento del mando 276. Esta potencia se puede o bien almacenar en un condensador integral o bien se puede almacenar en una célula opcional 284 que está acoplada eléctricamente a la célula piezoeléctrica 282. Tal disposición obvia el requisito del dispositivo de protección 270 de tener su propia fuente de potencia sustituible, mientras que permite al dispositivo de protección ser operado cuando no está conectado al PC 10. La carga generada por la célula piezoeléctrica es transitoria y después de un periodo de tiempo (por ejemplo, 5 minutos), la carga se disipa y cualquier número PIN introducido por medio del mando 276 se pierde de la memoria del dispositivo de protección 270 y no se puede recuperar más tarde incluso cuando se suministra potencia. Esto proporciona un rasgo de seguridad adicional al dispositivo de protección 270. Por supuesto, si el dispositivo de protección 270 se conecta al PC 10 mientras que la carga aún está presente (dentro de los 5 minutos de introducir el PIN en el ejemplo dado anteriormente), el PIN se puede verificar y el dispositivo de protección entonces puede obtener potencia del PC 10 a través del conector 254 que permite que las operaciones de autenticación descritas anteriormente sean realizadas a pesar de la naturaleza transitoria de la potencia desde la célula piezoeléctrica 282.

Las Figuras 10A a 10D muestran una quinta configuración del dispositivo de protección 290. En esta realización el dispositivo de protección 290 comprende una parte de cuerpo principal 292 a la cual el conector eléctrico 254 se une en una posición fija y una tapa de protección desmontable 294 que, cuando está en posición, cubre el cuerpo principal 292 y el conector 254 para proteger esos componentes y dotar al dispositivo de protección 290 con una apariencia externa atractiva.

En el extremo superior del cuerpo principal 292 un mando anular 296 está montado al cuerpo 292 para rotación con respecto al cuerpo 292, como se muestra por la flecha 298. El mando 296 incluye una serie de marcas 300 visibles al usuario del dispositivo de protección 290 – por ejemplo, cada marca 300 que indica un dígito diferente desde 0 a 9. Una marca 302 se proporciona en la parte superior de la carcasa 292. En esta realización, el primer dígito del número PIN del usuario se introduce rotando el mando 96 hasta que el dígito correcto del número PIN (indicado en 300) se alinea con la marca 302. Cuando el dígito pertinente y la marca 302 están alineados, el usuario detiene la rotación de mando 296. Cuando se detiene el movimiento del mando 296, la posición del mando 296 se registra por el dispositivo de protección 290 de manera que se puede detectar el dígito del número PIN. El siguiente dígito del número PIN se introduce rotando el mando 296 en una dirección en sentido antihorario (opuesta a la flecha 298) hasta que el dígito pertinente del número PIN se alinea con la marca 302'. De nuevo, cuando se detiene la rotación del mando, la posición del mando se registra de manera que el número PIN se puede registrar por el dispositivo de

protección 290. El siguiente dígito del número PIN se introduce por rotación en sentido horario del mando 296 y así sucesivamente, hasta que todos los dígitos del número PIN se han introducido. La manera de la entrada de datos que usa el mando 296 y la marca 302 es similar a la usada para introducir la combinación de una caja fuerte.

El dispositivo de protección 290 además incluye una cámara digital opcional 304 montada en el eje de rotación del mando 296 (pero fija con respecto al cuerpo principal 292). El dispositivo de protección 290 incluye medios de procesamiento y memoria para almacenar una o más imágenes capturadas por la cámara 304 y permite que estas imágenes sean transferidas al PC 10 usando el conector 254.

Las Figuras 11A a 11C muestran una sexta configuración de un dispositivo de protección 310. El dispositivo de protección 310 comprende una carcasa 312 que tiene una abertura 314 en un lado de la misma. Contenida dentro de la carcasa 312 está una parte de acoplamiento 316 a la cual se fija el conector eléctrico 254. La parte de acoplamiento 316 está conectada a la carcasa 312 de tal manera que la parte de acoplamiento 316 es rotativa alrededor de un eje indicado por la línea de puntos 318.

Conectado al conector de bucle 244 está un anillo 320, que proporciona un medio conveniente por medio de una parte deslizable 322, que se monta para deslizarse con respecto a la carcasa 312, se puede mover con respecto a la carcasa 312 en la dirección de la flecha 324. Por medio de una cremallera y un piñón o cualquier otro mecanismo adecuado (no mostrado) el movimiento de la parte deslizante 322 con respecto a la carcasa 312 en la dirección de la flecha 324 se traduce en un movimiento de rotación de la parte de acoplamiento 316 alrededor del eje 318. Las diferentes posiciones a través de las que se mueve la parte de acoplamiento 316 a medida que la parte deslizante 322 se mueve con respecto a la carcasa 312 se muestran por las líneas discontinuas en la Figura 11C.

Cuando la parte deslizante 322 alcanza su recorrido máximo en la dirección de la flecha 324, la parte de acoplamiento 316 se rota 180º con respecto a la carcasa 312. La parte de acoplamiento 316 se devuelve a la posición mostrada en las Figuras 11A y 11B deslizando la parte deslizante 322 en la dirección opuesta a la flecha 324. Cuando la parte de acoplamiento 316 está en la posición mostrada en las Figuras 11A y 11B, el conector 254 está protegido por la parte deslizante 322.

Las realizaciones mostradas en las Figuras 8, 9, 10 y 11 proporcionan diversos medios por los cuales el conector eléctrico 254 se pueden ocultar y proteger cuando no se requiere.

En la realización de la Figura 9 la fuente de potencia del dispositivo de protección es una célula piezoeléctrica 282.

Una fuente de potencia similar se puede proporcionar en los dispositivos de protección ilustrados en las Figuras 8, 10 y 11, con potencia que se genera por movimiento del elemento de cierre 256 del dispositivo de protección 250 de la Figura 8, el movimiento del mando 296 del dispositivo de protección 290 de la Figura 107 o el movimiento de la parte deslizante 322 de la Figura 11. Alternativa o adicionalmente, estos dispositivos de protección pueden incluir una batería sustituible o una batería recargable que se recarga cuando el dispositivo de protección 250, 280, 290, 310 se conecta al PC 10.

Mientras que los dispositivos de protección descritos incluyen un conector eléctrico 254 que se muestra como un conector USB, se debería apreciar que se puede proporcionar cualquier otro tipo adecuado de conector eléctrico. Por ejemplo, el conector 254 puede ser un dispositivo SmartMedia (marca registrada). Alternativamente, los datos y/o la potencia se pueden transmitir entre el dispositivo de protección y el PC 10 mediante tecnología “de campo cercano”, por ejemplo, según el protocolo de Interfaz y Protocolo de Comunicación de Campo Cercano (NFCIP-1). Si se emplea tecnología de campo cercano, la provisión de un conector eléctrico móvil 254 no será necesaria.

Los dispositivos de protección de las Figuras 8 a 11 pueden incluir o no el controlador de interfaz de dispositivo de protección 36 descrito en relación con las Figuras 3 y 4.

Los dispositivos de protección de las Figuras 9 y 10 pueden permitir que el PIN sea pasado al PC 10 para validación o tal validación se puede realizar dentro del dispositivo de protección para mejorar la seguridad.

Por supuesto, los dispositivos de protección de las Figuras 8 y 11 se pueden dotar con un medio de entrada de PIN si se requiere.

REIVINDICACIONES

1. Un método para llevar a cabo un proceso de autenticación para autenticar una transacción posterior por cualquiera de una pluralidad de usuarios con cualquiera de una pluralidad de proveedores de productos o servicios (22) por medio de un aparato de proceso de datos (10), en el que:

durante el proceso de autenticación el aparato de proceso de datos (10) ha asociado operativamente con él uno seleccionado de una pluralidad de medios de almacenamiento de autenticación (12) respectivos a los usuarios, cada medio de almacenamiento de autenticación (12) que almacena información de autenticación predeterminada y que es registrable con un sistema de telecomunicaciones común (16) para el cual los usuarios tienen terminales de telecomunicaciones respectivos,

el método que incluye el paso de llevar a cabo el proceso de autenticación a través de un enlace de comunicaciones con el sistema de telecomunicaciones común (16), el proceso de autenticación que se lleva a cabo por un sistema de autenticación (102) incorporado en el sistema de telecomunicaciones (16) y que implica el uso de la información de autenticación predeterminada almacenada por el seleccionado de los medios de almacenamiento de autenticación (12), la información de autenticación predeterminada almacenada por cada medio de almacenamiento de autenticación (12) que corresponde a información que se usa para autenticar ese terminal de telecomunicaciones de usuario en relación con el sistema de telecomunicaciones (16) pero el proceso de autenticación para autenticar la transacción por ese usuario con el aparato de proceso de datos (10) que no requiere uso de ese terminal de telecomunicaciones de usuario que no requiere al terminal de telecomunicaciones ser autenticado realmente por esa información en relación con el sistema de telecomunicaciones (16),

en donde el proveedor de productos o servicios (22) genera en respuesta a una petición de un usuario, hecha usando el aparato de proceso de datos (10), un paquete de datos de petición de transacción que incluye datos indicativos de la identidad del usuario, la identidad del proveedor de productos o servicios (22) y la transacción particular a ser autenticada; y

en donde a fin de autenticar la transacción el método incluye:

transmitir el paquete de datos de petición de transacción entre el aparato de proceso de datos (10) y el sistema (16) a través de un gestor de transacción (14) implementado por el aparato de proceso de datos (10),

analizar en el sistema de autenticación (102) el paquete de datos de petición de transacción y extraer del mismo la identidad del usuario;

transmitir desde el sistema de autenticación (102) una señal de petición de autenticación a los medios de almacenamiento de autenticación de usuario (12) a través del aparato de proceso de datos (10);

recibir a través del aparato de proceso de datos (10) una respuesta de los medios de almacenamiento de autenticación de usuario en el sistema de autenticación (102);

analizar dicha respuesta en el sistema de autenticación (102) para determinar si dicha respuesta corresponde a una respuesta esperada con referencia al conocimiento de dicha información de autenticación predeterminada para ese usuario;

generar un testigo de autenticación y proporcionar éste al proveedor de productos o servicios (22) a través del aparato de proceso de datos (10);

establecer si el testigo de autenticación corresponde al paquete de datos de petición de autenticación, cuya correspondencia indica al proveedor de productos o servicios que el usuario está autenticado por el sistema de autenticación (102) para la transacción particular.

2. Un método según la reivindicación 1, en donde cada usuario se autentica en el sistema por medio del uso de una tarjeta inteligente o módulo de identidad de abonado (por ejemplo, SIM) y en el que los medios de almacenamiento de autenticación (12) respectivos a ese usuario corresponden a o simulan la tarjeta inteligente para ese usuario.

3. Un método según la reivindicación 2, en donde la tarjeta inteligente o SIM autentica la transacción cuando la tarjeta inteligente o SIM es operable en un terminal utilizable en un sistema de telecomunicaciones móvil y/o celular.

4. Un método según la reivindicación 3, en donde la tarjeta inteligente o SIM es operable para autenticar el terminal en el sistema de telecomunicaciones móvil y/o celular.

5. Un método según cualquiera de las reivindicaciones precedentes, en el cual los medios de almacenamiento de autenticación (12) se incorporan en un portador de datos para datos o software para uso por el aparato de proceso de datos (10).

6. Un método según cualquier reivindicación precedente, en el cual el proceso de autenticación implica el envío de un mensaje y la generación de una respuesta dependiente del mensaje y la información predeterminada.

7. Un método según cualquier reivindicación precedente, que incluye acoplar operativamente los medios de almacenamiento de autenticación (12) a un portador (32).

8. Un método según la reivindicación 7, en donde el portador (32) se acopla operativamente al aparato de proceso de datos (10) mediante un enlace inalámbrico.

9. Un método según la reivindicación 7 u 8, en donde los medios de almacenamiento de autenticación (12) se acoplan desmontablemente al portador (32).

10. Un método según la reivindicación 7, 8 o 9, que comprende usar dicho portador (32) para obtener datos de seguridad independientemente del aparato de proceso de datos (10) y analizar los datos de seguridad para determinar si permitir acceso a la información predeterminada.

11. Un método según la reivindicación 10, en donde los datos de seguridad se obtienen por medios de entrada de datos alfanuméricos.

12. Un método según la reivindicación 10 u 11, en donde los datos de seguridad comprenden un Número de Identificación Personal (PIN) y el paso de análisis compara el PIN obtenido por los medios de entrada de datos de seguridad con un PIN almacenado en los medios de almacenamiento de autenticación y permite solamente acceso a la información predeterminada cuando los PIN respectivos coinciden.

13. Un método según cualquiera de las reivindicaciones 7 a 12, en donde la comunicación con el aparato de proceso de datos (10) se controla por un módulo de proceso de datos (36).

14. Un método según la reivindicación 13, en donde el módulo de proceso de datos (36) del portador (32) descifra datos cifrados recibidos desde un módulo de proceso de datos (38) correspondiente del aparato de proceso de datos (10).

15. Un método según la reivindicación 13 o 14, en donde el módulo de proceso de datos (36) del portador (32) cifra datos transmitidos a un módulo de proceso de datos (38) correspondiente del aparato de proceso de datos (10).

16. Un método según la reivindicación 14 o 15, en donde los módulos de proceso de datos (36, 38) respectivos comprenden una clave (40, 42) para permitir cifrado y/o descifrado de datos.

17. Un método según la reivindicación 16, en donde la clave (40, 42) comprende una clave de secreto compartido para cada uno de los módulos de proceso de datos (36, 38) respectivos.

18. Un método según cualquiera de las reivindicaciones 7 a 17, en donde la portadora (32) se acopla operativamente a un pluralidad de medios de almacenamiento de autenticación (12) para permitir respectivamente el proceso de autenticación citado y uno o más de otros procesos de autenticación.

19. Un método según cualquier reivindicación precedente, que incluye encaminar comunicaciones entre los medios de almacenamiento de autenticación (12) y el sistema (16) a través del gestor de transacción (14).

20. Un método según cualquier reivindicación precedente, en donde el gestor de transacción (14) se implementa por el aparato de proceso de datos.

21. Un método según cualquier reivindicación precedente, en donde el gestor de transacción (14) detecta el acoplamiento operativo de los medios de almacenamiento de autenticación (12).

22. Un método según la reivindicación 19, 20 o 21, en donde el gestor de transacción (14) transmite datos relativos a una transacción autenticada a la entidad (22) a la que se refiere esa transacción.

23. Un aparato de proceso de datos (10) en combinación con uno seleccionado de una pluralidad de medios de almacenamiento de autenticación (12) con respecto a los usuarios y cada uno para almacenar información de autenticación predeterminada relativa a llevar a cabo un proceso de autenticación para autenticar una transacción por el usuario con cualquiera de una pluralidad de proveedores de productos o servicios (22) por medio del aparato de proceso de datos (10), los medios de almacenamiento de autenticación (12) todos que son registrables con un sistema de telecomunicaciones común (16) y para el cual los usuarios tienen un terminal respectivo, los medios de almacenamiento de autenticación (12) cuando se asocian operativamente con el aparato de proceso de datos (10) que es operativo para llevar a cabo el proceso de autenticación a través de un enlace de comunicaciones con ese sistema (16), el proceso de autenticación que se lleva a cabo mediante medios de autenticación (102) incorporados en el sistema (16) y que implican el uso de la información de autenticación predeterminada almacenada por el seleccionado de los medios de almacenamiento de autenticación (12), la información de autenticación predeterminada almacenada por cada medio de almacenamiento de autenticación (12) que corresponde a información que se usa para autenticar que el terminal de telecomunicaciones de usuario en relación con el sistema

de telecomunicaciones (16) excepto el proceso de autenticación para autenticar la transacción por ese usuario con el aparato de proceso de datos (10) que no requiere uso de ese terminal de telecomunicaciones de usuario no requiriendo que el terminal de telecomunicaciones sea autenticado realmente por esa información en relación con el sistema de telecomunicaciones (16), en donde el proveedor de productos o servicios (22) es operable para generar en respuesta a una petición de un usuario, hecha usando el aparato de proceso de datos (10), un paquete de datos de petición de transacción que incluye datos indicativos de la identidad del usuario, la identidad del proveedor de productos o servicios (22) y la transacción particular a ser autenticada y, en donde, a fin de autenticar la transacción:

el paquete de datos de petición de transacción se transmite entre el aparato de proceso de datos (10) y el sistema de telecomunicaciones (16) a través de un gestor de transacción (14) implementado por el aparato de proceso de datos (10),

el sistema de autenticación (102) analiza el paquete de datos de petición de transacción y extrae del mismo la identidad del usuario;

el sistema de autenticación (102) transmite una señal de petición de autenticación a los medios de almacenamiento de autenticación de usuario (12) a través del aparato de proceso de datos (10);

el sistema de autenticación (102) recibe una respuesta de los medios de almacenamiento de autenticación de usuario a través del aparato de proceso de datos (10);

el sistema de autenticación (102) analiza la respuesta para determinar si dicha respuesta corresponde a una respuesta esperada con referencia al conocimiento de dicha información de autenticación predeterminada para ese usuario y

un testigo de autenticación se genera y proporciona al proveedor de productos o servicios (22) a través del aparato de proceso de datos (10), el proveedor de productos o servicios (22) que es operable para establecer si el testigo de autenticación corresponde al paquete de datos de petición de transacción, cuya correspondencia indica al proveedor de productos o servicios que el usuario está autenticado por el sistema de autenticación (102) para la transacción particular.

24. Un aparato según la reivindicación 22, en el que cada usuario se autentica en el sistema por medio del uso de una tarjeta inteligente o módulo de identidad de abonado (por ejemplo, SIM) y en el que los medios de almacenamiento de autenticación (12) respectivos a ese usuario corresponden a o simulan la tarjeta inteligente para ese usuario.

25. Un aparato según la reivindicación 24, en donde la tarjeta inteligente o SIM es operable en un terminal utilizable en un sistema de telecomunicaciones móvil y/o celular para autenticar la transacción.

26. Un aparato según la reivindicación 25, en donde la tarjeta inteligente o SIM es operable para autenticar el terminal en el sistema de telecomunicaciones móvil y/o celular.

27. Un aparato según cualquiera de las reivindicaciones 23 a 26, en el que el proceso de autenticación implica el envío de un mensaje y la generación de una respuesta dependiente del mensaje y de la información predeterminada.

28. Un aparato según cualquiera de las reivindicaciones 23 a 27, en donde se proporciona un portador (32) para los medios de almacenamiento de autenticación (12) y los medios de almacenamiento de autenticación son acoplables operativamente al portador (32).

29. Un aparato según la reivindicación 28, que incluye medios para permitir una comunicación inalámbrica entre el portador (32) y el aparato de proceso de datos (10).

30. Un aparato según la reivindicación 28 o 29, que incluye medios para acoplar desmontablemente el portador (32) a los medios de almacenamiento de autenticación (12).

31. Un aparato según cualquiera de las reivindicaciones 28 a 30, en donde el portador (32) incluye medios (46) para obtener datos de seguridad independientemente del aparato de proceso de datos (10) y medios para analizar los datos de seguridad para determinar si permitir acceso a la información predeterminada.

32. Un aparato según la reivindicación 31, en donde el portador (32) comprende medios de entrada de datos alfanuméricos (46) para permitir que los datos de seguridad sean obtenidos.

33. Un aparato según la reivindicación 31, en donde los datos de seguridad comprenden un número de identificación personal (PIN) y los medios de análisis son operables para comparar el PIN obtenido por los medios de entrada de datos de seguridad con un PIN almacenado en los medios de almacenamiento de autenticación (12) y para permitir solamente acceso a la información predeterminada cuando los PIN respectivos coinciden.

34. Un aparato según cualquiera de las reivindicaciones 28 a 33, en donde el portador (32) comprende un módulo de proceso de datos (36) para controlar la comunicación con el aparato de proceso de datos (10).

35. Un aparato según la reivindicación 34, en donde el módulo de proceso de datos (36) del portador (32) incluye medios para descifrar datos cifrados recibidos desde un módulo de proceso de datos (38) correspondiente del aparato de proceso de datos (10).

36. Un aparato según la reivindicación 34 o 35, en donde el módulo de proceso de datos (36) del portador (32) cifra datos transmitidos a un módulo de proceso de datos (38) correspondiente del aparato de proceso de datos (70).

37. Un aparato según la reivindicación 35 o 36, en donde los módulos de proceso de datos respectivos comprenden una clave (40, 42) para permitir cifrado y/o descifrado de datos.

38. Un aparato según la reivindicación 37, en donde la clave (40, 42) comprende una clave de secreto compartido para cada uno de los módulos de proceso de datos (36, 38) respectivos.

39. Un aparato según cualquiera de las reivindicaciones 28 a 38, en donde el portador (32) incluye medios para acoplar operativamente la portadora a un pluralidad de medios de almacenamiento de autenticación (12) para permitir respectivamente al proceso de autenticación citado y a uno o más de otros procesos de autenticación ser realizados.

40. Un aparato según cualquiera de las reivindicaciones 23 a 39, en donde las comunicaciones de datos entre los medios de almacenamiento de autenticación (12) y el sistema (16) se encaminan a través del gestor de transacción (14).

41. Un aparato según cualquiera de las reivindicaciones 23 a 40, en donde el gestor de transacción (14) se implementa por el aparato de proceso de datos (10).

42. Un aparato según cualquiera de las reivindicaciones 23 a 41, en donde el gestor de transacción (14) es operable para detectar el acoplamiento operativo de los medios de almacenamiento de autenticación (12) a los medios de proceso de datos (10).

43. Un aparato según cualquiera de las reivindicaciones 23 a 42, en donde el gestor de transacción (14) es operable para transmitir datos relativos a una transacción autenticada a la entidad (22) a la que se refiere esa transacción.

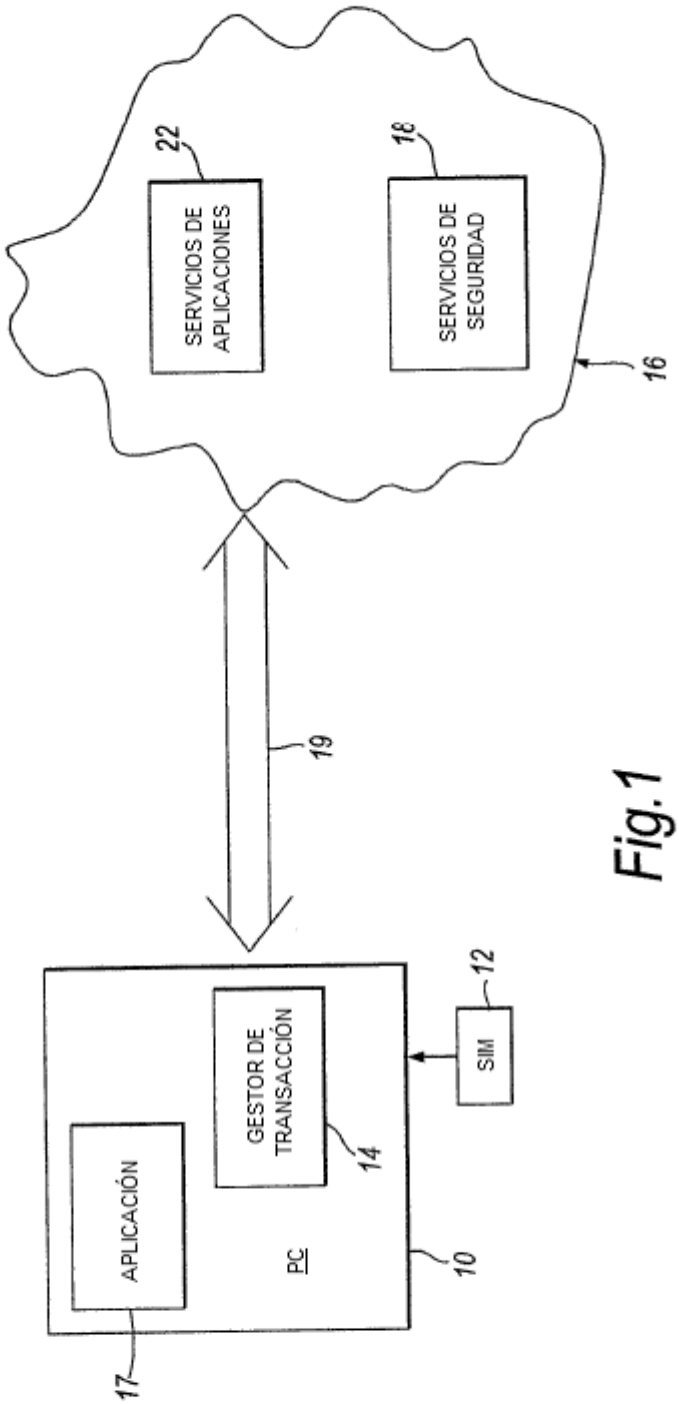
22
SERVICIOS DE APLICACIONES
18
SERVICIOS DE SEGURIDAD
16
19
12
SIM
GESTOR DE TRANSACCIÓN
14
APLICACIÓN
PC
10
17

Fig.1

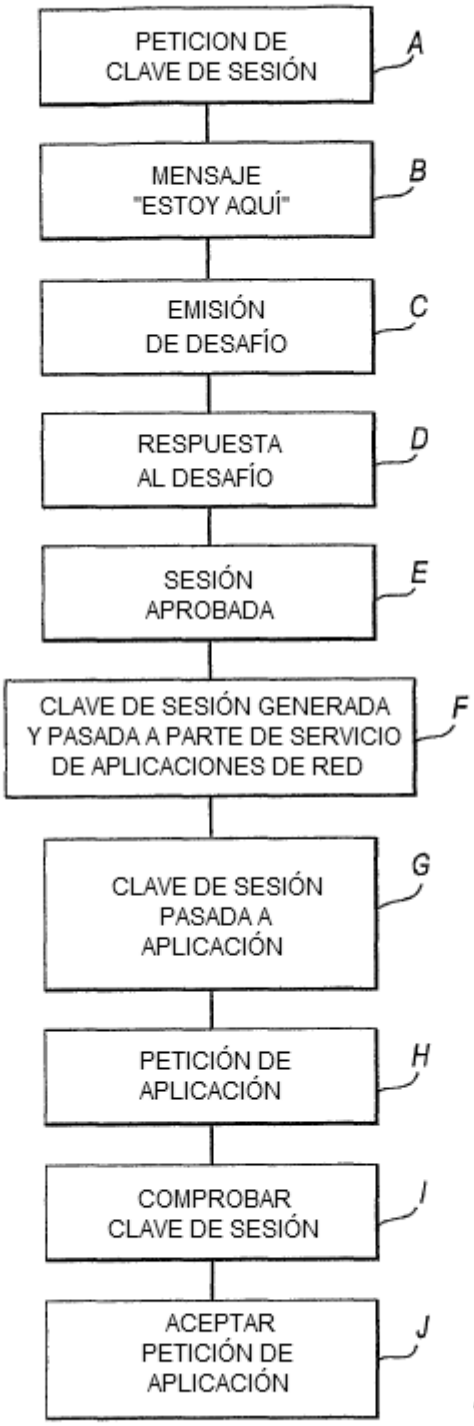
PETICION DE CLAVE DE SESIÓN
A
MENSAJE "ESTOY AQUÍ"
B
EMISIÓN DE DESAFÍO
C
RESPUESTA AL DESAFÍO
D
SESIÓN APROBADA
E
CLAVE DE SESIÓN GENERADA Y PASADA A PARTE DE SERVICIO DE APLICACIONES DE RED
F
CLAVE DE SESIÓN PASADA A APLICACIÓN
G
PETICIÓN DE APLICACIÓN
H
COMPROBAR CLAVE DE SESIÓN
I
ACEPTAR PETICIÓN DE APLICACIÓN
J

Fig.2

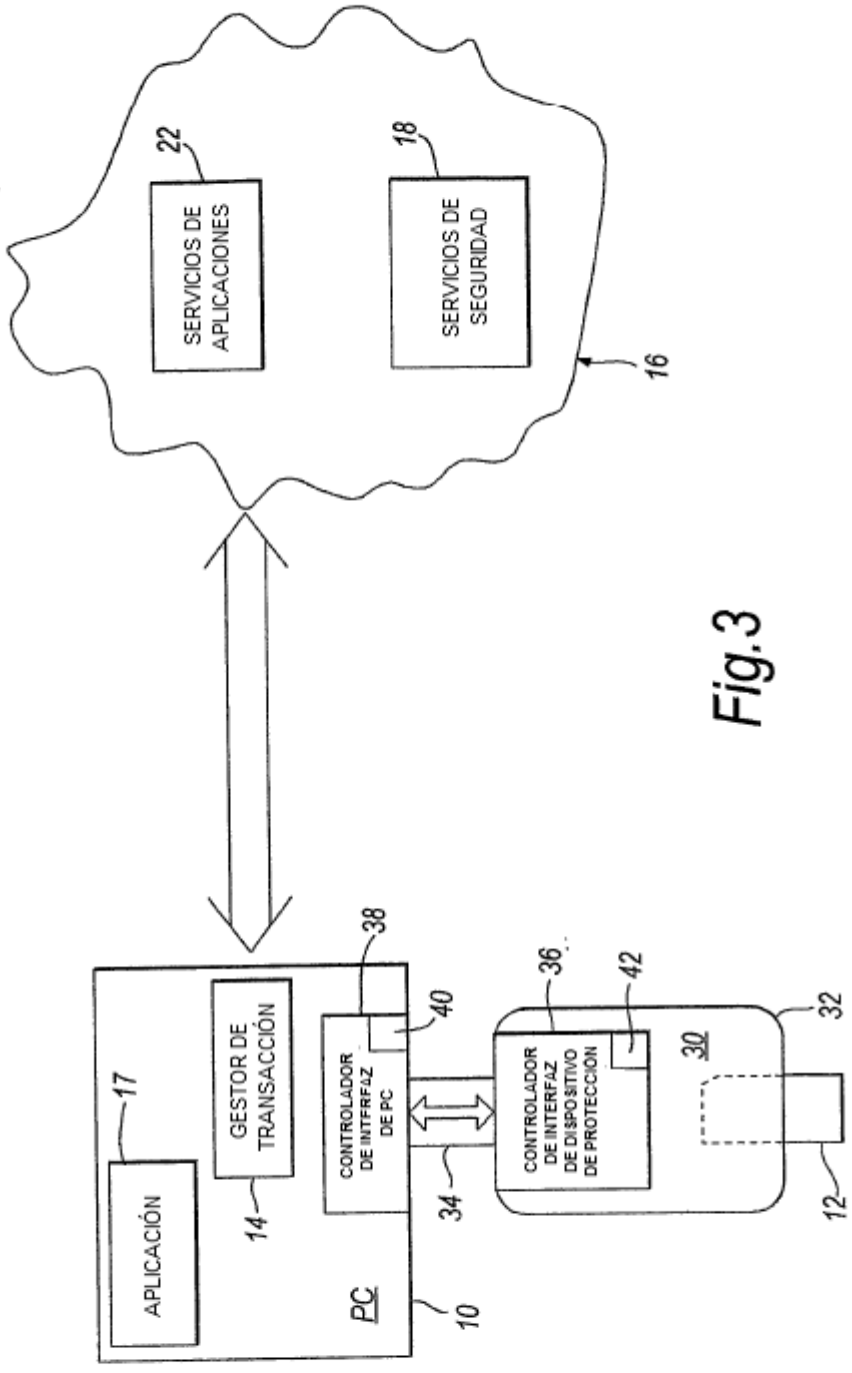
SERVICIOS DE APLICACIONES
22
SERVICIOS DE SEGURIDAD
18
16
APLICACIÓN
17
GESTOR DE TRANSACCIÓN
14
CONTROLADOR DE INTFRFAZ DE PC
38
40
34
CONTROLADOR DE INTERFAZ DE DISPOSITIVO DE PROTECCIÓN
36
42
30
32
12
PC
10

Fig.3

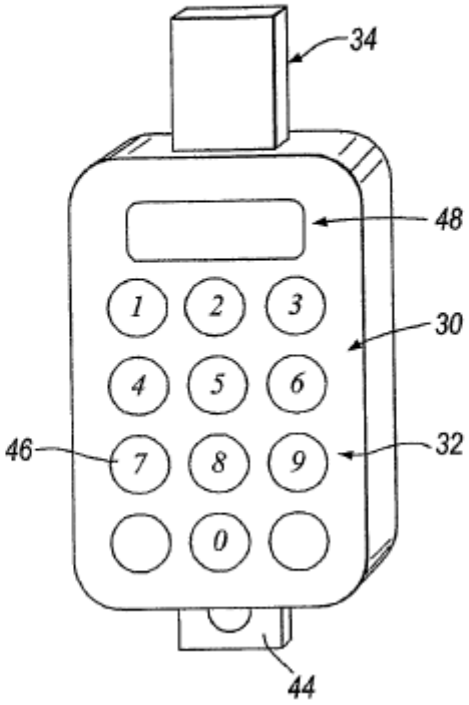

Fig.4

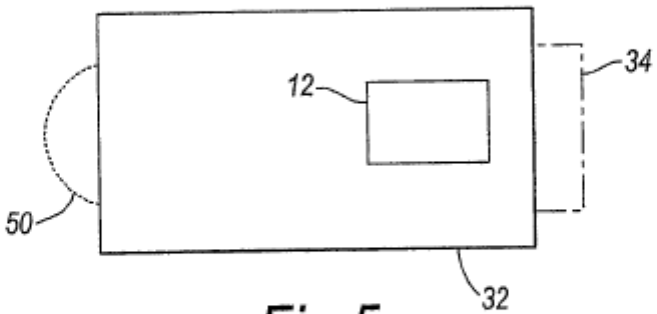

Fig.5

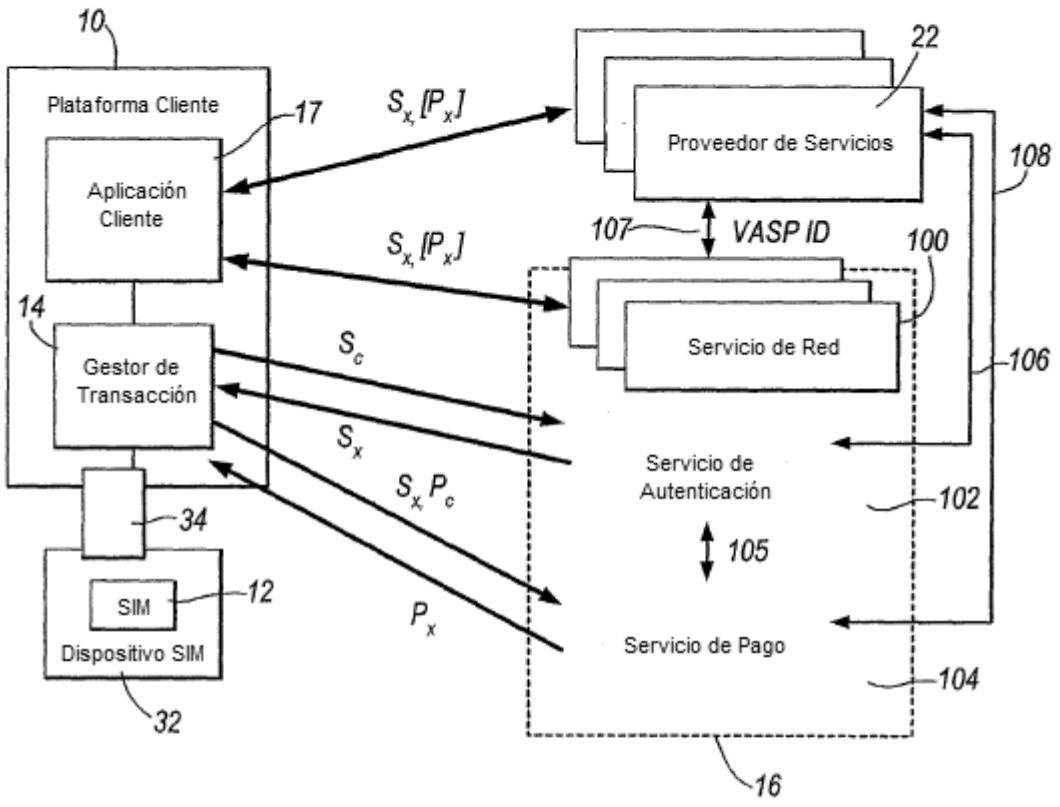
10
Plataforma Cliente
17
Aplicación Cliente
14
Gestor de Transacción
34
SIM
12
Dispositivo SIM
32
$S_x, [P_x]$
$S_x, [P_x]$
S_c
S_x
S_x, P_c
P_x
22
Proveedor de Servicios
108
107
VASP ID
100
Servicio de Red
106
Servicio de Autenticación
102
105
Servicio de Pago
104
16

Fig.6

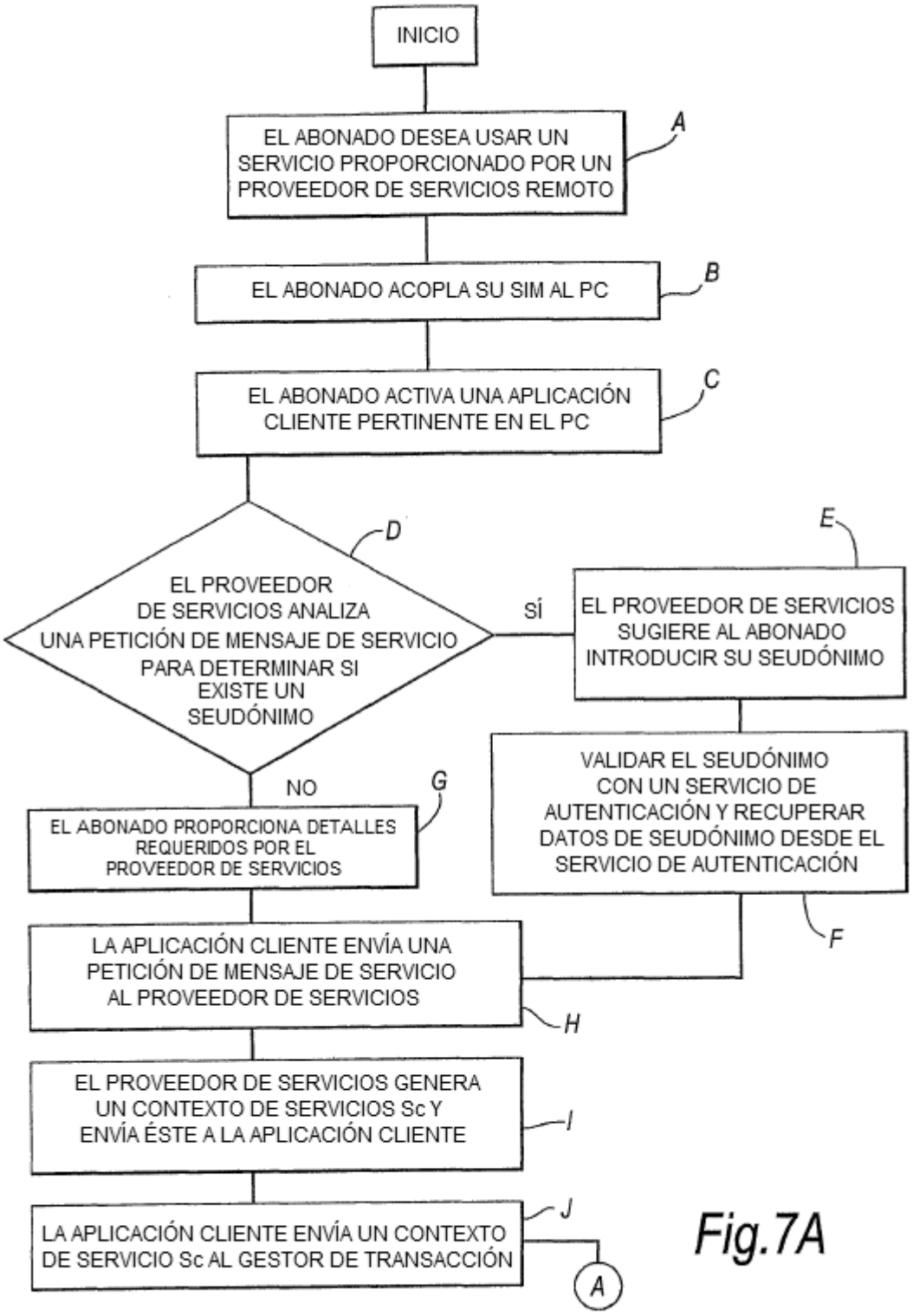
INICIO
EL ABONADO DESEA USAR UN SERVICIO PROPORCIONADO POR UN PROVEEDOR DE SERVICIOS REMOTO
A
EL ABONADO ACOPLA SU SIM AL PC
B
EL ABONADO ACTIVA UNA APLICACIÓN CLIENTE PERTINENTE EN EL PC
C
EL PROVEEDOR DE SERVICIOS ANALIZA UNA PETICIÓN DE MENSAJE DE SERVICIO PARA DETERMINAR SI EXISTE UN SEUDÓNIMO
D
SÍ
EL PROVEEDOR DE SERVICIOS SUGIERE AL ABONADO INTRODUCIR SU SEUDÓNIMO
E
VALIDAR EL SEUDÓNIMO CON UN SERVICIO DE AUTENTICACIÓN Y RECUPERAR DATOS DE SEUDÓNIMO DESDE EL SERVICIO DE AUTENTICACIÓN
F
NO
EL ABONADO PROPORCIONA DETALLES REQUERIDOS POR EL PROVEEDOR DE SERVICIOS
G
LA APLICACIÓN CLIENTE ENVÍA UNA PETICIÓN DE MENSAJE DE SERVICIO AL PROVEEDOR DE SERVICIOS
H
EL PROVEEDOR DE SERVICIOS GENERA UN CONTEXTO DE SERVICIOS Sc Y ENVÍA ÉSTE A LA APLICACIÓN CLIENTE
I
LA APLICACIÓN CLIENTE ENVÍA UN CONTEXTO DE SERVICIO Sc AL GESTOR DE TRANSACCIÓN
J
A

Fig.7A

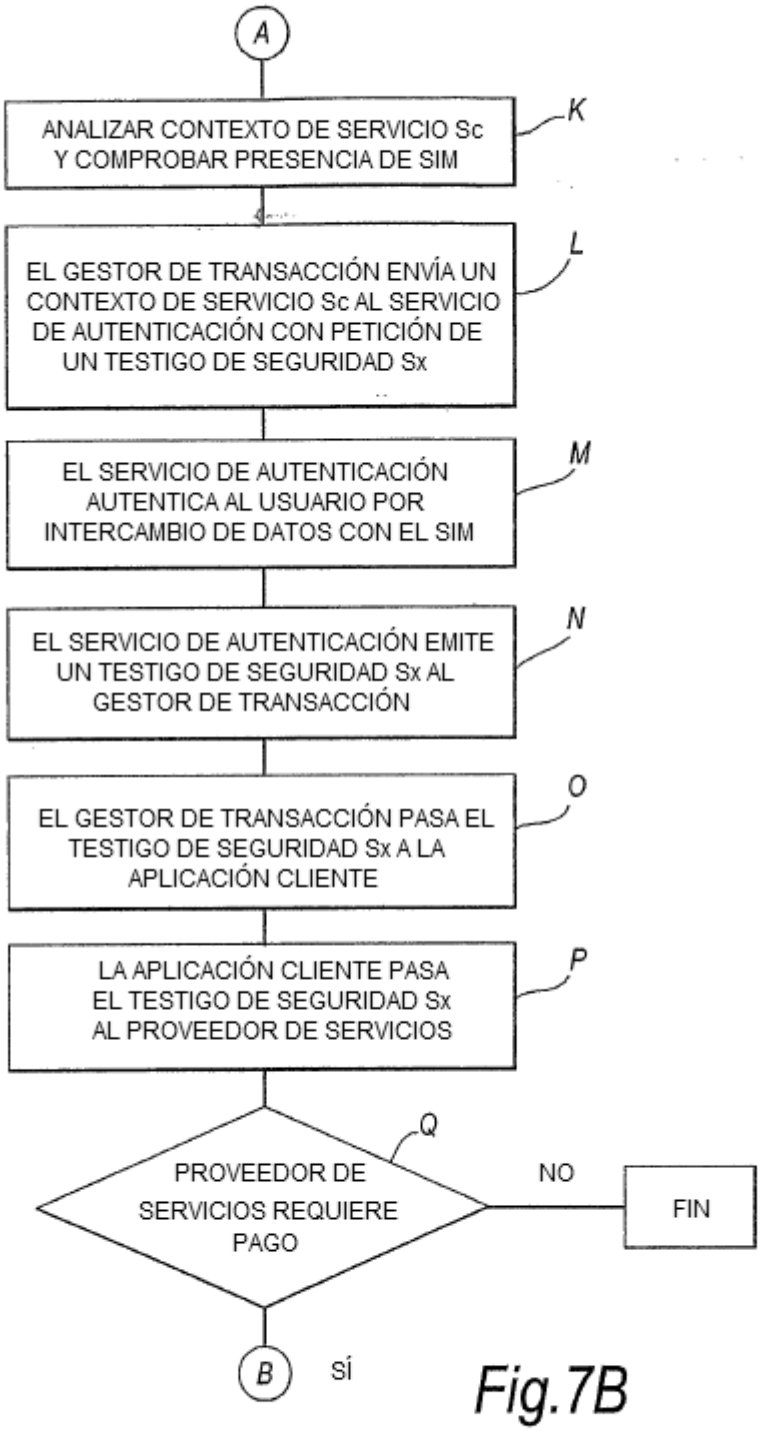
A
ANALIZAR CONTEXTO DE SERVICIO Sc Y COMPROBAR PRESENCIA DE SIM
K
EL GESTOR DE TRANSACCIÓN ENVÍA UN CONTEXTO DE SERVICIO Sc AL SERVICIO DE AUTENTICACIÓN CON PETICIÓN DE UN TESTIGO DE SEGURIDAD Sx
L
EL SERVICIO DE AUTENTICACIÓN AUTENTICA AL USUARIO POR INTERCAMBIO DE DATOS CON EL SIM
M
EL SERVICIO DE AUTENTICACIÓN EMITE UN TESTIGO DE SEGURIDAD Sx AL GESTOR DE TRANSACCIÓN
N
EL GESTOR DE TRANSACCIÓN PASA EL TESTIGO DE SEGURIDAD Sx A LA APLICACIÓN CLIENTE
O
LA APLICACIÓN CLIENTE PASA EL TESTIGO DE SEGURIDAD Sx AL PROVEEDOR DE SERVICIOS
P
PROVEEDOR DE SERVICIOS REQUIERE PAGO
Q
NO
FIN
B
SÍ

Fig.7B

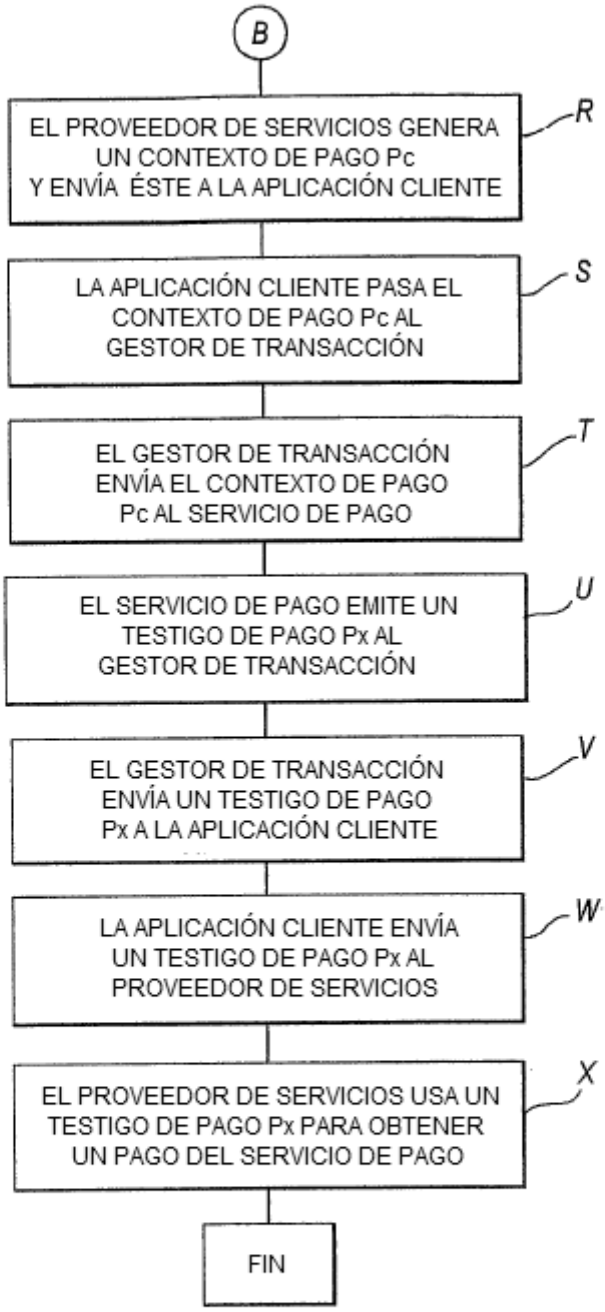
B
EL PROVEEDOR DE SERVICIOS GENERA UN CONTEXTO DE PAGO Pc Y ENVÍA ÉSTE A LA APLICACIÓN CLIENTE
R
LA APLICACIÓN CLIENTE PASA EL CONTEXTO DE PAGO Pc AL GESTOR DE TRANSACCIÓN
S
EL GESTOR DE TRANSACCIÓN ENVÍA EL CONTEXTO DE PAGO Pc AL SERVICIO DE PAGO
T
EL SERVICIO DE PAGO EMITE UN TESTIGO DE PAGO Px AL GESTOR DE TRANSACCIÓN
U
EL GESTOR DE TRANSACCIÓN ENVÍA UN TESTIGO DE PAGO Px A LA APLICACIÓN CLIENTE
V
LA APLICACIÓN CLIENTE ENVÍA UN TESTIGO DE PAGO Px AL PROVEEDOR DE SERVICIOS
W
EL PROVEEDOR DE SERVICIOS USA UN TESTIGO DE PAGO Px PARA OBTENER UN PAGO DEL SERVICIO DE PAGO
X
FIN

Fig.7C

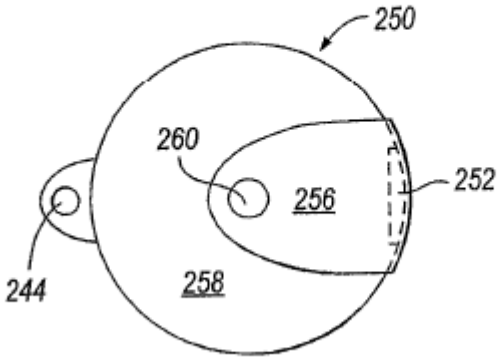

Fig.8A

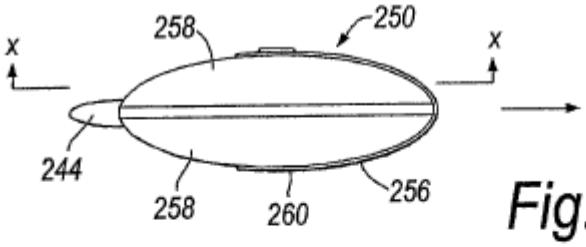

Fig.8B

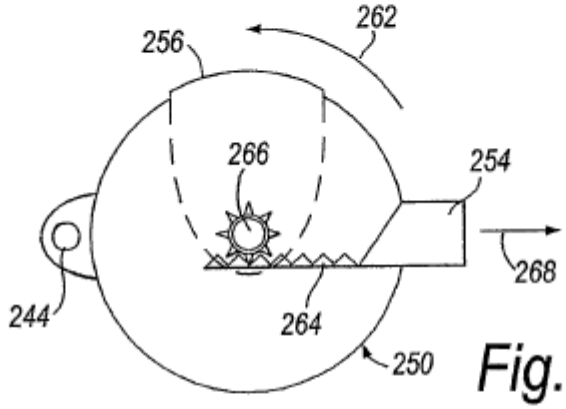

Fig.8C

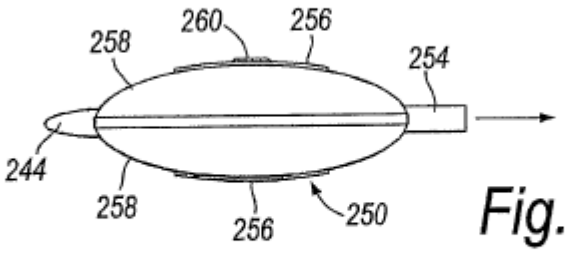

Fig.8D

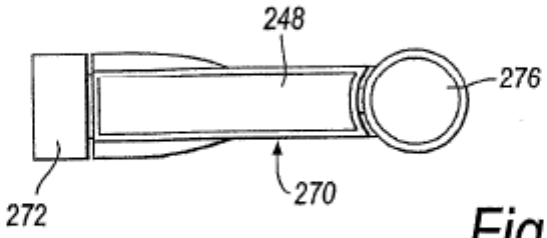

Fig.9A

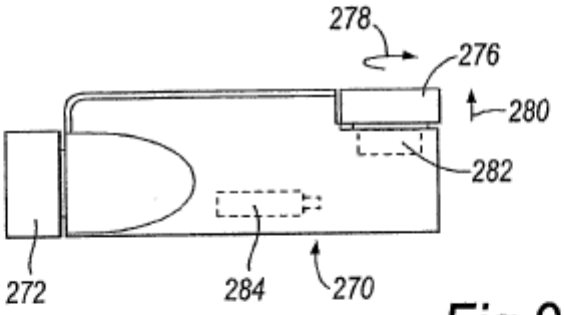

Fig.9B

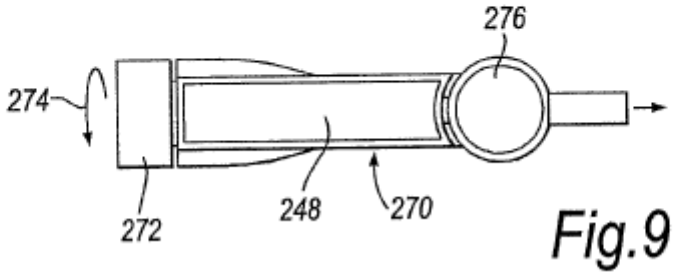

Fig.9C

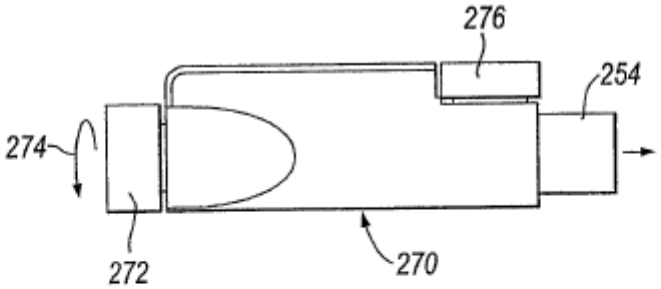

Fig.9D

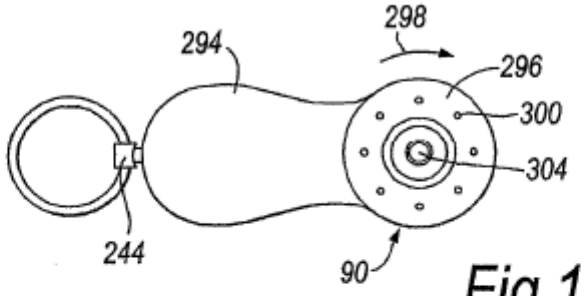

Fig.10A

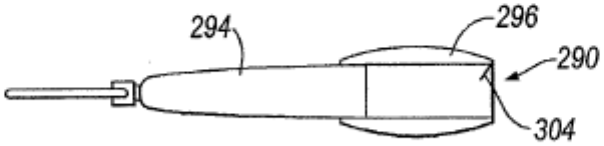

Fig.10B

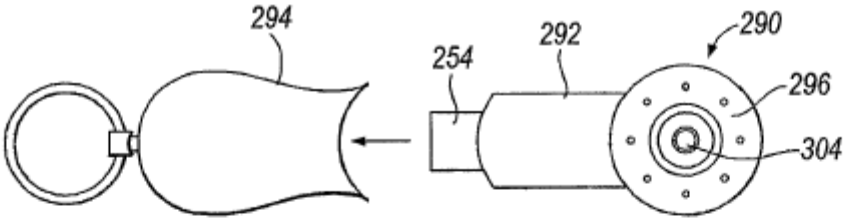

Fig.10C

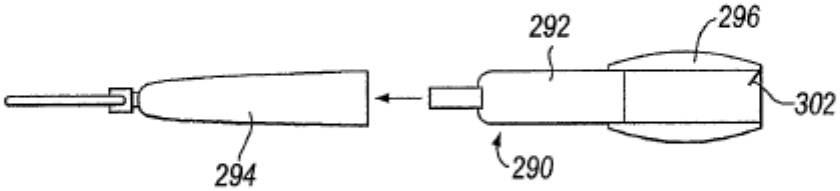

Fig.10D

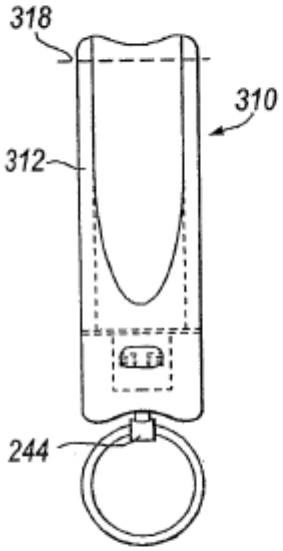

Fig.1A

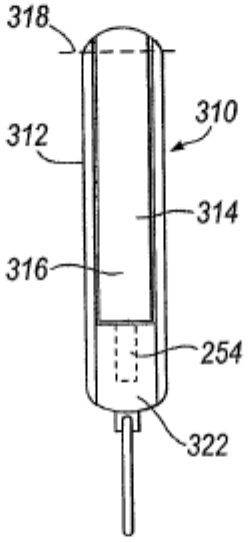

Fig.11B

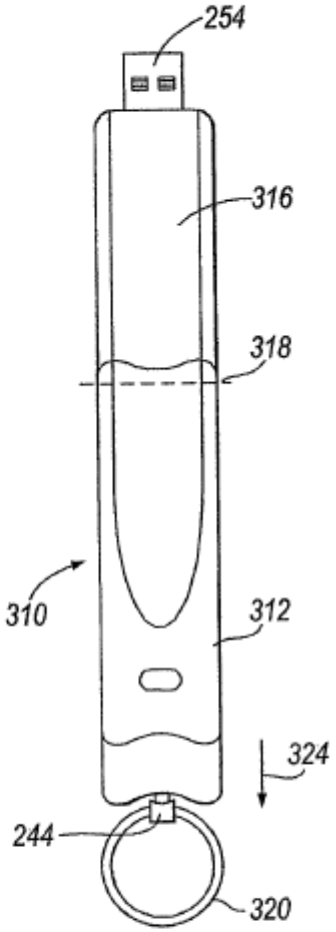

Fig.11C