(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 642 441**

(51) Int. CI.:

G06Q 20/02 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/42 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.07.2014 E 14176007 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.06.2017 EP 2966605**

(54) Título: **Procedimiento y sistema para autentificar a un usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.11.2017

(73) Titular/es:

FINPIN TECHNOLOGIES GMBH (100.0%)
Wienerbergstraße 11/12a
1100 Wien, AT

(72) Inventor/es:

GÜRTLER, MARKUS;
KOPPEL, ALEXANDER y
RANDA, FLORIAN

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Procedimiento y sistema para autentificar a un usuario

La presente invención se refiere a un procedimiento y a un sistema para la autentificación de un usuario con la ayuda de un servicio de autentificación así como de un terminal móvil que está en conexión con él.

En particular, la invención se refiere a un procedimiento y a un sistema, que proporciona, para aplicaciones de Internet (es decir, aplicaciones prácticamente discrecionales), para las que, naturalmente, no está disponible una autentificación biométrica, una seguridad y facilidad de uso de una autentificación biométrica de usuarios a través de una interfaz genérica. Un punto de partida para la invención es la propagación cada vez más amplia de aparatos biométricos de lectura, que se emplean a veces incluso en Smartphones. No obstante, en general, en terminales móviles equipados de manera correspondiente se emplea una autentificación biométrica solamente para aplicaciones locales, por ejemplo, para controlar el acceso al terminal propiamente dicho. Para tales aplicaciones locales es típico que se inicie el proceso de autentificación en el terminal, es decir, que se solicite al usuario, debido a una interacción con el terminal móvil propiamente dicho, una entrada de una característica de seguridad biométrica (pudiendo utilizarse también esta entrada propiamente dicha como interacción inicial, por ejemplo al desbloquear un aparato). Para aplicaciones externas - también por razones de seguridad - no se concede acceso directo desde el exterior a aparatos biométricos de lectura, de manera que tales aplicaciones deben transferirse en adelante a otros mecanismos de autentificación como la entrada de una palabra de paso. Para poder introducir una autentificación biométrica, deben alojarse las aplicaciones al menos parcialmente en el terminal, para que puedan realizarse al menos las etapas de autentificación localmente. Sin embargo, esto representa un gasto comparativamente alto para las aplicaciones individuales, que apenas es significativo económicamente a la vista de los terminales diferentes y en la mayoría de los casos no están equipados (todavía) con instalaciones adecuadas.

Un procedimiento de este tipo se muestra, por ejemplo, en el documento EP 1 102 150 A2, en el que el procedimiento mostrado allí presenta algunos puntos débiles, puesto que no se pueden activar determinadas transacciones, sino que sólo se pueden identificar, en general, el usuario. El procedimiento de autentificación no es en este caso transparente para la aplicación mostrada, puesto que la dirección del terminal móvil se determina a través de la aplicación o bien debe conocerse la aplicación para que pueda iniciar una autentificación correspondiente. De manera correspondiente, debe establecerse también entre la aplicación y el terminal móvil una confianza directa (por ejemplo, a través de intercambio correspondiente de claves). Además, a partir del documento EP 1 102 150 A2 no se puede deducir cómo se utiliza una identificación por medio de impresión digital para la autentificación frente a la aplicación.

La invención se basa en la idea de proporcionar la posibilidad de una autentificación biométrica a través de un servicio de autentificación empleado, por decirlo así, como intermediario, de manera que la conexión al servicio de autentificación se puede realizar con preferencia a través de interfaces y protocolos de autentificación muy propagados ya para otros fines. La conexión de una aplicación existente a tal servicio de autentificación se puede realizar de manera comparativamente sencilla y en muchos casos está presente ya para otros servicios de autentificación.

En principio, se conocen de la misma manera tales servicios de autentificación centrales, que posibilitan a aplicaciones externas la autentificación de un usuario a través de un terminal móvil. El documento US 2003/0061163 A1 muestra, por ejemplo, un procedimiento, en el que se pueden confirmar o bien liberar transacciones de tarjetas de crédito en tiempo real a través de un terminal móvil, realizándose el pago ya después de la liberación. En este caso, el titular de la tarjeta de crédito, con la que se la realizado un pago a un comerciante, es contactado a través de un puesto de mediación central y es requerido a confirmar o rechazar la transacción.

También el documento US 7.447.784 B2 describe un procedimiento y un sistema para la autentificación de un usuario de Internet, de manera que, por ejemplo, durante la compra en una página de Internet o en una aplicación, se verifica la identidad del usuario a través de un servicio de autentificación de un operador de telefonía móvil, emitiendo el servicio de autentificación de un operador de telefonía móvil una consulta de autentificación al teléfono móvil del usuario, a la que éste debe responder para la liberación con una palabra de paso.

El documento WO 2010/004576 A1 describe un procedimiento para la auten5tication de transacciones de pago en tiempo real, en el que un usuario es autenticado a través de la entrada de un PIN en un terminal móvil y la transmisión del PIN introducido hacia un servidor de autentificación.

El documento WO 2012/123727 A1 describe otro procedimiento para la autentificación de un usuario, en el que se emite una consulta a un servicio de autentificación, que conectada, por su parte, con un terminal móvil, obtiene una autorización y, dado el caso, confirma la autentificación. Se puede realizar una autentificación local en el terminal a través de la entrada de un PIN.

El cometido de la invención es proponer un procedimiento o bien un sistema, que proporciona a una aplicación externa las ventajas de una autentificación biométrica y al mismo tiempo evita los inconvenientes que están unidos

especialmente con la instalación inicial necesaria para la autentificación segura entre la aplicación y el terminal móvil (y de esta manera se reduce significativamente la aceptación de tales procedimientos y sistemas).

Este cometido se soluciona en un procedimiento del tipo indicado al principio según la invención porque una aplicación externa transmite una consulta con datos de identificación a un servicio de autentificación, el servicio de autentificación, sobre la base de los datos de identificación calcula la dirección de un terminal móvil enlazado con el usuario (como dirección se aplican en este contexto todos los datos a través de los cuales se puede establecer contacto con el terminal móvil, por ejemplo una dirección-IP, un número de teléfono, una dirección de hardware o datos comparables) y transmite una solicitud con la identificación de una transacción al terminal móvil, el terminal móvil (o bien una aplicación de autentificación instalada en el terminal móvil) recibe la solicitud y activa a través de la recepción de la solicitud una consulta para la entrada de una característica de seguridad biométrica, después de la recepción, la característica de seguridad biométrica es autenticada y solamente en el caso de la entrada de una característica de seguridad biométrica autenticada se concede el acceso a una clave privada registrada en el terminal móvil, con la clave privada se firma la identificación de la transacción y se transmite la identificación de la señalización firmada de retorno al servicio de autentificación, y el servicio de autentificación verifica la firma de la identificación de la transacción firmada y en el caso de presencia de una firma autenticada se transmite una confirmación de la solicitud para la liberación de la aplicación de retorno a la aplicación. De manera correspondiente, el cometido anterior se soluciona en un sistema del tipo indicado al principio, que comprende un servidor de autentificación, que alberga un servicio de autentificación, y un terminal móvil, que está instalado para la comunicación con el servidor de autentificación, en el que el servidor de autentificación presenta una memoria que contiene datos de identificación para la identificación del usuario y una dirección del terminal móvil enlazada con los datos de identificación, en el que el servicio de autentificación está instalado para la recepción de una consulta con datos de identificación de una aplicación externa, en el que el terminal móvil está instalado para la verificación local de una característica de seguridad biométrica y presenta una memoria, que contiene una clave privada protegida por una característica de seguridad biométrica, de acuerdo con la invención porque el terminal móvil está instalado para recibir una solicitud con una identificación de la transacción desde el servicio de autentificación, para realizar, a la recepción de una solicitud, una consulta para la entrada de una característica de seguridad biométrica, para autenticar después de la entrada localmente la característica de seguridad biométrica introducida, para conceder sólo en el caso de la entrada de una característica de seguridad biométrica autoriza el acceso a la clave privada, para firmar con la clave privada la identificación de la transacción y para transmitir la identificación de la transacción firmada de retorno al servicio de autentificación, y en el que el servicio de autentificación está instalado para verificar la firma de la identificación de la transacción firmada y en el caso de presencia de una firma autenticada transmitir una confirmación de la solicitud para la liberación de la aplicación de retorno a la aplicación. El servicio de autentificación forma de esta manera un punto de contacto central para la autentificación de los usuarios registrados, en el que los terminales móviles utilizados para la autentificación propiamente dicha y el ciclo de la autentificación biométrica para la aplicación que accede son transparentes (es decir, no visibles). La aplicación sólo debe acoplarse una vez con el servicio de autentificación o bien sólo debe establecerse una vez una confianza mutua. Las autenticaciones siguientes se pueden iniciar entonces con preferencia a través de la comunicación inicial de la aplicación con el servidor de la autentificación. El servicio de autentificación está acoplado evidentemente, además, con cada terminal móvil o bien con el aparato biométrico de lectura, pero es suficiente realizar este proceso sólo una vez para un número discrecional de aplicaciones externas. En particular, las etapas de procesamiento representadas anteriormente, que tienen lugar en el terminal móvil, pueden estar implementadas por una aplicación de autentificación instalada en el terminal móvil, de manera que un terminal móvil se puede instalar también posteriormente a través de reequipamiento (por ejemplo, descarga) de la aplicación de autentificación para el presente procedimiento. Los datos de identificación, que utilizan el servicio de autentificación para calcular el terminar móvil a contactar, o bien pueden identificar un usuario, de manera que se pueden determinar los terminales móviles registrados a través de este usuario o se puede remitir de otra manera al terminal móvil asociado al usuario. Puesto que el acceso a la clave privada sólo se concede después de la entrada de una característica de seguridad biométrica autorizada, el procedimiento es equivalente a una autentificación biométrica directa o bien local. Es decir, que la clave privada en el terminal móvil está reservada exclusivamente para la finalidad de la autentificación biométrica. En este caso, las propiedades (longitud, duración de la validez, algoritmo utilizado) de la clave privada deben seleccionarse para que la seguridad de la autentificación sea de esta manera igual o bien aproximadamente igual a la seguridad de una autentificación biométrica directa. Como característica de seguridad biométrica se contemplan, por ejemplo, una impresión digital, un escaneo del iris, una reconocimiento facial o un análisis de ADN, pudiendo limitarse en muchos casos el número de ensayos de autentificación y el intervalo de tiempo entre los ensayos para dificultar elusiones de la autenticidad y elevar, en general, la seguridad del procedimiento. Para informar al usuario adicionalmente a la correlación temporal (la transacción se activa normalmente por el usuario propiamente dicho en el marco de la aplicación externa) de por qué es necesaria una autentificación, adicionalmente a la identificación de la transacción se puede transmitir un motivo de la autentificación, por ejemplo una descripción de la transacción, al terminal móvil y se puede representar al usuario con la consulta de la característica de seguridad. Además, la aplicación puede emitir después de la recepción de la confirmación de la consulta un mensaje sobre la liberación realizada al usuario o bien se puede representar para éste, pudiendo realizarse el mensaje también implícitamente sólo a través de la liberación del acceso a una parte asegurada de la aplicación.

El procedimiento de autentificación se puede emplear prácticamente en cualquier momento y, por lo tanto, de forma universal, cuando el servicio de autentificación está conectado con el terminal móvil a través de una comunicación de datos móvil (es decir, sin cables, de gran alcance), por ejemplo 3G, UMTS, LTE o tecnologías comprables. Con preferencia, también la aplicación que realiza la consulta está conectada para la iniciación de la comunicación con el servidor de autentificación de la misma manera a través de una conexión-TCP/IP. Se puede emplear prácticamente cualquier comunicación de datos móvil, que posibilita una comunicación a través de una conexión-TCO/IP entre el terminal móvil y el servicio de autentificación. De esta manera se pueden desarrollar también ciclos de autentificación diarios como al encargar una película en un descodificador, en el cajero automático, en oficinas bancarias en la ventanilla, durante la compra o para controles de acceso aplicando el presente procedimiento de autentificación.

Para poder identificar claramente el terminal, con el ha sido realizada la autentificación, y para poder verificar si se trata en este caso del terminal móvil determinado para la finalidad de la autentificación, que corresponde a los datos de identificación y contactado por el servicio de autentificación, es ventajoso que el servicio de autentificación verifique la identificación de la transacción firmada con una clave pública, que está enlazada con los datos de identificación y está depositada en la memoria del servidor de autentificación. De manera correspondiente, tal verificación se realiza con éxito cuando la identificación de la transacción ha sido firmada con aquella clave privada, que corresponde con la clave pública depositada. Si hubiera firmado la identificación de la transacción otro terminal que el terminar contactado, la verificación fallaría también cuando la firma se puede verificar o bien se puede descifrar con otra clave pública, dado el caso, incluso registrada.

Además, es importante que el servicio de autentificación firme la confirmación con una clave privada independiente del usuario. La confirmación sería firmada de manera correspondiente antes de la transmisión de retorno a la aplicación. De esta manera se puede impedir que la confirmación sacar conclusiones sobre el usuario o el terminal móvil que van más allá de los datos de identificación. En particular, la confirmación no contiene ninguna firma que se pueda asociar al usuario o al terminal móvil u otras propiedades características, que no están contenidas ya en los datos de identificación - conocidos de todos modos de manera necesaria por la aplicación. De esta manera, los datos privados del usuario, por ejemplo en qué periodos de tiempo utiliza qué terminal móvil, con qué frecuencia cambia el terminal móvil o similares, están protegidos por el servicio de autentificación y son ocultados para las aplicaciones que acceden.

Además, se ha comprobado que es especialmente ventajoso que con la identificación de la transacción se transmita una propiedad de la transacción que puede ser modificada por el usuario en el terminal móvil y con la identificación de la transacción firmada se transmita una propiedad de la transacción correspondiente, dado el caso modificada, La propiedad de la transacción puede contener en este caso datos discrecionales enlazados con la consulta o bien con la identificación de la transacción. Mientras que la identificación de la transacción es con preferencia unívoca e incluso única, para evitar una confusión de diferentes transacciones en el servicio de identificación ,a propiedad de la transacción puede adoptar valores discrecionales. En particular, en este caso se trata de datos y valores que caracterizan una transacción, de manera que la autentificación se puede aplicar, por ejemplo, como liberación condicionada de una transacción específica más exacta a través de la propiedad de la transacción. De manera correspondiente, se transmite un valor confirmado a través de la autentificación de la propiedad de la transacción, en particular teniendo en cuente eventuales modificaciones realizadas en el terminal móvil, con la confirmación en la aplicación. Como propiedad de la transacción se pueden asociar a la transacción, por ejemplo, una importe de pago liberado durante un proceso de pago o la duración de una liberación durante una prestación de servicio o un cálculo temporal. Durante la transmisión de un importe de pago liberado se puede liberar de esta manera tal vez sólo una parte de una suma de transacción y a continuación se puede intentar por parte de la aplicación hacer liberar el resto de la suma de la transacción por otra vía, por ejemplo a través de otro usuario enlazado con la transacción, cuyos datos de identificación son conocidos por la aplicación. De esta manera se pueden dividir y en cada caso pagar parcialmente facturas comunes de varios abonados. Mientras que la identificación de la transacción se genera o bien se predetermina con preferencia por el servicio de autentificación, la propiedad de la transacción se predetermina o al menos se inicia y, dado el caso se modifica por el terminal móvil.

Sobre todo para transacciones críticas para la seguridad o para verificar un consenso entre varios autorizados, es especialmente favorable, además, que el servicio de autentificación determine sobre la base de los datos de identificación las direcciones de al menos dos terminales móviles y transmita una solicitud de la consulta a la aplicación sólo cuando se ha recibido desde todos los terminales un reconocimiento de la transacción firmado auténticamente. De esta manera, se puede realizar, por ejemplo, una verificación de una transacción de acuerdo con el principio de cuatro ojos, es decir, que dos (o más) usuario deben liberar la transacción, cuando los datos de la identificación están enlazados de manera correspondiente con al menos dos usuarios. En este caso, los al menos dos terminales móviles están enlazados, respectivamente, con los diferentes usuarios. Pero de esta manera también se puede asegurar adicionalmente una autentificación biométrica múltiple de un usuario individual cuando los al menos dos terminales móviles están enlazados con el mismo usuario y verifican diferentes características de seguridad biométricas, por ejemplo tanto una impresión digital como también un reconocimiento visual. De manera similar es igualmente concebible que dos usuarios diferentes sean invitados uno detrás del otro a la entrada de una característica de seguridad biométrica respectiva en el mismo terminal móvil.

En conexión con una autentificación múltiple de este tipo es ventajoso que el servicio de autentificación contenga una secuencia de la verificación, de manera que se transmite una identificación de la transacción firmada auténticamente por un primer terminal móvil a un segundo terminal móvil, y en el que solamente se transmite una confirmación de la consulta cuando existe una identificación de la transacción firmada auténticamente por todos los terminales móviles. De esta manera se puede establecer previamente un ciclo de la autentificación y se puede realizar, por ejemplo, una liberación escalonada. Por ejemplo, en el caso de una pluralidad de consultas no autorizadas se puede delegar una selección previa, de manera que la última autentificación solo se inicia en la secuencia de la verificación cuando la transacción respectiva ya ha sido liberada o bien autorizada en una selección previa de una o más fases.

Para que la aplicación se pueda realizar también después de un cambio del terminal móvil o en el caso de la aplicación de varios terminales móviles la autentificación sin adaptación de la consulta y, por lo tanto, sin modificación de la aplicación, es favorable que los datos de identificación presenten una identificación del usuario registrada por el usuario durante el servicio de autentificación, independiente de la identificación del usuario. Por lo tanto, la identificación del usuario es prácticamente representante de uno o varios terminales móviles del usuario o bien de al menos un usuario, para el que se realiza en último término la autentificación biométrica. De esta manera, en el caso de utilización de otro terminal móvil adicional, puede darlo a conocer de manera sencilla sólo al servicio de autentificación, inmediatamente después de lo cual todas las aplicaciones que acceden al servicio de autentificación pueden hacer uso del nuevo terminal y se pueden aprovechar del mismo.

Para impedir una manipulación del procedimiento de autentificación o bien para dificultarla o más posible, es ventajoso que para la iniciación del procedimiento de autentificación, se genere la clave privada en el terminal móvil y se enlace con una característica de seguridad biométrica autorizada. La clave privada es registrada con preferencia en una memoria protegida del terminal móvil y nunca debe abandonar el terminal móvil. De manera correspondiente, se genera una pareja de claves internamente en el terminal móvil y sólo se transmite la clave pública de la pareja de claves al servicio de autentificación. Para evitar una falsificación a través de una transmisión incorrecta de la clave privada, se puede utilizar una IMEI (International Mobile Equipment Identity = Identidad Internacional de Equipo Móvil) del terminal móvil como parte de la clave. Por ejemplo, la IMEI, o una característica de identificación comparable del terminal móvil, se puede colgar en una clave generada de forma aleatoria o se puede colocar delante de la clave.

Para asegurar el procedimiento de autentificación y para evitar un abuso de un terminal móvil robado por terceros, es favo9rable que para la terminación del procedimiento de autentificación el servicio de autentificación transmite una instrucción de borrado al terminal móvil y el terminal móvil, a la recepción de la instrucción de borrado, borre la clave privada de manera duradera. De esta manera, es imposible crear con el terminal móvil en adelante firmas válidas para reconocimientos de transacciones, y el terminal móvil es inadecuado para autenticaciones futuras.

A continuación se explica en detalle todavía la invención con la ayuda de ejemplos de realización especialmente preferidos, a los que no se limita, sin embargo, la invención, y con referencia a los dibujos. En este caso, en particular:

La figura 1 muestra un caso de aplicación con un usuario, que se autentifica para el acceso a una aplicación móvil en un terminal móvil.

La figura 2 muestra un diagrama esquemático de secuencias para el ciclo de una autentificación en el caso de aplicación representado en la figura 1.

La figura 3 muestra otro caso de aplicación con tres usuarios, en el que dos usuarios autentifican el acceso de un tercer usuario a una aplicación.

La figura 4 muestra un diagrama esquemático de secuencias para el ciclo de una autentificación en el caso de aplicación representado en la figura 3; y

La figura 5 muestra un diagrama esquemático de secuencias para el ciclo de una autentificación en el caso de aplicación representado en la figura 3.

En el ejemplo de realización representado en la figura 1, un usuario 1 accede con un ordenador portátil 2 a una aplicación. La aplicación 3 se representa o bien se ejecuta en forma de un cliente 5 conectado con la aplicación 3 a través de una comunicación de datos 4 en el ordenador móvil 2. Partes de la aplicación 3 están protegidas contra acceso y requieren una autentificación de un usuario autorizado. En la situación representada en la figura 1, el usuario 1 accede a tal parte de la aplicación 3 protegida contra acceso. La aplicación 3 establece a continuación una comunicación de datos 6 con un servicio de autentificación 8 que se ejecuta en un servidor de autentificación 7 y transmite al servicio de autentificación 8 una consulta, que comprende al menos datos de identificación del usuario

1. El servicio de autentificación 8 genera a continuación en primer lugar una identificación inequívoca de la transacción, que está enlazada con la consulta. El servicio de autentificación 8 está conectado con una memoria 9 del servidor de autentificación 7, cuya memoria 9 es administrada en forma de una base de datos. La base de datos comprende una colección de usuarios registrados, en la que con cada usuario está enlazado con preferencia al menos un terminal móvil. Es decir, que la base de datos comprende una tabla con asociaciones entre los usuarios y las direcciones de los terminales móviles enlazados en cada caso. Con la ayuda de los datos de identificación obtenidos, el servicio de autentificación 8 puede determinar de esta manera las direcciones de aquellos terminales móviles, que están asociados al usuario 1 designado a través de los datos de identificación. Si no se puede hallar ninguna dirección correspondiente, la autentificación falla y la aplicación 3 es informada de manera correspondiente. En el caso de que se encuentre al menos una dirección de un terminal móvil 10, el servicio de autentificación 8 establece una comunicación de datos 11 con el terminal móvil 10 y transmite una invitación con la identificación de la transacción generada anteriormente a través de esta comunicación de datos al terminal móvil 10. El terminal móvil 10 comprende una memoria 12, en la que está registrada una clave privada 13. Además, el terminal móvil 10 presenta una instalación de lectura 14 para una característica de seguridad biométrica, en particular un aparato de lectura de impresión digital. El acceso a la clave privada 13 registrada localmente en el terminal móvil 10 o bien en su memoria 12 está protegido en este caso por una característica de seguridad biométrica del usuario 1 que puede ser inscrita por medio de una instalación de lectura 14 igualmente local, integrada con preferencia en el terminal móvil 10, es decir, que se concede el acceso a la clave privada 13 sólo y después de la entrada de una característica de seguridad biométrica autorizada. A la recepción de la invitación desde el servicio de autentificación 8, el terminal móvil 10 realiza una consulta para la entrada de una característica de seguridad biométrica del usuario 1 en la instalación de lectura 14, es decir, que el usuario 1 es informado por el terminal móvil 10, por ejemplo en forma de una señal de tono y/o de vibración, de que está pendiente una autentificación y es necesaria la entrada de una característica de seguridad biométrica para la liberación. Por consiguiente, la invitación es activada por la aplicación 3 prácticamente por mando a distancia y, en general, sin interacción del usuario con el terminal móvil 10. Tan pronto como el usuario 1 acepta la invitación e introduce una característica de seguridad biométrica autorizada, se libera - como ya se ha explicado - en primer lugar localmente el acceso a la clave privada 13. El resultado de la entrada del usuario propiamente dicho, es decir, la característica de seguridad biométrica introducida, se utiliza sólo para el control de acceso a la clave privada y no se transmite de ninguna manera desde el terminal móvil 10 hacia fuera, en particular tampoco al servicio de autentificación 8. Con la clave privada 13 ahora accesible se señaliza en el terminal móvil 10 la identificación de la transacción obtenida desde el servicio de autentificación 8. En este caso, se codifica, por ejemplo, la identificación de la transacción propiamente dicha o una almohadilla de la identificación de la transacción con la clave privada 13 y el resultado se cuelga como firma en la identificación de la transacción. La identificación de la transacción firmada es transmitida a continuación de retorno al servicio de autentificación 8. En la memoria 9 del servicio de autentificación 8 se registra la clave pública (no mostrada) que se corresponde con la clave privada 13, que se utiliza ahora para la verificación de la firma. En este caso, se descodifica la firma con la clave pública y se compara el resultado con la identificación de la transacción o bien con su almohadilla. En el caso de que la comparación tenga éxito, es decir, en el caso de que se establezca una coincidencia, la firma debe considerar auténtica y el servicio de autentificación 8 transmite una confirmación positiva de la consulta de retorno a la aplicación 3. Para asegurar adicionalmente la verificación, se pueden asegurar claves públicas, asociadas con las direcciones de los terminales móviles 10, en la memoria 9, con las que no sólo se puede verificar la autenticidad de la firma sino también su origen, es decir, la identidad del terminal móvil 10 que expone la firma. Además, el servicio de autentificación 8 puede proveer la confirmación con una firma propia (independiente del usuario (o bien global), que se crea con una clave privada del servicio de autentificación 7 registrada en el servidor de la autentificación 7. La aplicación 3 puede verificar la firma de la confirmación con una única clave pública, a saber, la del servicio de autentificación 8. Tan pronto como la aplicación 3 recibe una confirmación positiva y con preferencia firmada desde el servicio de autentificación 8, se puede liberar el acceso a la parte asegurada de la aplicación 3.

La figura 2 representa de nuevo en detalle el ciclo descrito de forma general ya anteriormente. En este caso, en primer lugar el usuariol 1 solicitará acceso a una parte de la aplicación 3 (etapa 15). A la invitación 15, la aplicación 3 responde con una consulta 16 de una identificación del usuario. Después de la entrada 17 de la identificación del usuario, la aplicación 3 transmite una consulta 18 con los datos correspondientes de la identificación al servicio de autentificación 8. El servicio de autentificación 8 realiza localmente una consulta de la base de datos 19 de las direcciones de los terminales móviles asociados a los datos de la identificación y genera una identificación de la transacción asociada a la consulta 18. A continuación, el servicio de autentificación 8 transmite al menos a un terminal móvil 19 accesible a través de las direcciones halladas una invitación 20 con la identificación de la transacción. En el teminal móvil 10, que recibe una invitación 20, se realiza una consulta 21 desde el usuario para la entrada de una característica de seguridad biométrica. Tan pronto como el usuario ha realizado una entrada 22 de la característica de seguridad biométrica consultada, se concede en el terminal móvil 10 acceso a una clave privada 13 registrada localmente y se firma con la clave privada al menos la identificación de la transacción recibida desde el servicio de autentificación 8 (etapa 23). Se realiza una transmisión 24 de la identificación de la transacción firmada desde el terminal móvil 10 hasta el servicio de autentificación 8. Este último realiza una verificación 25 de la firma y en el caso de salida positiva de la verificación 25 transmite una confirmación 26 de la consulta o bien de la autentificación con éxito de retorno a la aplicación 3. La aplicación 3 emite finalmente un mensaje 27 sobre la liberación realizada al usuario 1, de manera que el mensaje se puede realizar también implícitamente sólo a través

de la liberación del acceso a una parte asegurada de la aplicación 3.

Otro caso de aplicación se representa de forma esquemática en la figura 3 y el ciclo correspondiente de la autentificación se muestra en la figura 4. En este caso, un primer usuario 28 activa en un terminal de la aplicación 29 (por ejemplo un cajero automático) una transacción. La aplicación 3 que se ejecuta en el terminal de la aplicación 29 reconoce en este caso con la ayuda de una identificación del usuario introducida por el primer usuario 28 (por ejemplo, un número de tarjeta o número de cuenta) que es necesaria una liberación de la transacción a través del servicio de autentificación 8. De manera correspondiente, la aplicación 3 emite una consulta 30 con los datos de identificación del primer usuario 28 al servicio de autentificación 8. En la memoria 9 del servicio de autentificación 8 dos terminales móviles 31, 32 diferentes están enlazados con los datos de identificación y se establece que es necesaria una autentificación 31, 32 en ambos terminales 31, 32. El servicio de identificación 8 emite, por lo tanto, en ambos terminales 31, 32 solicitudes de autentificación 33, 34 correspondientes, estando conectado el servicio de autentificación 8 con los terminales 31, 32, respectivamente, a través de conexiones de Internet. Ambos terminales 31, 32 realizan a continuación una consulta 35, 36 de una característica de seguridad biométrica del usuario 37, 38 respectivo y emiten dado el caso después de realizar la entrada 39, 40 de manera conocida identificaciones firmadas de la transacción 41, 42 de retorno al servicio de autentificación 8. Éste emite la confirmación 43 de la consulta 30 de retorno a la aplicación sólo cuando han llegado desde todos los terminales móviles 31, 32 necesarios identificaciones de la transacción firmadas y verificadas.

Un ciclo alternativo de la autentificación con una secuencia de verificación establecida se representa en la figura 5, en la que para las etapas o partes individuales del procedimiento se utilizaron los mismos signos de referencia que en la figura 4. Para evitar repeticiones se remite, por lo tanto, a las descripciones anteriores con respecto a los procesos individuales, de manera que a diferencia de la figura 4, la secuencia de las etapas 33, 34, 35, 36, 39, 40, 41 y 42 es otra. En particular, la solicitud de autentificación sólo se transmite al segundo terminal móvil después de que el servicio de autentificación 8 ha establecido una identificación de la transacción 41 firmada auténticamente y de esta manera una autentificación con éxito en el primer terminal móvil 31. De esta manera, se predetermina fijamente la secuencia, en la que deben autenticarse los dos usuarios 37, 38 de los terminales móviles 31, 32. La ventaja en este procedimiento reside en que en el caso de una denegación de la autentificación a través del primer usuario 37, el segundo usuario 38 no es cargado con una solicitud de autentificación - de todos modos innecesaria en este caso -. En este procedimiento según la figura 4 se puede conseguir una ventaja similar por que en el caso de una denegación de la autentificación en un terminal 31, 32, se rechaza automáticamente la solicitud de autentificación 34, 33 del otro o de los restantes terminales 32, 31, respectivamente.

En el marco de los ciclos del procedimiento y sistemas descritos aquí es evidente prever, según la opinión del técnico, medidas prevención de seguridad generales adicionales. Esto se aplica especialmente para las comunicaciones de datos entre el servicio de autentificación 8 y los terminales móviles 10, 31, 32, de manera que con preferencia durante el registro de un terminal se establece una autentificación bidireccional entre el terminal 10, 31, 32 y el servicio de autentificación 8 y se utiliza para todos los mensajes intercambiados una comunicación codificada de manera correspondiente. Medidas similares se pueden prever también entre la o las aplicaciones 3 y el servicio de autentificación 8. A la vista de la dependencia de la aplicación 3 de la disponibilidad del servicio de autentificación 8 se pueden prever, en principio, también varias instancias redundantes del servicio de autentificación 8 o bien varios servidores de autentificación 7.

REIVINDICACIONES

1.- Procedimiento para la autentificación de un usuario (1), en el que una aplicación externa (3) transmite una consulta (18) con datos de identificación a un servicio de autentificación (8), el servicio de autentificación (8), sobre la base de los datos de identificación calcula la dirección de un terminal móvil (10) enlazado con el usuario (1) y transmite una solicitud (20) con la identificación de una transacción al terminal móvil (10), el terminal móvil (10) recibe la solicitud (20) y activa a través de la recepción de la solicitud (20) una consulta (21) para la entrada de una característica de seguridad biométrica, después de la recepción (22), la característica de seguridad biométrica es autenticada localmente y solamente en el caso de la entrada de una característica de seguridad biométrica autenticada se concede el acceso a una clave privada (13) registrada en el terminal móvil (10), con la clave privada (14) se firma la identificación de la transacción y se transmite la identificación de la señalización firmada de retorno al servicio de autentificación (8), y el servicio de autentificación (8) verifica la firma de la identificación de la transacción firmada y en el caso de presencia de una firma autenticada se transmite una confirmación (26) de la solicitud (18) para la liberación de la aplicación (3) de retorno a la aplicación (3).

2.- Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque el servicio de autentificación (8) está conectado con el terminal móvil (10) a través de una comunicación de datos móvil (11).

3.- Procedimiento de acuerdo con una de las reivindicaciones 1 ó 2, **caracterizado** porque el servicio de autentificación (8) verifica la identificación de la transacción firmada con una clave pública, que está enlazada con los datos de identificación.

4.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado** porque el servicio de autentificación (8) firma la confirmación (26) con una clave privada independiente del usuario.

5.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado** porque con la identificación de la transacción se transmite una propiedad de la transacción modificable en el terminal móvil (10) por el usuario y con la identificación de la transacción firmada se transmite una propiedad de la transacción correspondiente, dado el caso modificada.

6.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado** porque el servicio de autentificación (8) calcula sobre la base de los datos de identificación las direcciones de al menos dos terminales móviles (31, 32) y transmite una solicitud (33, 34) con una identificación de la transacción a los al menos dos terminales móviles, en el que solamente se transmite una confirmación (43) de la consulta (30) a la aplicación (3) cuando por todos los terminales (31, 32) ha sido recibida una identificación de la transacción firmada auténticamente.

7.- Procedimiento de acuerdo con la reivindicación 6, **caracterizado** porque el servicio de autentificación (8) contiene una secuencia de verificación, en el que se transmite una identificación de la transacción firmada auténticamente desde un primer terminal móvil (31) a un segundo terminal móvil (32), y en el que solamente se transmite una confirmación (43) de la consulta (30) cuando existe un reconocimiento de la transacción firmada auténticamente por todos los terminales móviles (31, 32).

8.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado** porque los datos de identificación presentan un reconocimiento del usuario registrado por el usuario (1) en el servicio de autentificación (8), independiente de la dirección del terminal móvil (10).

9.- Procedimiento para la iniciación de un procedimiento de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado** porque la clave privada (13) es generada en el terminal móvil (10) y es enlazada con una característica de seguridad biométrica autorizada.

10.- Procedimiento para la terminación de un procedimiento de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado** porque el servicio de autentificación (8) transmite una instrucción de borrado al terminal móvil (10) y el terminal móvil (10) borra, a la recepción de la instrucción de borrado, la clave privada (13) de forma duradera.

11.- Sistema para la autentificación de un usuario (1), que comprende un servidor de autentificación (7), que alberga un servicio de autentificación (8), y un terminal móvil (10), que está instalado para la comunicación con el servidor de autentificación (7), en el que el servidor de autentificación (7) presenta una memoria (9) que contiene datos de identificación para la identificación del usuario (1) y una dirección del terminal móvil (10) enlazada con los datos de identificación, en el que el servicio de autentificación (8) está instalado para la recepción de una consulta (18) con datos de identificación de una aplicación externa (3), en el que el terminal móvil (10) está instalado para la verificación local de una característica de seguridad biométrica y presenta una memoria (12), que contiene una clave privada (13) protegida por una característica de seguridad biométrica, **caracterizado** porque el terminal móvil (10) está instalado para recibir una solicitud (20) con una identificación de la transacción desde el servicio de

autentificación (8), para realizar, a la recepción de una solicitud (20), una consulta (21) para la entrada (22) de una característica de seguridad biométrica, para autenticar después de la entrada (22) localmente la característica de seguridad biométrica introducida, para conceder sólo en el caso de la entrada de una característica de seguridad biométrica autoriza el acceso a la clave privada (13), para firmar con la clave privada (13) la identificación de la transacción y para transmitir la identificación de la transacción firmada de retorno al servicio de autentificación (8), y en el que el servicio de autentificación (8) está instalado para verificar la firma de la identificación de la transacción firmada y en el caso de presencia de una firma autenticada transmitir una confirmación (26) de la solicitud (18) para la liberación de la aplicación (3) de retorno a la aplicación (3).

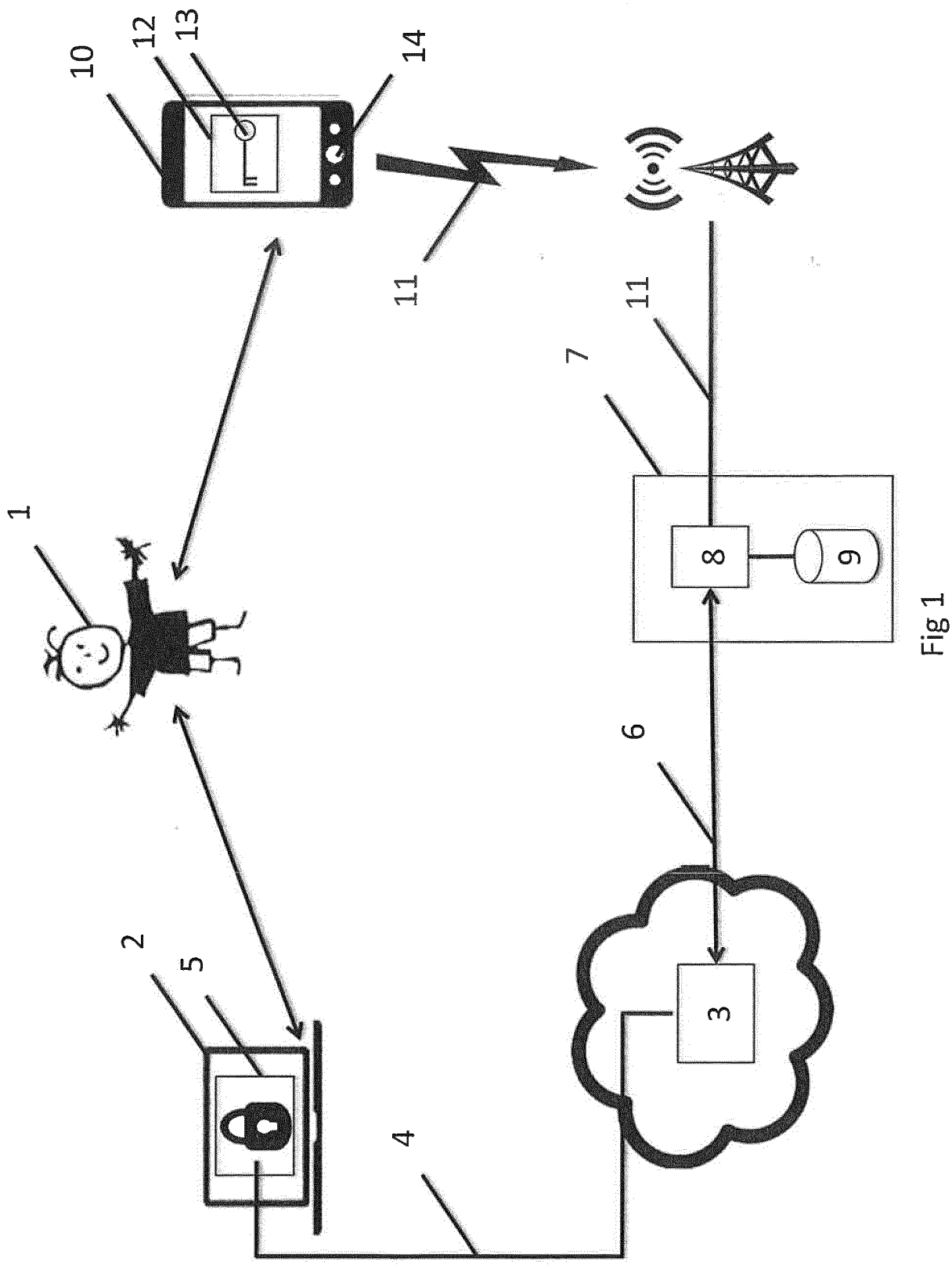

Fig 1

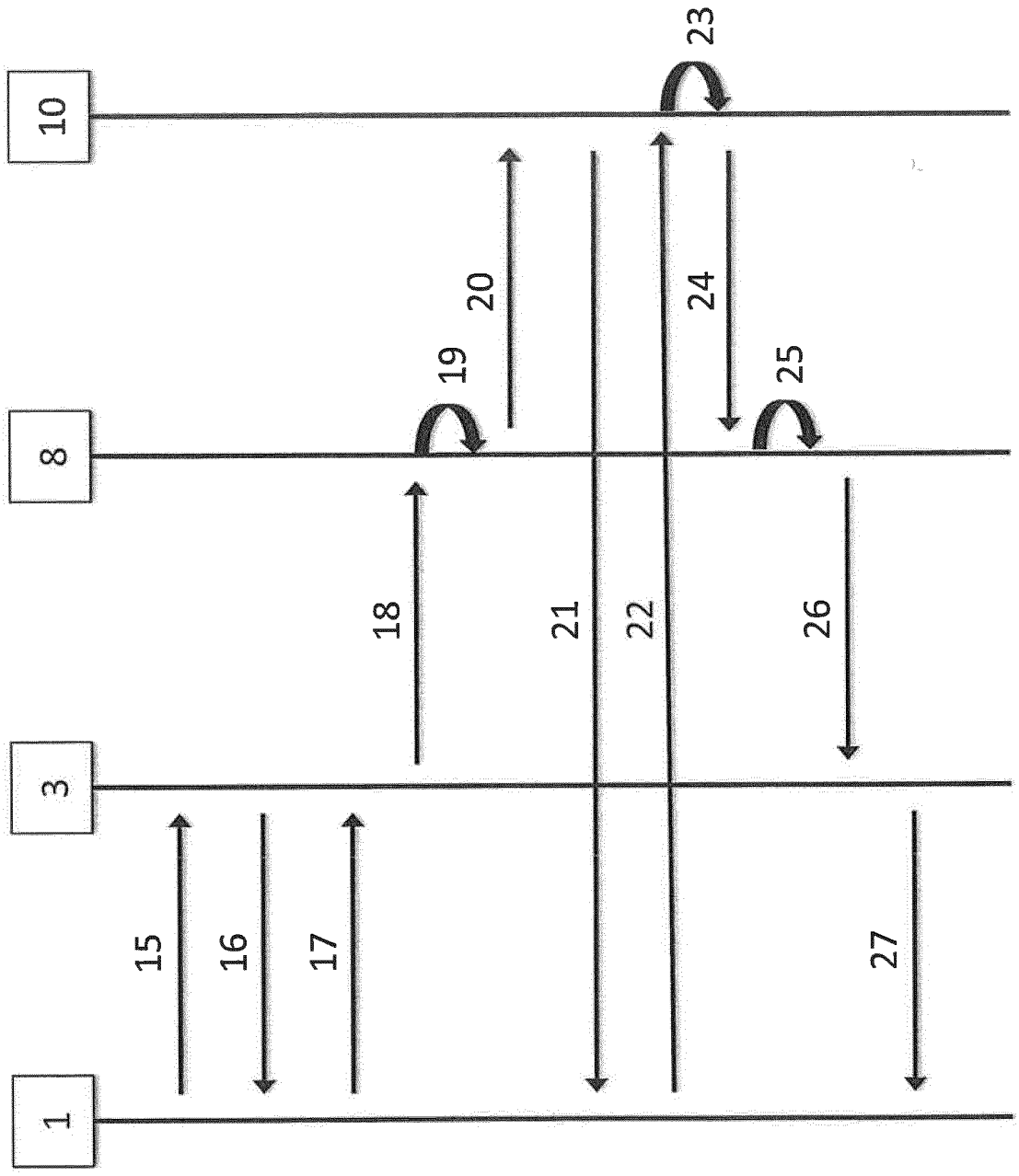

Fig 2

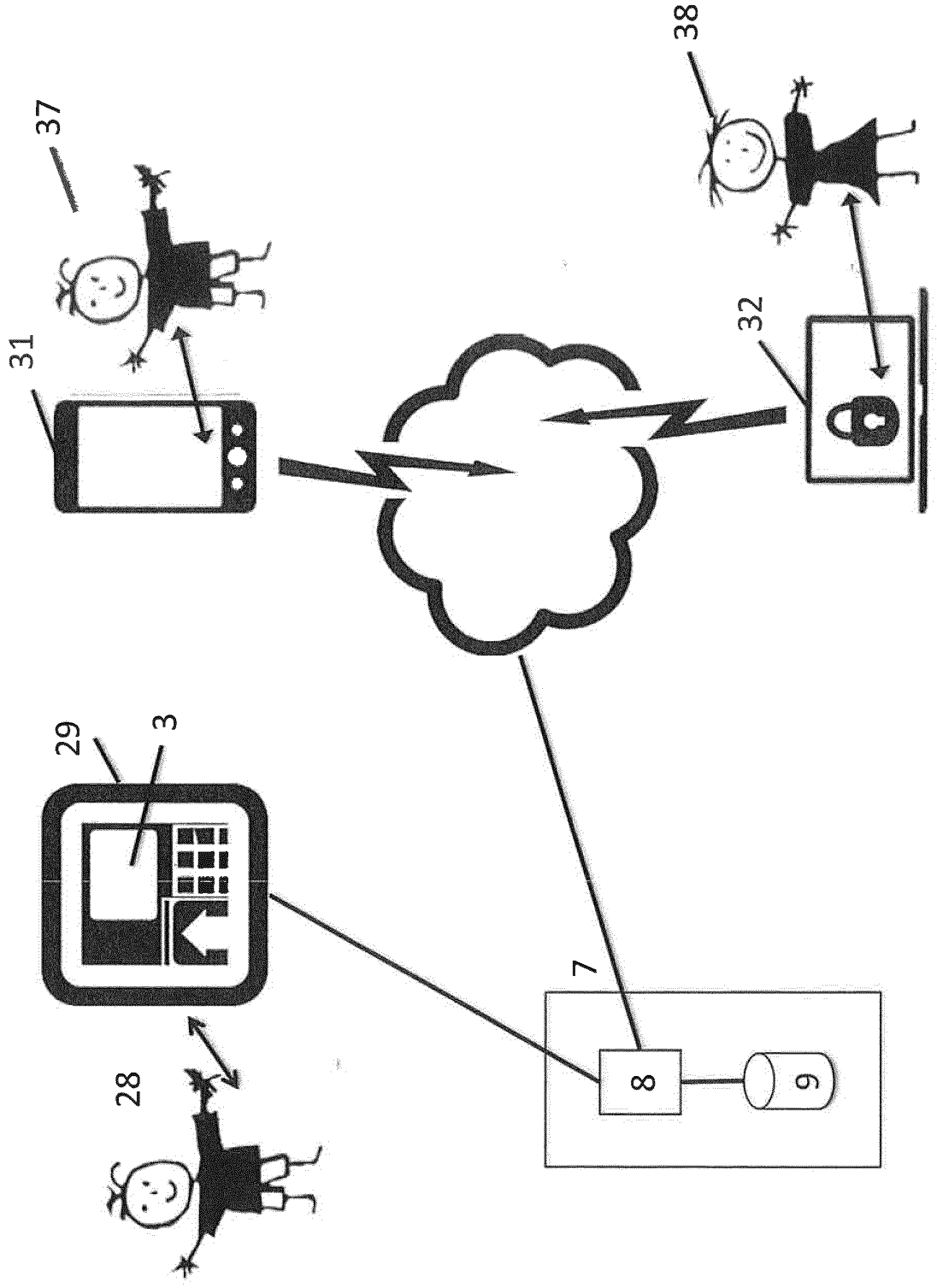

Fig 3

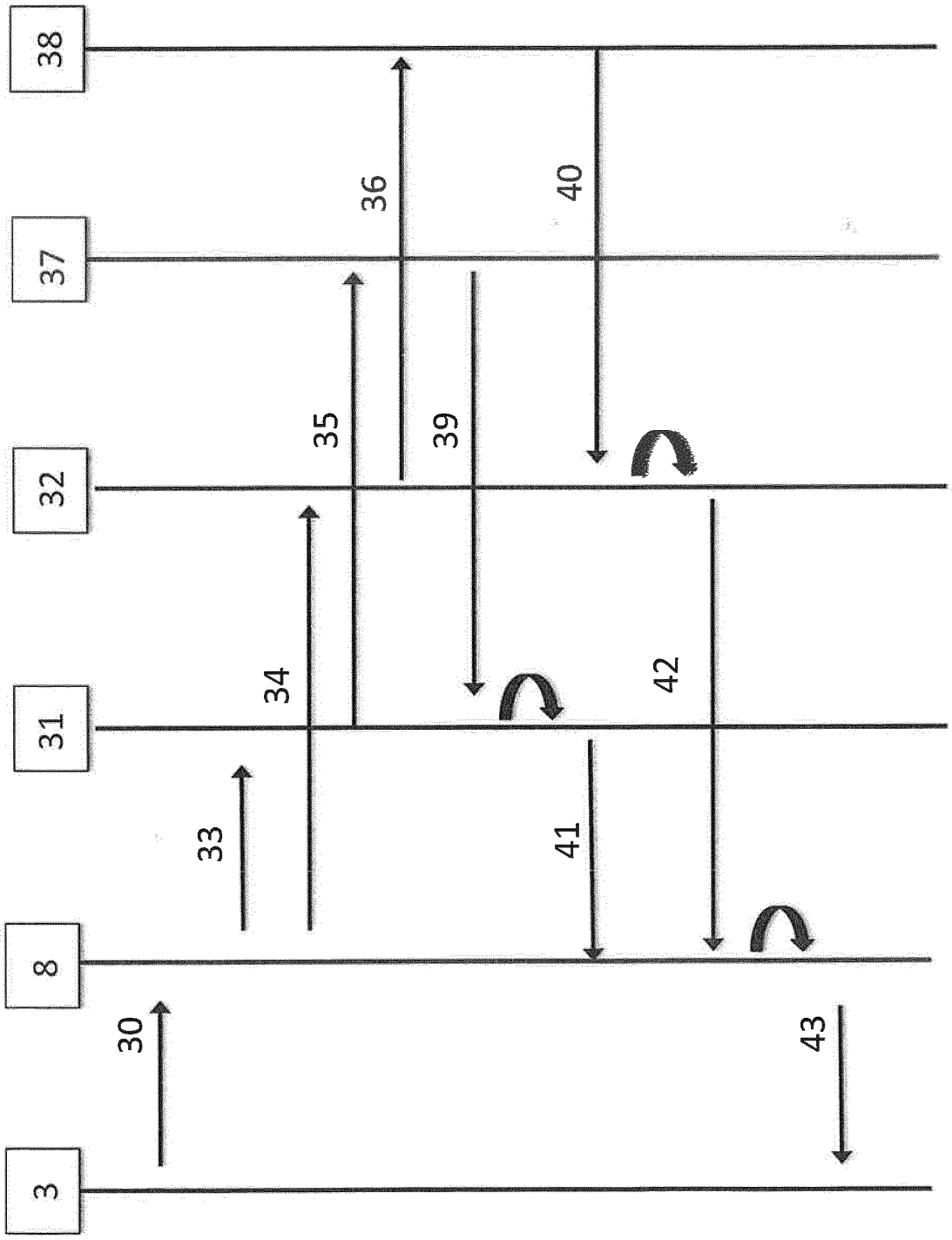

Fig 4

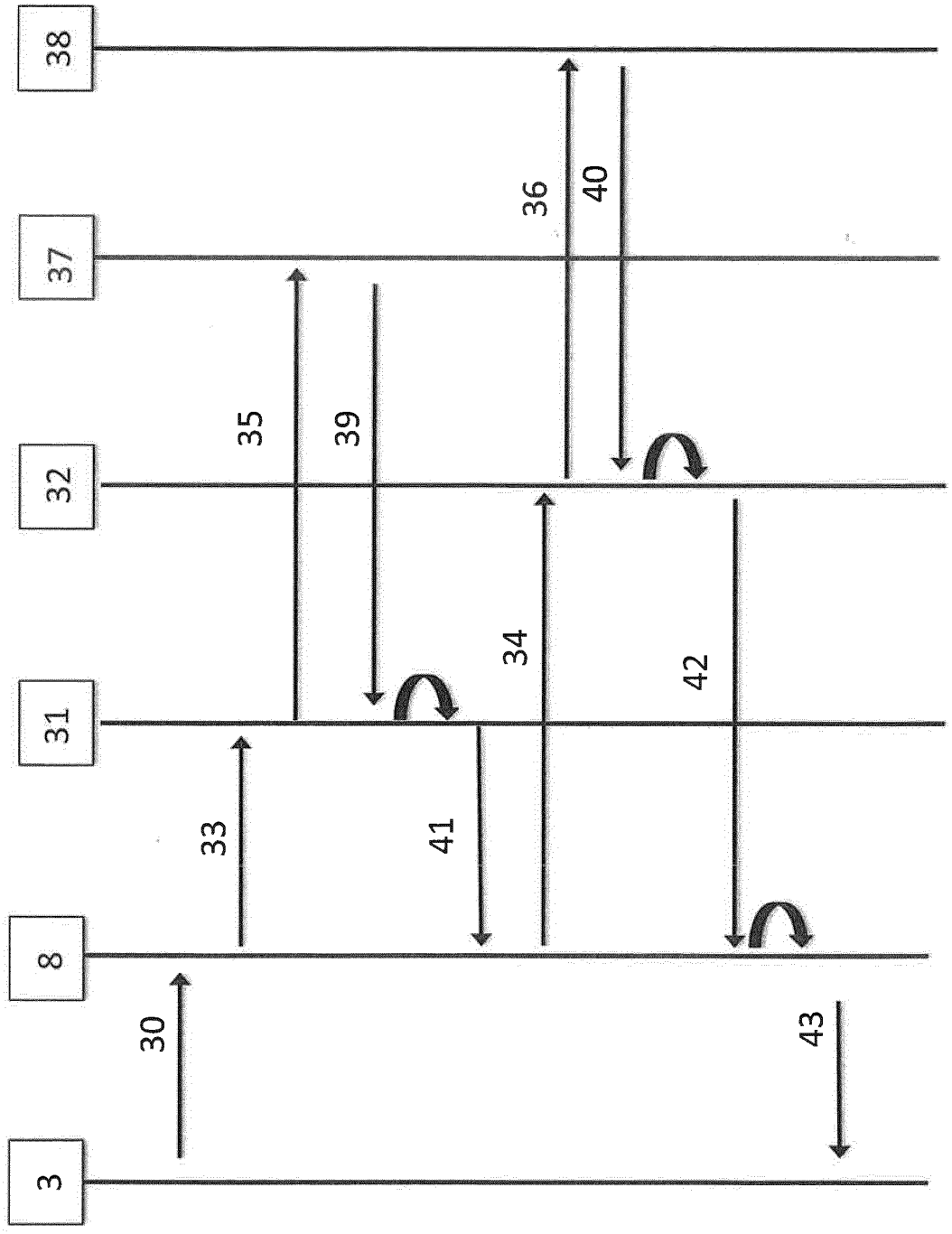

Fig 5