(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 477 597**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.02.2011 E 11704442 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.04.2014 EP 2537286**

(54) Título: **Procedimiento de autentificación biométrica, sistema de autentificación y programa correspondiente**

(30) Prioridad:

01.03.2010 FR 1051464
19.02.2010 FR 1051216

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.07.2014

(73) Titular/es:

COMPAGNIE INDUSTRIELLE ET FINANCIÈRE D'INGÉNIERIE "INGENICO" (100.0%)
192 avenue Charles de Gaulle
92200 Neuilly sur Seine, FR

(72) Inventor/es:

NACCACHE, DAVID

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento de autentificación biométrica, sistema de autentificación y programa correspondiente

1. Campo de la invención

El campo de la invención es el de la autentificación de usuarios mediante biometría.

Más precisamente, la invención se refiere a los sistemas de autentificación biométrica que permiten a los usuarios efectuar una acción predeterminada, como por ejemplo realizar un pago.

2. Antecedentes de la invención

La biometría se utiliza comúnmente con el fin de identificar y/o autentificar a los usuarios en base a características físicas individuales.

Una identificación de ese tipo mediante biometría, realizada mediante un sistema de autentificación biométrica, comprende las tres etapas principales siguientes:

- captura de una muestra biométrica de referencia que proceda del usuario autorizado (por ejemplo una imagen de referencia de un usuario autorizado);

- creación de un fichero de referencia, o “firma de referencia” (que comprende al menos un elemento característico de la imagen de referencia), mediante un tratamiento específico aplicado a la muestra biométrica de referencia, y posteriormente almacenamiento de este fichero de referencia;

- verificación en la que, de la misma manera que en las etapas de captura y creación antes citadas, se realiza una captura de una muestra biométrica a comparar procedente del usuario a autentificar y una creación de un fichero a comparar, o “firma a comparar”, y posteriormente la comparación del fichero de referencia con el fichero a comparar para determinar su tasa de similitud y tomar la decisión que se imponga.

De ese modo, las informaciones almacenadas no son las muestras biométricas, sino unos modelos matemáticos de estas muestras que distinguen una muestra biométrica de otra. Este modelo se denomina una “firma” o una “plantilla”.

La creación de una firma de referencia se efectúa durante la fase denominada de afiliación (o de aprendizaje) que reagrupa las etapas de captura de la muestra biométrica de referencia, de creación y de almacenamiento de la firma de referencia y de almacenamiento de informaciones sobre la identidad del usuario como su nombre, su apellido, su identificador (número de identificación personal).

La autentificación de un usuario mediante biometría puede basarse particularmente en la medición (o captura) de al menos una de las muestras biométricas siguientes, o una combinación de una o varias de las muestras biométricas siguientes:

- su huella digital;

- su huella palmar (huella de la mano);

- la huella de su retina;

- la huella de su iris;

- la huella de su rostro (la forma de su rostro);

Un inconveniente de estos sistemas de autentificación biométrica de la técnica anterior reside en su lentitud cuando se utilizan para referenciar un gran número de usuarios (por ejemplo para controlar el acceso al metro en una gran población o autentificar a un usuario de una tarjeta bancaria).

En efecto, la duración de la etapa de verificación, durante la que se toma la decisión de autentificación propiamente dicha, depende del número de usuarios referenciados en el sistema de autentificación. Cuanto mayor sea el número de usuarios referenciados, mayor será el número de comparaciones potenciales a efectuar para determinar o no la autentificación de un usuario.

De ese modo, cuanto mayor sea el número de usuarios referenciados, más lento será sistema. Además, el crecimiento del número de usuarios tiende a aumentar la probabilidad de colisión entre datos biométricos y por tanto la fiabilidad general del sistema (fenómeno conocido para el experto en la técnica con la expresión de “falso positivo”).

Un corolario de este último inconveniente es que es difícil realizar un método de pago con la ayuda de datos biométricos. En efecto, para poder realizar un método de pago de ese tipo, es necesario comparar los datos

biométricos del usuario con un gran número de datos biométricos de otros usuarios, datos que pertenecen de manera muy probable a los establecimientos financieros y que por tanto pueden llegar a ser complejos de obtener. O el usuario, por principio, no debe divulgar informaciones relativas a la banca de la que es cliente y la comparación de los datos biométricos del usuario se debe realizar sobre el conjunto de los datos registrados en el sistema de autentificación.

La invención se aplica de modo particular a unos dispositivos móviles tales como los teléfonos móviles, los GPS portátiles, los asistentes digitales personales (denominados PDA), los ordenadores portátiles y cualquier otro aparato ("dispositivo móvil") que tenga vocación de comunicarse a través de una red de telecomunicación móvil, para disponer o ser la fuente de una información de localización precisa o aproximada y para ser llevado generalmente al alcance de la mano de sus propietarios.

La invención se aplica igualmente, en al menos un modo de realización, a unos dispositivos de verificación y de adquisición de transacciones tales como los terminales de pago y de verificación de identidad, las cerraduras electrónicas, las cajas registradoras y los puestos de control de acceso o los puestos de transportes colectivos ("terminal de transacciones"). Teniendo estos dispositivos vocación de comunicar a través de una red de telecomunicación y de tener una localización geográfica precisa o aproximada conocida para sus gestores.

El documento de patente US 6 591 242 B1 de E. Karp publicado el 8 de julio de 2003 expone un sistema de trazado de un usuario cuando atraviesa unos lugares predeterminados empleando unos parámetros biométricos para su autentificación.

El documento de patente WO 2009/128854 A1 de W. Camp y adjudicado a Sony Ericsson Mobile Comm AB publicado el 22 de octubre de 2009 expone una base de datos indexada sobre un identificador de estación base en el seno de un procedimiento de autentificación.

El documento de patente US 2003/140246 A1 de D. Kammer publicado el 24 de julio de 2003 expone una base de datos de reglas de seguridad indexada sobre la posición del dispositivo.

Los documentos de patente WO 2006/128171 A2 de G. Di Mambro et ál. y adjudicado a Porticus Technology Inc. publicado el 30 de noviembre de 2006, y US 2006/120568 A1 de P. McConville publicado el 8 de junio de 2006 exponen unos procedimientos de autentificación biométrica en el seno de los que se adquiere la posición del usuario.

3. Objetivos de la invención

La invención tiene por objetivo particularmente paliar estos inconvenientes de la técnica anterior.

Más precisamente, un objetivo de la invención, en al menos uno de sus modos de realización, es proporcionar una técnica de autentificación biométrica que sea rápida y fiable, en el caso del sistema que referencie a un gran número de usuarios, para permitir al usuario realizar una acción tal como un pago.

La invención tiene de ese modo por objetivo proporcionar una técnica de ese tipo que sea igualmente ergonómica para el usuario.

Otro objetivo de la invención es proporcionar una técnica de ese tipo que sea poco costosa y fácil de realizar.

4. Exposición de la invención

La invención propone una solución novedosa que no presenta el conjunto de esos inconvenientes de la técnica anterior, en la forma de un procedimiento de autentificación biométrico de un usuario a autentificar entre una pluralidad de usuarios acerca de un sistema de autentificación que almacena un conjunto de datos biométricos de referencia asociados cada uno a uno de dichos usuarios, comprendiendo las etapas de:

- proporcionar por el usuario a autentificar, un dato biométrico de autentificación, con la ayuda de un dispositivo de obtención de datos biométricos de un terminal de transacciones;

- búsqueda entre un subconjunto de dicho conjunto de datos biométricos de referencia almacenados por dicho sistema de autentificación, de un dato biométrico de referencia que corresponda a dicho usuario a autentificar, en función de dicho dato biométrico de autentificación,

Según la invención, dicha etapa de búsqueda comprende una etapa de filtrado de dichos datos de dicho conjunto de datos biométricos en función:

- de una estación base de una red de comunicación móvil; y

- de un conjunto de dispositivos móviles para los que se activa un indicador de conexión para dicha estación base,

y estando dicho terminal de transacciones sensiblemente próximo a una zona de cobertura de dicha estación base.

De ese modo, la invención permite restringir fuertemente el número de datos biométricos de referencia para los que es necesario realizar una comparación con los datos biométricos suministrados por el usuario a autentificar. Esta restricción permite acelerar en gran medida el proceso de autentificación y por ejemplo realizar un pago utilizando procedimientos de autentificación de la invención. En efecto, el número de dispositivos móviles conectados simultáneamente a una estación base es extremadamente reducido con relación a un número potencial de usuarios para los que sería obligatorio realizar la búsqueda en el procedimiento de la invención. La operación de autentificación, y por tanto la operación de pago es por lo tanto mucho más rápida. Esta operación de autentificación es igualmente mucho más segura puesto que la localización implícita del dispositivo móvil del usuario (el dispositivo móvil está igualmente conectado a la estación base, sin que la etapa de búsqueda sea infructuosa), asegura que el usuario que desea realizar el pago se encuentra en el emplazamiento en el que tiene lugar la autentificación.

El interés de este procedimiento de autentificación no está, por supuesto, limitado al pago. Es totalmente posible realizar un procedimiento de ese tipo para realizar un control de acceso en base a la posesión de un dispositivo móvil, por ejemplo en el caso de un acceso a una empresa. La estación base se sustituye entonces por un punto de acceso Wi-Fi y el dispositivo móvil debe poseer entonces unas capacidades de conexión Wi-Fi.

De ese modo, la invención se basa en un enfoque novedoso e inventivo de la autenticación biométrica en un sistema que referencia a un gran número (por ejemplo unos millones) de usuarios, según el que las informaciones de referencia asociadas a los usuarios del sistema se filtran en función de los usuarios que disponen de un dispositivo móvil conectado a la estación base cuya zona de cobertura cubre el emplazamiento del terminal de transacciones. De ese modo, el número de usuarios para los que es necesario comparar los datos biométricos se restringe en función de la localización misma del usuario que efectúa la acción, tal como el pago. No es por tanto necesario comparar los datos biométricos del usuario con un gran número de datos biométricos, sino con un número mucho más restringido (del orden del millar), lo que es netamente más rápido y comporta un riesgo mucho menor de falsos positivos.

De ese modo, la autentificación del usuario se realiza bajo un subconjunto de dicho conjunto de datos biométricos de referencia, identificados por la estación base de la red de comunicación del operador de comunicación o del suministrador de servicios.

Este enfoque permite una identificación rápida de un usuario, y comprendido en un sistema que comprende un gran número de usuarios referenciados, mediante el filtrado del conjunto de las informaciones de referencia y procediendo a su división en varios subconjuntos.

Según un modo de realización particular de la invención, dicha etapa de filtrado comprende:

- una etapa de identificación de dicha estación base que cubre dicha zona de cobertura en la que se sitúa dicho terminal de transacciones;

- una etapa de identificación de dicho conjunto de dispositivos móviles para los que se activa un indicador de conexión para dicha estación base, proporcionando un conjunto de identificadores de dispositivos móviles candidatos;

- una etapa de obtención de dicho subconjunto de dicho conjunto de datos biométricos de referencia en función de dicho conjunto de identificadores de los dispositivos móviles candidatos.

Según una característica particular de la invención dichos datos biométricos pertenecen al grupo que comprende:

- las huellas digitales;

- las huellas palmares;

- las huellas de retina;

- las huellas del iris;

- las formas del rostro;

- las combinaciones de dichas informaciones biométricas antes citadas.

Según un modo de realización particular de la invención, dicho procedimiento de autentificación biométrica comprende además una etapa de introducción, por dicho usuario, de un código confidencial.

De ese modo, la invención permite consolidar la confirmación de la autentificación que se ha proporcionado tras la búsqueda y tras la comparación de los datos biométricos del usuario.

Según un modo de realización particular de la invención, dicha etapa de filtrado comprende además una etapa de

introducción de una información representativa del sexo de dicho usuario.

De ese modo, se divide estadísticamente por dos el tiempo necesario para la autentificación. Esta etapa de introducción tiene lugar en el terminal de transacciones.

Según un modo de realización particular de la invención, dicha etapa de filtrado comprende además una etapa de selección de un operador telefónico en el que está registrado dicho dispositivo móvil de dicho usuario.

De ese modo, la realización de la invención no está limitada a un único operador telefónico. Esta etapa de introducción tiene lugar en el terminal de transacciones.

Según una característica particular de la invención, dicho procedimiento comprende además una etapa de introducción, por dicho usuario, de un código confidencial.

Según una característica particular de la invención, dicho código confidencial se transmite a dicho sistema de autentificación simultáneamente a dichos datos biométricos suministrados por dicho usuario.

Según un modo de realización particular de la invención, dicho terminal de transacciones es un terminal de pago móvil conectado a dicha red de comunicación móvil a la que pertenece dicha estación base.

Según una característica particular de la invención dicho terminal de transacciones está conectado a dicha estación base.

Según un modo particular de realización de la invención, dicho procedimiento comprende además una etapa de transmisión, a dicho terminal de transacciones, de dicho subconjunto de dicho conjunto de datos biométricos y porque dicha etapa de filtrado se realiza en el seno de dicho terminal de transacciones.

Según un modo de realización particular de la invención, dicho procedimiento comprende además una etapa de transmisión hacia una estación base de destino a la que dicho usuario es susceptible de conectarse, de dichos datos biométricos que se refieren a dicho usuario, siendo realizada dicha transmisión a partir de una estación base actual a la que dicho usuario está conectado.

La invención se refiere igualmente a un sistema de autentificación biométrico de un usuario a autentificar entre una pluralidad de usuarios en un sistema de autentificación que almacena un conjunto de datos biométricos de referencia cada uno asociado a uno de dichos usuarios, comprendiendo unos medios de:

- suministro por dicho usuario a autentificar, de un dato biométrico de autentificación, con la ayuda de un dispositivo de obtención de datos biométricos de un terminal de transacciones;

- búsqueda entre un subconjunto de dicho conjunto de datos biométricos de referencia almacenados por dicho sistema de autentificación, de un dato biométrico de referencia que corresponda a dicho usuario a autentificar, en función de dicho dato biométrico de autentificación.

Según la invención dichos medios de búsqueda comprenden unos medios de filtrado de dichos datos de dicho conjunto de datos biométricos en función:

- de una estación base de una red de comunicación móvil; y

- de un conjunto de dispositivos móviles para los que se activa un indicador de conexión para dicha estación base,

y dicho dispositivo de obtención de datos biométricos está sensiblemente próximo a una zona de cobertura de dicha estación base.

La invención se refiere igualmente a un producto programa de ordenador que puede descargarse desde una red de comunicación y/o registrarse en un soporte legible por un ordenador y/o ejecutable por un procesador, que comprende unas instrucciones de código de programa para la realización del procedimiento de autenticación biométrica descrito anteriormente.

5. Lista de las figuras

Surgirán más claramente otras características y ventajas de la invención con la lectura de la descripción a continuación de un modo de realización particular, dado a título de ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, entre los que:

- la figura 1 presenta el contexto de realización del procedimiento de autentificación biométrica según la invención;

- la figura 2 ilustra las etapas de un modo de realización particular del procedimiento según la invención.

6. Descripción del modo de realización de la invención

6.1. Principio general

El principio general de la invención se basa en la delegación de la localización y de la identificación de un usuario en una pluralidad de equipos de una red de comunicación con el fin de que se facilite proporcionar una confirmación de autentificación en base a los datos biométricos suministrados por el usuario. Estos datos biométricos se comparan con un conjunto de datos biométricos relativos a los usuarios referenciados en un sistema de autentificación biométrica. Según la invención, la localización geográfica del usuario, por ejemplo por medio de su dispositivo móvil (teléfono móvil, PDA, tablet), permite reducir de manera drástica el número de comparaciones a realizar para por una parte identificar y por otra parte autentificar, al usuario.

Una de las características principales de las redes de terminales móviles es que un dispositivo móvil, cualquiera que sea, está permanentemente cubierto con una estación base (denominada “BTS” de “Base Transceiver Station”).

Cuando el aparato sale de la zona de cobertura de una estación base, se transfiere a otra estación base. Esta transferencia se efectúa con el fin de mejorar la calidad de la señal.

En otros términos, el operador de telecomunicaciones conoce en tiempo real la posición geográfica aproximada de un dispositivo móvil en la red de telecomunicación móvil; el dispositivo móvil se sitúa en la zona de cobertura de la estación base a la que está adscrito.

El procedimiento de la invención, de manera general, aprovecha esta localización. El procedimiento de la invención permite por un lado utilizar un dispositivo móvil poseído por el usuario como un vector que permite la autentificación y por otra parte evitar los problemas de lentitud y de colisión (falsos positivos) inherentes a los sistemas de autentificación que referencian un gran número de usuarios, particularmente los sistemas de autentificación biométricos. Además, el procedimiento de la invención funciona cualquiera que sea el tipo de dispositivo móvil del usuario; no es necesario que el usuario disponga de un dispositivo móvil de última generación o muy sofisticado para poder beneficiarse de las ventajas aportadas por la invención.

Dichos sistemas pueden utilizarse para realizar simplemente unos pagos, sin que sea necesario que el usuario utilice una tarjeta bancaria o disponga de un dispositivo móvil particular.

Dichos sistemas pueden utilizarse igualmente para controlar el acceso a un edificio, empresa, zona geográfica, espectáculo, evento, instalación o medio de transporte en una gran población, y de ese modo referenciar un gran número de usuarios.

Se considera en lo que sigue, para ilustrar el procedimiento según la invención, un sistema de ese tipo que permita realizar, mediante autentificación biométrica, un pago en un centro comercial. En este caso, un usuario que desee realizar una compra se autentifica gracias por un lado a su dispositivo móvil y por otro lado a una o varias características biométricas.

Según la invención, con el fin de evitar una lentitud demasiado excesiva del sistema, y permitir a los usuarios referenciados no ser retrasados por la autentificación biométrica y por lo tanto realizar rápidamente la transacción, se realiza una localización del dispositivo móvil del usuario.

Más particularmente, esta información de localización se obtiene mediante la comparación de los datos biométricos del usuario con un número restringido de datos biométricos, a saber los datos biométricos de los otros usuarios que se sitúan en la misma zona de localización que el usuario, es decir conectados al mismo equipo del operador de comunicaciones, como por ejemplo una estación base. Como regla general, el número máximo de usuarios conectados a una estación base es del orden del millar. Se realiza por tanto un filtrado de los datos biométricos a comparar con los suministrados por el usuario.

De ese modo, en lugar de verificar la autenticidad de un usuario entre todos los usuarios referenciados, lo que es altamente consumidor de tiempo y susceptible de “falsos positivos”, el procedimiento según la invención permite verificar la autenticidad de un usuario en el subconjunto de usuarios referenciados (del orden del millar), reduciendo de ese modo la duración de la autentificación y su eficacia.

Se presenta, en relación con la figura 1, un contexto técnico general de realización del procedimiento de la invención. Se conecta una estación base (SB1), por intermedio de una red de comunicación (R1), a un servidor de autentificación (SRV-AUTH). La estación base posee una zona de cobertura (ZC-SB1) en el seno de la que se identifican y conectan o están recientemente conectados unos dispositivos móviles (por ejemplo los terminales T1 a T5). La conexión de un dispositivo se define por la presencia de un indicador de conexión del dispositivo móvil. Por ejemplo, si el dispositivo móvil está conectado, se sitúa un indicador de conexión. Si el dispositivo móvil estaba conectado recientemente (por ejemplo hace menos de cinco minutos) se sitúa igualmente un indicador de conexión para el dispositivo móvil. El servidor de autentificación (SRV-AUTH), que en un modo de realización específica de la invención puede ser el MSC (del inglés “Mobile services Switching Center”) o el VLR (del inglés “Visitor Location Register”) o el HLR (del inglés “Home Location Register”) comprende una base de datos biométricos (BDD-A) que

comprende más particularmente unos datos biométricos de usuarios de dispositivos móviles. Cuando el servidor de autentificación es el MSC, éste contiene ventajosamente los datos biométricos sólo de los terminales T1 a T5 conectados a la estación base (SB1). En el marco de la realización de la invención, se dispone igualmente de un terminal de transacciones TP1 que se sitúa en la zona de cobertura (ZC-SB1) de la estación base (SB1) y que comprende unos medios de obtención de datos biométricos (como un escáner de huellas digitales). En el marco de este ejemplo, se considera que el usuario U2, que dispone del dispositivo móvil T2 desea efectuar una compra y pagar ésta, utilizando el terminal de transacciones TP1. Por supuesto, este sistema se puede realizar en otros casos de figuras, como la autentificación de un puesto de fronteras o el acceso a una zona de seguridad. De manera general, en el marco de la invención, el terminal de transacciones comprende o está conectado a un dispositivo de obtención de datos biométricos. En numerosos casos, el terminal de transacciones integra directamente el dispositivo de obtención de datos biométricos.

Previamente a la gestión de la identificación y de la autentificación del usuario según la invención, se prevé una fase de registro del usuario que desea beneficiarse de las ventajas proporcionadas por la invención acerca de un suministrador de servicios, como un operador de comunicaciones.

En el transcurso de esta fase de registro, el usuario entre otros datos, presenta un documento de identidad, selecciona u obtiene un código confidencial (por ejemplo un código que comprende cuatro caracteres decimales) y uno o varios datos biométricos denominados de referencia (por ejemplo una huella digital). Estos datos se registran de manera apropiada por el suministrador de los servicios. Esta fase de registro se puede realizar o bien por intermedio de un servicio Web al que el usuario se conecta, o bien de manera preferente físicamente, en el seno de un emplazamiento dedicado por el suministrador de los servicios, por ejemplo para obtener las informaciones biométricas de manera segura.

Entre las ventajas proporcionadas por la invención, se encuentran las ventajas siguientes:

- totalmente desprovisto de la necesidad de equiparse con un nuevo material: no es necesario suministrar un nuevo material al usuario. Esta solución es por tanto económicamente muy interesante.

- la solución de la invención es totalmente “manos libres”: durante la operación de pago, el usuario no utiliza más que su mano. No tiene necesidad de sacar su teléfono de su bolsillo y extraer una tarjeta bancaria de su portafolio (menos riesgos de robos).

- funciona con absolutamente cualquier tipo de teléfono: no es necesario cambiar el dispositivo móvil para que el sistema funcione. El simple hecho de disponer de un dispositivo móvil es suficiente.

- el sistema es simple para el usuario, lo que permite una adopción rápida.

- el sistema es seguro: para poder cometer un fraude, es necesario por una parte robar el dispositivo móvil del usuario, cortarle el dedo (cuando los datos biométricos son representativos de la huella digital) y determinar su código confidencial. El fraude es por lo tanto muy poco probable.

- finalmente, los operadores de telecomunicaciones están siempre a la búsqueda de medios para limitar la volatilidad de sus abonados (en otros términos, para fidelizar a sus abonados), el hecho de asociar unas funciones de pago a un dispositivo móvil es por naturaleza debilitador de la volatilidad y fidelizador del abonado.

6.2. Descripción de un modo de realización

Se presentan ahora, en relación con la figura 2, las principales etapas del procedimiento de autentificación biométrica según la invención en la que el terminal de transacciones es un terminal de pago que permite realizar unas compras y el dispositivo móvil es un teléfono. Este terminal de transacciones comprende, en este modo de realización, un dispositivo de obtención de datos biométricos, que es por ejemplo un lector de huellas digitales.

De manera general, en el momento de realizar una compra, un usuario debe proporcionar dos informaciones mediante la interfaz del sistema de autentificación, tal como el terminal de transacciones:

- un dato biométrico de autentificación 10;

- una información de confirmación del pago 14 (tal como un código confidencial, o incluso únicamente una validación del tipo “OK”).

La información biométrica de autentificación 10 se utiliza durante una etapa de búsqueda 12 del dispositivo móvil del usuario, entre una pluralidad de terminales móviles conectados a una estación base de la que depende el terminal de transacciones utilizado para suministrar el dato biométrico. Esta búsqueda se efectúa comparando el dato biométrico de autentificación con una pluralidad de datos biométricos de referencia previamente almacenados en el seno de la red del operador.

Más precisamente, en un primer modo de realización de la invención, el procedimiento de autentificación biométrica comprende las etapas siguientes:

- una etapa de obtención 10 de un dato biométrico del usuario (por ejemplo una huella digital obtenida a partir de un lector de huellas idóneo montado por ejemplo en un terminal de transacciones);

- una etapa de transmisión 11 de los datos biométricos a un servidor de autentificación (que puede situarse por ejemplo en el seno de la red de telecomunicaciones gestionada por el operario de comunicaciones). En este modo de realización, la transmisión de los datos biométricos viene acompañada de la transmisión del montante de la transacción previamente introducido por el comerciante en cuyo establecimiento el usuario desea realizar una compra.

- una etapa de búsqueda 12, del dato biométrico de referencia correspondiente al dato biométrico previamente obtenido, entre la pluralidad de datos biométricos de referencia que corresponden a la pluralidad de usuarios conectados a la estación base del operador de comunicaciones. Se realiza de ese modo un filtrado inteligente de los datos biométricos de referencia a comparar.

Esta etapa de búsqueda/filtrado comprende varias etapas:

- una etapa de obtención 12-1 de al menos un identificador de la estación base de referencia en la zona en la que se sitúa el dispositivo de obtención de datos biométricos (por ejemplo el terminal de transacciones);

- una etapa de obtención 12-2 de un conjunto de identificadores de dispositivos móviles conectados a dicha al menos una estación base de referencia;

- una etapa de obtención 12-3 de una pluralidad de datos biométricos a partir de los identificadores de dispositivos móviles, que corresponde al filtrado propiamente dicho;

- una etapa de comparación 12-4 de estos datos biométricos con el dato biométrico obtenido por el dispositivo de obtención de datos biométricos.

- cuando el dispositivo móvil del usuario se identifica, a partir del dato biométrico obtenido por parte del usuario y del conjunto de los datos biométricos de los usuarios cuyos terminales están conectados a la estación base de referencia, el procedimiento comprende una etapa de transmisión 13 al usuario de una solicitud de obtención de un código confidencial, seguida de una etapa de introducción 14 de este código confidencial y de una etapa de validación de la transacción 15.

- este código confidencial es el código proporcionado en el transcurso de la fase de registro;

- el código confidencial se introduce en el terminal de transacciones, como de costumbre, por el usuario.

- el código confidencial se verifica y la transacción se valida por el operador: lo deduce de la cuenta del usuario y lo abona en la cuenta del comerciante.

Si la etapa de búsqueda no permite identificar al dispositivo móvil del usuario como conectado a la estación base, se pueden presentar varios casos:

- abandono puro y simple de la transacción;

- solicitud del suministro de una tarjeta de pago: la transacción se prosigue entonces clásicamente utilizando una tarjeta de pago y el código confidencial de la tarjeta de pago del usuario.

Cuando el código confidencial del procedimiento de la invención, introducido con ocasión de la validación, no es válido, se pueden presentar varios casos:

- abandono puro y simple de la transacción;

- posibilidad de realizar una nueva tentativa (hasta tres tentativas por ejemplo). Si fracasan tres tentativas, la cuenta del usuario se bloquea y no podrá realizar el pago mediante este medio. Deberá contactar con el suministrador del servicio para reactivar su cuenta.

En un segundo modo de realización de la invención, la introducción del código confidencial es opcional. En efecto, esta introducción es una medida de seguridad suplementaria, pero no es obligatoria. Permite no obstante asegurar que el usuario dispone de esta información. Se concibe, en al menos otro modo de realización, la conversión de esta introducción es obligatoria únicamente si la transacción excede de una cierta cantidad, parametrizable en función del usuario, por ejemplo durante su fase de registro.

En un tercer modo de realización, el código no es confidencial y sirve únicamente para discriminar (identificar) los datos biométricos del usuario más rápidamente.

6.3. Búsqueda y comparación de las informaciones

La identificación y la autentificación propiamente dicha tienen lugar, durante una fase de búsqueda 12, que tiene en

cuenta el dato biométrico suministrado por el usuario 10.

El dato biométrico de autentificación 10 corresponde a una muestra biométrica “simple” del usuario a autentificar, tal como una huella digital, una huella palmar, una huella de retina, una huella de iris, una forma de rostro, etc., o en una combinación de varias de estas muestras “simples”, por ejemplo una combinación de una huella digital y de una huella de iris.

La fase de búsqueda 12 comprende de manera clásica, además de las etapas anteriormente mencionadas, al menos dos etapas: una primera etapa que consiste en determinar una “firma” biométrica del usuario a autentificar, a partir del dato biométrico de autentificación suministrado, y una segunda etapa que consiste en comparar esta “firma” biométrica con las firmas, o datos biométricos de referencia contenidos en una base de datos previamente identificada, con el fin de proporcionar una decisión de autentificación.

La primera etapa corresponde a la aplicación de un tratamiento específico clásico a la muestra biométrica, de manera que se obtenga una firma que pueda compararse a continuación con otras informaciones del mismo tipo. Esta firma se obtiene mediante los algoritmos de creación de firma, conocidos por sí mismos en el campo de la biometría.

La segunda etapa efectúa las comparaciones sucesivas de la firma obtenida durante la etapa precedente, con cada uno de los datos biométricos de referencia, o firmas de referencia almacenadas en la base referida, *únicamente para los terminales conectados a las estaciones base de referencia*. En función de los criterios predeterminados, se proporciona la decisión de autentificación, positiva cuando una firma de referencia corresponde a la firma obtenida, negativa, cuando no corresponde a ninguna de las firmas de referencia contenidas en la base, *únicamente para los terminales conectados a las estaciones base de referencia*.

De ese modo, se comprende fácilmente que esta segunda etapa de autentificación es más rápida en el procedimiento según la invención, porque el número máximo de comparaciones que puede efectuar corresponde a un número de firmas limitado, y no al número total de firmas almacenadas en el sistema de autentificación.

Además, otra ventaja del procedimiento de autentificación de la invención reside en el reparto en sí de los datos biométricos entre las diferentes estaciones base.

En efecto, el procedimiento de la invención minimiza los riesgos de colisión, es decir los riesgos de tener, para una misma estación base, unos datos biométricos de usuarios próximos susceptibles de ser considerados como idénticos por un sistema de autentificación. Esta ventaja está ligada directamente a la utilización de las estaciones base y de los dispositivos móviles para permitir un filtrado y conducir a la autentificación del usuario.

Según un modo de realización específica de la invención, el terminal de transacciones está directamente conectado a la red de comunicaciones móviles del operador. En efecto, en los modos de realización anteriormente presentados, el terminal de transacciones está conectado a una red por intermedio de un acceso cableado. Esto significa que el procedimiento de autentificación debe realizar una identificación de la estación base y de los dispositivos móviles conectados (o recientemente conectados) a esta estación base para realizar un filtrado de los datos biométricos a comparar.

En este modo de realización específica de la invención, el terminal de transacciones se conecta por sí mismo a una red móvil del operador de comunicaciones. De ese modo, la obtención del identificador de la estación base y de los identificadores de los dispositivos móviles se facilita ampliamente: la estación base es aquella a la que el terminal de transacciones se conecta y los dispositivos móviles son los que están conectados a esta misma estación base.

Además del procedimiento de autentificación tal como el descrito anteriormente, la invención trata igualmente sobre un sistema de autentificación que comprende unos medios de realización del procedimiento anteriormente descrito.

6.4. Otros modos de realización y características complementarias

6.4.1. Transmisión del código confidencial

Según una característica particular de la invención, el código confidencial introducido por el usuario se transmite al operador con los datos biométricos (es decir o bien al mismo tiempo que los datos biométricos o bien antes de los datos biométricos). Esto presenta una gran ventaja práctica porque esto convierte a la identificación del usuario en casi inmediata.

En efecto, cuando se transmite el código confidencial al operador con la huella, el operador reduce el subconjunto de datos biométricos de referencia a comparar (subconjunto ya muy reducido), de los usuarios presentes próximos a la estación base, a la de los usuarios presentes próximos a la estación base y que tienen un código confidencial dado.

La probabilidad de que dos usuarios tengan el mismo código confidencial es ya muy reducida (pero no es nula). En el raro caso de que se produzca una colisión de este tipo, esta característica particular de la invención permite separar a los dos usuarios mediante la comparación de sus huellas con la huella transmitida por el terminal de transacciones. Es importante observar que incluso si ha sido localizado en el campo de la estación base un único

usuario que tenga el código confidencial transmitido por el terminal de transacciones, la comparación de los datos biométricos continúa siendo siempre necesaria para la validación de una transacción.

6.4.2. Conectividad del terminal de transacciones

Según un modo de realización particular de la invención, la posición geográfica del terminal de transacciones se deduce igualmente, y de manera automática, de su aceptación por una estación base dada (lo que supone que el terminal de transacciones está equipado con una tarjeta SIM, lo que es muy corriente). Esto es importante porque una realización de ese tipo hace abstracción total de cualquier noción de coordenada geográfica. El hecho para unos teléfonos móviles de estar en el campo de la estación base que cubre de ese modo un terminal de transacciones significa que los teléfonos móviles están en la proximidad del terminal de transacciones en cuestión. Esto es suficiente para la comparación. Las grandes ventajas de este método son:

1. No requiere tomas de mediciones geográficas sobre el terreno;

2. Se adapta de manera automática a unos vendedores itinerantes que llevan con ellos un terminal de transacciones móviles y van de puerta a puerta.

6.4.3. Extensión de la zona de localización

Según una característica particular de la invención, la comparación de la huella enviada por el terminal de transacciones no está limitada a las huellas de los usuarios presentes en el campo de la estación base que cubre el terminal de transacciones. En una variante de ese tipo la comparación de la huella enviada por el terminal de transacciones se extiende a las huellas de los usuarios presentes en los campos de las estaciones base adyacentes o próximas a la estación que cubre al terminal de transacciones. En efecto, no es raro que por razones de saturación de la red un usuario pueda estar adscrito a una estación base un poco más alejada pero menos cargada en un momento dado.

6.4.4. Multiplicidad de los usuarios y de los terminales

Según un modo de realización particular de la invención, durante la fase de registro de los usuarios, el sistema permite asociar varias huellas digitales al mismo teléfono (por ejemplo el mismo teléfono puede servir para identificar diferentes miembros de una misma familia que utilicen este aparato por turnos). Incluso una misma huella digital podría asociarse completamente a varios teléfonos (por ejemplo, una persona puede poseer varias suscripciones y pagar con no importa cuál de los teléfonos que posea).

6.4.5. Selección del operador móvil

Según un modo de realización particular de la invención, el procedimiento comprende una etapa de identificación de un operador de comunicaciones hacia el que se transmiten los datos biométricos del usuario. En efecto, el problema planteado por la multiplicación de los operadores es que una vez que se ha adquirido la huella digital, el terminal de transacciones debe saber a cuál operador conviene hacerla llegar, para comparación. Esta identificación se puede efectuar según varios métodos:

- el terminal de transacciones ofrece a un comerciante la elección entre diversos operadores (por ejemplo “Operador #1: teclee 1, Operador #2 teclee 2, Operador #3, teclee 3”). El comerciante plantea la cuestión oralmente al usuario, e introduce, en el teclado del terminal de transacciones, la información (en este caso 1, 2 o 3) lo que permite encaminar la huella a un operador en particular con la finalidad de comparación.

- o también los datos biométricos se transmiten de manera automática a todos los operadores que se encargan de compararla con sus propias bases de datos.

- o también se solicita al usuario introducir su código confidencial sobre el terminal de transacciones antes de transmitir los datos biométricos al operador. El código confidencial codifica entonces una información que indica de qué operador se trata (por ejemplo en la última cifra decimal del código confidencial será una cifra que caracteriza al operador: 1 para el Operador #1, 2 para el Operador #2, 3 para el Operador #3, etc.). En base a esta información codificada denominada “identificador del operador codificada en el código confidencial”, el terminal de transacciones encamina los datos hacia el operador correcto.

- o también el gestor del sistema crea una base de datos central que reagrupa los identificadores biométricos de todos los usuarios, cualquiera que sea su operador. Los operadores suministran en tiempo real las informaciones de posición aproximada de sus abonados presentes en la base de datos central y es el gestor del sistema el que efectúa las operaciones de identificación de la huella.

Es importante observar, en todo caso, que la presentación del código confidencial es facultativa. Por supuesto, una realización sin código confidencial genera menos ventajas, pero siempre funcionará.

Según un modo de realización particular de la invención, cuando el usuario es un abonado de un operador extranjero (OE) que tenga un acuerdo de itinerancia (“roaming agreement”) con un operador nacional (ON), procede

de la manera siguiente: la presencia de un abonado extranjero en el campo de la estación base de un ON es una información conocida para el ON. El ON efectúa entonces las dos operaciones siguientes (en un orden cualquiera o incluso simultáneamente, para ganar tiempo): 1. El ON busca los datos biométricos y el código confidencial en su base de datos. Si los datos biométricos y el código confidencial se encuentran en la base de datos del ON, el sistema procede como se ha explicado anteriormente. 2. El ON transmite los datos biométricos a comparar y el código confidencial introducido por un usuario a todos los OE con los que tiene un acuerdo de itinerancia y cuyos abonados están presentes en la proximidad de la estación de base relacionada. Los OE proceden a la comparación de los datos biométricos y del código confidencial transmitido por el ON con sus bases de datos. Si los datos biométricos y el código confidencial se encuentran en la base de datos de un OE, el OE en cuestión señaliza este hecho al ON, y el sistema procede como se ha explicado anteriormente.

Según un modo de realización particular de la invención, cuando el usuario es un abonado de un operador extranjero (OE) que tenga un acuerdo de itinerancia ("roaming agreement") con un operador nacional (ON), se procede así: la presencia de un abonado extranjero en el campo de la estación base de un ON es una información conocida para el ON. El ON efectúa entonces una solicitud de transferencia de informaciones al OE. Con la recepción de una solicitud de ese tipo de transferencia de informaciones, el OE transmite al ON los datos biométricos del abonado así como el código confidencial asociado. De ese modo, el abonado extranjero es añadido dinámicamente al sistema del ON y este abonado extranjero en curso de itinerancia puede efectuar unas operaciones de pago. Con el fin de no saturar la base de datos del ON a largo plazo, un abonado extranjero así añadido a una base de datos de un ON es borrado de la lista cuando el ON constata su ausencia en territorio nacional durante un cierto periodo (por ejemplo 2 semanas, lo que significa por ejemplo que el turista ha vuelto a su país).

6.4.6. Selección de una característica del usuario

Según una característica particular de la invención, previamente a la introducción de los datos biométricos por parte del usuario, el comerciante constata el sexo del usuario que ha depositado su dedo sobre el terminal de transacciones (hombre o mujer) y consigna esa información manualmente en el terminal de transacciones (por ejemplo: pulsa sobre la tecla "1" para hombre o sobre la "2" para mujer). Esta información se transmite al operador con los datos biométricos. Cada registro en la base de datos de los datos biométricos del operador comprende un campo "sexo". De ese modo, estadísticamente, las operaciones de comparación de las huellas digitales se efectúan a una velocidad doble. El tiempo necesario para la autentificación se divide por lo tanto estadísticamente por dos.

6.4.7. Latencia temporal

Según un modo de realización de la invención, el procedimiento implementa una noción de "latencia temporal de tolerancia". En los modos de realización anteriormente descritos, el usuario se encuentra en la proximidad de la estación base. En este modo de realización de la invención, el procedimiento está adaptado igualmente a los usuarios que se encontraban hace poco tiempo cerca de una estación base (por ejemplo menos de cinco minutos). En un modo de realización de ese tipo, se tienen en cuenta unos indicadores de conexión que se sitúan en el seno de las estaciones base y/o en el seno de los controladores (BSC por "Base Station Controller") y/o en el seno de las centrales telefónicas (los "MSC") y/o en el seno de los registros (VLR, por "Visitor Location Register", HLR por "Home Location Register") y otros equipos situados en el núcleo de la red ("Core Network"). En efecto, cuando los dispositivos móviles se desplazan en el seno de la red de comunicación del operador, se marcan sus pasos por las estaciones base (por ejemplo en el VLR o el HLR e igualmente en otros equipos). Este marcado se utiliza particularmente en el marco de los procedimientos de "handover", con el fin de acelerar la transición del dispositivo móvil de una estación base a otra. En este modo de realización de la invención, los inventores han tenido la idea de utilizar este marcado con el fin de verificar la presencia reciente del dispositivo móvil en la zona de cobertura de la estación base.

Por ejemplo, el funcionamiento se adapta a unas situaciones particulares como el caso típico de un parking subterráneo en el que no hay recepción de señal para los terminales de comunicación móviles. La red móvil ha constatado la presencia del usuario en la red y posteriormente lo ha perdido. Un minuto más tarde emana una solicitud de pago del terminal de transacciones del parking y el usuario entonces ya no está detectable.

En este modo de realización, la información de presencia del usuario se ha conservado en la estación base, o en la red de comunicación, de manera que sea posible, aunque el usuario no esté ya adscrito a la estación base en cuestión, comparar los datos biométricos introducidos con los de los usuarios cuyas señales se han perdido recientemente.

La utilidad y la eficacia del sistema se mejoran entonces grandemente utilizando este modo de realización de la invención.

6.4.8. Autentificación fuera de línea

Según una característica particular de la invención, una variante del procedimiento permite realizar una autentificación en modo "desconectado". En esta variante la red transmite, a intervalos regulares, al conjunto de los terminales de transacciones en la proximidad de un usuario dado, los datos biométricos y el código confidencial de

este usuario para el caso de que el usuario se decida a utilizar uno de los terminales de transacciones. Cuando un usuario sale de la proximidad de la estación base, la red da a los terminales de transacciones afectados, la orden de borrar los datos biométricos y el código confidencial de este usuario.

Así en caso de solicitud de transacción, el terminal de transacciones dispone ya que todas las informaciones necesarias y puede realizar la autentificación sin que sea necesario realizar una conexión.

Este modo de realización está adaptado particularmente al caso de superficies comerciales de densidades reducidas, que comprenden pocos puntos de pago y un número limitado de terminales móviles. Según una característica particular de la invención, la transmisión de los datos biométricos y de los códigos confidenciales a los terminales de transacciones, en el caso anteriormente expuesto se realiza durante la inactividad del terminal de transacciones. Así se incrementa la probabilidad de no tener necesidad de ponerse en línea y por tanto se disminuye estadísticamente el tiempo de la transacción.

En otro modo de realización de la invención, cada estación base recibe y registra permanentemente los datos biométricos y los códigos confidenciales de los usuarios que están bajo su gestión. Cuando un usuario transita hacia una nueva estación base, la estación base a la que ha estado conectado anteriormente transmite estos datos a la nueva estación base simultáneamente o posteriormente al procedimiento de traspaso. De ese modo, la nueva estación base economiza la necesidad de tener recursos en el núcleo de la red (“core network”) durante la realización del procedimiento de autentificación según la invención.

REIVINDICACIONES

1. Procedimiento de autentificación biométrica de un usuario (U2) a autentificar entre una pluralidad de usuarios acerca del sistema de autentificación que almacena un conjunto de datos biométricos de referencia cada uno asociado a uno de dichos usuarios, comprendiendo las etapas de:

- proporcionar (10) por dicho usuario a autentificar, un dato biométrico de autentificación, con la ayuda de un dispositivo de obtención de datos biométricos de un terminal de transacciones (TP1);

- búsqueda (12) entre un subconjunto de dicho conjunto de datos biométricos de referencia almacenados por dicho sistema de autentificación, de un dato biométrico de referencia que corresponda a dicho usuario (U2) a autentificar, en función de dicho dato biométrico de autentificación,

caracterizado por que dicha etapa de búsqueda comprende una etapa de filtrado (12-3) de dichos datos de dicho conjunto de datos biométricos en función:

- de una estación base (SB1) de una red de comunicación móvil (R1); y

- de un conjunto de dispositivos móviles (T1-T5) para los que se activa un indicador de conexión para dicha estación base, estando dicho terminal de transacciones (TP1) sensiblemente próximo a una zona de cobertura de dicha estación base (SB1).

2. Procedimiento de autentificación biométrica, según la reivindicación 1, caracterizado por que dicha etapa de filtrado comprende:

- una etapa de identificación de dicha estación base que cubre dicha zona de cobertura en la que se sitúa dicho terminal de transacciones;

- una etapa de identificación de dicho conjunto de dispositivos móviles para los que se activa un indicador de conexión para dicha estación base, proporcionando un conjunto de identificadores de dispositivos móviles candidatos;

- una etapa de obtención de dicho subconjunto de dicho conjunto de datos biométricos de referencia en función de dicho conjunto de identificadores de los dispositivos móviles candidatos.

3. Procedimiento de autentificación biométrica según una cualquiera de las reivindicaciones 1 y 2, caracterizado por que dichos datos biométricos pertenecen al grupo que comprende:

- las huellas digitales;

- las huellas palmares;

- las huellas de retina;

- las huellas del iris;

- las formas del rostro;

- las combinaciones de dichas informaciones biométricas antes citadas.

4. Procedimiento de autentificación biométrica según una cualquiera de las reivindicaciones 2 y 3, caracterizado por que dicha etapa de filtrado comprende además una etapa de introducción de una información representativa del sexo de dicho usuario.

5. Procedimiento de autentificación biométrica según una cualquiera de las reivindicaciones 2 a 4, caracterizado por que dicha etapa de filtrado comprende además una etapa de selección, de un operador telefónico acerca del que está registrado el dispositivo móvil de dicho usuario.

6. Procedimiento de autentificación biométrica según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que comprende además una etapa de introducción, por dicho usuario, de un código confidencial.

7. Procedimiento de autentificación biométrica según la reivindicación 6, caracterizado por que dicho código confidencial se transmite a dicho sistema de autentificación simultáneamente a dichos datos biométricos suministrados por dicho usuario.

8. Procedimiento de autentificación según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que dicho terminal de transacciones es un terminal de pago móvil conectado a dicha red de comunicación móvil a la que pertenece dicha estación base.

9. Procedimiento de autentificación según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que dicho

terminal de transacciones está conectado a dicha estación base.

10. Procedimiento de autentificación según una cualquiera de las reivindicaciones 1 a 9, caracterizado por que comprende además una etapa de transmisión, a dicho terminal de transacciones, de dicho subconjunto de dicho conjunto de datos biométricos y porque dicha etapa de filtrado se realiza en el seno de dicho terminal de transacciones.

11. Procedimiento de autentificación según una cualquiera de las reivindicaciones 1 a 9, caracterizado por que comprende además una etapa de transmisión hacia una estación base de destino a la que dicho usuario es susceptible de conectarse, de dichos datos biométricos que se refieren a dicho usuario, siendo realizada dicha transmisión a partir de una estación base actual a la que dicho usuario está conectado.

12. Sistema de autentificación biométrica de un usuario (U2) a autentificar entre una pluralidad de usuarios acerca de un sistema de autentificación que almacena un conjunto de datos biométricos de referencia asociados cada uno a uno de dichos usuarios, comprendiendo unos medios de:

- suministro (10) por dicho usuario a autentificar, de un dato biométrico de autentificación, con la ayuda de un dispositivo de obtención de datos biométricos de un terminal de transacciones (TP1);

- búsqueda (12) entre un subconjunto de dicho conjunto de datos biométricos de referencia almacenados por dicho sistema de autentificación, de un dato biométrico de referencia que corresponda a dicho usuario (U2) a autentificar, en función de dicho dato biométrico de autentificación,

caracterizado por que dichos medios de búsqueda comprenden unos medios de filtrado (12-3) de dichos datos de dicho conjunto de datos biométricos en función:

- de una estación base (SB1) de una red de comunicación móvil (R1); y

- de un conjunto de dispositivos móviles (T1-T5) para los que se activa un indicador de conexión para dicha estación base,

estando dicho dispositivo de obtención de datos biométricos sensiblemente próximo a una zona de cobertura de dicha estación base.

13. Producto programa de ordenador que puede descargarse desde una red de comunicación (R1) y/o registrarse en un soporte legible por un ordenador y/o ejecutable por un procesador, caracterizado por que comprende unas instrucciones de código de programa para la realización del procedimiento de autenticación biométrica según una al menos de las reivindicaciones 1 a 11.

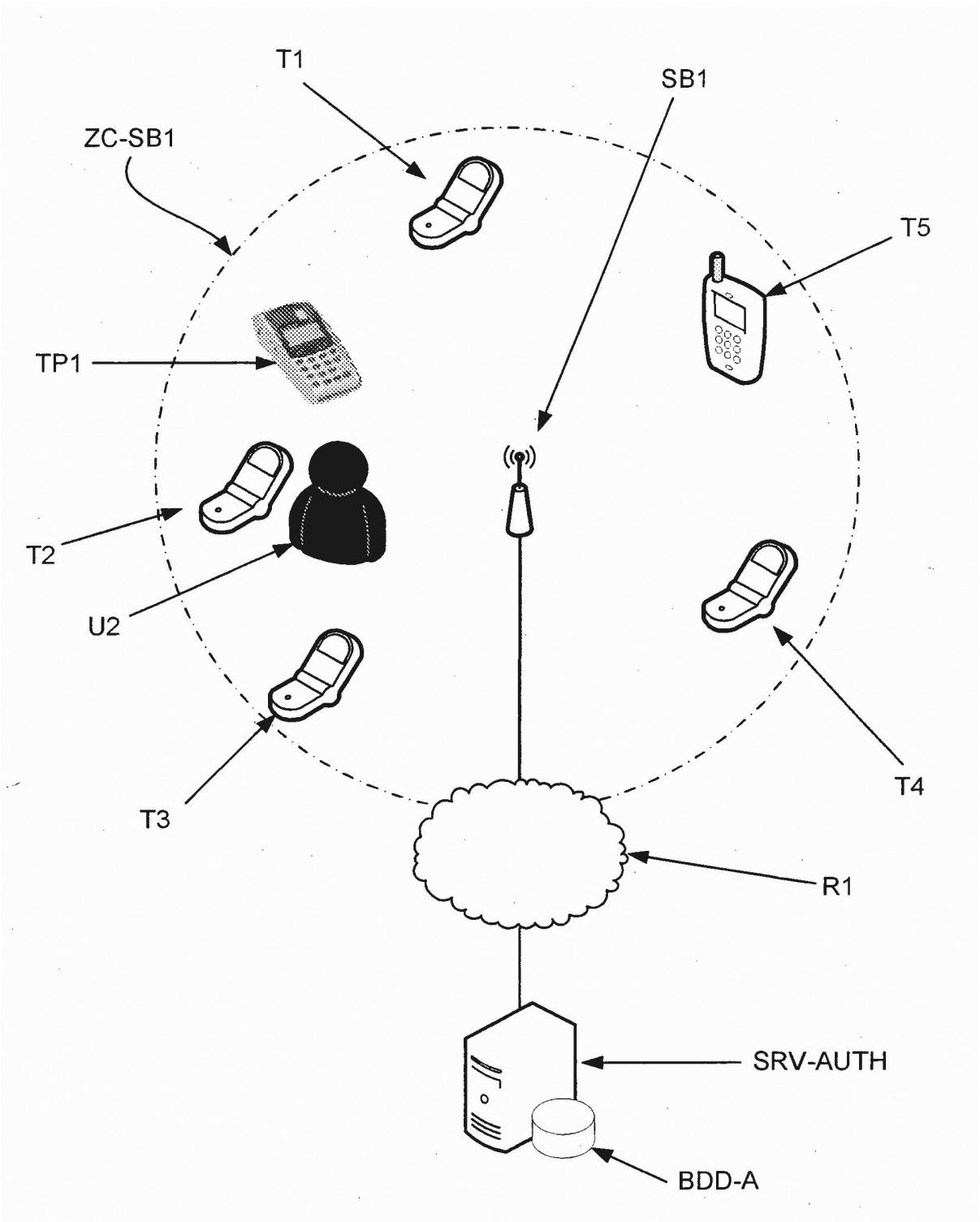

Figura 1

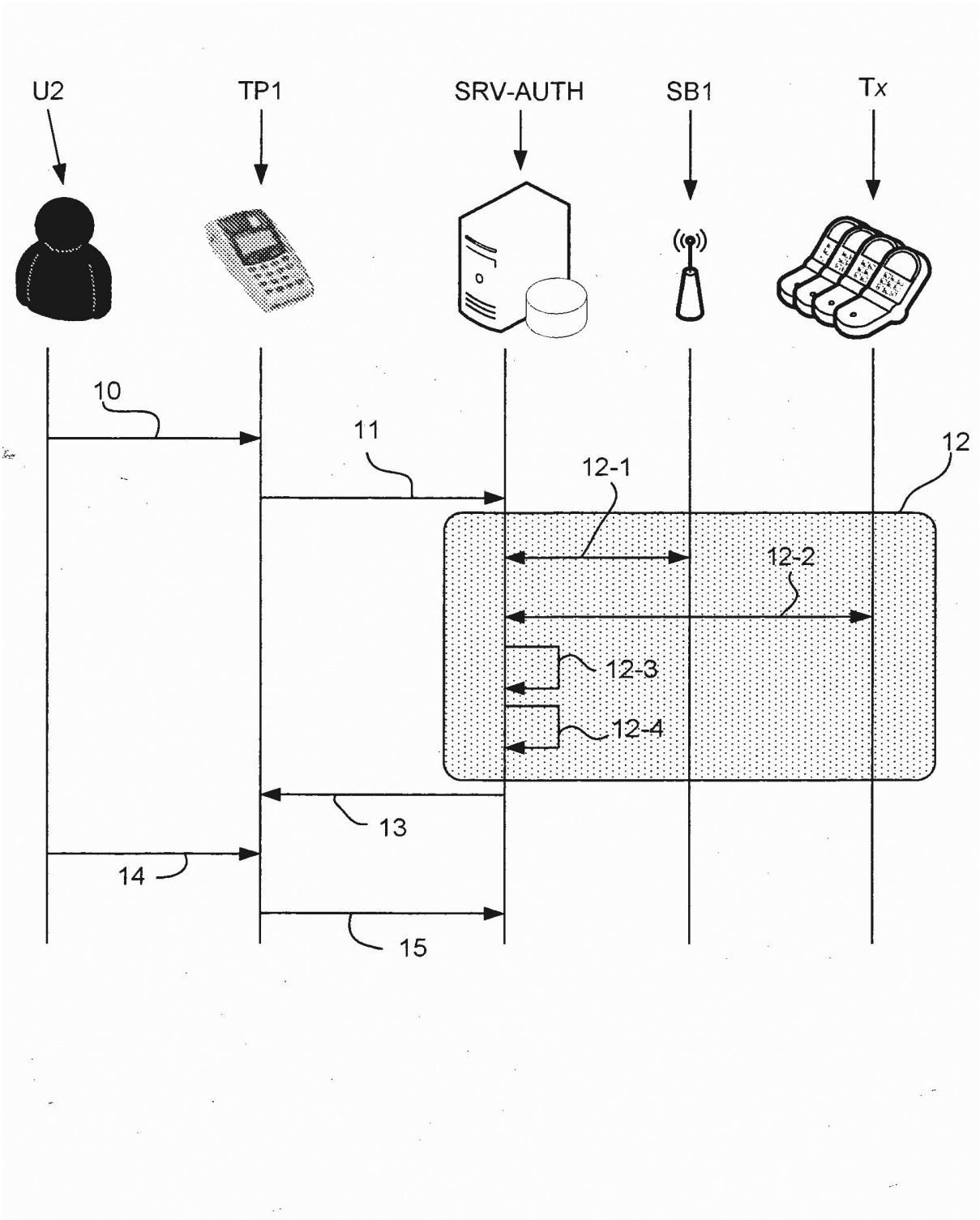

Figura 2