(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 690 973**

(51) Int. CI.:

G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **14.01.2015 E 15151047 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 2897095**

(54) Título: **Procedimiento de refuerzo de la seguridad de una transacción realizada mediante tarjeta bancaria**

(30) Prioridad:

16.01.2014 FR 1450356

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2018

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

LEGER, MICHEL

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de refuerzo de la seguridad de una transacción realizada mediante tarjeta bancaria

1. Campo de la invención

La invención se refiere al campo del refuerzo de la seguridad de transacciones realizadas mediante tarjeta bancaria. Más en particular, la técnica que se propone permite mejorar el refuerzo de la seguridad de transacciones realizadas por un usuario en la utilización de su tarjeta (por ejemplo, con el concurso de un teléfono inteligente, de una tableta, de un ordenador).

2. Estado de la técnica

Desde hace muchos años, la tarjeta bancaria ha desbancado, en cuanto a volumen de transacciones, a los medios de pago convencionales como son el efectivo o los cheques. La tarjeta bancaria, por su utilización masiva, es el soporte de pago priorizado de las compras a distancia, ya sean éstas en línea, en plataformas de pago, o bien por teléfono.

Para hacer segura la utilización de las tarjetas bancarias en el contexto de pago a distancia, se han puesto en práctica abundantes métodos: métodos de cifrado; la integración, en los datos de tarjeta que han de proporcionarse, de un trigrama visual;

A pesar de ello, estos métodos no permiten, en su mayoría, comprobar la identidad de la persona que utiliza los datos de tarjeta bancaria (ya sea en línea o por teléfono). En efecto, detrás de una pantalla o detrás de un aparato telefónico, es muy difícil comprobar que la persona que proporciona los datos de la tarjeta es realmente el titular de la misma.

Por supuesto, se han propuesto métodos de localización de transacción. Tales métodos permiten obtener una zona geográfica en la que se efectúa la transacción: por ejemplo, cuando la transacción se efectúa en línea, por mediación de un ordenador, de una tableta, se han propuesto métodos para localizar físicamente el ordenador o el terminal desde el cual se realiza la transacción. Así, estos métodos permiten detectar transacciones fraudulentas detectando una diferencia de país, por ejemplo, entre el lugar donde se sitúa el terminal y el lugar habitual de residencia del titular de la tarjeta bancaria. Asimismo, se han propuesto técnicas de este tipo para los terminales móviles (los teléfonos o los teléfonos inteligentes): se detecta la presencia del terminal de comunicación en una zona geográfica dada para tratar de detectar un uso fraudulento.

Estas técnicas, en efecto, permiten responder a ciertos intentos de fraude, principalmente con origen en países extranjeros. En cambio, estas técnicas no permiten contrarrestar fraudes que se sitúan en una zona geográfica próxima a la zona geográfica habitual de utilización de los datos de la tarjeta bancaria. Típicamente, las técnicas del estado de la técnica no permiten detectar la utilización indebida, por una persona de la familia o del entorno cercano del titular, de los datos de tarjeta bancaria pertenecientes a este titular.

De este modo, en su conjunto, los actuales métodos son ineficaces para detectar un fraude "local". Por otro lado, los actuales métodos también son poco eficaces en su conjunto para detectar fraudes por teléfono, es decir, cuando un usuario proporciona datos de tarjeta bancaria a un operador telefónico.

Existe, por tanto, una necesidad de proporcionar un método que permita identificar que un autor de una transacción remota que conlleva la provisión de datos de tarjetas bancarias es el titular de la tarjeta bancaria utilizada. El documento US 6356868 describe un sistema de control de acceso a recursos protegidos (ordenadores, edificios, datos bancarios, etc.). Este sistema de control se funda en una autenticación biométrica por voz de un usuario. Con anterioridad a la utilización de este sistema, se ha invitado a cada usuario potencialmente autorizado a acceder a la totalidad o parte de estos recursos protegidos a elegir una contraseña (o una frase clave), que éste ha pronunciado en voz alta con el fin de permitir al sistema establecer y grabar una firma de voz para este usuario. El conjunto de las firmas de voz de todos los usuarios se almacena en una base de datos del sistema.

El documento US 5517558 describe un sistema que permite a un usuario autenticarse vía teléfono con el fin de ser autorizado a acceder a ciertos servicios. Con objeto de realizar esta autenticación –que se funda en un análisis de su voz– se invita al usuario a deletrear por teléfono una cadena de caracteres (que puede ser vista como una contraseña). Entonces se llevan a la práctica dos fases:

- una primera fase de reconocimiento de la voz de los caracteres deletreados (“lo que se ha dicho”): cuando se han reconocido todos los caracteres constitutivos de la cadena de caracteres, el sistema está en condiciones de comprobar la validez de esta cadena de caracteres;

- una segunda fase de autenticación biométrica de la voz (“quién lo ha dicho”) con el fin de determinar si la cadena de caracteres ha sido pronunciada realmente por el usuario legítimo: esta fase se funda en una comparación de la voz del llamante con una firma de voz grabada previamente en el sistema para este usuario y esta cadena de caracteres.

La primera fase permite al sistema saber quién dice ser el llamante (fase de identificación), en tanto que la segunda fase permite comprobar esta identidad (fase de autenticación).

3. Sumario de la invención

La técnica que se propone no presenta estos inconvenientes del estado de la técnica. La técnica que se propone permite hacer segura la utilización de los datos de tarjeta en pagos realizados a distancia, ya sea en línea, por mediación de un sitio web, o bien por teléfono, en contacto con un operador humano. La técnica se refiere a un procedimiento de refuerzo de la seguridad de una transacción realizada mediante tarjeta bancaria según la reivindicación 1. De este modo, además de la firma de voz, se dispone de un elemento de comparación suplementaria que permite identificar al usuario de los datos de tarjeta bancaria. Por lo tanto, se fortalece aún más el refuerzo de la seguridad de la transacción.

De este modo, la comparación del número de teléfono interviene como criterio de comparación secundario que permite identificar al usuario de los datos de tarjeta bancaria.

De acuerdo con una forma particular de realización, dicha etapa de obtención de dicha muestra sonora se pone en práctica de manera concomitante con dicha etapa de obtención de dichos datos textuales, cuando dichos datos textuales son comunicados vía teléfono.

De este modo, no es necesario hacer que el usuario repita varias veces los datos necesarios para la transacción.

De acuerdo con una forma particular de realización, dicha etapa de obtención de dicha muestra sonora y dicha etapa de cálculo de dicha firma de voz actual se ponen en práctica por mediación de un terminal de comunicación en poder de dicho usuario.

De acuerdo con una forma particular de realización, el procedimiento comprende entonces las siguientes etapas:

- recepción, por parte del terminal de comunicación, de una petición de transmisión con origen en un servidor de gestión de transacción;

- presentación, por parte del terminal de comunicación, de una solicitud de introducción de un código de identificación personal,

- introducción, por parte del usuario, del código de identificación personal, y

- cuando el código de identificación personal es correcto, transmisión de la firma de voz actual al servidor de gestión.

De este modo, el usuario legítimo de los datos de tarjeta bancaria no se ve obligado a deletrear los mismos en voz alta. Así, se conserva la confidencialidad de las transacciones realizadas en un lugar público.

En otra forma de realización, la técnica se refiere asimismo a un servidor de control de una validez de una transacción según la reivindicación 5.

De acuerdo con una implementación preferida, las diferentes etapas de los procedimientos según la invención se llevan a la práctica mediante uno o varios equipos lógicos o programas de ordenador, que comprenden instrucciones lógicas destinadas a ser ejecutadas por un procesador de datos de un módulo relevador según la invención y que está diseñado para regir la ejecución de las diferentes etapas de los procedimientos.

En consecuencia, la invención también está encaminada a un programa, susceptible de ser ejecutado por un ordenador o por un procesador de datos, incluyendo este programa instrucciones para regir la ejecución de las etapas de un procedimiento tal como se ha mencionado anteriormente.

Este programa puede utilizar cualquier lenguaje de programación y hallarse en forma de código fuente, código objeto, o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La invención también se encamina a un soporte de información legible por un procesador de datos y que incluye instrucciones de un programa de ordenador tal y como se ha mencionado anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de grabación magnética, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de información puede ser un soporte transmisible, tal como una señal eléctrica u óptica, que se puede conducir por intermedio de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención se puede descargar en particular en una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que va incorporado el programa,

estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

De acuerdo con una forma de realización, la invención se lleva a la práctica por medio de componentes de soporte lógico y/o de soporte físico. En esta línea, el término "módulo" puede corresponder, en este documento, tanto a un componente de soporte lógico, como a un componente de soporte físico o a un conjunto de componentes de soporte físico y lógico.

Un componente de soporte lógico corresponde a uno o varios programas de ordenador, uno o varios subprogramas de un programa o, de manera más general, a todo elemento de un programa o de un soporte lógico apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Tal componente de soporte lógico es ejecutado por un procesador de datos de una entidad física (terminal, servidor, pasarela, encaminador, etc.) y está posibilitado de acceso a los recursos de soporte físico de esta entidad física (memorias, soportes de grabación, buses de comunicación, tarjetas electrónicas de entrada/salida, interfaces de usuario, etc.).

De la misma manera, un componente de soporte físico corresponde a todo elemento de un conjunto de soporte físico (o hardware) apto para llevar a la práctica una función o un conjunto de funciones, según lo descrito a continuación en relación con el módulo de que se trate. Puede ser un componente de soporte físico programable o con procesador integrado para la ejecución de soporte lógico, por ejemplo un circuito integrado, una tarjeta inteligente, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microprograma (firmware), etc.

Por supuesto, cada componente del sistema anteriormente descrito pone en práctica sus propios módulos de lógica.

Las diferentes formas de realización antes mencionadas son combinables entre sí para la puesta en práctica de la invención.

4. Figuras

Otras características y ventajas de la invención se pondrán más claramente de manifiesto con la lectura de la siguiente descripción de una forma preferente de realización, dada a título de mero ejemplo ilustrativo y no limitativo, y de los dibujos que se acompañan, de los que:

- la figura 1 presenta un sinóptico de la técnica propuesta para la transmisión de datos;

- la figura 2 presenta un sinóptico de la técnica propuesta entre un terminal y un servidor de gestión;

- la figura 3 describe la provisión, por parte de un terminal de comunicación, de una firma de voz actual pregrabada; y

- la figura 4 ilustra esquemáticamente los componentes de un servidor de gestión para la puesta en práctica de la técnica propuesta.

5. Descripción detallada

5.1. Recapitulación del principio

El principio general del método que se propone consiste en hacer deletrear al menos algunos de los datos de la tarjeta bancaria, por parte del usuario, en el momento de la transacción. Es evidente la inmediata mejora que se obtiene mediante esta técnica cuando la transacción se realiza por teléfono: hacer deletrear estos datos no precisa de ninguna acción complementaria ni por parte del usuario ni por parte del operador, ya que el usuario está obligado a deletrear estos datos para realizar una transacción.

Los presentes inventores han puesto en práctica una técnica que permite sacar provecho de esta situación. Típicamente, la técnica puesta en práctica comprende las siguientes etapas, descritas en relación con la figura 1, que se desarrollan en el momento del pago:

- una etapa de obtención (10) de datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse, llamados datos textuales (DT);

- una etapa de obtención (20) de al menos una porción de los datos textuales (DT) en forma de un flujo de datos de audio, denominado muestra sonora (ES), resultante de la lectura de los datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse;

- une etapa de cálculo (30) de una firma de voz actual (SVc) a partir de dicha muestra sonora (ES);

- una etapa de comparación (40) de dicha firma de voz actual (SVc) con una firma de voz de referencia (SVr) grabada previamente y asociada a dichos datos textuales (DT) de la tarjeta bancaria; y

- cuando la firma de voz de referencia (SVr) difiere de la firma de voz actual (SVc) en un valor superior a un primer valor definido por un parámetro predeterminado (PPd), una etapa de denegación (50) de la transacción.

La técnica propuesta comprende asimismo una comparación complementaria de números de teléfono en caso de duda acerca de la autenticidad de la firma de voz actual. Este aspecto se describe posteriormente.

Por supuesto, la firma de referencia y la firma de voz actual corresponden a porciones de texto leído que son idénticas. Estas porciones de texto leído pueden corresponder al conjunto de datos textuales o a algunos de ellos (por ejemplo, solamente el número de la tarjeta bancaria, o solamente el criptograma visual). De este modo, la técnica propuesta permite asegurar una importante fiabilidad de la transacción. En efecto, la probabilidad de que el usuario pueda reproducir la voz del titular de la tarjeta es relativamente baja. Típicamente, este caso puede producirse cuando el usuario es grabado, a sus espaldas, y realiza una compra utilizando la técnica propuesta. Sin embargo, para obtener una grabación de buena calidad, un autor de fraude tiene entonces que encontrarse en unas condiciones de grabación particulares: un entorno no ruidoso, hallarse próximo al usuario. Ahora bien, la mayor parte del tiempo, las compras a distancia que precisan de la utilización de los datos de tarjeta bancaria se realizan en el domicilio del propio titular de la tarjeta o en el lugar de trabajo del mismo. Es muy difícil, a partir de entonces, "piratear" este tipo de lugar para reproducir las citadas condiciones de grabación fraudulentas (es decir, unas condiciones ideales). De este modo, la probabilidad de que la voz del titular de la tarjeta sea pirateada en el momento en que deletrea los números de tarjeta es cercana a cero. Por otro lado, en una situación en la que el pago se efectuara por teléfono, el operador sería informado inmediatamente de un cambio de voz: entre la voz del autor de fraude que haya efectuado el pedido de bien o de servicio y la utilizada para deletrear la información de la tarjeta bancaria, una diferencia pondría inmediatamente en alerta al operador, quien, entonces, podría anular la transacción.

La técnica propuesta se puede llevar a la práctica de diferentes maneras. Más en particular, como queda expuesto en la penúltima etapa del método anteriormente presentado, esta técnica precisa de la utilización de una firma de voz de referencia (SVr). Esta firma de voz de referencia (SVr) es necesaria para la puesta en práctica de la técnica. Puede ser adquirida de varias maneras diferentes. Es posible, por ejemplo, adquirirla al abrir una cuenta bancaria en una entidad bancaria. Una apertura de cuenta bancaria muchas veces precisa de la presencia física del futuro titular de la tarjeta bancaria. Es posible realizar una grabación de la voz del mismo en esta ocasión. También es concebible obtener tal firma en la primera utilización de la tarjeta bancaria. Las entidades que proporcionan las tarjetas bancarias muchas veces ponen en práctica una operativa específica para la primera utilización. Es posible prever que esta operativa pueda comprender una etapa de grabación de la voz del titular y la creación de una firma de voz de referencia (SVr) a partir de la misma. Finalmente, en otra forma de realización, es posible obtener esta firma a partir de una grabación en línea, por mediación de un servicio web específicamente dedicado al efecto y disponible en el sitio seguro de la entidad bancaria. Consiste asimismo otra técnica en hacer leer la información de la tarjeta bancaria del titular en un servidor de voz dedicado. Este servidor de voz genera entonces la firma en función de la voz que es leída. De manera complementaria, con la llamada del usuario a este servidor de voz, se graba el número de teléfono llamante de manera concomitante con la firma. Entonces, este número de teléfono puede ser utilizado, en ciertas formas de realización, para comprobar que concuerda con el número de teléfono con el que se realiza una transacción.

En una forma particular de realización, descrita en relación con la figura 2, la técnica propuesta se lleva a la práctica por mediación de un servidor de gestión (SrvG) de transacciones bancarias. En esta forma de realización, previamente a la aceptación de la transacción, el servidor de gestión (SrvG) pone en práctica una etapa de comparación (40) de la firma de voz de referencia (SVr) con la firma de voz actual (SVc). La firma de voz actual (SVc) puede ser calculada (30) por el propio servidor de gestión (SrvG): el servidor de gestión (SrvG) recibe (20) entonces una muestra sonora (ES), a más de la recepción (10) de los datos textuales (DT) de la tarjeta bancaria. La firma de voz actual (SVc), alternativamente, se puede calcular (30) en un terminal (Term) conectado al servidor de gestión (SrvG): en este caso, es la firma de voz actual (SVc) la que directamente se transmite (20) a más de los datos textuales (DT) de la tarjeta bancaria.

En una forma particular de realización, descrita en relación con la figura 3, la técnica propuesta se lleva ingeniosamente a la práctica por mediación de un terminal, como por ejemplo un terminal de comunicación (TermC) móvil de tipo teléfono inteligente, del cual dispone el titular de la tarjeta. En esta forma de realización, una aplicación particular es la encargada de la conservación, en un espacio de memoria seguro, de una firma de voz, que cumple la misión de firma de voz actual (SVc), asociada al titular de la tarjeta. Esta firma de voz actual (SVc) se ha generado, por ejemplo, a partir de la voz del titular de la tarjeta con posterioridad a la instalación de una aplicación particular en el terminal de comunicación (TermC) (aplicación de tipo android, ios o Windows phone), aplicación que permite la puesta en práctica, del lado del terminal, de la técnica descrita.

En esta forma de realización, la firma de voz actual (SVc), que está grabada en el seno de un terminal de comunicación (TermC), se transmite (X20) en el momento de la introducción o de la provisión de los datos textuales (DT) de la tarjeta bancaria. Esta transmisión (X20) de la firma se puede realizar directamente al servidor de gestión (SrvG) de transacción bancaria presentado previamente. Así, en esta forma de realización, por ejemplo, este servidor de gestión (SrvG) recibe los datos de la tarjeta bancaria con origen en el proveedor de productos y/o de servicios (ocasionalmente, por mediación de un servidor transaccional, que encuentra interpuesto al servidor de gestión), en tanto que la firma de voz actual (SVc) se transmite (X20) directamente, desde el terminal del usuario, hacia el servidor de gestión (SrvG) de transacción bancaria (ocasionalmente, por mediación de un servidor transaccional, que se encuentra interpuesto al servidor de gestión). La ventaja de esta forma de realización es que el

titular de la tarjeta (o el usuario), no necesita expresarse en voz alta para deletrear sus identificadores bancarios. Esta forma de realización resulta particularmente adecuada para la compra de bienes y de servicios por mediación, por ejemplo, de un sitio web. El procedimiento comprende entonces las siguientes etapas complementarias:

- recepción (X05), por parte del terminal de comunicación (termC), de una petición de transmisión (ReqT) con origen en el servidor de gestión (SrvG) (o en el servidor transaccional);

- presentación (X10), por parte del terminal de comunicación (termC), de una solicitud de introducción de un código de identificación personal (PIN),

- introducción (X15), por parte del usuario, del código de identificación personal (PIN), y

- cuando el código de identificación personal es correcto, transmisión (X20) de la firma de voz actual (SVc) al servidor de gestión (SrvG).

De este modo, previamente a la transmisión de la firma, el usuario tiene que probar que está en poder de un dato de desbloqueo, como un código de identificación personal, lo cual preserva de un uso fraudulento del terminal en caso de robo del mismo de manera concomitante con el robo de la propia tarjeta bancaria. Hay que distinguir bien entre esta técnica y otras que pueden precisar de la introducción de un código de identificación personal en un terminal de comunicación (TermC) móvil. El objeto de esta introducción, en el contexto de la presente técnica, no es el de autorizar la transacción, sino permitir la transmisión de la firma de voz actual (SVc) hacia el servidor. Esto es significativamente diferente, ya que el servidor de gestión es precisamente el que, *in fine*, acepta o no la transacción. La introducción del código de identificación personal por el usuario del terminal de comunicación (TermC) no se asimila a la aceptación de la transacción. Esta introducción tan solo permite desbloquear la transmisión de la firma de voz actual (SVc) hacia el servidor.

5.1. Descripción de una forma de realización

En una forma de realización de la técnica propuesta, descrita en relación con la figura 4, previamente se crea una firma por mediación de un acceso del titular de la tarjeta bancaria a un servidor de voz. Este acceso se realiza a la recepción de la tarjeta bancaria, previamente a su primera utilización. El titular de la tarjeta recibe la tarjeta y llama a un número de teléfono particular. En esta llamada, el servidor de voz requiere, por una parte, la introducción por parte del titular de la tarjeta de al menos un dato de identificación de esta tarjeta (por ejemplo, el número) y, por otra, un dato de desbloqueo (por ejemplo, el código PIN de la tarjeta). Cuando se han introducido estos datos, el servidor de voz solicita al titular que deletree los datos que figuran sobre la tarjeta (por ejemplo, los apellidos y el nombre del titular, el número de la tarjeta, su fecha de caducidad y el código de seguridad de tres cifras). El servidor de voz graba al titular de la tarjeta cuando este último deletrea los datos de esta tarjeta. Con el concurso del flujo de audio grabado, el servidor de voz pone en práctica un módulo de generación de firma que permite obtener una firma de voz de referencia (SVr) de la voz del titular.

En la utilización de la tarjeta bancaria, por ejemplo para realizar una compra por teléfono, se pone en práctica el método anteriormente descrito con posterioridad a la designación, por parte del usuario, de los bienes o servicios que van a comprarse:

- una etapa de lectura, por parte del usuario, de los datos necesarios que figuran sobre la tarjeta bancaria (CB) que va a utilizarse, en funciones de obtención (10) de los datos (DT) que figuran sobre la tarjeta bancaria (CB) que va a utilizarse para realizar el pago;

- una etapa de obtención (20), por parte de un módulo de grabación (ModENr), al tiempo que va leyendo el usuario, de los datos deletreados en forma de un flujo de datos de audio, que suministra la muestra sonora (ES);

- una etapa de transmisión (25) de dicha muestra sonora (ES) y de los datos textuales a un servidor de gestión (ServG);

- una etapa de cálculo (30) de una firma de voz actual (SVc) a partir de dicha muestra;

- una etapa de comparación (40) de dicha firma con una firma de voz de referencia (SVr) grabada previamente en el seno de una base de datos (DB) y asociada a dichos datos de la tarjeta bancaria; y

- cuando la firma de voz de referencia (SVr) es significativamente diferente de la firma de voz actual (SVc), una etapa de denegación (50) de la transacción.

De manera complementaria, el operador telefónico al que se han deletreado los datos de la tarjeta puede ser informado de la naturaleza de la denegación (es decir, fallo de autenticación del titular).

Aparte de una comparación entre la firma de voz de referencia (SVr) y la firma de voz actual (SVc), se propone asimismo comparar números de teléfono: en efecto, al crear su cuenta bancaria, el cliente generalmente indica uno o varios números de teléfono que sirven de contacto con su banco o su proveedor de servicios de pago. El número de teléfono del usuario llamante es comparado asimismo con los números de teléfono de referencia a disposición del

banco.

A la hora de cursar pedido, se pone en práctica una comparación suplementaria. Esta comparación suplementaria, que no tiene un grado de importancia tan alto como el de la firma de voz de referencia, se puede tener en cuenta, no obstante, en caso de duda acerca de la autenticidad de la firma de voz actual. En efecto, la comparación de las firmas de voz es necesariamente una comparación estadística y/o probabilística. Ahora bien, tal comparación de firma puede acarrear considerables índices de error. Puesto que es poco concebible denegar todas las transacciones bancarias con el motivo de que la comparación de las firmas queda situada bajo un umbral de comparación determinado (por ejemplo, bajo el umbral del 90%), la comparación complementaria de los números de teléfono permite despejar una duda en lo que respecta a la identidad del locutor.

De este modo, por ejemplo, cuando el porcentaje de identidad de las firmas está comprendido entre el 80 y el 95%, el número de teléfono del llamante sirve de factor de decisión secundario para aceptar o no la transacción: si el número del llamante no forma parte de la lista de los números de referencia, la transacción será denegada.

Esto permite aumentar aún más el refuerzo de la seguridad de los pagos a distancia.

5.2. Servidor de gestión

Se describe, en relación con la figura 5, un servidor de gestión (SrvG) puesto en práctica para controlar la validez de una transacción, desde el punto de vista del servidor de gestión (SrvG), según el procedimiento previamente descrito.

Por ejemplo, el servidor de gestión (SrvG) comprende una memoria 51 constituida a partir de una memoria intermedia, una unidad de procesamiento 52, equipada, por ejemplo, con un microprocesador, y pilotada por el programa de ordenador 53, que pone en práctica un procedimiento de control de validez.

Con la inicialización, las instrucciones de código del programa de ordenador 53 se cargan, por ejemplo, en una memoria, antes de ser ejecutadas por el procesador de la unidad de procesamiento 52. La unidad de procesamiento 52 recibe como entrada al menos un dato textual y un dato representativo de una muestra. El microprocesador de la unidad de procesamiento 52 pone en práctica las etapas del procedimiento de control de la validez, según las instrucciones del programa de ordenador 53.

Para ello, el servidor de gestión (SrvG) comprende, aparte de la memoria intermedia 51, unos medios de comunicación, tales como módulos de comunicación de red, medios de transmisión de datos y ocasionalmente un procesador de cifrado.

Estos medios pueden materializarse en forma de un procesador particular implementado en el seno del servidor de gestión (SrvG), siendo dicho procesador un procesador seguro. De acuerdo con una forma particular de realización, este servidor de gestión (SrvG) pone en práctica una aplicación particular que es la encargada de la recepción y de la decodificación de los datos, siendo proporcionada esta aplicación, por ejemplo, por el fabricante del procesador en cuestión, con el fin de permitir la utilización de dicho procesador. Para conseguir esto, el procesador comprende medios de identificación únicos. Estos medios de identificación únicos permiten asegurar la autenticidad del procesador.

Por otro lado, el servidor de gestión (SrvG) comprende además los medios de generación de firmas de voz y/o medios de comparación de firmas de voz. Estos medios se presentan asimismo como interfaces de comunicaciones que permiten intercambiar datos en redes de comunicación, medios de consulta y de actualización de base de datos, medios de comparación de datos. Estos diferentes medios pueden, dependiendo de las formas de realización, materializarse en forma de soporte lógico o en forma de soporte físico, por ejemplo en forma de procesadores particulares. Este puede ser el caso, por ejemplo, de los medios de generación y de comparación de firmas de voz, que, por motivos de prestaciones, pueden ser procesadores dedicados específicamente a esta tarea.

REIVINDICACIONES

1. Procedimiento de refuerzo de la seguridad de una transacción realizada mediante tarjeta bancaria, transacción que conlleva la provisión remota, por parte de un usuario, de datos que figuran sobre una tarjeta bancaria en su poder, comprendiendo dicho procedimiento:

- una etapa de obtención (10) de datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse, llamados datos textuales (DT);

- una etapa de obtención (20) de al menos una porción de los datos textuales (DT) en forma de un flujo de datos de audio, denominado muestra sonora (ES), resultante de la lectura de los datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse;

- una etapa de cálculo (30) de una firma de voz actual a partir de dicha muestra sonora (ES);

- una etapa de obtención de un número de teléfono utilizado para la provisión remota de los datos textuales (DT), llamado número de teléfono actual;

- una etapa de comparación (40) de dicha firma de voz actual con una firma de voz de referencia grabada previamente y asociada a dichos datos textuales (DT) de la tarjeta bancaria; y

- cuando la firma de voz de referencia (SVr) difiere de la firma de voz actual (SVc) en un valor superior a un primer valor definido por un parámetro predeterminado (PPd), una etapa de denegación (50) de la transacción;

- cuando la firma de voz de referencia (SVr) difiere de la firma de voz actual (SVc) en un valor superior a un segundo valor definido por el parámetro predeterminado (PPd):

  - una etapa de comparación del número de teléfono actual con al menos un número de teléfono de referencia grabado previamente y asociado a dichos datos textuales (DT) de la tarjeta bancaria; y

  - cuando el número de teléfono actual no es idéntico a uno de los números de teléfono de referencia, una etapa de denegación de la transacción.

2. Procedimiento según la reivindicación 1, caracterizado por que dicha etapa de obtención de dicha muestra sonora se pone en práctica de manera concomitante con dicha etapa de obtención de dichos datos textuales.

3. Procedimiento según la reivindicación 1, caracterizado por que dicha etapa de obtención de dicha muestra sonora y dicha etapa de cálculo de dicha firma de voz actual se ponen en práctica por mediación de un terminal de comunicación (TermC) en poder de dicho usuario.

4. Procedimiento según la reivindicación 3, caracterizado por comprender además las siguientes etapas:

- recepción (X05), por parte del terminal de comunicación (termC), de una petición de transmisión con origen en un servidor de gestión (SrvG) de transacción;

- presentación (X10), por parte del terminal de comunicación (termC), de una solicitud de introducción de un código de identificación personal (PIN),

- introducción (X15), por parte del usuario, del código de identificación personal (PIN), y

- cuando el código de identificación personal es correcto, transmisión (X20) de la firma de voz actual (SVc) al servidor de gestión (SrvG).

5. Servidor de control de una validez de una transacción que conlleva la provisión remota, vía teléfono, por parte de un usuario, de datos que figuran sobre una tarjeta bancaria, comprendiendo dicho servidor:

- medios de obtención de datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse, llamados datos textuales (DT);

- medios de obtención de al menos una porción de los datos textuales (DT) en forma de un flujo de datos de audio, denominado muestra sonora (ES), resultante de la lectura de los datos que figuran sobre la tarjeta bancaria (CB) que va a utilizarse;

- medios de cálculo de una firma de voz actual (SVc) a partir de dicha muestra sonora (ES);

- medios de obtención de un número de teléfono utilizado para la provisión remota de los datos textuales (DT), llamado número de teléfono actual;

- medios de comparación de dicha firma de voz actual con una firma de voz de referencia grabada previamente y asociada a dichos datos textuales (DT) de la tarjeta bancaria; y

- cuando la firma de voz de referencia (SVr) difiere de la firma de voz actual en un valor superior a un primer valor definido por un parámetro predeterminado (PPd), medios de denegación de la transacción;

- cuando la firma de voz de referencia (SVr) difiere de la firma de voz actual (SVc) en un valor superior a un segundo valor definido por el parámetro predeterminado (PPd):

- medios de comparación del número de teléfono actual con al menos un número de teléfono de referencia grabado previamente y asociado a dichos datos textuales (DT) de la tarjeta bancaria; y

- cuando el número de teléfono actual no es idéntico a uno de los números de teléfono de referencia, medios de denegación de la transacción.

6. Producto de programa de ordenador descargable desde una red de comunicaciones y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, comprendiendo dicho producto de programa de ordenador instrucciones de código de programa para la ejecución de un procedimiento de control según la reivindicación 1, cuando se ejecuta en un ordenador.

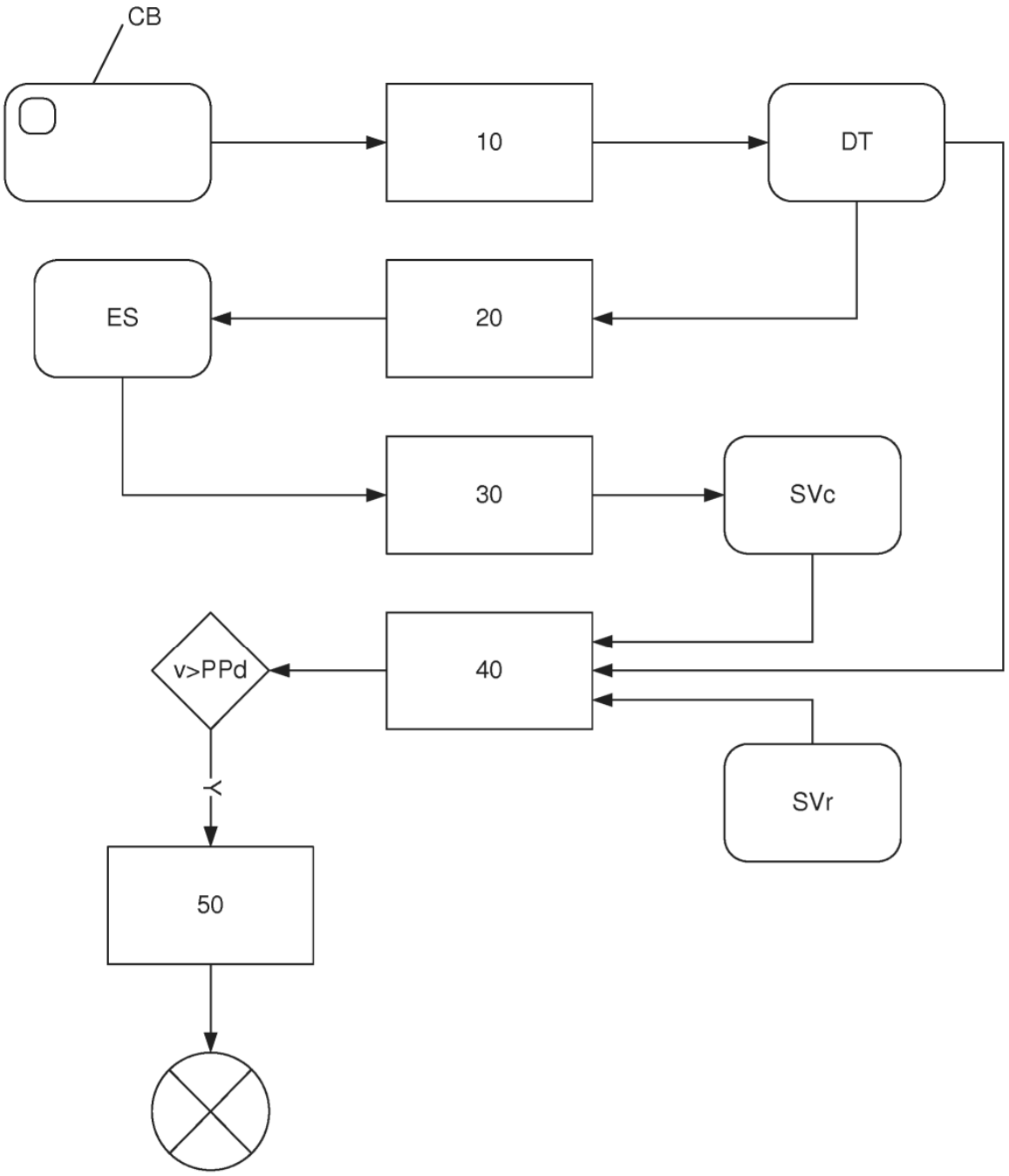

Figura 1

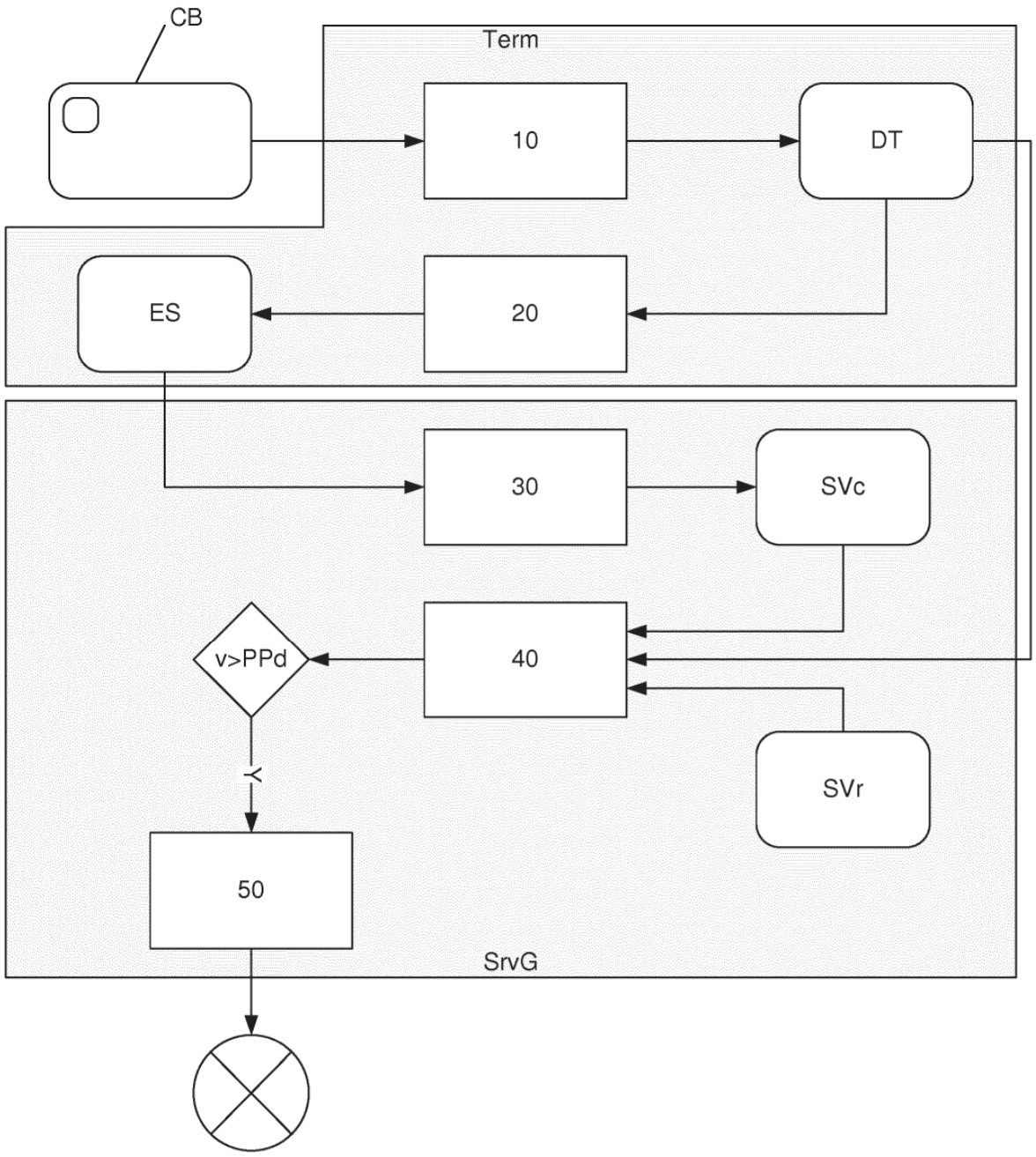

Figura 2

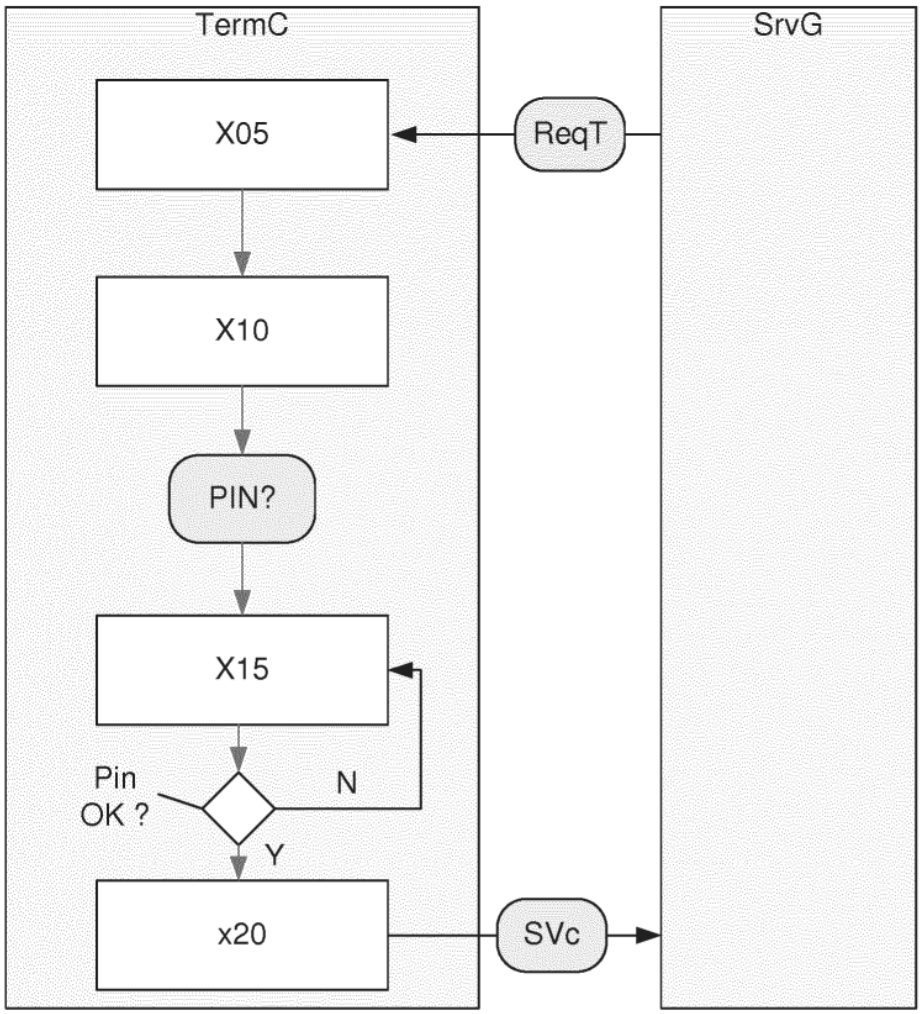

Figura 3

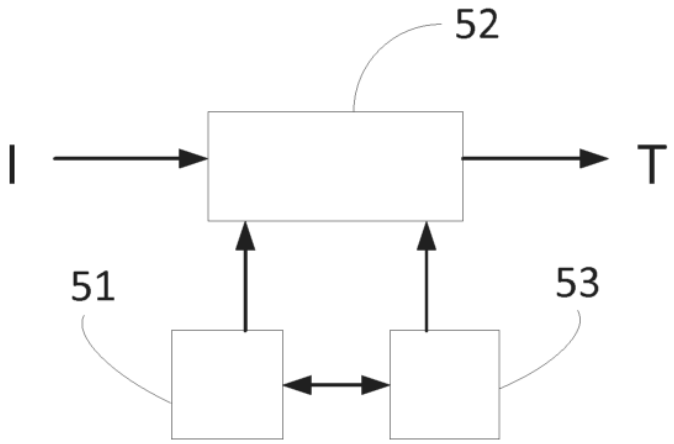

Figura 5

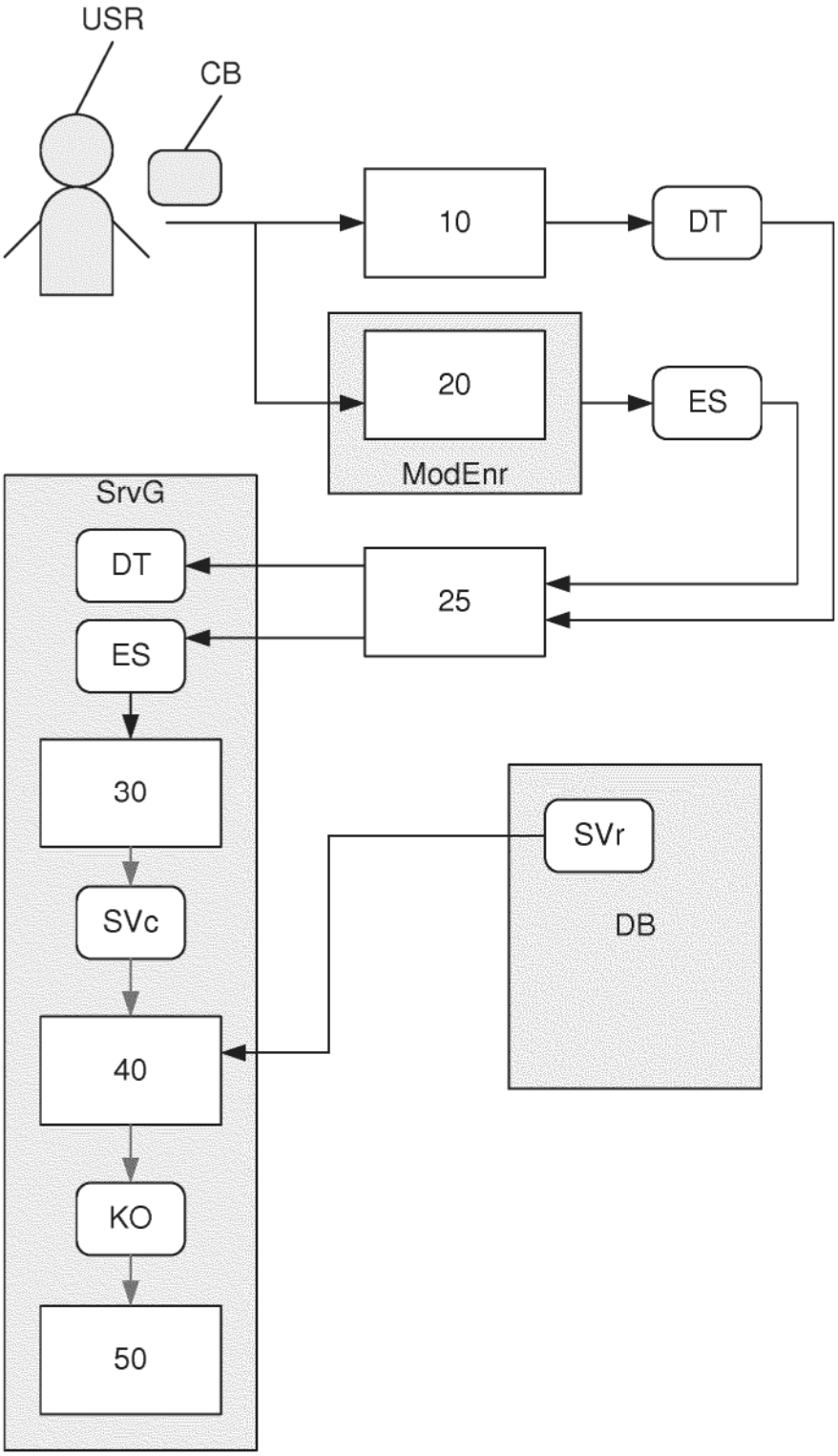

Figura 4