(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 545 537**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.02.2006 E 06709348 (4)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2015 EP 1875446**

(54) Título: **Dispositivo, procedimiento y sistema de seguridad para transacciones financieras, que se basan en la identificación de un individuo gracias a su perfil biométrico, y que utiliza una tarjeta con microprocesador**

(30) Prioridad:

07.03.2005 FR 0502247

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.09.2015

(73) Titular/es:

CHEMLA, YVES (50.0%)
103 Rue du Chateau
F-92100 Boulogne-Billancourt, FR y
RICHARD, CHRISTOPHE (50.0%)

(72) Inventor/es:

CHEMLA, YVES y
RICHARD, CHRISTOPHE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo, procedimiento y sistema de seguridad para transacciones financieras, que se basan en la identificación de un individuo gracias a su perfil biométrico, y que utiliza una tarjeta con microprocesador

La presente invención concierne a un dispositivo innovador para asegurar los pagos, o transacciones, efectuados por tarjeta con microprocesador, y para validar la identidad del portador de la tarjeta con microprocesador por intermedio de un control biométrico cliente/servidor, ya sean realizados estos pagos o transacciones directamente en el punto de venta o a partir de un PC (ordenador personal u ordenador de libre servicio compartido) conectado a Internet, o bien por teléfono móvil, por ordenador portátil (denominado también laptop), por PDA (Personal Device Assistant) u otro, o incluso por intermedio de cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción. La presente invención concierne igualmente al caso de un empleado de un Establecimiento Financiero portador de una tarjeta con microprocesador y que efectúe una transferencia interbancaria a título profesional. Esta invención puede aplicarse perfectamente a las transferencias electrónicas de fondos de Estados a Estados, o de Comunidad de Estados a Comunidad de Estados, o a Estados, o también de organismos internacionales a Estados, y recíprocamente.

La presente invención está concebida para ser un sistema de Autenticación de identidad, de tipo cliente/servidor, de un portador de tarjeta con microprocesador, que se basa, por una parte, en la utilización de la tarjeta con microprocesador y, por otra, en la identificación del portador por medio de datos biométricos almacenados en una tarjeta con microprocesador de memoria expandida, por comparación con una base de datos biométricos, externa y distante asegurada y operada por el Tercero de Autenticación o por el Establecimiento Financiero, no obstante sin realizar, por razones de seguridad y de rendimiento, transferencia de los citados datos biométricos a través de la red de telecomunicación.

Actualmente en el mundo, los pagos o transacciones son efectuados generalmente con la ayuda de una tarjeta de pista magnética, en los que la factura emitida debe ser firmada durante un acto de compra. En ciertos países, la firma es reemplazada por un Código PIN de varias cifras, que es comparado con el residente en la memoria de la tarjeta con microprocesador.

Por una parte, habida cuenta del volumen en alto crecimiento en el mundo, de las transacciones de compra o de las transferencias financieras, utilizando como soporte una tarjeta con o sin microprocesador, cada vez más pagos, o transacciones, son susceptibles de ser objeto de fraudes, no requiriendo ciertas transacciones Código PIN. El Código PIN asegura una mejor seguridad que la sola firma de la factura de compra, pero puede ser igualmente usurpado o robado a su propietario.

Por otra parte, actualmente los portadores de tarjetas, de microprocesador o no, son identificados por su documento de identidad; se constata entonces que numerosos fraudes de la tarjeta, de microprocesador o no, sobrevienen con la expedición de varias tarjetas por diferentes Establecimientos Financieros a un mismo individuo, sin que sea posible confundirle por su identidad tal como ésta es facilitada actualmente en los Establecimientos Financieros emisores. Entre otras cosas, estos fraudes son debidos a la utilización de documentación falsa, a la usurpación de identidad en cualquier forma que ésta sea, o incluso el robo puro y simple de tarjetas con microprocesador o no, vírgenes o ya asignadas.

Podrá referirse igualmente al documento WO 2004/10053 que describe un sistema de Autenticación que utiliza datos biométricos. Pero, este sistema consiste solamente en comparar los datos biométricos con datos almacenados en una base de datos.

El dispositivo de acuerdo con la invención permite poner remedio a estos inconvenientes y a estos fraudes, facilitando a los Establecimientos Financieros un modo de aseguramiento reforzado e inviolable para las transacciones realizadas con una tarjeta con microprocesador.

Estos dispositivos son posibles, actualmente, por el aumento efectivo del tamaño de memoria de las tarjetas con microprocesador que pasa de un nivel inferior a 100 Ko a un nivel de más de 512 Ko. Este aumento notable del tamaño de memoria de las tarjetas con microprocesador permitirá incluir en el interior de las tarjetas información almacenada o software desarrollado en entorno Java® (Sun) o .net® (Microsoft), o con cualquier otro lenguaje disponible.

Además, la puesta a disposición de tarjetas que permiten ser utilizadas a la vez en un puerto de conexión de bajo caudal – utilizado actualmente – y un puerto rápido de alto caudal compatible, permite proceder a intercambios rápidos en tiempo real en estas tarjetas con microprocesador, y poder leer el software, o informaciones almacenadas, a gran velocidad. La disponibilidad de los dos puertos de telecomunicación en microprocesador, permitirá la migración completa y progresiva del parque de los terminales de pago, sin ningún bloqueo o incompatibilidad.

Esta capacidad de memoria disponible permitirá, por una parte, almacenar informaciones gráficas con un nivel de precisión suficiente para ser perfectamente explotables y, por otra, embarcar claves de software así como algoritmos de cálculo, y también endurecer estos algoritmos, a medida de las posibilidades ofrecidas por nuevos desarrollos. Se indicará que el tamaño actual y corriente de las memorias de las tarjetas con microprocesador, así como la no disponibilidad de un puerto de comunicación rápida de alto caudal, no permitía en ningún caso un proceso de este tipo.

El dispositivo Global de la invención comprende a su vez varios dispositivos que son descritos a continuación. Estos dispositivos tienen una nomenclatura en X00100.

La figura 1 representa el Dispositivo Global de la invención.

1. Descripción de los Cuatro Dispositivos de acuerdo con la invención:

1.1 [X00100] Descripción del Primer Dispositivo:
Formato de almacenamiento de la información en la tarjeta con microprocesador.

Este dispositivo de acuerdo con la invención corresponde al almacenamiento en el microprocesador de la tarjeta con microprocesador personal expedida por el Establecimiento Financiero, de uno o varios datos biométricos encriptados que son facilitados por el portador de la tarjeta, y que están asociados a un identificador de convergencia de acuerdo con el dispositivo [X00200]. Los datos biométricos son encriptados antes del almacenamiento en la memoria del microprocesador incluido en la tarjeta con microprocesador.

Para una huella biométrica cualquiera, digital, facial, iris, retina, voz u otra, el software asociado al hardware (Microcontrolador asociado a una Memoria Flash, o dispositivo equivalente) detectará una serie de puntos críticos.

Por razones tanto de seguridad como técnicas, el sensor será programado para seleccionar un número de puntos más o menos grande de 5 a más de 30. En efecto, según la potencia de cálculo disponible en el terminal, que evolucionará en el tiempo, y el tiempo necesario para efectuar los cálculos, así como la transmisión de los elementos resultantes de estos mismos cálculos, los parámetros serán modificables. Cada punto será descrito por coordenadas en el sensor..

1.2 [X00200] Descripción del Segundo Dispositivo:
Dispositivo de información de la base de datos biométricos.

Este dispositivo corresponde a la información de la base de datos biométricos, y comprende el sistema, de acuerdo con la invención, de emisión o de refutación de emisión como consecuencia de una usurpación de identidad. El control de identidad está fundado en el establecimiento de dos archivos.

El primer archivo contiene una secuencia del tipo: Número de convergencia, Apellido, Nombre, Número Nacional de identidad, Fecha de nacimiento, Establecimiento Bancario, Número de Agencia, Número de cuenta, y cualquier otra información necesaria para la buena explotación de los servicios financieros y bancarios. Inicialmente, el identificador de convergencia será un identificador temporal, siendo facilitado el identificador definitivo solamente al final de la conformidad de la validez de los datos por el Tercero de Autenticación.

El segundo archivo contiene una secuencia del tipo: Número de Convergencia ligado a las informaciones biométricas almacenadas en la base de datos biométricos de los servidores distantes del Tercero de Autenticación.

Por razones de seguridad, un servidor maestro que comprende el segundo archivo, el del Tercero de Autenticación, será instalado de modo redundante en los locales del Establecimiento Financiero, y entonces podrá ser utilizado en el caso de un fallo momentáneo de los servidores distantes.

El Tercero de Autenticación dispondrá solamente de un extracto del primer archivo, o sea el Número de convergencia, Apellido, Nombre, Número Nacional de identidad, Fecha de nacimiento, Establecimiento Bancario, Número de Agencia. El Número de Cuenta no será almacenado en los servidores distantes del Tercero de Autenticación.

Las Figuras 2 y 3 representan el Segundo Dispositivo [X00200], o dispositivo de información de la base de datos biométricos.

1.3 [X00300] Descripción del Tercer Dispositivo:
Dispositivo de transferencia de los datos biométricos registrados por los establecimientos financieros hacia los servidores distantes del Tercero de Autenticación.

El dispositivo de acuerdo con la invención representa, por individuo solicitante o portador de una tarjeta con microprocesador, datos biométricos y de identidad personal (apellido, nombre, fecha de nacimiento, etc..), recogidos por el Establecimiento Financiero, la transacción y la duplicación en el servidor del Tercero de Autenticación o servidores distantes. Estos datos son transferidos por el Establecimiento Financiero a los servidores distantes, y comprenden un número de identificador temporal generado por el software facilitado por el Tercero de Autenticación al Establecimiento Financiero.

Una vez almacenados los datos, el dispositivo de acuerdo con la invención efectúa un análisis comparativo de los datos facilitados con los datos existentes en la base de datos de los servidores distantes del Tercero de Autenticación, si estos datos existen ya. A continuación, se efectuará una correlación entre los datos personales y biométricos a fin de informar al Establecimiento Financiero sobre la autenticación del individuo.

Si el individuo existe ya con datos biométricos similares pero de identidad personal diferente, la autenticación será rechazada y señalada al Establecimiento Financiero. En respuesta, el Establecimiento Financiero recibirá el identificador temporal asociado a un código de refutación. Este código de refutación será interpretado inmediatamente por el software facilitado por el Tercero de Autenticación al Establecimiento Financiero, y volverá a mandar una no emisión de la tarjeta por causa de usurpación de identidad.

En el caso en que el individuo no esté representado ya por sus datos biométricos y personales en los servidores distantes del Tercero de Autenticación, su identidad será registrada como válida. Se generará un número de identificador. Este identificador se denominará identificador de convergencia. El identificador temporal emitido por el Establecimiento Financiero será asociado entonces al identificador de convergencia, y estos dos tipos de identificador serán retransmitidos simultáneamente al Establecimiento Financiero solicitante. La transmisión de estos datos al servidor del Establecimiento Financiero confirmará la autenticación del individuo para emisión de la tarjeta con microprocesador.

Se observará que un individuo podrá tener varios identificadores de convergencia diferentes, si ha efectuado una solicitud de tarjeta bancaria a varios Establecimientos Financieros diferentes, pero un solo identificador de convergencia por Establecimiento Financiero. Se observará además, que si un individuo establece varias solicitudes simultáneas de obtención de tarjeta con microprocesador en una misma red bancaria (el mismo Establecimiento Financiero), a partir de la segunda solicitud, el número de identificador temporal, asociado a un código señalado y reconocido como un solicitador múltiple, será emitido y transferido al Establecimiento Financiero, recayendo la decisión de emitir una tarjeta o no al Establecimiento Financiero.

Ofreciendo el Tercero de Autenticación sus servicios a varios Establecimientos Financieros, el dispositivo de acuerdo con la invención ofrecerá una seguridad tanto mayor cuanto más exhaustivo sea el número de informaciones recibidas.

Se señala que, por razones de seguridad y de rendimiento, el dispositivo de acuerdo con la invención no prevé el transporte de los datos biométricos.

Las figuras 4, 5 y 6 representan el Tercer Dispositivo [X00300], o dispositivo de transferencia de los datos biométricos registrados por los establecimientos financieros hacia los servidores distantes del Tercero de Autenticación.

1.4 [X00400] Descripción del Cuarto Dispositivo:
Dispositivo de Autenticación biométrica: se trata del procedimiento cliente/servidor de validación de la identidad de un usuario de tarjeta con microprocesador durante una compra, o una transacción, en punto de venta o por Internet, o bien por intermedio de cualquier otra red de telecomunicación alámbrica o inalámbrica (de tipo GSM, UMTS, Bluetooth, Wifi, u otra), o bien por teléfono móvil, por ordenador portátil (denominado también laptop), por PDA (Personal Device Assistant) u otro, o también por intermedio de cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción.

1.4.1. Principio original de pago biométrico por tarjeta con microprocesador, durante una compra, o una transacción, en punto de venta o por Internet, o bien por intermedio de cualquier otra red de telecomunicación alámbrica o inalámbrica (de tipo GSM, UMTS, Bluetooth, Wifi, u otra), o bien por teléfono móvil, por ordenador portátil (denominado también laptop), por PDA (Personal Device Assistant) u otro, o también por intermedio de cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción.

El pago, o la transacción, se efectúan por la utilización de un terminal de pago por tarjeta con microprocesador en el punto de venta, que tenga, por una parte, un sistema de conexiones local con un sensor de huella biométrica y, por otra, un Microcontrolador asociado a una Memoria Flash, o cualquier otro dispositivo equivalente, incorporado al

terminal. Este Microcontrolador asociado a una Memoria Flash, o cualquier otro dispositivo equivalente, incluye la versión original del software – parte integrante del dispositivo de acuerdo con la invención – que efectuará el cálculo de comparación con respecto a la selección de los puntos aleatoriamente elegidos, como se describió en el primer dispositivo [X00100].

Modalidades del proceso software/Microcontrolador asociado a una Memoria Flash, o a cualquier otro dispositivo equivalente:

I. Captación de la huella biométrica,
II. Lectura de los identificadores,
III. Muestreo de los puntos destacables, elegidos aleatoriamente
IV. Cálculo algorítmico
V. Encriptado de los resultados, envío al Establecimiento Financiero de los resultados de los cálculos encriptados y del identificador de convergencia, estando estos últimos asociados a la solicitud de pago o de transacción.

1.4.2 Despliegue software y hardware:
Un Microcontrolador asociado a una Memoria Flash, o cualquier otro dispositivo equivalente, que contenga la imagen de software descrita anteriormente, será incorporado en el terminal del punto de venta. Se facilitará un lector de tarjeta con microprocesador de memoria expandida, conectada a un puerto rápido de tipo USB, o IEEE1394, u otro equivalente, para los usuarios que deseen efectuar un pago o una transacción por intermedio de una red de telecomunicación, de tipo Internet u otra. De la misma manera, una imagen de software podrá ser integrada al ordenador personal o PC, al teléfono móvil, al ordenador portátil (denominado también laptop), al PDA (personal Device Assistant) u otro, o también a cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción, o también a cualquier otra herramienta que utilice una conectividad a través de una red distante y que incorpore un sensor biométrico, un ordenador y una memoria que permita el almacenamiento del citado software (memoria volátil o no volátil).

Los algoritmos serán facilitados en un soporte físico de tipo CD o DVD Rom, o telecargable, que el usuario de un sistema distante podrá cargar en su máquina.

Versiones de actualización (actualizadas) se desplegarán con frecuencia variable a fin de poder generar algoritmos diferentes, que ofrezcan resultados de cálculo diferentes; estas variantes permiten al gestor de los identificadores garantizar un nivel muy alto de seguridad y de calidad sobre la validación de la identidad de las personas que utilizan este sistema.

De manera idéntica, sea en el terminal del punto de venta, o en el ordenador personal distante conectado, o bien en cualquier otra herramienta conectada, se procederá a la verificación de la versión de software incluida y disponible en cada máquina. En el terminal del punto de venta, o en la versión de ordenador personal, o bien en cualquier otra herramienta conectada, podrá decidirse efectuar una telecarga que pueda permitir otro cálculo de autenticación, en el caso en que la versión utilizada durante la transacción precedente sea obsoleta.

El ordenador personal o PC, el teléfono móvil, el ordenador portátil (denominado también laptop), el PDA (Personal Device Assistant) u otro, o también cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción, o cualquier otra herramienta que utilice una conectividad a través de una red distante y que incorpore un ordenador, y una memoria que permita el almacenamiento del citado software (memoria volátil o no volátil), deberán comprender uno o varios sensores biométricos, integrados, o bien conectados como periféricos.

1.4.3 Procedimiento y arquitectura relativos a la autenticación del portador de tarjeta con microprocesador
En el punto de venta, durante una compra, un consumidor presentará su tarjeta con microprocesador, se le solicitará entonces colocar, por ejemplo, su dedo sobre el sensor biométrico.

El Dispositivo de acuerdo con la invención – basado en una arquitectura cliente/servidor, que comprende hardware – un Microcontrolador asociado a una Memoria Flash, o dispositivo equivalente – sensores biométricos (dedos, facial, iris, retina, voz u otros) y un software original programado y almacenado en la tarjeta con microprocesador – se encarga de la identificación del portador de la tarjeta con microprocesador.

El dispositivo de acuerdo con la invención se basa en una arquitectura de petición única, que comprende dos partes, la primera una solicitud de transacción con destino al Establecimiento Financiero, y la segunda, una solicitud de validación de identidad con destino a los servidores del Tercero de Autenticación, o del Establecimiento Financiero.

1.4.3.1. Primera parte del Dispositivo [X00400]:
El Dispositivo [X00400] de acuerdo con la invención efectúa una correlación en modo local, entre los datos encriptados almacenados en el microprocesador de la tarjeta con microprocesador y descritos en el primer dispositivo [X00100], y los datos biométricos recogidos del portador de la tarjeta con microprocesador. Esto es posible gracias a un software original desarrollado de acuerdo con la invención e integrado en un Microcontrolador asociado a una Memoria Flash, o a cualquier otro dispositivo equivalente, que está insertado en el terminal soporte de la transacción.

El software y el Microcontrolador asociado a una memoria Flash, o a cualquier otro dispositivo equivalente, incorporarán una gestión de la traslación de la matriz ortonormada, a fin de evitar las dificultades de posicionamiento en el sensor (se puede, por ejemplo, orientar su dedo varios grados a la derecha o a la izquierda con respecto al eje teórico de sensor).

La posición de los puntos con respecto al sistema de referencia (Matriz del sensor) así como la posición de los puntos entre ellos, así como su orientación vectorial será objeto de un análisis que, en un primer tiempo, será comparado en el mismo cálculo disponible en la propia tarjeta con microprocesador.

Esta comparación hará aparecer una correlación inmediata o no con respecto a la huella viva.

Se observará que el sensor de huella será de tipo termométrico u otro, a fin de verificar si el individuo está vivo o no, y si no se trata de una copia imagen de la citada huella. Los otros tipos de sensor comprenderán una verificación infrarroja, u otra, que controle la temperatura del individuo.

1.4.3.2 Segunda Parte del Dispositivo [X00400]:
El dispositivo de acuerdo con la invención [X00400] efectúa una correlación entre los datos encriptados descritos en el Dispositivo [X00200], y los datos encriptados residentes en los servidores distantes del Tercero de Autenticación, esto por intermedio de un cálculo local cuyos resultados son retransmitidos a los servidores distantes del Tercero de Autenticación, o del Establecimiento Financiero, que efectúan los mismos cálculos y analizan de nuevo sus resultados. Estos resultados van acompañados del identificador de convergencia encriptado y de la parte de código Java® (Sun) o .net® (Microsoft), o de cualquier otro lenguaje disponible, almacenados en la tarjeta con microprocesador, así como de las informaciones relativas a la propia transacción.

El identificador de convergencia, los resultados de cálculo local, la parte de código Java® (Sun) o .net® (Microsoft), o de otro lenguaje disponible, son retransmitidos en una petición única, por el terminal, al Establecimiento Financiero, que éste mismo retransmite al Tercero de Autenticación, o al Establecimiento Financiero, el identificador de convergencia, los resultados del cálculo local, la parte de código Java® (Sun) o.net® (Microsoft), o cualquier otro lenguaje disponible, para verificación de identidad.

Durante la preparación de los resultados por el Tercero de Autenticación, el Establecimiento Financiero efectúa sus propias verificaciones financieras sobre la cuenta del portador de la tarjeta con microprocesador, a la espera de la aceptación o de la refutación de la identidad del portador de la tarjeta con microprocesador por el Tercero de Autenticación, o por el propio Establecimiento Financiero. Una vez pronunciada por el Tercero de Autenticación la aceptación o refutación de la tarjeta con microprocesador, el Establecimiento Financiero cierra la transacción.

Las operaciones de control de identidad son efectuadas en tiempo real.

El procedimiento será estrictamente idéntico si la compra se hace a través de Internet, o por cualquier otro medio, o bien por intermedio de cualquier otra red de telecomunicación alámbrica o inalámbrica (de tipo GSM, UMTS, Bluetooth, Wifi, u otra), o bien por teléfono móvil, por ordenador portátil (denominado también laptop), por PDA (Personal Device Assistant) u otro, o también por intermedio de cualquier otro equipo móvil, o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción.

Las figuras 7 y 8 representan el Cuarto Dispositivo [X00400], o dispositivo cliente/servidor de validación de la identidad de un usuario de tarjeta con microprocesador durante una compra en punto de venta o por Internet o bien por intermedio de cualquier otra red de telecomunicación alámbrica o inalámbrica (de tipo GSM, UMTS, Bluetooth, Wifi, u otro), o bien por teléfono móvil, por ordenador portátil (denominado también laptop), por PDA (Personal Device Assistant) u otro, o también por intermedio de cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la ciada transacción.

2. [X00500]: Descriptivo por etapas del dispositivo de autenticación de acuerdo con la invención, y descrito anteriormente
Etapa 1: El Establecimiento Financiero recibe por parte de un portador una solicitud de emisión de una tarjeta con microprocesador.

Etapa 2: El Establecimiento Financiero solicita al futuro portador de la tarjeta con microprocesador someterse a una captura de sus huellas biométricas.

Etapa 3: Procedimiento de almacenamiento de las huellas biométricas en el servidor de la agencia bancaria, y después transferencia al servidor central del Establecimiento Financiero, con destrucción de los datos presentes en el servidor de la agencia por razones de seguridad.

Etapa 4: Procedimiento de almacenamiento de las huellas biométricas en los servidores distantes del Tercero de Autenticación.

Etapa 5: El Establecimiento Financiero solicita una validación de la identidad emitiendo una petición a los servidores distantes del Tercero de Autenticación.

Etapa 6: La petición precedente es aceptada, no habiendo sido depositada ya ninguna huella biométrica similar por el solicitante para la emisión de una tarjeta con microprocesador.

Etapa 7: El Establecimiento Financiero decide emitir la tarjeta a nombre del solicitante, y la o las huellas biométricas facilitadas, el identificador de convergencia, los resultados del cálculo local, la parte de código Java® (Sun) o .net® (Microsoft), o de cualquier otro lenguaje disponible, son almacenadas en el Microcontrolador asociado a una Memoria Flash, o a cualquier otro dispositivo equivalente, incluido en la tarjeta con microprocesador.

Etapa 8: El portador de la tarjeta con microprocesador se presenta en un punto de venta y quiere proceder a la compra de una mercancía de un valor de 100 Euros.

Etapa 9: La tarjeta con microprocesador del portador es insertada en el terminal de pago, y se solicita al portador colocar su dedo, o cualquier otra parte del cuerpo, sobre el sensor biométrico o frente al sensor biométrico apropiado, según la región del cuerpo que deba ser validada.

Etapa 10: En modo local, el terminal de pago valida la coherencia de las dos huellas, la de la tarjeta y la del sensor.

Etapa 11: Habiendo validado en modo local la coherencia de las dos huellas (la almacenada en la tarjeta con microprocesador, y la de la parte viva del cuerpo), el terminal de pago envía, en modo distante, una petición única que comprende dos partes, una con destino al Establecimiento Financiero, y la otra con destino a los servidores del Tercero de Autenticación, como se describió en [X00400].

Etapa 12: El Tercero de Autenticación valida a su vez la coherencia de la identidad biométrica del portador de la tarjeta con microprocesador y de la identidad biométrica almacenada en sus servidores; éste, en constatación, emite entonces un código de validación o de refutación de identidad con destino al Establecimiento Financiero.

Etapa 13: El Establecimiento Financiero autoriza o no la transacción de 100 Euros, en función de los datos de solvencia financiera, enviando una orden positiva o negativa al terminal de pago (véase la Figura 11).

De la misma manera, el Establecimiento Financiero autoriza o no la transacción de 100 Euros, en función de los datos de solvencia financiera, enviando una orden positiva o negativa por uno cualquiera de los otros tipos de terminales disponibles en el mercado, como el teléfono móvil, el ordenador portátil (denominado también laptop), el PDA (Personal Device Assistant) u otro, o también cualquier otro equipo móvil o fijo, susceptible de conectarse a través de una red de telecomunicación cualquiera, y de efectuar una transacción en la que la biometría entre en juego a partir del punto generador de la citada transacción (véase la Figura 12).

Las Figuras 9, 10, 11 y 12 representan el dispositivo por etapas [X00500].

REIVINDICACIONES

1. Sistema destinado a facilitar una autenticación biométrica de un portador de tarjeta con microprocesador que efectúa una transacción electrónica en la que la biometría entra en juego a partir del punto generador de la citada transacción, estando conectado el citado portador de tarjeta con microprocesador a un medio de comunicación y a un terminal de pago biométrico, o cualquier otro terminal transaccional que comprenda un lector de tarjeta con microprocesador concebido para recibir un software específico que actúe como una pasarela de comunicación con servidores distantes de un Tercero de Autenticación, y que comprende una conexión a uno o varios sensores biométricos, integrados o no en el terminal, el cual está conectado a un ordenador unido al citado medio de comunicación;
caracterizado por que comprende:

- un primer dispositivo (X00100) adaptado para almacenar en el microprocesador de la tarjeta con microprocesador personal expedida por un establecimiento financiero, uno o varios datos biométricos encriptados facilitados por el portador de la tarjeta, y asociados a un identificador de convergencia procedente de un segundo dispositivo, siendo los datos biométricos de característica morfológica – huellas digitales, faciales, iris, voz u otra, y encriptados antes del almacenamiento en la memoria del microprocesador incluido en la tarjeta con microprocesador,
- el citado segundo dispositivo (X00200) adaptado para recibir los datos biométricos del portador, y calcular un identificador de convergencia temporal asociado a estos datos biométricos, y adaptado para informar a la base de datos biométricos de los citados servidores distantes, y para controlar la identidad con la ayuda de archivos, por una parte un archivo procedente de una toma de huella biométrica temporal y, por otra, una base de datos central que comprende para cada individuo un archivo maestro estable en los servidores distantes que comprende una secuencia de datos que contienen un identificador de convergencia fuente vinculado a las informaciones biométricas almacenadas en la base de datos biométricos de los servidores distantes del Tercero de Autenticación, que permite efectuar la correlación de las identidades por comparación de los dos archivos, siendo inicialmente el identificador de convergencia un identificador convergencia temporal generado por un software facilitado por el Tercero de Autenticación al establecimiento financiero, siendo facilitado un identificador definitivo solamente al final de la conformidad de la validez de los datos por parte del Tercero de Autenticación,
- un tercer dispositivo (X00300) que permite la transferencia de los datos biométricos registrados por el establecimiento financiero hacia los servidores distantes del Tercero de Autenticación, comprendiendo estos datos el identificador de convergencia temporal;

siendo puestos en práctica los primero, segundo y tercer dispositivos durante el registro de los datos biométricos;

- un cuarto dispositivo (X00400) que es puesto en práctica para la autenticación biométrica y que permite la citada Autenticación biométrica, efectuando un cálculo de correlación local entre los datos encriptados almacenados en el microprocesador de la tarjeta con microprocesador y descritos en el primer dispositivo, y los datos biométricos recogidos del portador de la tarjeta con microprocesador, cuyo resultado es retransmitido a los servidores distantes del Tercero de Autenticación y del establecimiento financiero, efectúa el mismo cálculo y analiza de nuevo su resultado, efectuando una correlación distante entre los datos de los archivos procedentes de una toma de huella biométrica en tiempo real y encriptados, y los datos encriptados residentes en los servidores distantes del Tercero de Autenticación, a saber el archivo maestro estable de cada individuo, utilizando el identificador de convergencia.

2. Sistema de acuerdo con la reivindicación 1, **caracterizado por que** el terminal de lectura de la tarjeta con microprocesador es un terminal móvil, personal y portátil cuyo medio de comunicación con el servidor distante de autenticación es la red Internet, o cualquier otra red de telecomunicación alámbrica o inalámbrica de tipo GSM5, UMTS, Bluetooth, Wifi, u otra.

3. Sistema de acuerdo con la reivindicación 1, **caracterizado por que** el primer archivo contiene una secuencia del tipo: Número de convergencia, Apellido, Nombre, Número Nacional de identidad, Fecha de nacimiento, Establecimiento Bancario, Número de Agencia, Número de Cuenta.

4. Sistema de acuerdo con la reivindicación 1, **caracterizado por que** el segundo fichero contiene una secuencia de tipo: Número de convergencia, denominado también identificador de convergencia, ligado a las informaciones biométricas almacenadas en la base de datos biométricos de los servidores distantes del Tercero de Autenticación.

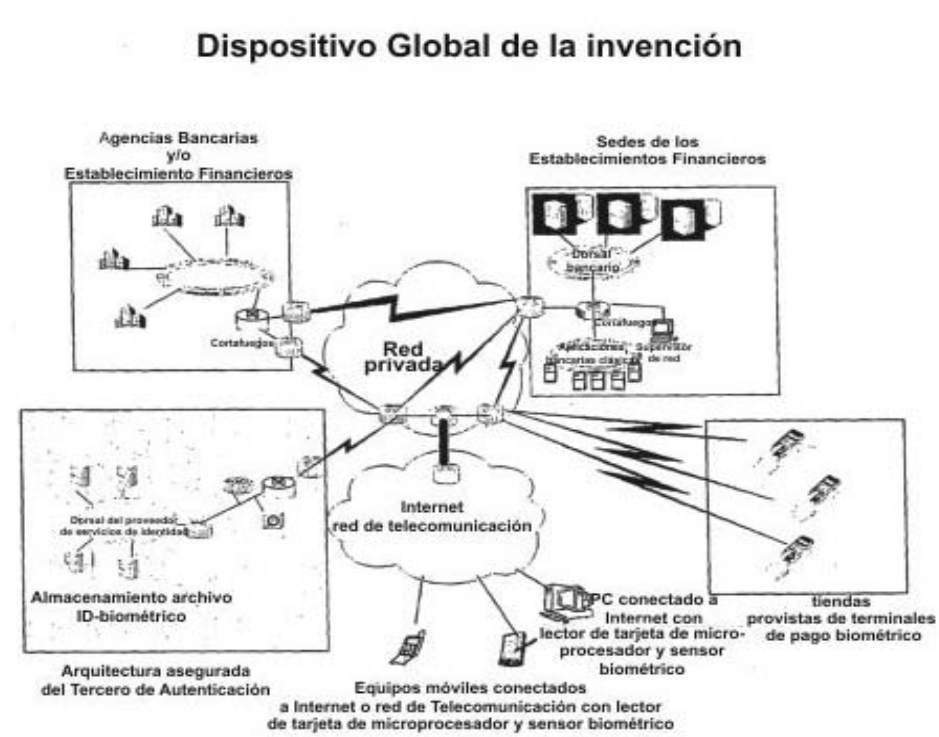

Fig1: Dispositivo [X00100]

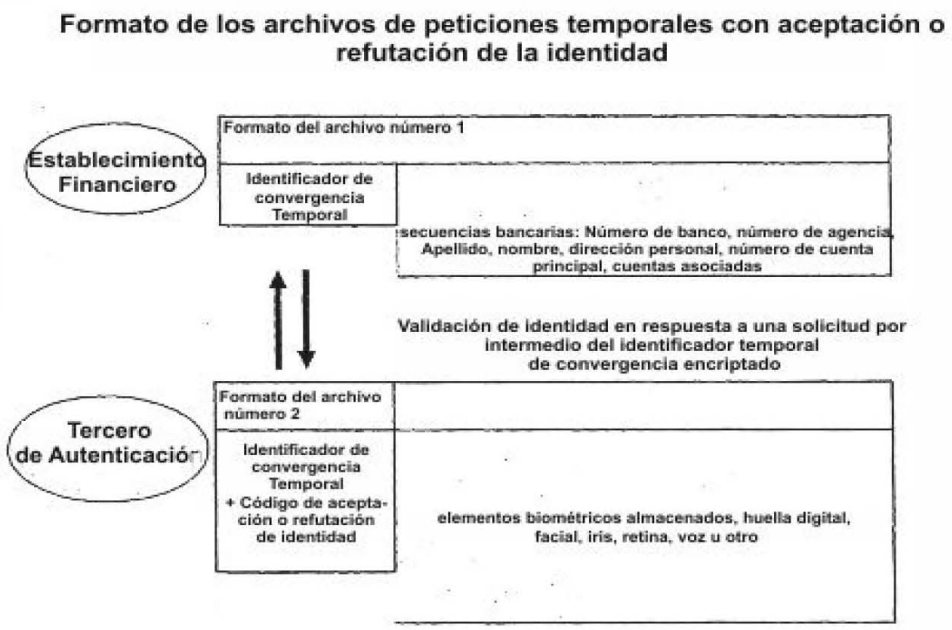

Fig 2: Dispositivo [X00200]

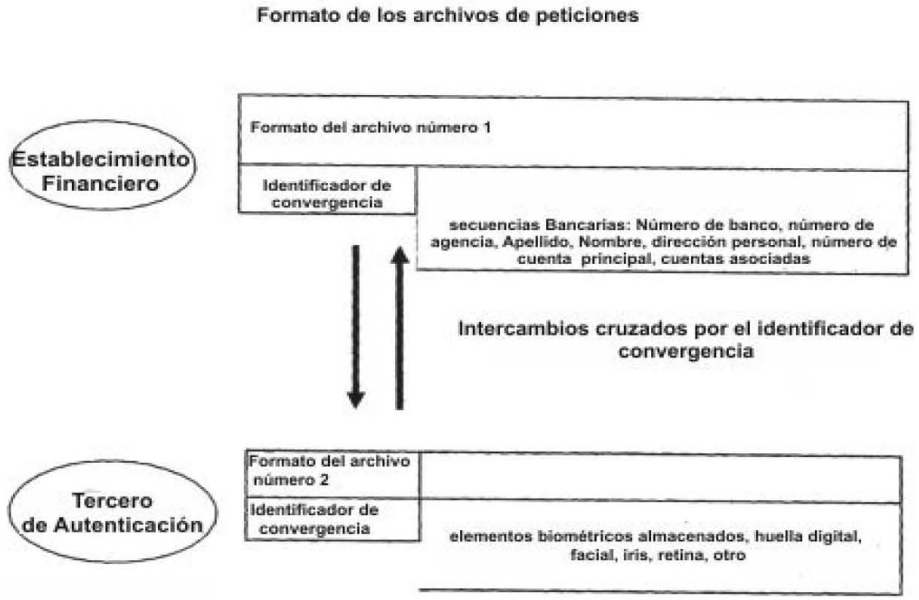

Fig 3: Dispositivo [X00200]

Fig 4: Dispositivo X00300]

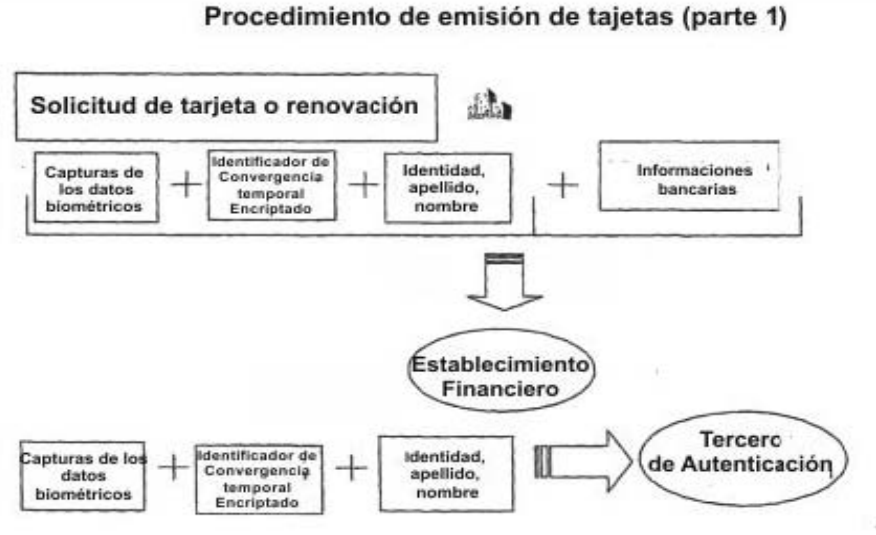

Fig 5: Dispositivo [00300]

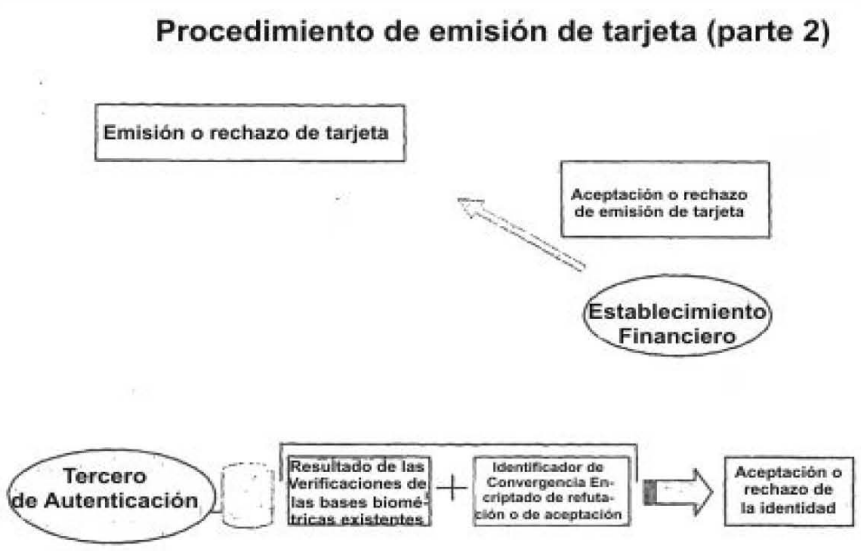

Fig 6: Dispositivo [X00300]

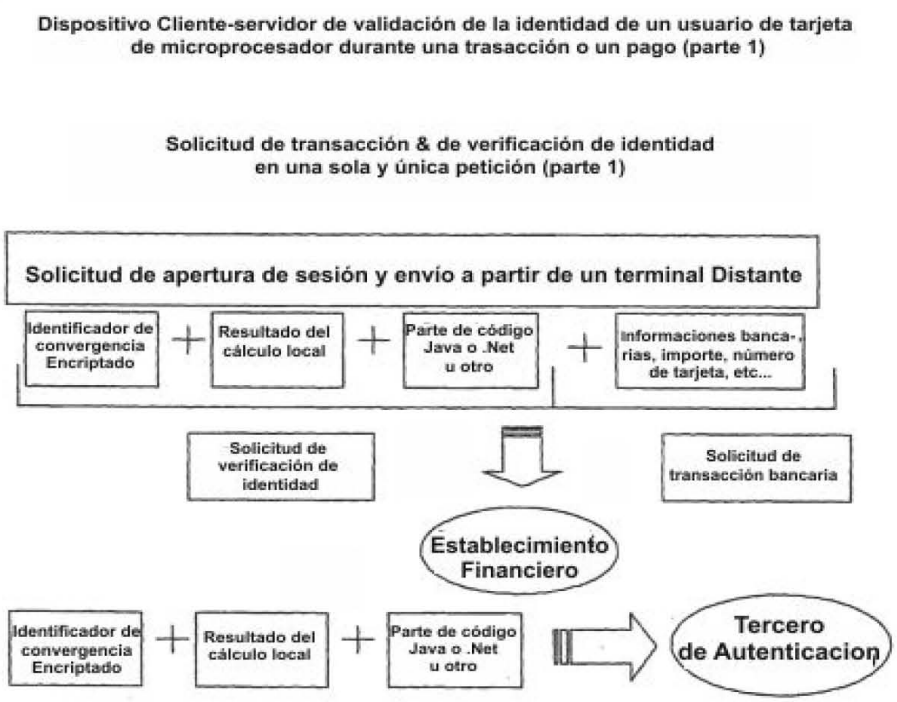

Fig 7: Dispositivo [X00400]

Dispositivo Cliente-Servidor de validación de la identidad de un usuario de tarjeta de microprocesador durante una transacción o un pago (parte 2)

Fig 8: Dispositivo [X00400]

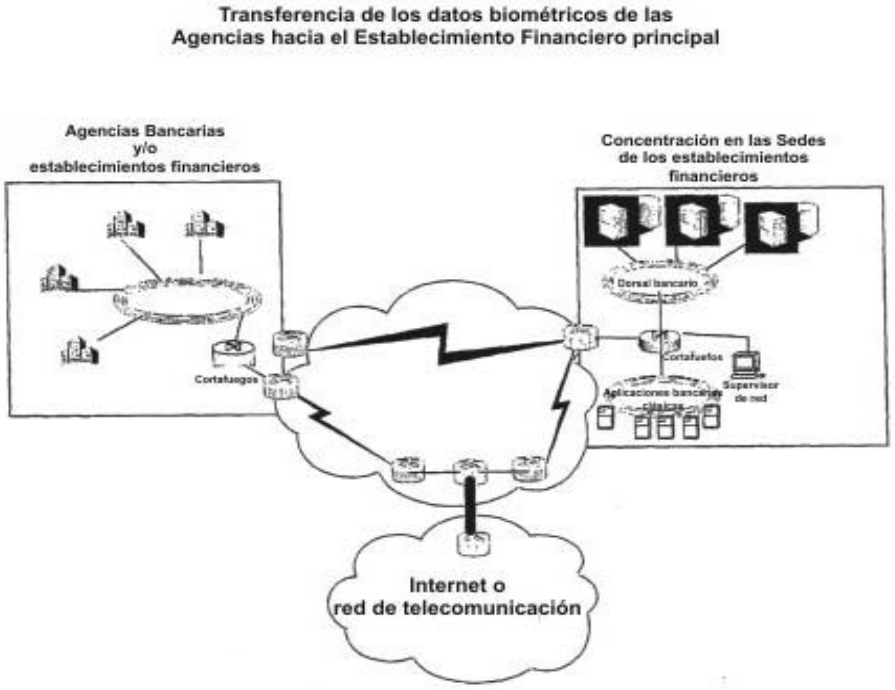

Fig 9: Dispositivo [X00500] Etapa 1, 2, 3-

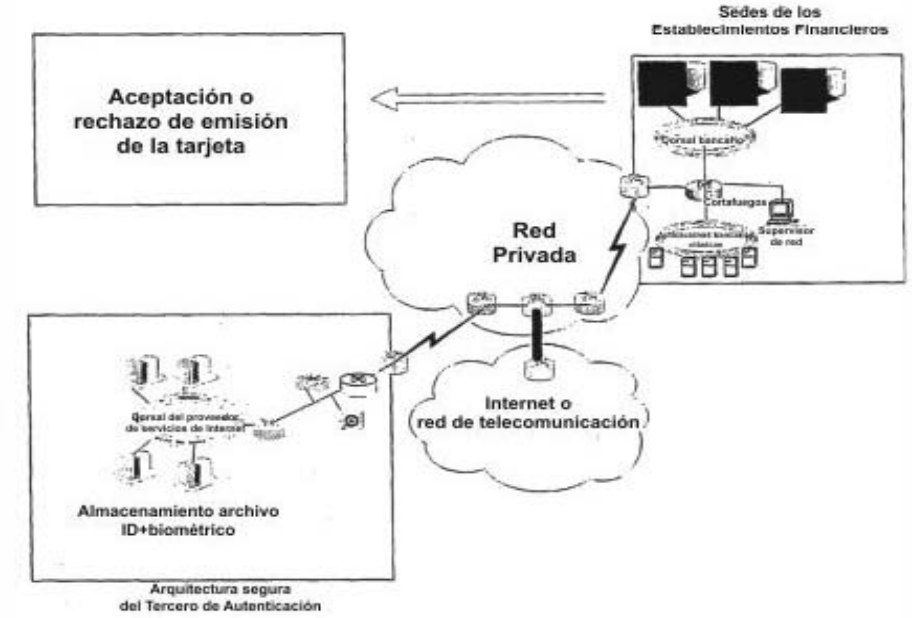

Fig 10: Dispositivo [X00500] Etapa 4, 5, 6, 7 del procedimiento

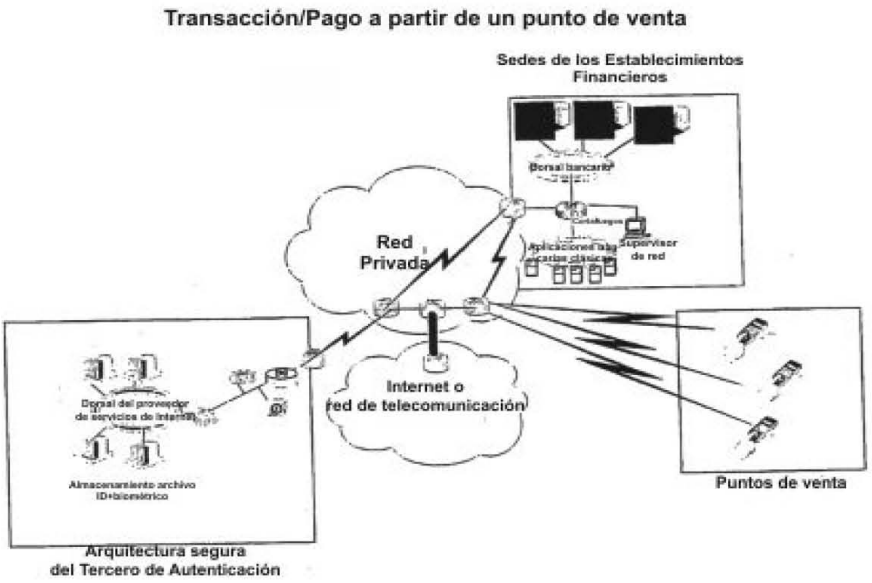

Fig 11: Dispositivo [X00500] Etapa 8, 9, 10, 11, 12, 13 del procedimiento

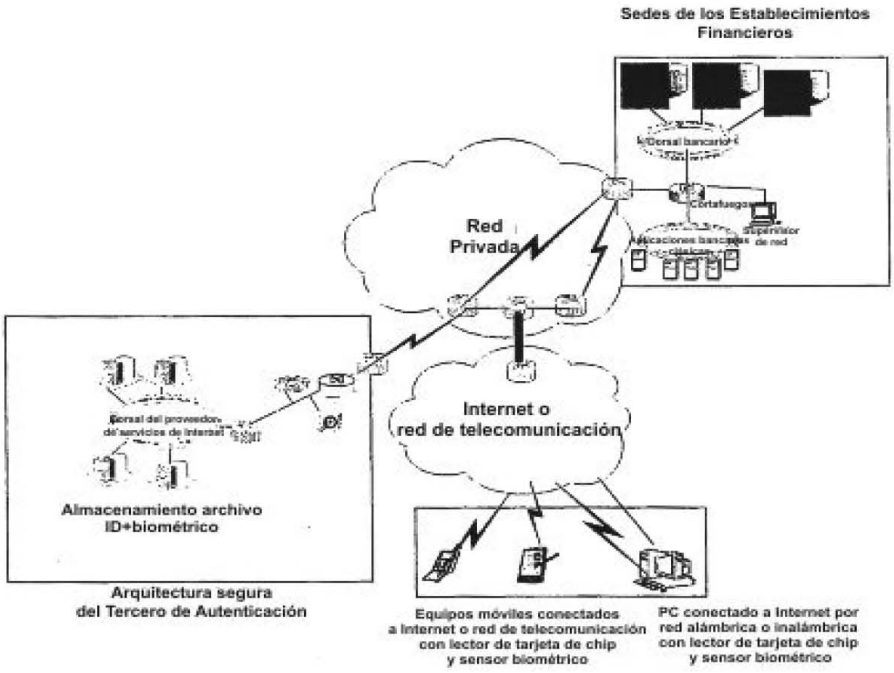

Fig 12: Dispositivo [X00500] Etapa 8, 9, 10, 11, 12, 13 (con otros terminales) del procedimiento