(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 331 314**

(51) Int. Cl.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05253914 .5**
(96) Fecha de presentación : **23.06.2005**
(97) Número de publicación de la solicitud: **1679666**
(97) Fecha de publicación de la solicitud: **12.07.2006**

(54) Título: **Método de renovación y aparato de renovación para un medio que tiene funciones de autenticación biométrica.**

(30) Prioridad: **11.01.2005 JP 2005-4516**

(45) Fecha de publicación de la mención BOPI:
29.12.2009

(45) Fecha de la publicación del folleto de la patente:
29.12.2009

(73) Titular/es: **FUJITSU LIMITED**
1-1, Kamikodanaka 4-chome
Nakahara-ku, Kawasaki-shi
Kanagawa 211-8588, JP
Fujitsu Frontech Limited

(72) Inventor/es: **Awatsu, Kiyotaka;**
Imamura, Hiroshi;
Fujiwara, Masako y
Kudou, Takahiro

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Método de renovación y aparato de renovación para un medio que tiene funciones de autenticación biométrica.

Esta invención se refiere a un método de renovación y aparato de renovación para un medio que tiene funciones de autenticación biométrica para realizar autenticación de un individuo utilizando características de una porción del cuerpo del individuo, y en particular se refiere a un método de renovación y aparato de renovación para un medio que tiene funciones de autenticación biométrica apropiadas para realizar autenticación de un individuo y para evitar la divulgación de información biométrica (a continuación "biometría"). El medio anterior puede ser en forma de una tarjeta CI, por ejemplo.

Hay numerosas porciones del cuerpo humano que pueden diferenciar el individuo, tal como huellas dactilares y huellas de los dedos del pie, la retina de los ojos, las características faciales, y los vasos sanguíneos. Con los avances en tecnología biométrica en los últimos años, se han facilitado varios aparatos que identifican las características biométricas de una porción del cuerpo humano para autenticar individuos.

Por ejemplo, dado que los vasos sanguíneos y las huellas de las palmas y dedos de las manos proporcionan una cantidad comparativamente grande de datos característicos individuales, son adecuados con respecto a la fiabilidad de la autenticación de un individuo. En concreto, las configuraciones de los vasos sanguíneos (venas) no cambian durante toda la vida desde la infancia, y se considera que son completamente únicos, y por ello son adecuados para la autenticación de un individuo. En los métodos de autenticación de la palma, cuando el usuario pone su palma cerca de un aparato de captura de imágenes al tiempo del registro o la autenticación, el aparato de captura de imágenes emite rayos infrarrojos cercanos, que inciden sobre la palma de la mano. El aparato de captura de imágenes usa un sensor para capturar rayos infrarrojos cercanos que rebotan de la palma de la mano.

La hemoglobina en los corpúsculos rojos que fluyen en las venas ha perdido oxígeno. Esta hemoglobina (hemoglobina reducida) absorbe rayos infrarrojos cercanos a longitudes de onda de cerca de 760 nanómetros. En consecuencia, cuando inciden rayos infrarrojos cercanos en la palma de una mano, la reflexión se reduce solamente en las zonas en que hay venas, y la intensidad de los rayos infrarrojos cercanos reflejados puede ser usada para identificar las posiciones de las venas.

El usuario usa primero un aparato de captura de imágenes para registrar datos de imagen de las venas de la palma de la propia mano en un servidor o en una tarjeta. Entonces, con el fin de realizar autenticación de un individuo, el usuario emplea el aparato de captura de imágenes para leer los datos de imagen de las venas de su mano. La imagen de las venas registrada recuperada usando la ID del usuario es verificada contra la configuración de venas de la imagen de las venas para verificación así leída para realizar autenticación de un individuo (véase, por ejemplo, la Publicación de Patente japonesa número 2004-062826).

Tal sistema de autenticación biométrica debe asegurar que los datos de características biométricas no se divulguen a terceras partes. Por lo tanto, en el campo de la autenticación de huellas dactilares, se ha propuesto un método en el que los datos de características de las huellas dactilares de un individuo se registran con anterioridad en una tarjeta CI (circuito integrados) que tiene funciones de autenticación biométrica, y los datos de características de las huellas dactilares leídos de un sensor de huellas dactilares son verificados contra los datos dentro de la tarjeta CI para realizar autenticación de un individuo (Publicación de Patente japonesa número 2000-293643).

En este método, al tiempo de la autenticación de un individuo se usa una tarjeta CI de modo que se pueda evitar la divulgación de los datos de características biométricas a terceras partes, y se pueda mantener la seguridad de loa datos individuales.

Por otra parte, tales tarjetas CI también tienen una fecha de caducidad especificada, y las tarjetas CI deben ser renovadas. En los casos de tarjetas de banda magnética y tarjetas CI no que tienen funciones de autenticación, se adopta un método en el que el emisor envía al usuario una nueva tarjeta con datos registrados, y el usuario destruye la tarjeta antigua.

Sin embargo, en el caso de una tarjeta CI con funciones de autenticación biométrica, como se ha descrito anteriormente, los datos de características biométricas se almacenan solamente en la tarjeta CI, de modo que el emisor no puede emitir una nueva tarjeta en la que estén registrados los datos de características biométricas. Por lo tanto, si el usuario no vuelve a registrar los datos de características biométricas en la tarjeta CI nueva, no se pueden usar las funciones de autenticación biométrica.

En el re-registro de datos de características biométricas en una tarjeta CI nueva, si una persona que ha traído una tarjeta CI nueva enviada por el emisor puede registrar datos de características biométricas, y si la persona no es el individuo en cuestión, entonces se registran los datos de características biométricas de otro individuo, con la posibilidad de uso ilícito de la tarjeta. A la inversa, si se permite la recuperación de datos de características biométricas de una tarjeta CI, existe el problema de que los datos de características biométricas puedan ser divulgados a terceros.

US 2004/123114 describe un método y sistema para la generación, gestión y uso de una Ficha de Identificación Personal Única. Una vez que la Ficha de Identificación Personal Única ha sido concedida a un individuo, el individuo puede almacenar información en un formato electrónico seguro para uso en varias interacciones.

Consiguientemente, es deseable proporcionar un método de renovación y aparato de renovación para medios que tienen funciones de autenticación biométrica, para ejecutar la renovación de los medios en un entorno seguro manteniendo al mismo tiempo el secreto de los datos de características biométricas.

También es deseable proporcionar un método de renovación y aparato de renovación para medios que tienen funciones de autenticación biométrica, para evitar el re-registro de información biométrica por personas distintas del individuo en cuestión, manteniendo al mismo tiempo el secreto de los datos de características biométricas.

Además, es deseable proporcionar un método de renovación y aparato de renovación para medios que tienen funciones de autenticación biométrica, para ejecutar la renovación de los medios en un entorno seguro evitando al mismo tiempo la divulgación de los datos de características biométricas a terceras partes.

Tales medios indicados anteriormente pueden ser tarjetas CI. Un aspecto de esta invención es un aparato de renovación de medio que realiza la renovación de un medio en el que están registrados los datos de características biométricas detectados de un cuerpo, los datos de características biométricas detectadas del cuerpo son verificados contra los datos de características biométricas registrados, y se lleva a cabo autenticación biométrica. El aparato de renovación tiene un dispositivo de detección para detectar los datos biométricos, un dispositivo de lectura/escritura de medio para leer y escribir un medio antiguo a renovar y un medio nuevo, y una unidad de control para extraer los datos de características biométricas de la salida del dispositivo de detección y transferir los datos de características biométricas al medio antiguo. La unidad de control usa las funciones de autenticación biométrica del medio antiguo para verificar los datos de características biométricas registrados contra los datos de características biométricas transferidos, y cuando el resultado permite la autenticación biométrica satisfactoria, registra los datos de características biométricas extraídos en el medio nuevo.

Otro aspecto de esta invención es un método de renovación de tarjetas CI para realizar renovación de una tarjeta CI en la que se registran datos de características biométricas detectados de un cuerpo, y que tiene funciones para verificar los datos de características biométricas registrados contra datos de características biométricas detectados del cuerpo y para realizar autenticación biométrica. El método de renovación de tarjetas CI tiene los pasos de detectar los datos biométricos y extraer datos de características biométricas; de transmitir los datos de características biométricas extraídos a una tarjeta CI antigua a renovar; de verificar los datos de características biométricas registrados contra los datos de características biométricas transmitidos usando las funciones de autenticación biométrica de la tarjeta CI antigua; y de registrar los datos de características biométricas extraídos en una tarjeta CI nueva en respuesta a una autenticación biométrica satisfactoria basada en el resultado de la verificación.

En esta invención, es preferible que, después del registro en la tarjeta CI nueva, la unidad de control bloquee las funciones de autenticación biométrica de la tarjeta CI antigua. En esta invención, es preferible que la unidad de control verifique la información de propiedad de la tarjeta CI antigua leída por el dispositivo de lectura/escritura de tarjetas CI contra la de la tarjeta CI nueva, y que confirme la legitimidad de la correspondencia entre la tarjeta CI antigua y la tarjeta CI nueva.

En esta invención, es preferible que la unidad de control confirme la legitimidad de la tarjeta CI antigua y de la tarjeta CI nueva a partir de la información del emisor de la tarjeta CI antigua y de la tarjeta CI nueva, leída por el dispositivo de lectura/escritura de tarjetas CI.

En esta invención, es preferible que la unidad de control, después del registro en la tarjeta CI nueva, borre los datos de características biométricas en la tarjeta CI antigua.

En esta invención, es preferible que el dispositivo de detección incluya un dispositivo de captura de imágenes para capturar imágenes del cuerpo del usuario.

En esta invención, es preferible que el dispositivo de captura de imágenes incluya una unidad que capture imágenes de vasos sanguíneos del usuario.

En esta invención, es preferible que el dispositivo de lectura/escritura de tarjetas CI incluya un primer dispositivo de lectura/escritura de tarjetas CI que lea/escriba la tarjeta CI antigua, y un segundo dispositivo de lectura/escritura de tarjetas que lea/escriba la tarjeta CI nueva.

En esta invención, es preferible que la unidad de control, después del registro de los datos de características biométricas en la tarjeta CI nueva, detecte de nuevo los datos biométricos del dispositivo de detección, extraiga los datos de características biométricas de la salida del dispositivo de detección, transmita los datos de características biométricas a la tarjeta CI nueva, y verifique los datos de características biométricas registrados en la tarjeta CI nueva contra los datos de características biométricas transmitidos.

En esta invención, es preferible que en la tarjeta CI antigua y en la tarjeta CI nueva, solamente las funciones de autenticación biométrica de las tarjetas CI antigua y nueva accedan a los datos de características biométricas registrados en ellas.

Según esta invención, la identidad del individuo se confirma realizando autenticación biométrica usando las funciones de autenticación biométrica de la tarjeta CI antigua, de modo que la identidad del individuo pueda ser confirmada rigurosamente usando una tarjeta CI con funciones de autenticación biométrica, y se pueda evitar el uso ilícito al tiempo de la renovación. En particular, cuando una tarjeta CI es robada, o un tercero obtiene una tarjeta CI extraviada, se puede evitar el registro de los datos biométricos de una persona distinta del usuario en cuestión en una tarjeta CI de nueva emisión.

Además, si la confirmación de identidad es satisfactoria, los datos biométricos obtenidos en autenticación biométrica se registran en una tarjeta CI nueva cuya legitimidad ha sido confirmada. En consecuencia, con una sola captura de imagen, datos biométricos que han sido confirmados como los del individuo en cuestión usando la tarjeta CI antigua pueden ser registrados en la tarjeta CI nueva sin ser divulgados a terceras partes, y los datos biométricos se pueden pasar fácilmente a la tarjeta CI nueva.

Se hace referencia, a modo de ejemplo solamente, a los dibujos acompañantes en los que:

La figura 1 representa la configuración del sistema de autenticación biométrica de una realización de la invención.

La figura 2 representa la configuración del aparato de renovación de tarjetas CI de la figura 1.

La figura 3 representa la configuración del dispositivo de captura de imágenes de la figura 1 y la figura 2.

La figura 4 es un diagrama de bloques del aparato de renovación de tarjetas CI de la figura 2.

La figura 5 representa la configuración de la tarjeta CI de la figura 1 y la figura 4.

La figura 6 explica los datos de autenticación de la tarjeta CI de la figura 5.

La figura 7 explica el método de autenticación de la tarjeta CI de la figura 6.

La figura 8 es un diagrama de bloques funcionales del procesado de registro/verificación de información biométrica en una realización de la invención.

La figura 9 explica la imagen de vasos sanguíneos de la figura 8.

La figura 10 explica los datos de imagen de vasos sanguíneos de la figura 9.

La figura 11 explica los datos de características A, B de la figura 8.

La figura 12 explica el procesado de renovación de tarjetas CI en una realización de la invención.

La figura 13 es un (primer) diagrama de flujo del procesado de renovación de la tarjeta CI de la figura 12.

La figura 14 es un (segundo) diagrama de flujo de procesado de renovación de la tarjeta CI de la figura 12.

La figura 15 es un (primer) diagrama explicativo de pantallas de guía para el procesado de renovación de la figura 13 y la figura 14.

La figura 16 es un (segundo) diagrama explicativo de pantallas de guía para el procesado de renovación de la figura 13 y la figura 14.

La figura 17 representa la configuración de un aparato de renovación de tarjetas CI de otra realización de la invención.

La figura 18 es un diagrama de bloques del aparato de renovación de tarjetas CI de la figura 17.

La figura 19 es un (primer) diagrama explicativo de pantallas de guía para el procesado de renovación de la figura 17 y la figura 18. Y,

La figura 20 es un (segundo) diagrama explicativo de pantallas de guía para el procesado de renovación de la figura 17 y la figura 18.

A continuación se explican realizaciones de la invención siguiendo el orden de un sistema de autenticación biométrica, procesado de autenticación biométrica, un método de renovación de tarjetas CI, procesado de renovación de tarjetas CI, otras realizaciones de aparato de renovación de tarjetas CI, y otras realizaciones.

Sistema de autenticación biométrica

La figura 1 representa la configuración del sistema de autenticación biométrica de una realización de la invención, la figura 2 representa la configuración del aparato de renovación de tarjetas CI de la figura 1, la figura 3 representa la configuración del dispositivo de captura de imágenes de la figura 1 y la figura 2, la figura 4 es un diagrama de bloques del aparato de renovación de tarjetas CI de la figura 2, y la figura 5 representa la configuración de la tarjeta CI de la figura 1 a la figura 3.

La figura 1 representa, como un ejemplo de un sistema de autenticación biométrica, un sistema de autenticación de venas de la palma en una institución financiera. En la zona de servicio 2 de la institución financiera se ha dispuesto el dispositivo de captura de imágenes de la palma 1 explicado en la figura 2 y la figura 3 y un terminal de sucursal (por ejemplo, un ordenador personal) 3 conectado a él. Un usuario que solicita autenticación de la configuración de las venas pone la mano sobre el dispositivo de captura de imágenes de la palma (a continuación el "dispositivo de captura de imágenes") 1. El dispositivo de captura de imágenes 1 lee la palma, y el proceso de extracción de imágenes de los vasos sanguíneos lo realiza el terminal 3 para extraer la configuración de las venas, que se registra como datos de venas en el terminal 3.

Estos datos de venas se registran en un dispositivo de almacenamiento portátil (por ejemplo, una tarjeta CI) 5 que lleva el usuario. El servidor 4 está conectado a un terminal de zona de servicio 8 en la zona de servicio 7 de la institución financiera, y el terminal de zona de servicio 8 está conectado al dispositivo de captura de imágenes 1.

Para efectuar una retirada de fondos o realizar alguna otra transacción financiera en la zona de servicio 7 de la institución financiera, el usuario introduce una tarjeta CI en el lector de tarjetas CI explicado en la figura 2 y la figura 4, y mantiene la mano sobre el dispositivo de captura de imágenes 1 dispuesto en la zona de servicio 7. El dispositivo de captura de imágenes 1 lee la palma de la mano, y a través del procesado de extracción de imágenes de los vasos sanguíneos realizado por el terminal de zona de servicio 8, extrae la configuración de las venas. El terminal de zona de servicio 8 realiza procesado de verificación para verificar la configuración de las venas, como datos de venas, contra datos de venas registrados en la tarjeta CI 5, para autenticar el individuo.

El servidor 4 está conectado a un CA (máquina automática de depósito/extracción de dinero en efectivo) 6 de la institución financiera; el CA 6 puede ser usado en transacciones basadas en autenticación de venas. Con el fin de hacer una extracción o realizar alguna otra transacción financiera usando el CA 6, el usuario mantiene su mano sobre el dispositivo de captura de imágenes 1-1 dispuesto en el CA 6. El dispositivo de captura de imágenes 1-1 lee la palma de la mano. Al igual que el terminal de zona de servicio 8, el CA 6 extrae la configuración de las venas (imagen de los vasos sanguíneos), y la verifica como datos de venas contra los datos de venas registrados en la tarjeta CI 5 que lleva el usuario, para autenticar al individuo.

El servidor 4 está conectado además al aparato de renovación de tarjetas CI 20 explicado en la figura 2 y la figura 4.

La figura 2 representa la configuración del aparato de renovación de tarjetas CI de la figura 1. Como se representa en la figura 2, el aparato de renovación de tarjetas CI 20 tiene una unidad principal de dispositivo de renovación 22, un dispositivo de autenticación 26 que tiene un lector de tarjetas CI y un dispositivo de captura de imágenes de la palma (sensor de venas), y el lector de tarjetas CI 9-1. La unidad principal de dispositivo de renovación 22 incluye por ejemplo un ordenador personal, y tiene una porción de operación de cliente 24 incluyendo una pantalla táctil.

El dispositivo de lectura/escritura de tarjetas CI 9-1 realiza lectura y escritura del chip CI y la banda magnética de una tarjeta CI 5 del usuario, descrita más adelante en la figura 5. Un módulo de aplicación de seguridad (SAM) está dispuesto en el dispositivo de lectura/escritura de tarjetas CI 9; solamente se acepta el acceso autenticado, para mantener la seguridad de la tarjeta CI 5.

Como se representa en la figura 2, el dispositivo de autenticación 26 está equipado con una unidad sensora 18 sustancialmente en el centro de la unidad principal 10. En la porción delantera (en el lado del usuario) de la unidad sensora 18 se ha dispuesto una guía delantera 14; en la porción trasera se ha dispuesto una guía trasera 19. La guía delantera 14 incluye una hoja de resina sintética, transparente o sustancialmente transparente.

La guía delantera 14 cumple la finalidad de guiar la mano del usuario en la parte delantera y de soportar la muñeca. Por lo tanto, la guía delantera 14 proporciona guía al usuario para guiar y soportar la muñeca encima de la unidad sensora 18. Como resultado, la postura de la palma de la mano, es decir, la posición, la inclinación y el tamaño sobre la unidad sensora 18 pueden ser controlados. La forma en sección transversal de la guía delantera 14 tiene un cuerpo vertical y, en la porción superior, una porción horizontal 14-1 para soportar la muñeca. Se ha formado una depresión 14-2 de forma continua en el centro de la porción horizontal 14-1, para facilitar la colocación de la muñeca. La guía trasera 19 cumple la finalidad de soportar los dedos de la mano.

Como se representa en la figura 3, la unidad sensora 18 está provista de un sensor de infrarrojos (sensor CMOS) y lente de enfoque 16 y un sensor de distancia 15 en el centro; en su periferia se ha dispuesto una pluralidad de elementos emisores de luz infrarroja cercana (LEDs) 12. Por ejemplo, los elementos emisores de luz infrarroja cercana están dispuestos en ocho lugares en la periferia, para emitir rayos infrarrojos cercanos hacia arriba.

La región legible de esta unidad sensora 18 V es regulada por la relación entre el sensor, lente de enfoque, y región de emisión de luz infrarroja cercana. Por lo tanto, la posición y la altura de la guía delantera 14 se establecen de tal manera que la muñeca soportada se coloque en la región legible V.

Cuando la mano 52 se extiende con la palma plana, la palma tiene una zona máxima, y además es plana, de modo que cuando la palma se somete a captura de imagen en la región de captura de imagen V de la unidad sensora 18, se obtiene una configuración exacta de las venas que puede ser usada en el registro y la verificación. Cuando la distancia de la unidad sensora 18 a la palma está dentro de un rango preestablecido, el sensor 16 de la unidad sensora 18 obtiene una imagen nítida enfocada.

Por lo tanto, como se representa en la figura 3, haciendo que la guía delantera 14 soporte la muñeca 52 encima de la unidad sensora 18, la posición, la inclinación y la altura de la palma encima de la unidad sensora 18 resultan exactas con respecto al rango de captura de imagen de la unidad sensora 18, y la mano del usuario puede ser guiada y soportada.

Los dispositivos de captura de imagen de la palma 1 y 1-1 en la figura 1 tienen una configuración similar. Además del dispositivo de captura de imágenes de la palma 1, el dispositivo de autenticación 26 de la figura 2 tiene además un dispositivo de lectura/escritura de tarjetas CI 9 dispuesto en la unidad principal 10.

Como se representa en la figura 4, la unidad principal de dispositivo de renovación 22 opera de acuerdo con la unidad de operación de cliente 24, y tiene una aplicación de renovación 30 que realiza el procesado de renovación de una tarjeta CI 5, y una librería de autenticación de venas (programa) 34 para el procesado de autenticación de venas. La aplicación de renovación 30 está conectada al host (servidor) 4, y envía notificaciones del estado de renovación.

El dispositivo de autenticación 26 tiene un dispositivo de lectura/escritura de tarjetas CI 9, un sensor de venas 1, y un controlador (módulo de aplicación segura) 32. El dispositivo de lectura/escritura de tarjetas CI 28 tiene un dispositivo de lectura/escritura de tarjetas CI 9-1 y un controlador (módulo de aplicación segura) 36.

La figura 5 es un diagrama de bloques de una tarjeta CI que tiene funciones de autenticación biométrica de la figura 1 a la figura 4. Como se representa en la figura 5, la tarjeta CI 5 tiene una CPU (unidad central de procesado) 50, ROM (memoria de lectura solamente) 54, RAM (memoria de acceso aleatorio) 56, y una EEPROM 58. Una ROM 54 guarda un OS (sistema operativo) y similares.

Un programa 510 para la aplicación de autenticación de venas 51, un cortafuegos 53, una aplicación financiera 55, un cortafuegos para la misma 57, y otras aplicaciones 59 y archivos 520 están almacenados en la EEPROM 58. El programa 510 de la aplicación de autenticación de venas 51 tiene lógica de procesado de registro de lectura, lógica de procesado de registro de actualización, y lógica de procesado de verificación. La lógica de procesado de verificación incluye lógica de autenticación de venas (algoritmo de verificación secundaria) 512.

Por otra parte, los datos de porción de vena A (descritos más tarde usando la figura 9) y los datos de porción B de vena (descritos más tarde usando la figura 9), escritos por un terminal al tiempo del registro de venas, están almacenados en los archivos 520. Los datos de porción de vena A son referenciados por la lógica de procesado de registro de lectura del terminal al tiempo de verificación de las venas (verificación primaria). Los datos de porción B de vena son referenciados por la lógica de autenticación de venas 512 al tiempo del procesado de orden de verificación (verificación secundaria), y se han previsto para verificación secundaria por la lógica de autenticación de venas 512.

Otros datos 526 son datos en el formato RSA (clave privada/clave pública) conocido usado en tarjetas CI de dinero en efectivo, y son referenciados por la lógica de procesado de registro de lectura del terminal durante la autenticación de tarjeta (procesado SDA).

Es decir, como se representa en la figura 6, los otros datos 526 incluyen datos SDA y un número de cuenta y otra información para el portador. Los datos SDA incluyen unos datos estáticos de autenticación, unos datos de aplicación firmados encriptados en unos datos estáticos de autenticación usando la clave secreta del emisor, y un certificado de clave pública del emisor que es la clave pública del emisor encriptada usando la clave privada CA de la autoridad de certificado (CA) 100 y emitida por la autoridad de certificado 100. Los terminales 3, 6, 8, 22 realizan autenticación fuera de línea para confirmar que estos datos SDA sean emitidos por el emisor legítimo de la tarjeta.

Como se representa en la figura 7, un certificado de clave pública del emisor encriptado usando la clave privada CA y leído de la tarjeta CI 5 es desencriptado por un terminal 3, 6, 8, o 22 usando la clave pública CA, para recuperar la clave pública del emisor. A continuación, los datos de aplicación firmados encriptados usando la clave privada del emisor, que se leen de la tarjeta CI 5, son desencriptados por el terminal 3, 6, 8 o 22 usando la clave pública del emisor recuperada, para recuperar los datos estáticos de autenticación. Y los datos estáticos de autenticación leídos de la tarjeta CI 5 se comparan con los datos estáticos de autenticación desencriptados para verificar la legitimidad. Mediante esto, el terminal confirma en procesado fuera de línea que una tarjeta fue emitida por un emisor legítimo.

Por otra parte, se usa una clave compartida en un método de autenticación DES de mutua autenticación de una tarjeta CI 5 y un terminal (o host); con el fin de autenticar el terminal, los datos de autenticación son encriptados por el terminal usando la clave compartida para obtener un código de autenticación, y este código de autenticación es

transmitido a la tarjeta CI 5. En la tarjeta CI 5, los datos de autenticación son encriptados usando la clave compartida y el resultado se compara con el código de autenticación, para verificar la legitimidad del código de autenticación.

Con el fin de autenticar la tarjeta CI, los datos de autenticación son encriptados por la tarjeta CI usando la clave compartida para obtener un código de autenticación, que es transmitido al terminal; en el terminal, el código de autenticación se compara con los datos de autenticación encriptados con el código de autenticación usando la clave compartida, para verificar la legitimidad del código de autenticación.

Método de procesado de autenticación biométrica

La figura 8 es un diagrama de bloques de procesado de autenticación biométrica en una realización de la invención, la figura 9 explica la imagen detectada de vasos sanguíneos de la figura 8, la figura 10 explica el procesado de verificación de la figura 8, y la figura 11 explica los datos de registro de venas A, B para el procesado de verificación.

Como se representa en la figura 8, los terminales de zona de servicio 3 y 8 conectados al dispositivo de captura de imágenes 1 y la librería de autenticación 34 del aparato de renovación de tarjetas CI 20 ejecutan la serie de registro y procesado de verificación 34-1 a 34-6. Como se describe más adelante, la CPU 50 del chip CI en la tarjeta CI 5 también realiza procesado de verificación (verificación secundaria) 34-3.

El procesado de detección de distancia/contorno de la mano 34-1 recibe la distancia medida por el sensor de distancia 15 del dispositivo de captura de imágenes 1, 1-1, determina si la palma de la mano u otro objeto está a una distancia del rango preestablecido de la unidad sensora 18 y también detecta el contorno de la mano de la imagen capturada por la unidad sensora 18, y determina a partir del contorno si la imagen puede ser usada en el registro y procesado de verificación. Por ejemplo, la palma puede no aparecer suficientemente en la imagen.

El procesado de salida de mensaje de guía 34-5 envía a la pantalla de los terminales de zona de servicio 3, 8 y la unidad de operación de cliente 24 del aparato de renovación de tarjetas CI 20 un mensaje que guía la palma a la izquierda o a la derecha, hacia delante o hacia atrás, hacia arriba o hacia abajo, cuando la distancia medida por el sensor de distancia 15 indica que la mano está fuera del rango de captura de imagen, o cuando la extracción del contorno de la mano indica que la imagen no puede ser usada en el registro y procesado de verificación. Mediante esto, la mano del usuario es guiada a posición sobre el dispositivo de captura de imágenes 1.

El procesado de extracción de imágenes de los vasos sanguíneos 34-2 extrae una imagen de las venas de la imagen de la mano cuando el procesado de detección del contorno de la mano 34-1 determina que una imagen ha sido capturada con la mano mantenida correctamente. Es decir, se obtienen datos en escala de grises de la imagen de la palma, tal como la de la figura 10, a través de diferencias de reflectividad, como se ha explicado anteriormente con referencia a la técnica anterior. La configuración de imagen de las venas es una imagen análoga a la representada en la figura 9; los datos son datos en escala de grises como los de la figura 10.

El proceso de búsqueda de imagen de vasos sanguíneos registrada 34-4 recupera datos registrados de imagen de vasos sanguíneos A correspondientes a la ID del individuo (número de cuenta) de la porción de almacenamiento 56 del chip CI en la tarjeta CI 5 representada en la figura 1, figuras 4 y 5. El procesado de verificación 34-3 compara los datos de imagen de vasos sanguíneos N1 extraídos en el procesado de detección de imagen de vasos sanguíneos 34-2 con los datos registrados de imagen de vasos sanguíneos N2 representados en la figura 10, realiza procesado de verificación, y envía el resultado de la verificación.

Como se representa en la figura 11 y también se puede ver en la figura 9, los datos sencillos (datos de imagen de vasos sanguíneos) R pueden ser clasificados en troncos Aa, ramificaciones gruesas Ab, y ramificaciones finas Ac conectadas a ramificaciones gruesas. Los troncos A1 y las ramificaciones gruesas A2 se dividen en datos de características comparativamente bastos A, y las ramificaciones finas Ac se dividen en datos de características comparativamente finos B, para crear datos registrados A, B. Los datos registrados A son comparativamente bastos y así no muestran características finas, sino que representan características bastas. Los datos registrados B son comparativamente finos, y así representan características finas.

El procesado de registro 34-6 divide los datos de imagen de vasos sanguíneos detectados en datos de imagen de vasos sanguíneos de nivel comparativamente basto A y datos de imagen de vasos sanguíneos de nivel comparativamente fino B, y guarda los datos en el chip CI 50 de la tarjeta CI 5 mediante el dispositivo de lectura/escritura de tarjetas CI 9.

Es decir, la librería de autenticación 34 del terminal referencia los datos de porción de vena A de la tarjeta CI 5 explicados en la figura 5 y realiza verificación (llamada verificación primaria). Por otra parte, la lógica de autenticación de venas 512 de la aplicación de autenticación de venas 510 de la tarjeta CI 5 explicada en la figura 5 referencia los datos de porción B en la tarjeta CI 5 y realiza verificación (llamada verificación secundaria).

En este sistema de autenticación de imagen de vasos sanguíneos, mantener simultáneamente el secreto de los datos de imagen de vasos sanguíneos y la fiabilidad de la renovación de tarjeta CI sirve para asegurar la renovación de una tarjeta CI que tiene funciones de autenticación biométrica.

Método de renovación de tarjetas CI

La figura 12 explica el procedimiento del método de renovación de tarjetas CI en una realización de la invención, y presenta un ejemplo que usa el aparato de renovación de tarjetas CI 20 de la figura 1, la figura 2 y la figura 4.

(1) El usuario introduce una tarjeta CI 5 con funciones de autenticación biométrica, cuya fecha de caducidad ha pasado (llamada una tarjeta CI antigua), y una tarjeta CI reemitida con funciones de autenticación biométrica (llamada una tarjeta CI nueva) 5-1, en los dispositivos de lectura/escritura de tarjeta CI 9 y 9-1 respectivamente. Los respectivos dispositivos de lectura/escritura de tarjeta CI 9 y 9-1 supervisan la extracción de las tarjetas CI después de la introducción de la tarjeta CI hasta la terminación del procesado de re-registro, y si se saca alguna tarjeta CI, se interrumpe el procesado.

(2) En primer lugar, la aplicación de renovación 30 del terminal 22 ejecuta autenticación de tarjeta de la tarjeta CI antigua 5 usando el método RSA explicado anteriormente usando la figura 6 y la figura 7, mediante el dispositivo de lectura/escritura de tarjetas CI 9, para confirmar la legitimidad de la tarjeta. Igualmente, el terminal 22 realiza autenticación de tarjeta de la tarjeta CI nueva 5-1 usando el método RSA explicado anteriormente usando la figura 6 y la figura 7 mediante el dispositivo de lectura/escritura de tarjetas CI 9-1, para confirmar la legitimidad de la tarjeta.

(3) A continuación, la aplicación de renovación 30 del terminal 22 lee y compara la información del individuo (número de cuenta y similar de los datos de tenedor en la figura 5) en la tarjeta CI antigua 5 y la información del individuo (número de cuenta y similar de los datos de tenedor en la figura 5) en la tarjeta CI nueva 5-1, mediante los dispositivos de lectura/escritura de tarjeta CI 9, 9-1. Mediante esto, se confirma que la tarjeta CI nueva 5-1 fue re-emitida para sustituir a la tarjeta CI antigua 5. El terminal 22 también confirma, a través del dispositivo de lectura/escritura de tarjetas CI 9, que los datos biométricos no han sido registrados en la tarjeta CI nueva 5-1.

(4) A continuación, la aplicación de renovación 30 del terminal 22 usa el sensor de venas 1 del aparato de autenticación 26 para la captura de imagen de los datos biométricos, con el fin de obtener datos de imagen de los vasos sanguíneos C de la palma. La aplicación de renovación 30 del terminal 22 usa la librería de autenticación (análisis y verificación) 34 para verificar los datos de imagen de vasos sanguíneos C contra los datos de venas A de la tarjeta CI antigua 5. Si el resultado de la verificación es satisfactorio, los datos de venas B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos a la tarjeta CI antigua 5, y la lógica de autenticación de venas de la tarjeta CI antigua 5 verifica los datos B' contra los datos de porción B de vena B en la tarjeta CI antigua 5. Mediante esto, se lleva a cabo autenticación biométrica usando la tarjeta CI antigua 5.

(5) Cuando la autenticación de un individuo se lleva a cabo mediante autenticación biométrica usando la tarjeta CI antigua 5, los datos biométricos son registrados en la tarjeta CI nueva 5-1, en base a los datos de imagen de vasos sanguíneos C capturados en (4). Es decir, los datos de venas A', B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos al dispositivo de lectura/escritura de tarjetas CI 9-1, y a través del procesado de registro actualizado de la tarjeta CI nueva 5-1, se escriben en las regiones 522, 524 de los archivos 520.

(6) Para verificación, la aplicación de renovación 30 del terminal 22 realiza captura de imagen de datos biométricos usando el sensor de venas 1 del dispositivo de autenticación 26, para obtener datos de imagen de vasos sanguíneos C de la palma. La aplicación de renovación 30 del terminal 22 usa la librería de autenticación (análisis y verificación) 34 para verificar los datos de venas A creados a partir de los datos de imagen de vasos sanguíneos C contra los datos de venas A' de la tarjeta CI nueva 5-1. Si el resultado de la verificación es satisfactorio, los datos de venas B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos a la tarjeta CI nueva 5-1, y por medio de la lógica de autenticación de venas 512 de la tarjeta CI nueva 5, son verificados contra los datos de porción B de vena en la tarjeta CI nueva 5-1. Mediante esto, se lleva a cabo el procesado de autenticación biométrica usando la tarjeta CI nueva 5.

(7) Cuando la autenticación de un individuo es exitosa mediante la autenticación biométrica usando la tarjeta CI nueva 5-1, la aplicación de renovación 30 del terminal 22 borra los datos biométricos A, B en la tarjeta CI antigua 5 a través del dispositivo de lectura/escritura de tarjetas CI 9. Por ejemplo, mediante el procesado de registro actualizado de la tarjeta CI antigua 5, se escriben nulos (todo "1"s) en las regiones 522, 524 de los archivos 520. Además, la aplicación de renovación del terminal 22 inactiva las funciones de autenticación de vena de la tarjeta CI antigua 5 a través del dispositivo de lectura/escritura de tarjetas CI 9. Es decir, la aplicación de autenticación de venas 51 queda bloqueada. Mediante esto, se borran los datos biométricos de la tarjeta CI antigua 5, y además se inactivan las funciones de autenticación de vena. Como resultado, la tarjeta CI antigua 5 es una tarjeta que ya no tiene funciones de autenticación biométrica.

Así, en primer lugar se confirma que la tarjeta CI antigua y la tarjeta CI nueva son tarjetas CI emitidas por un emisor legítimo, y se confirma la legitimidad de la tarjeta CI para renovación propiamente dicha. A continuación, mediante autenticación biométrica usando la tarjeta CI antigua, se confirma que la persona es el individuo en cuestión en base a autenticación biométrica. Por lo tanto, la confirmación del individuo usando una tarjeta CI con funciones de autenticación biométrica puede ser realizada rigurosamente, y se pueden evitar acciones ilícitas al tiempo de la renovación. En particular, cuando una tarjeta CI ha sido robada o un tercero obtiene una tarjeta CI extraviada, se puede evitar el registro de los datos biométricos de una persona distinta del usuario en cuestión en una tarjeta CI reemitida.

Si la confirmación del individuo tiene éxito, los datos biométricos obtenidos en la autenticación biométrica son registrados en la tarjeta CI nueva, cuya legitimidad ha sido confirmada. Mediante esto, a través de una sola captura de imagen, y usando la tarjeta CI antigua, los datos biométricos confirmados como los del individuo en cuestión pueden ser registrados en la tarjeta CI nueva sin divulgar datos biométricos a un tercero, de modo que la migración de datos biométricos a una tarjeta CI nueva puede ser realizada de forma fácil y fiable.

Se lleva a cabo autenticación de ensayo para verificar los datos biométricos registrados en la tarjeta CI nueva, y para verificar las funciones de autenticación biométrica de la tarjeta CI nueva renovada. Si esta verificación se lleva a cabo satisfactoriamente, se borran los datos biométricos en la tarjeta CI antigua y se inactivan las funciones de autenticación de vena de la tarjeta CI antigua, de modo que la tarjeta CI antigua 5 sea una tarjeta que no tenga funciones de autenticación biométrica, y ya no pueda ser usada.

En consecuencia, se puede evitar la divulgación de datos biométricos como resultado de la renovación de tarjeta CI. En particular, si los datos biométricos o las funciones de autenticación de vena permanecen en una tarjeta CI antigua, puede haber oportunidades para la divulgación de datos biométricos o la ingeniería inversa de funciones de autenticación, y la eliminación de tales oportunidades es altamente ventajosa.

Procesado de renovación de tarjetas CI

A continuación, se explica el procesado para el método de renovación de tarjetas CI explicado en la figura 12, usando las figuras 13 a 16. La figura 13 y la figura 14 son diagramas de flujo de procesado de la renovación de tarjeta CI, y la figura 15 y la figura 16 explican las pantallas de guía para este procesado.

(S10) La pantalla de selección de renovación G1 de la figura 15 se presenta en la unidad de operación de cliente 24 del aparato de renovación de tarjetas CI 20. Para pedir la renovación, el usuario pulsa un icono de inicio en la pantalla de selección G1. Como resultado, se inicia el procesado de renovación. El usuario introduce una tarjeta CI caducada 5 con funciones de autenticación biométrica (una tarjeta CI antigua) en el dispositivo de lectura/escritura de tarjetas 9, según la pantalla de guía de introducción de tarjeta CI antigua G2 de la figura 15. El dispositivo de lectura/escritura de tarjetas CI 9 lee el contenido (distinto del estado biométrico protegido por la aplicación de autenticación biométrica) de la tarjeta CI antigua 5 introducida, y presenta la pantalla de lectura actual G3 de la figura 15. El dispositivo de lectura/escritura de tarjetas CI 9 supervisa la extracción de la tarjeta CI de la introducción de la tarjeta CI hasta la terminación del procesado de re-registro. Si se saca la tarjeta CI, se interrumpe el procesado.

(S12) A continuación, el usuario introduce una tarjeta CI 5-1 con funciones de autenticación biométrica (una tarjeta CI nueva) en el dispositivo de lectura/escritura de tarjetas CI 9-1, según la pantalla de guía de introducción de tarjeta CI nueva G4 de la figura 15. El dispositivo de lectura/escritura de tarjetas CI 9-1 lee el contenido (regiones 526, 528 de los archivos 520) de la tarjeta CI nueva 5-1 introducida, y presenta la pantalla de lectura actual G5 de la figura 15. El dispositivo de lectura/escritura de tarjetas CI 9-1 supervisa la extracción de la tarjeta CI desde la introducción de la tarjeta CI hasta la terminación del procesado de re-registro. Si se saca la tarjeta CI, se interrumpe el procesado.

(S14) A continuación, la aplicación de renovación 30 del terminal 22 realiza autenticación de tarjeta de la tarjeta CI antigua 5 usando el método RSA explicado anteriormente usando las figuras 6 y 7, mediante el dispositivo de lectura/escritura de tarjetas CI, para confirmar la legitimidad de la tarjeta. Si el resultado de la autenticación no es satisfactorio, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S16) Si la legitimidad de la tarjeta CI antigua 5 queda confirmada satisfactoriamente, entonces el terminal 22 lleva a cabo igualmente la autenticación de tarjeta de la tarjeta CI nueva 5-1 usando el método RSA explicado en las figuras 6 y 7 anteriores, mediante el dispositivo de lectura/escritura de tarjetas CI 9-1, para confirmar la legitimidad de la tarjeta. Si el resultado de la autenticación no es satisfactorio, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S18) A continuación, la aplicación de renovación 30 del terminal 22 confirma, a partir de la información del individuo (la fecha de caducidad en los datos de tenedor de la figura 5) en la tarjeta CI antigua 5 leídos por el dispositivo de lectura/escritura de tarjetas CI 9, que la fecha de caducidad de la tarjeta CI antigua 5 ha pasado o está a punto de pasar. Además, la aplicación de renovación 30 compara la información del individuo (número de cuenta y similar) de la tarjeta CI antigua 5 con la información del individuo (número de cuenta en los datos de tenedor de la figura 5 y similar) de la tarjeta CI nueva 5-1. Mediante esto, se confirma que la tarjeta CI nueva 5-1 es una tarjeta re-emitida para sustituir a la tarjeta CI antigua 5. Si el resultado de la confirmación no es satisfactorio, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S20) Por otra parte, si el resultado de la confirmación es satisfactorio, el procesado avanza a la figura 14, y el terminal 22 confirma, mediante el dispositivo de lectura/escritura de tarjetas CI 9, que los datos biométricos no han sido registrados en la tarjeta CI nueva 5-1. Si los datos han sido registrados, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S22) A continuación, si no se han registrado datos, la aplicación de renovación 30 del terminal 22 visualiza la pantalla de guía de palma G6 de la figura 15, guiando al usuario en la colocación de su palma sobre el sensor de

venas 1 del dispositivo de autenticación 26. Entonces el sensor de venas 1 captura una imagen de la palma, se lleva a cabo el procesado de captura de imagen 34-1 explicado en la figura 8, y si el resultado de la captura de imagen no es satisfactorio, tiene lugar la guía de captura de imagen a través del procesado de mensaje de guía 34-5.

(S24) Si el resultado de la captura de imagen es satisfactorio, se obtienen datos de imagen de vasos sanguíneos C de la palma del procesado de extracción de imágenes de los vasos sanguíneos 34-2 de la figura 8. La aplicación de renovación 30 del terminal 22 verifica los datos de venas A' creados a partir de datos de imagen de vasos sanguíneos C contra los datos de venas A de la tarjeta TC antigua 5, usando la librería de autenticación (análisis y verificación) 34. Si el resultado de la verificación es satisfactorio, los datos de venas B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos a la tarjeta CI antigua 5, y la lógica de autenticación de venas 512 de la tarjeta CI antigua 5 se usa para verificar los datos B' contra los datos de porción B de vena B en la tarjeta CI antigua 5. Mediante esto, se lleva a cabo autenticación biométrica usando la tarjeta CI antigua 5. Si el resultado de la autenticación no es satisfactorio, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S26) Si el individuo en cuestión puede ser confirmado a través de autenticación biométrica usando la tarjeta CI antigua 5, aparece la pantalla de confirmación de individuo G8 en la unidad de operación de cliente 24, y en base a los datos de imagen de vasos sanguíneos C capturados en el paso S24, los datos biométricos son registrados en la tarjeta CI nueva 5-1. Es decir, los datos de venas A', B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos al dispositivo de lectura/escritura de tarjetas CI 9-1, y a través de procesado de registro actualizado de la tarjeta CI nueva 5-1, se lleva a cabo escritura en las regiones 522, 524 de los archivos 520.

(S28) Para verificación, la aplicación de renovación 30 del terminal 22 visualiza la pantalla de guía de palma G9 de la figura 15, para guiar la palma del usuario sobre el sensor de venas 1 del dispositivo de captura de imágenes 26. El sensor de venas 1 captura una imagen de la palma, se lleva a cabo el procesado de captura de imagen 34-1 explicado en la figura 8, y si el resultado de la captura de imagen no es satisfactorio, tiene lugar la guía de captura de imagen por el procesado de mensaje de guía 34-5.

(S30) Si el resultado de la captura de imagen es satisfactorio, se obtienen datos de imagen de vasos sanguíneos C de la palma a través del procesado de extracción de imágenes de los vasos sanguíneos 34-2 de la figura 8. La aplicación de renovación 30 del terminal 22 visualiza la pantalla de procesado de autenticación G10 de la figura 16 en la unidad de operación de cliente 24, y verifica los datos de venas A' creados a partir de datos de imagen de vasos sanguíneos C contra los datos de venas A' de la tarjeta CI nueva 5-1 mediante la librería de autenticación (análisis y verificación) 34. Si el resultado de la verificación es satisfactorio, los datos de venas B' creados a partir de los datos de imagen de vasos sanguíneos C son transmitidos a la tarjeta CI nueva 5-1, y la lógica de autenticación de venas 512 de la tarjeta CI nueva 5-1 verifica los datos transmitidos contra los datos de porción B de vena B' registrados en la tarjeta CI nueva 5-1. Mediante esto, se lleva a cabo el procesado de autenticación biométrica usando la tarjeta CI nueva 5. Si el resultado de la autenticación no es satisfactorio, aparece un mensaje de error en la unidad de operación de cliente 24, y el procesado termina.

(S32) Mediante autenticación biométrica usando la tarjeta CI nueva 5-1, se confirma la identidad del individuo, y la aplicación de renovación 30 del terminal 22 visualiza la pantalla de fin de registro 311 de la figura 16 en la unidad de operación de cliente 24, y entonces borra los datos biométricos A, B de la tarjeta CI antigua 5 mediante el dispositivo de lectura/escritura de tarjetas CI 9. Por ejemplo, el procesado de registro actualizado por la tarjeta CI antigua 5 escribe nulos (todo "1"s) en las regiones 522, 524 de los archivos 520.

(S34) Las tarjetas CI 5 y 5-1 pueden ser usadas en la autenticación biométrica de un agente distinto del individuo que ha recibido el consentimiento del individuo; y en consecuencia, es posible el registro de una imagen de vasos sanguíneos de la palma del agente. Cuando tal registro deba ser realizado, pulsando el icono de registro de datos biométricos en la unidad de operación de cliente 24, aparece la pantalla de continuación de registro G14 de la figura 16, y el procesado vuelve al paso S22.

(S36) Por otra parte, cuando no hay más datos biométricos a registrar, la aplicación de renovación 30 del terminal 22 inactiva las funciones de autenticación de vena de la tarjeta CI antigua 5 mediante el dispositivo de lectura/escritura de tarjetas 9. Es decir, la aplicación de autenticación de venas 51 queda bloqueada. Mediante esto, se borran los datos biométricos de la tarjeta CI antigua 5, y además se inactivan las funciones de autenticación de vena. Como resultado, la tarjeta CI antigua 5 es una tarjeta que no tiene funciones de autenticación biométrica. Entonces aparece la pantalla de devolución a tarjeta CI nueva 5-1 G12 en la unidad de operación de cliente 24, y la tarjeta CI nueva 5-1 es devuelta por el dispositivo de lectura/escritura de tarjetas 9-1. A continuación, aparece la pantalla de devolución de tarjeta CI antigua 5 G13 en la unidad de operación de cliente 24, y la tarjeta CI antigua 5 es devuelta por el dispositivo de lectura/escritura de tarjetas CI 9. Entonces termina el procesado.

De esta forma, se determina si la fecha de caducidad de la tarjeta CI antigua ha pasado o está a punto de pasar, se confirma que la tarjeta es una tarjeta CI emitida legítimamente por un emisor, y la continuidad con la tarjeta CI a usar para renovación se confirma en base a la información de tenedor en la tarjeta CI antigua y la tarjeta CI nueva.

A continuación, se emplea autenticación biométrica usando la tarjeta CI antigua para confirmar la identidad del individuo a través de autenticación biométrica. Mediante esto, la confirmación del individuo se puede llevar a cabo rigurosamente usando una tarjeta CI con funciones de autenticación biométrica. Por lo tanto, cuando roban una tarjeta

CI, o un tercero obtiene una tarjeta extraviada, se puede evitar el registro de los datos biométricos de una persona distinta del usuario en cuestión en una tarjeta CI reemitida.

Si la confirmación del individuo es satisfactoria, los datos biométricos obtenidos en la autenticación biométrica son registrados en la tarjeta CI nueva cuya legitimidad ha sido confirmada. Mediante esto, a través de una sola operación de captura de imagen, y usando una tarjeta CI antigua, los datos biométricos confirmados como del individuo pueden ser registrados en la tarjeta CI nueva sin ser divulgados a terceras partes, y los datos biométricos pueden pasar de forma fácil y fiable a la tarjeta CI nueva.

Además, con el fin de verificar los datos biométricos registrados en la tarjeta CI nueva, se lleva a cabo autenticación de ensayo, y se verifican las funciones de autenticación biométrica de la tarjeta CI nueva renovada. Si la verificación es satisfactoria, se borran los datos biométricos en la tarjeta CI antigua y se inactivan las funciones de autenticación de vena de la tarjeta antigua, de modo que la tarjeta CI antigua 5 sea una tarjeta que no tenga funciones de autenticación biométrica, y ya no se pueda usar.

En consecuencia, se puede evitar la divulgación de datos biométricos debido a renovación de tarjeta CI. En particular, si los datos biométricos y las funciones de autenticación de vena permanecen en la tarjeta CI antigua, puede haber oportunidades para la divulgación de datos biométricos o ingeniería inversa de funciones de autenticación, y la eliminación de tales oportunidades es altamente ventajosa.

Otras realizaciones del aparato de renovación de tarjetas CI

A continuación se explican otras realizaciones de renovación de tarjeta CI usando la máquina de transacción automática 6 de la figura 1. La figura 17 es una vista exterior de la máquina de transacción automática de la figura 1, y la figura 18 es un diagrama de bloques de la máquina de transacción automática de la figura 17.

Como se representa en la figura 17, el CA 6 tiene, en su cara delantera, un agujero de introducción/expulsión de tarjeta 6-4; un agujero de introducción/expulsión de libreta de banco 6-5; un agujero de introducción/dispensación de billetes 6-3; un agujero de introducción/dispensación de monedas 6-2; y un panel de operación de cliente 6-1 para operación y visualización.

En este ejemplo, el dispositivo de captura de imágenes 1-1 está dispuesto en el lado del panel de operación de cliente 6-1. La unidad sensora 18 explicada en la figura 2 y la figura 3 está montada en el lado delantero de la unidad principal 10 del dispositivo de captura de imágenes 1. En la porción delantera (en el lado del usuario) de la unidad sensora 18 se ha dispuesto una guía delantera 14. La guía delantera 14 incluye una hoja de resina sintética, transparente o sustancialmente transparente. Con el fin de que sirva para guiar la mano del usuario en la parte delantera y de soportar la muñeca, la forma en sección transversal de la guía delantera 14 tiene un cuerpo vertical y, en la porción superior, una porción horizontal 14-1 para soportar la muñeca. Se ha formado una depresión 14-2 de forma continua en el centro de la porción horizontal 14-1, para facilitar la colocación de la muñeca.

Además, la unidad sensora 18 de la unidad principal 10 mira hacia atrás y está inclinada hacia arriba, y detrás se ha previsto una porción plana 11. Un dispositivo de lectura/escritura de tarjetas CI 9-1 está dispuesto en la unidad principal 10 del dispositivo de captura de imágenes 1-1.

Como se representa en la figura 18, el CA 6 tiene una unidad CIP (impresora de lector de tarjetas) 60 que tiene un agujero de introducción/expulsión de tarjeta 6-4; una unidad de libreta de banco 64 que tiene un agujero de introducción/expulsión de libreta de banco 6-5; una unidad de recuento de billetes/monedas 66 que tiene un agujero de introducción/dispensación de billetes 6-3 y un agujero de introducción/dispensación de monedas 6-2; una unidad de operación de encargado 65; una unidad de control 67; un panel de operación de cliente (UOP) 6-1 para operación y visualización; y un dispositivo de captura de imágenes (sensor de venas) 1-1 incluyendo un dispositivo de lectura/escritura de tarjetas CI 9.

La unidad CIP 60 tiene un dispositivo de lectura/escritura de tarjetas CI 61 que lee y escribe la banda magnética y el chip CI de una tarjeta CI 5; una impresora de resguardos 63 que registra transacciones en un resguardo; una impresora de historial 62 que imprime la historia de transacciones en forma de diario; y un módulo de acceso seguro (SAM) 70.

La unidad de libreta de banco 64 registra transacciones en las páginas de una libreta de banco, y, cuando es necesario, pasa las páginas. La unidad de operación de encargado 65 es para operaciones realizadas por un encargado, que puede ver el estado y realizar operaciones a la aparición de un fallo o durante las inspecciones. La unidad de recuento de billetes/monedas 66 valida, cuenta, y guarda los billetes y monedas introducidos, y cuenta y dispensa billetes y monedas en las cantidades requeridas.

La unidad de control 67 comunica con el servidor 4, y tiene una aplicación CA 68 que controla la operación CA y una librería de autenticación (programa) 69 para procesado de autenticación. Una porción de esta aplicación CA 68 actúa de acuerdo con la librería de autenticación 69 para controlar las pantallas de guía de autenticación biométrica de la UOP 6-1.

En las relaciones entre la figura 17 y la figura 18 con la figura 2 y la figura 4, el dispositivo de lectura/escritura de tarjetas CI 61 de la figura 18 corresponde al dispositivo de lectura/escritura de tarjetas CI 9 de la figura 2, y el dispositivo de lectura/escritura de tarjetas CI 9-1 de la figura 17 y la figura 18 corresponde al dispositivo de lectura/escritura de tarjetas CI 9-1 de la figura 2. Y, la aplicación de renovación 30 de la figura 4 está dispuesta en la aplicación CA 68 de la figura 18.

Además, la UOP 6-1 de la figura 17 y la figura 18 corresponde a la unidad de operación de cliente 24 de la figura 2 y la figura 4, mientras que la librería de autenticación 69 de la figura 17 y la figura 18 corresponde a la librería de autenticación 34 de la figura 2 y la figura 4.

La figura 19 y la figura 20 explican pantallas de guía para procesado de renovación de tarjetas CI, incluyendo procesado de autenticación biométrica por la máquina de transacción automática. El procesado de renovación de tarjetas CI es el mismo que en la figura 13 y la figura 14.

La pantalla de selección de transacción G20 de la figura 19 aparece en la UOP 6-1 del CA 6. Aquí, se puede seleccionar cuatro tipos de transacción, que son actualización de libreta de banco, consulta de saldo, pago, y renovación de tarjeta CI. Dado que se desea la renovación, el usuario pulsa el icono de renovación de tarjeta CI en la pantalla de selección G20. Mediante esto, se inicia el procesado de renovación. Al igual que el paso S10, el usuario introduce una tarjeta CI caducada 5 con funciones de autenticación biométrica (una tarjeta CI antigua) en el dispositivo de lectura/escritura de tarjetas CI 9 según las pantallas de guía de introducción de tarjeta CI antigua G2, G3 de la figura 19.

A continuación, al igual que el paso S12, el usuario introduce una tarjeta CI 5-1 con funciones de autenticación biométrica (una tarjeta CI nueva) en el dispositivo de lectura/escritura de tarjetas CI 9-1, según las pantallas de guía de introducción de tarjeta CI G4, G5 de la figura 19.

Después de los pasos S14, S16, S18 y S20, al igual que el paso S22, aparece la pantalla de guía de palma G6 de la figura 19, y la palma del usuario es guiada al sensor de venas 1 del dispositivo de autenticación 26. Entonces, después del paso S24, aparece una pantalla G7 que indica que la autenticación está en curso, y en el paso S26 aparece la pantalla G8 de la figura 19 que indica que el individuo ha sido confirmado.

En el paso S28, a efectos de verificación, aparece la pantalla de guía de palma G9 de la figura 19, y la palma del usuario es guiada al sensor de venas 1 del dispositivo de captura de imágenes 26. Entonces, si en el paso S30 el resultado de la captura de imagen es satisfactorio, se obtienen datos de imagen de vasos sanguíneos C de la palma, y aparece la pantalla de procesado de autenticación G10 de la figura 20.

Entonces, si en el paso S32 la identidad del individuo es confirmada mediante autenticación biométrica usando la tarjeta CI nueva 5-1, aparece la pantalla G11 que indica el extremo de registro en la figura 20, y si la imagen de vasos sanguíneos de la palma de un agente ha de ser registrada para autenticación biométrica de un agente que ha recibido el consentimiento del individuo, pulsando el icono siguiente de registro de datos biométricos en la UOP 6-1, aparece la pantalla de continuación de registro G14 de la figura 20, y el procesado vuelve al paso S22.

Además, cuando en el paso S36 no se ha de registrar un conjunto siguiente de datos biométricos, se inactivan las funciones de autenticación de vena de la tarjeta CI antigua 5, aparece la pantalla de devolución de tarjeta CI nueva 5-1 G12 de la figura 20, y el dispositivo de lectura/escritura de tarjetas CI 61 devuelve la tarjeta CI nueva 5-1. Además, aparece la pantalla de devolución de tarjeta CI antigua 5 G13 de la figura 20, y el dispositivo de lectura/escritura de tarjetas CI 9-1 devuelve la tarjeta CI antigua 5.

Otras realizaciones

En las realizaciones anteriores, se explicó la autenticación biométrica para el caso de autenticación de la configuración de las venas de la palma; pero es posible una aplicación a autenticación usando configuraciones de las venas de los dedos, a huellas de las palmas, huellas dactilares, características faciales y otra biometría. Aunque la explicación anterior se refiere a una tarjeta CI, ésta es solamente un ejemplo de un medio de almacenamiento. Además, se explicaron dispositivos de renovación de tarjetas CI y equipo automatizado usado en operaciones financieras; pero es posible la aplicación a equipo automático de emisión de tickets, equipo automático de venta, y a máquinas automatizadas y ordenadores en otras zonas, así como a equipo de apertura/cierre de puertas en lugar de claves, y a otro equipo donde se requiere autenticación del individuo.

Además, se usaron dos conjuntos de datos de verificación en la verificación con un terminal y tarjeta CI; pero la verificación puede ser realizada con respecto a una tarjeta CI sola, y se puede usar solamente un tipo de datos de verificación. Igualmente, se explicó un ejemplo en el que se usaban dos dispositivos de lectura/escritura de tarjeta CI, pero la renovación puede ser realizada usando un solo dispositivo de lectura/escritura de tarjetas CI. Por ejemplo, se puede adoptar una configuración tal que, después de insertar la tarjeta CI antigua y realizar la lectura, la tarjeta antigua se guarde temporalmente, y se introduzca y lea la tarjeta CI nueva.

Además, las tarjetas CI antiguas pueden ser recogidas, adoptando un modo de uso en el que los datos biométricos en la tarjeta CI antigua no se borren, sino que se bloqueen las funciones de autenticación biométrica.

En lo anterior, se han explicado realizaciones de la invención; pero la invención se puede modificar de varias formas dentro del alcance de la invención, y estas modificaciones no quedan excluidas del alcance de la invención.

Dado que se emplea autenticación biométrica usando una tarjeta CI antigua para confirmar la identidad de un individuo a través de autenticación biométrica, la confirmación de la identidad del individuo puede ser realizada rigurosamente usando la tarjeta CI con funciones de autenticación biométrica, de modo que se pueda evitar el uso ilícito al tiempo de la renovación; además, si la confirmación del individuo es satisfactoria, los datos biométricos obtenidos en la autenticación biométrica pueden ser registrados en una tarjeta CI nueva cuya legitimidad haya sido confirmada. Mediante esto, con una sola captura de imagen, los datos biométricos que han sido confirmados como del individuo en cuestión que usa la tarjeta CI antigua, pueden ser registrados en la tarjeta CI nueva sin ser divulgados a terceras partes, y los datos biométricos se pueden pasar fácilmente a la tarjeta CI nueva.

REIVINDICACIONES

1. Un aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica, que lleva a cabo la renovación de una tarjeta CI (5) en la que se registran datos de características biométricas detectados de un cuerpo humano (52) y que tiene funciones para verificar datos de características biométricas detectados para dicho cuerpo (52) contra dichos datos registrados de características biométricas y realizar autenticación biométrica, incluyendo:

un dispositivo de detección (26), que detecta datos de dicho cuerpo (52); y

una unidad de control (22), que extrae dichos datos de características biométricas de la salida de dicho dispositivo de detección (26); **caracterizado** el aparato de renovación (20) por incluir:

un dispositivo de lectura/escritura de tarjetas CI (9), que lee y escribe una tarjeta CI antigua para renovación y una tarjeta CI nueva; y

donde dicha unidad de control (22) transmite los datos de características a dicha tarjeta CI antigua,

y donde dicha unidad de control (22) usa dichas funciones de autenticación biométrica de dicha tarjeta CI antigua para verificar dichos datos registrados de características biométricas contra dichos datos de características biométricas transmitidos, y según que la autenticación biométrica sea satisfactoria en base al resultado de la verificación, registra dichos datos extraídos de características biométricas en dicha tarjeta CI nueva.

2. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 1, donde dicha unidad de control (22), después del registro de datos en dicha tarjeta CI nueva, bloquea dichas funciones de autenticación biométrica de dicha tarjeta CI antigua.

3. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 1 o 2, donde dicha unidad de control (22) verifica la información de tenedor, leída por dicho dispositivo de lectura/escritura de tarjetas CI (9), para dicha tarjeta CI antigua y dicha tarjeta CI nueva, y confirma la legitimidad de la correspondencia entre dicha tarjeta CI antigua y dicha tarjeta CI nueva.

4. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de la reivindicación 1, 2, o 3 donde dicha unidad de control (22) confirma la legitimidad de dicha tarjeta CI antigua y de dicha tarjeta CI nueva a partir de la información del emisor, leída por dicho dispositivo de lectura/escritura de tarjetas CI 9) de dicha tarjeta CI antigua y dicha tarjeta CI nueva.

5. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 1 a 4, donde dicha unidad de control (22), después del registro de datos en dicha tarjeta CI nueva, borra dichos datos de características biométricas en dicha tarjeta CI antigua.

6. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 1 a 5, donde dicho dispositivo de detección (26) incluye un dispositivo de captura de imágenes (18) que captura imágenes del cuerpo (52) del usuario.

7. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 6, donde dicho dispositivo de captura de imágenes (18) incluye una unidad que captura imágenes de vasos sanguíneos de dicho usuario.

8. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 1 a 7, donde dicho dispositivo de lectura/escritura de tarjetas CI (9) incluye:

un primer dispositivo de lectura/escritura de tarjetas CI, que lee y escribe dicha tarjeta CI antigua; y

un segundo dispositivo de lectura/escritura de tarjetas CI, que lee y escribe dicha tarjeta CI nueva.

9. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 1 a 8, donde dicha unidad de control (22), después de registrar dichos datos de características en dicha tarjeta CI nueva, de nuevo detecta datos de dicho cuerpo (52) usando dicho dispositivo de detección (26), extrae dichos datos de características biométricas de la salida de dicho dispositivo de detección (26), transmite dichos datos de características biométricas a dicha tarjeta CI nueva, y hace que dicha tarjeta CI nueva lleve a cabo la verificación de dichos datos registrados de características biométricas contra dichos datos de características biométricas transmitidos.

10. El aparato de renovación (20) para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 1 a 9, donde dichas funciones de autenticación biométrica de dicha tarjeta CI antigua y dicha tarjeta CI nueva acceden solamente a dichos datos registrados de características biométricas.

11. Un método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica, en la que se registran datos de características biométricas detectados de un cuerpo humano (52), los datos de características biométricas detectados para dicho cuerpo (52) son verificados contra dichos datos registrados de características biométricas, y se lleva a cabo autenticación biométrica, incluyendo los pasos de:

detectar datos de dicho cuerpo (52) y extraer dichos datos de características biométricas; **caracterizado** el método por incluir los pasos de:

transmitir dichos datos extraídos de características biométricas a una tarjeta CI antigua a renovar;

verificar dichos datos registrados de características biométricas contra dichos datos de características biométricas transmitidos, usando dichas funciones de autenticación biométrica de dicha tarjeta CI antigua; y

registrar dichos datos extraídos de características biométricas en una tarjeta CI nueva en respuesta a autenticación biométrica satisfactoria según dicho resultado de la verificación.

12. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 11, incluyendo además un paso, después del registro de datos en dicha tarjeta CI nueva, de bloquear dichas funciones de autenticación biométrica de dicha tarjeta CI antigua.

13. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 11 o 12, incluyendo además un paso, anterior a dicha detección biométrica, de verificar la información de tenedor leída por un dispositivo de lectura/escritura de tarjetas CI (9) de dicha tarjeta CI antigua y de dicha tarjeta CI nueva, y de confirmar la legitimidad de la correspondencia entre dicha tarjeta CI antigua y dicha tarjeta CI nueva.

14. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica de la reivindicación 11, 12 o 13, incluyendo además un paso, anterior a dicha detección biométrica, de confirmar la legitimidad de dicha tarjeta CI antigua y de dicha tarjeta CI nueva a partir de la información del emisor, leída por un dispositivo de lectura/escritura de tarjetas CI (9), para dicha tarjeta CI antigua y para dicha tarjeta CI nueva.

15. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 11 a 14, incluyendo además un paso, después del registro de datos en dicha tarjeta CI nueva, de borrar dichos datos de características en dicha tarjeta CI antigua.

16. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquiera de las reivindicaciones 11 a 16, donde dicho paso de detección incluye un paso de capturar una imagen del cuerpo (52) del usuario con un dispositivo de captura de imágenes (18).

17. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 16, donde dicho paso de captura de imágenes incluye un paso de capturar una imagen de vasos sanguíneos de dicho usuario.

18. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica según la reivindicación 13, donde dicho paso de confirmación incluye:

un paso de leer dicha información de tenedor de un primer dispositivo de lectura/escritura de tarjetas CI que lee y escribe dicha tarjeta CI antigua; y

un paso de leer dicha información de tenedor de un segundo dispositivo de lectura/escritura de tarjetas CI que lee y escribe dicha tarjeta CI nueva.

19. El método de renovación para una tarjeta CI (5) que tiene funciones de autenticación biométrica de cualquier reivindicación 11 a 18, incluyendo además:

un paso, después del registro de dichos datos de características en dicha tarjeta CI nueva;

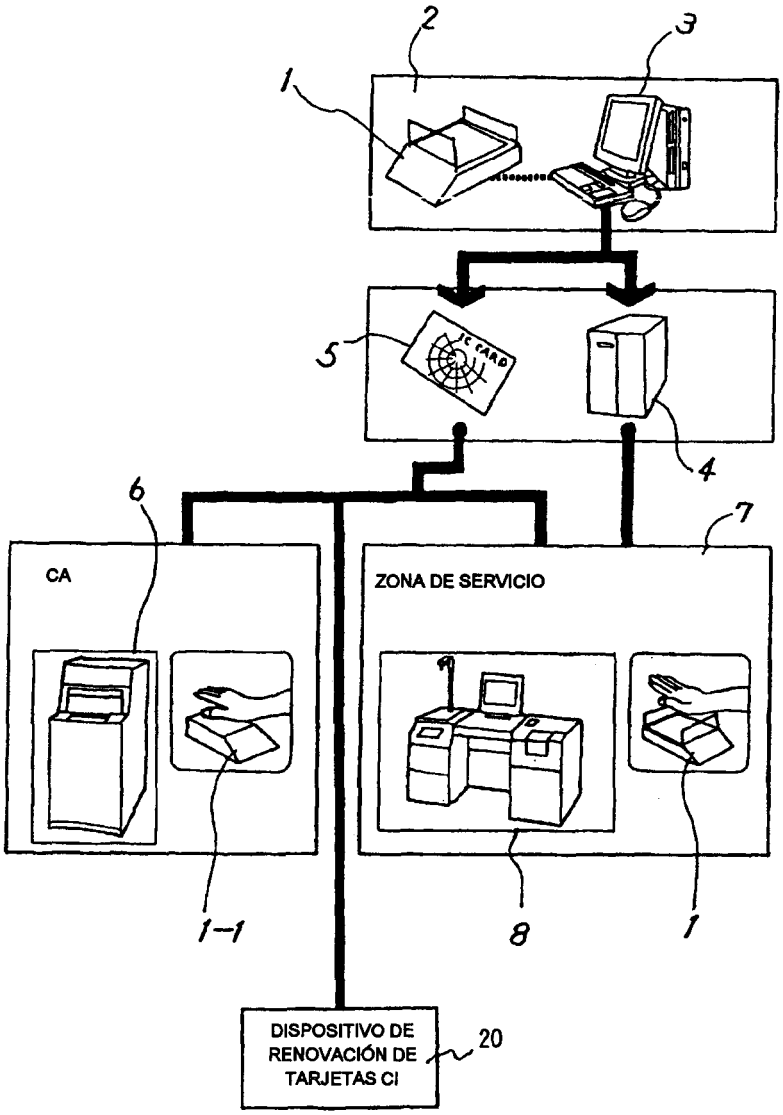
un paso de detectar nuevamente dichos datos biométricos de dicho dispositivo de detección (26);

un paso de extraer dichos datos de características biométricas de la salida de dicho dispositivo de detección (26);

un paso de transmitir dichos datos de características biométricas a dicha tarjeta CI nueva; y

un paso de verificar dichos datos de características biométricas registrados en dicha tarjeta CI nueva contra dichos datos de características biométricas transmitidos.

FIG. 1


2
3
1
5
IC CARD
4
6
7
CA
ZONA DE SERVICIO
1-1
8
1
DISPOSITIVO DE RENOVACIÓN DE TARJETAS CI
20

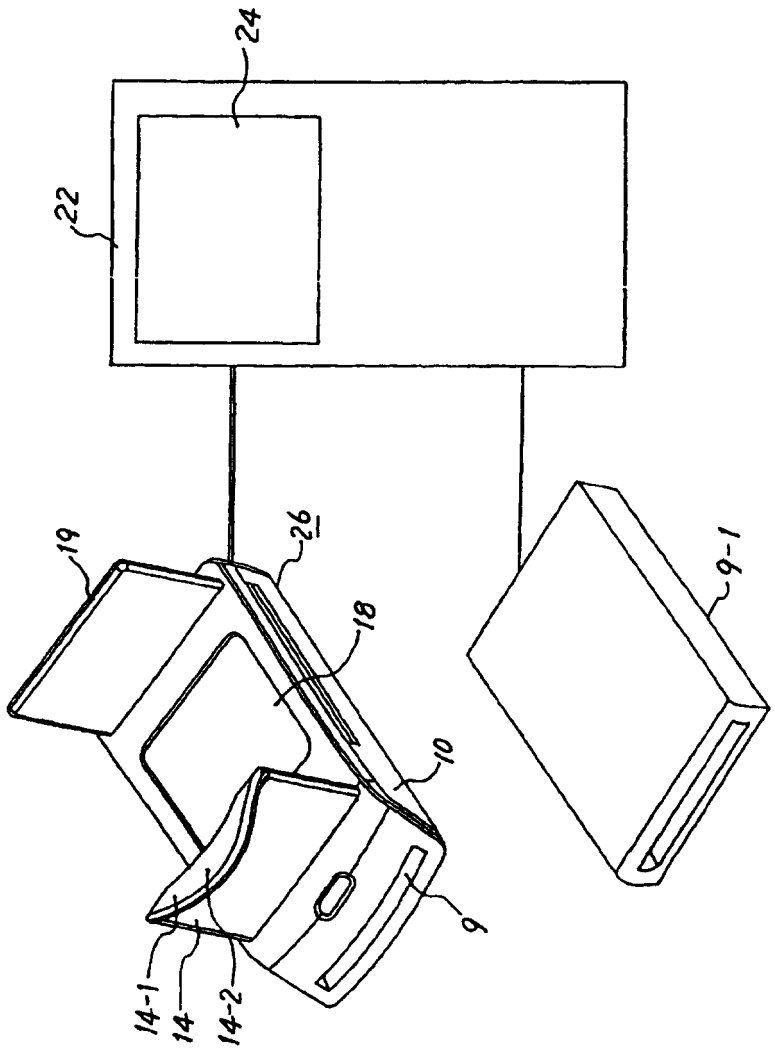


FIG. 2

FIG. 3

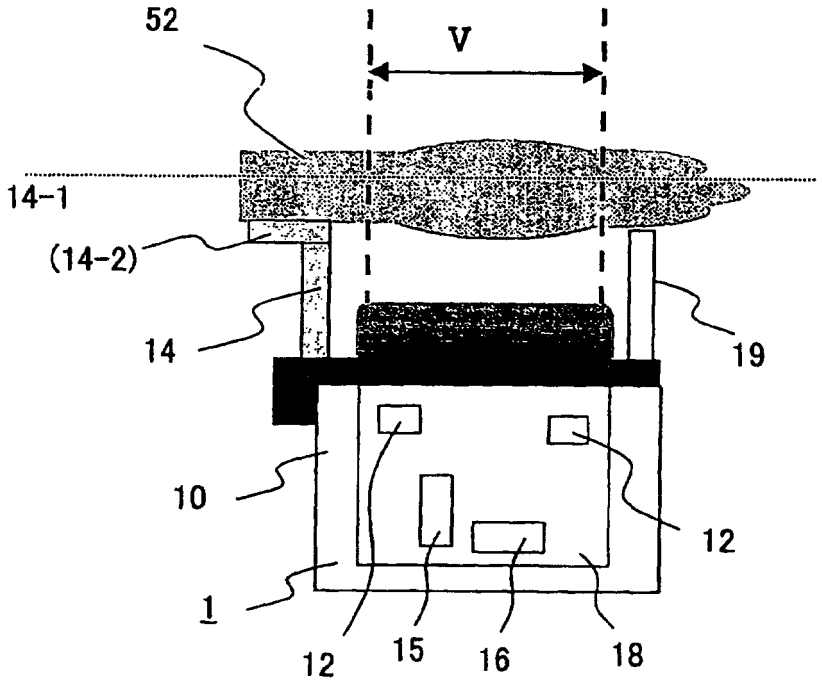


FIG. 4

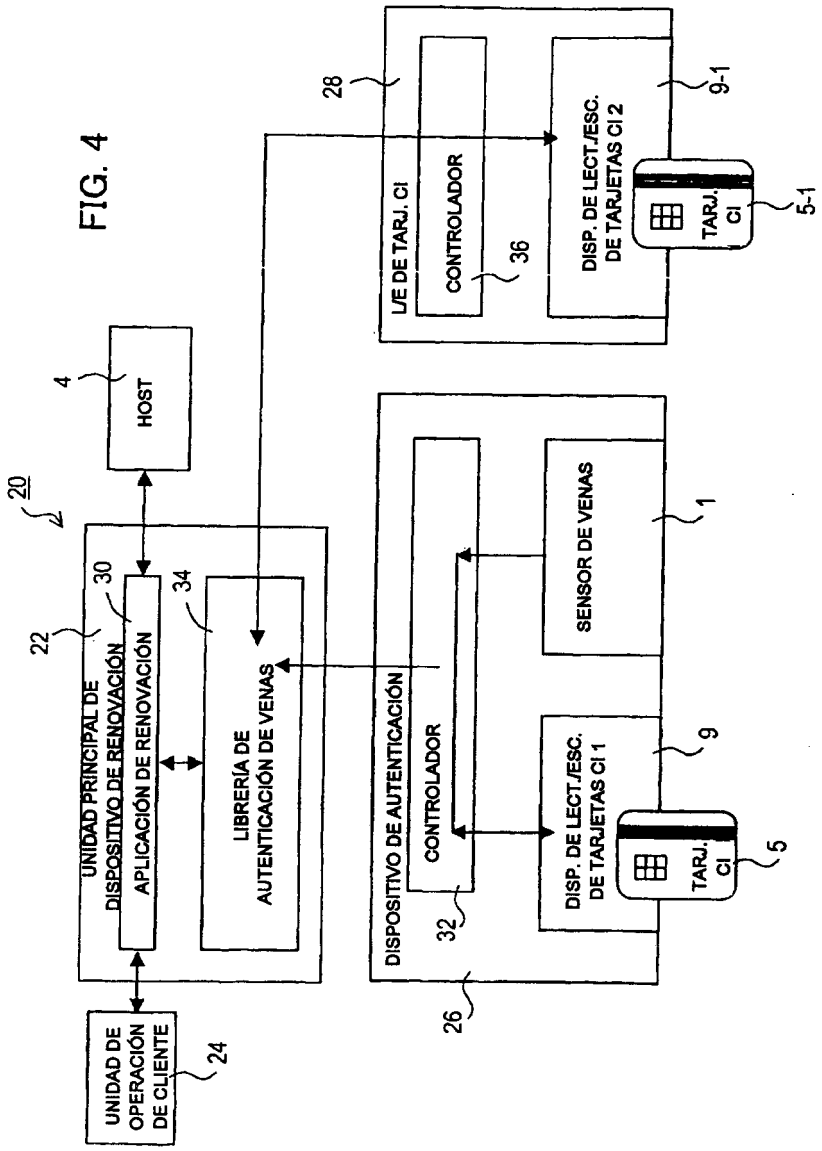
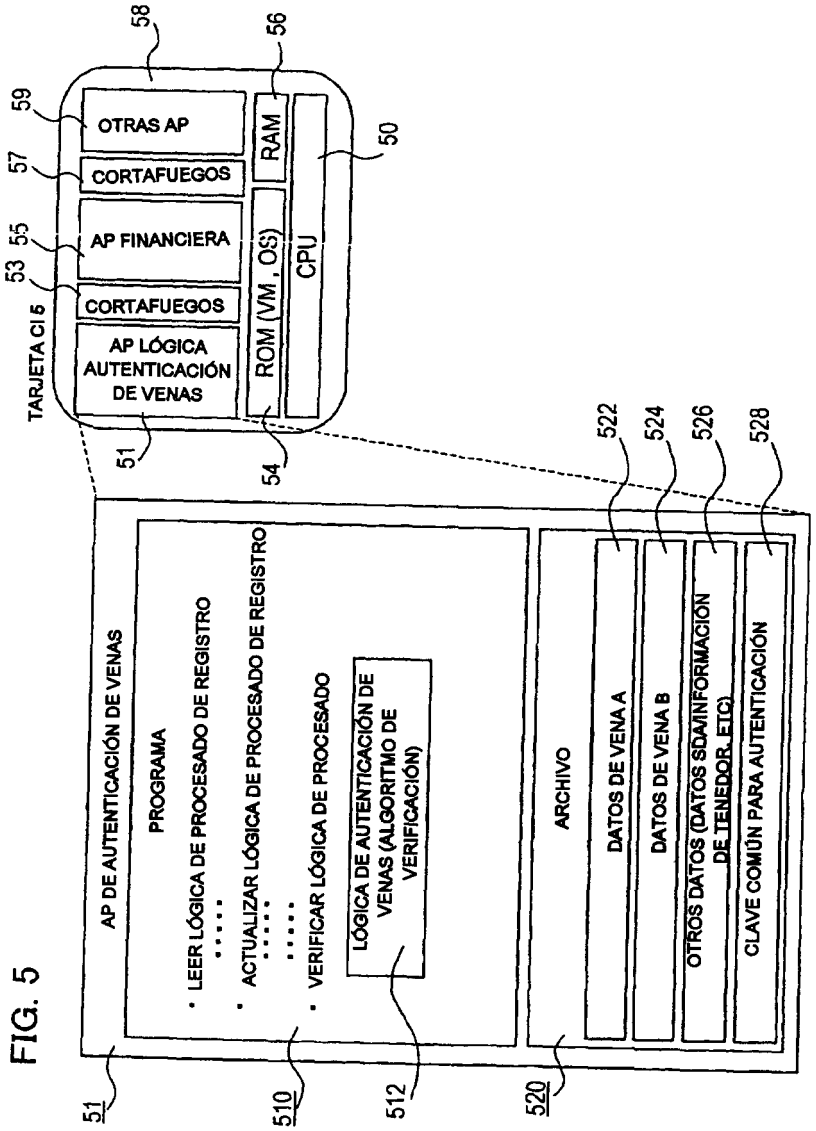

20
UNIDAD PRINCIPAL DE DISPOSITIVO DE RENOVACIÓN
22
APLICACIÓN DE RENOVACIÓN
30
LIBRERÍA DE AUTENTICACIÓN DE VENAS
34
HOST
4
UNIDAD DE OPERACIÓN DE CLIENTE
24
DISPOSITIVO DE AUTENTICACIÓN
26
CONTROLADOR
32
SENSOR DE VENAS
1
DISP. DE LECT./ESC. DE TARJETAS CI 1
9
TARJ. CI
5
L/E DE TARJ. CI
28
CONTROLADOR
36
DISP. DE LECT./ESC. DE TARJETAS CI 2
9-1
TARJ. CI
5-1

FIG. 5


TARJETA CI 5
OTRAS AP
CORTAFUEGOS
AP FINANCIERA
CORTAFUEGOS
AP LÓGICA AUTENTICACIÓN DE VENAS
ROM (VM, OS)
RAM
CPU
AP DE AUTENTICACIÓN DE VENAS
PROGRAMA
LEER LÓGICA DE PROCESADO DE REGISTRO
ACTUALIZAR LÓGICA DE PROCESADO DE REGISTRO
VERIFICAR LÓGICA DE PROCESADO
LÓGICA DE AUTENTICACIÓN DE VENAS (ALGORITMO DE VERIFICACIÓN)
ARCHIVO
DATOS DE VENA A
DATOS DE VENA B
OTROS DATOS (DATOS SDA/INFORMACIÓN DE TENEDOR, ETC)
CLAVE COMÚN PARA AUTENTICACIÓN
50
51
53
54
55
56
57
58
59
510
512
520
522
524
526
528

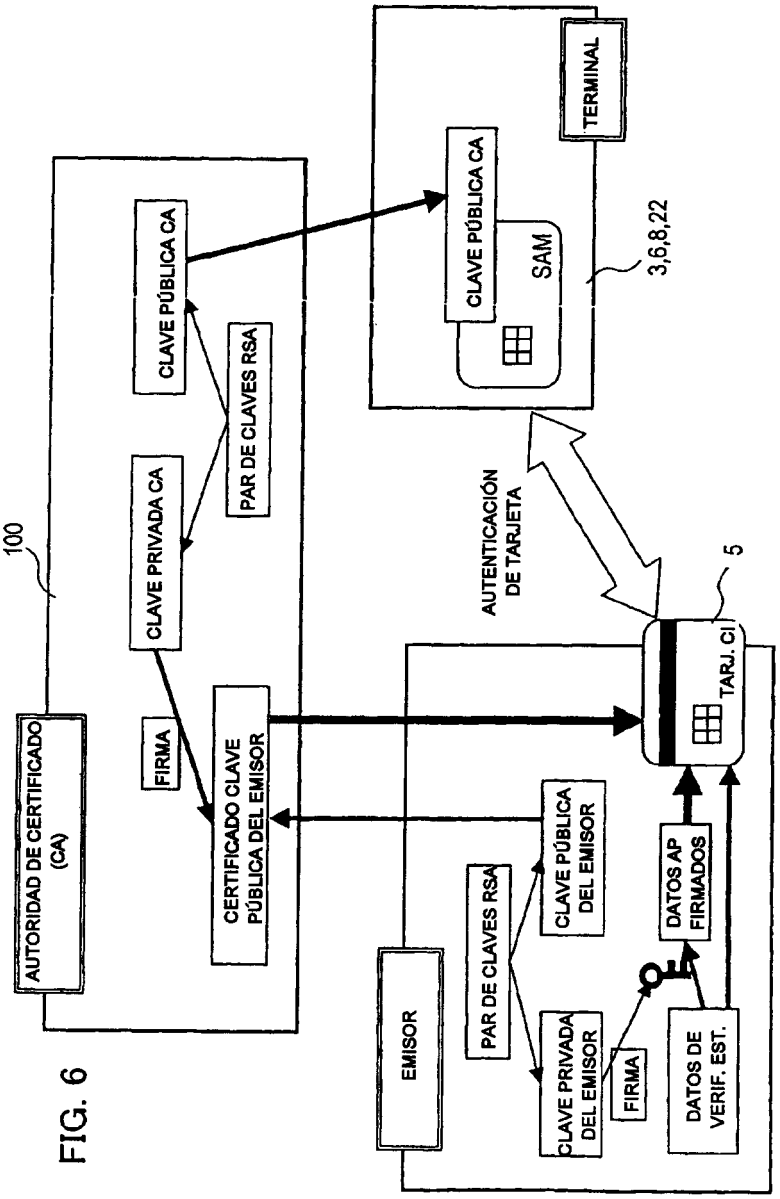

100
AUTORIDAD DE CERTIFICADO (CA)
CLAVE PÚBLICA CA
CLAVE PRIVADA CA
PAR DE CLAVES RSA
FIRMA
CERTIFICADO CLAVE PÚBLICA DEL EMISOR
TERMINAL
CLAVE PÚBLICA CA
SAM
3,6,8,22
AUTENTICACIÓN DE TARJETA
5
TARJ. CI
EMISOR
PAR DE CLAVES RSA
CLAVE PÚBLICA DEL EMISOR
CLAVE PRIVADA DEL EMISOR
FIRMA
DATOS AP FIRMADOS
DATOS DE VERIF. EST.

FIG. 6

FIG. 7

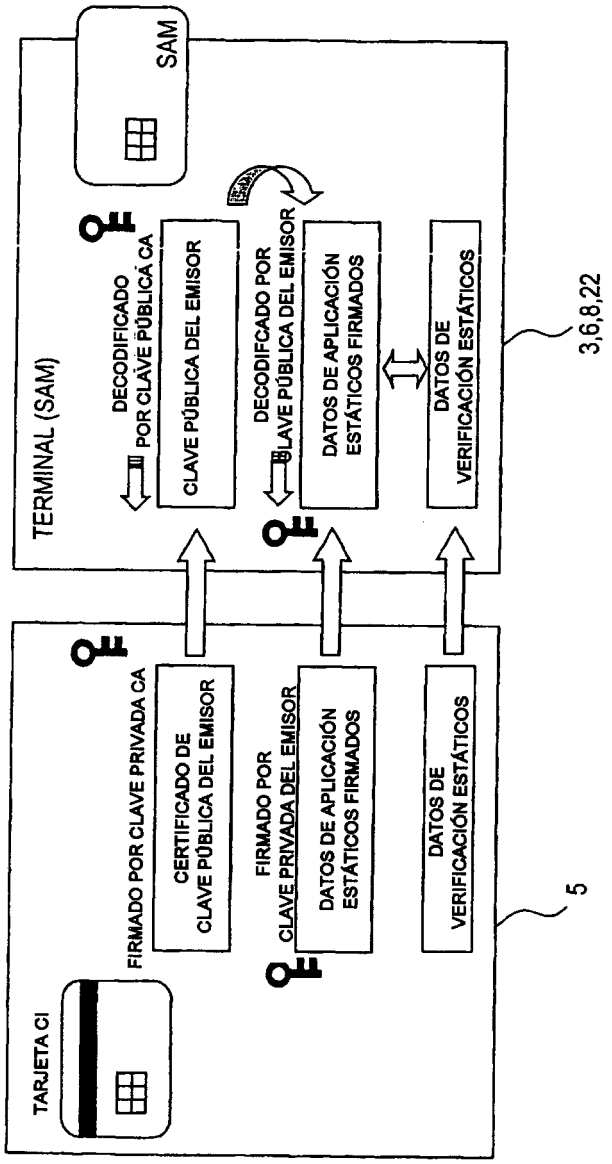

SAM
TERMINAL (SAM)
DECODIFICADO POR CLAVE PÚBLICA CA
CLAVE PÚBLICA DEL EMISOR
DECODIFCADO POR CLAVE PÚBLICA DEL EMISOR
DATOS DE APLICACIÓN ESTÁTICOS FIRMADOS
DATOS DE VERIFICACIÓN ESTÁTICOS
3,6,8,22
TARJETA CI
FIRMADO POR CLAVE PRIVADA CA
CERTIFICADO DE CLAVE PÚBLICA DEL EMISOR
FIRMADO POR CLAVE PRIVADA DEL EMISOR
DATOS DE APLICACIÓN ESTÁTICOS FIRMADOS
DATOS DE VERIFICACIÓN ESTÁTICOS
5

FIG. 8

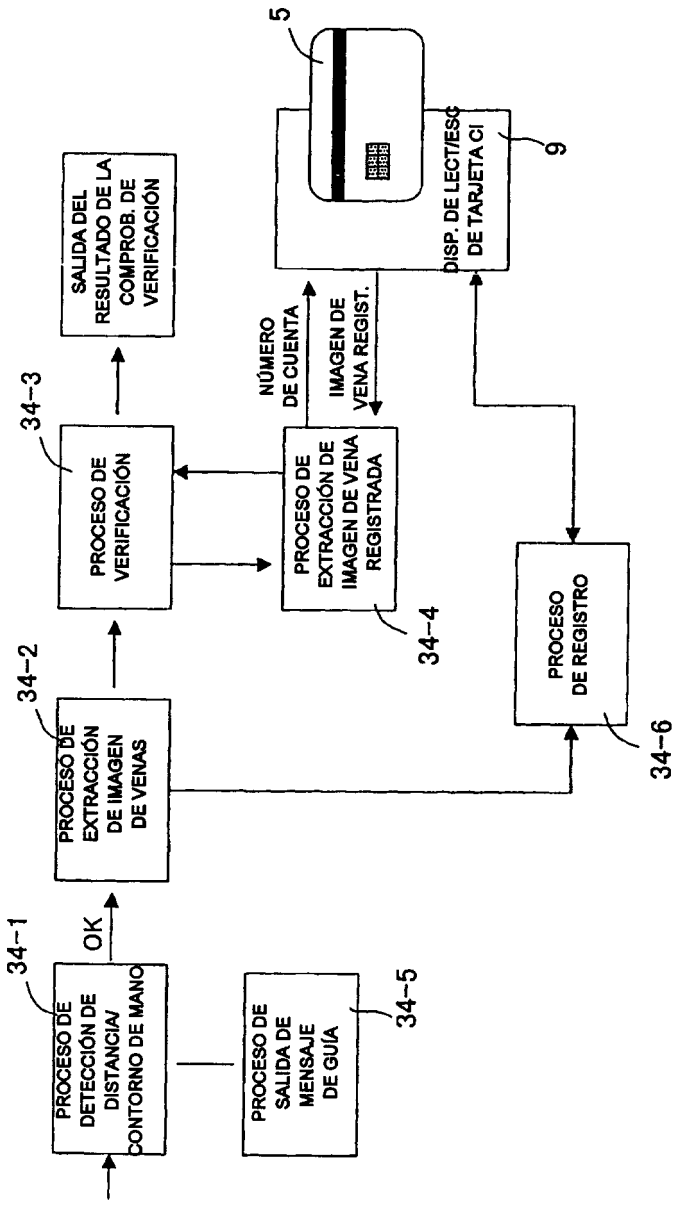

5
9
DISP. DE LECT/ESC DE TARJETA CI
SALIDA DEL RESULTADO DE LA COMPROB. DE VERIFICACIÓN
NÚMERO DE CUENTA
IMAGEN DE VENA REGIST.
34-3
PROCESO DE VERIFICACIÓN
PROCESO DE EXTRACCIÓN DE IMAGEN DE VENA REGISTRADA
34-4
34-2
PROCESO DE EXTRACCIÓN DE IMAGEN DE VENAS
PROCESO DE REGISTRO
34-6
34-1
OK
PROCESO DE DETECCIÓN DE DISTANCIA/ CONTORNO DE MANO
PROCESO DE SALIDA DE MENSAJE DE GUÍA
34-5

FIG. 9

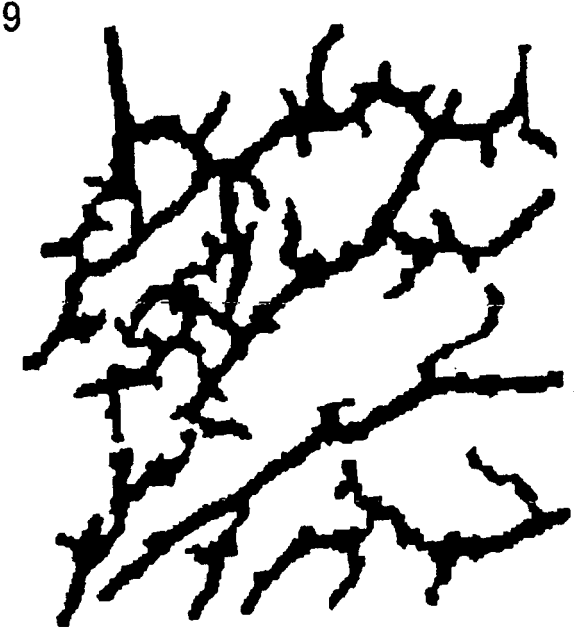


FIG. 10

IMAGEN DE VENA N1

	0	1	2	3	4
0	255	255	0	255	255
1	255	255	0	0	0
2	255	255	0	255	0
3	0	0	255	0	0
4	0	0	0	255	0

IMAGEN DE VENA N2

	0	1	2	3	4
0	255	255	0	0	255
1	255	255	255	0	0
2	255	255	0	255	255
3	0	0	255	255	0
4	0	0	0	255	255

FIG. 11

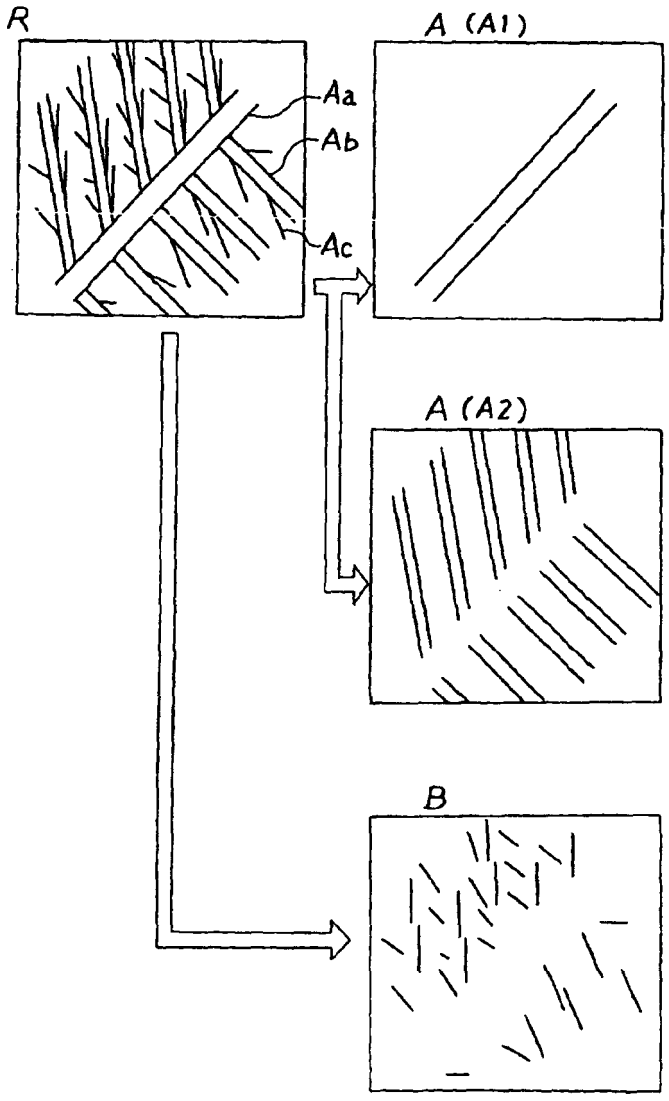


FIG. 12

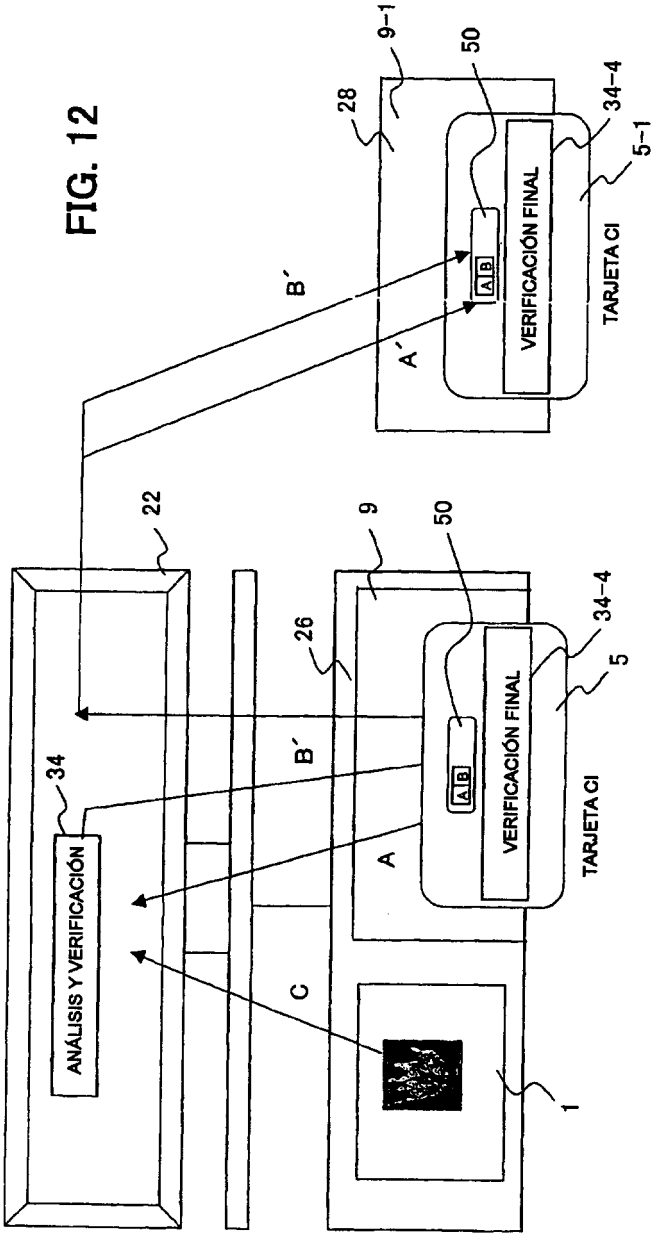

9-1
50
28
34-4
5-1
VERIFICACIÓN FINAL
TARJETA CI
A B
B´
A´
22
9
50
26
34-4
5
VERIFICACIÓN FINAL
TARJETA CI
A B
B´
A
34
ANÁLISIS Y VERIFICACIÓN
C
1

FIG. 13

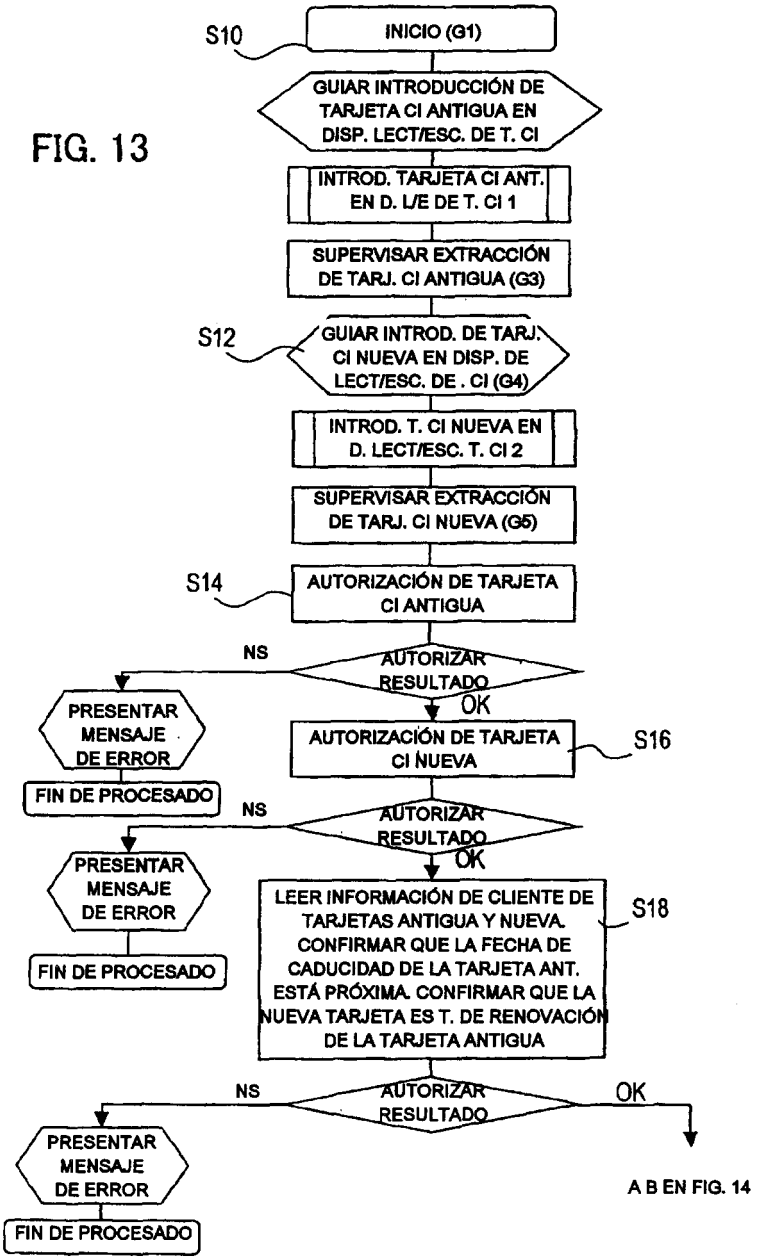
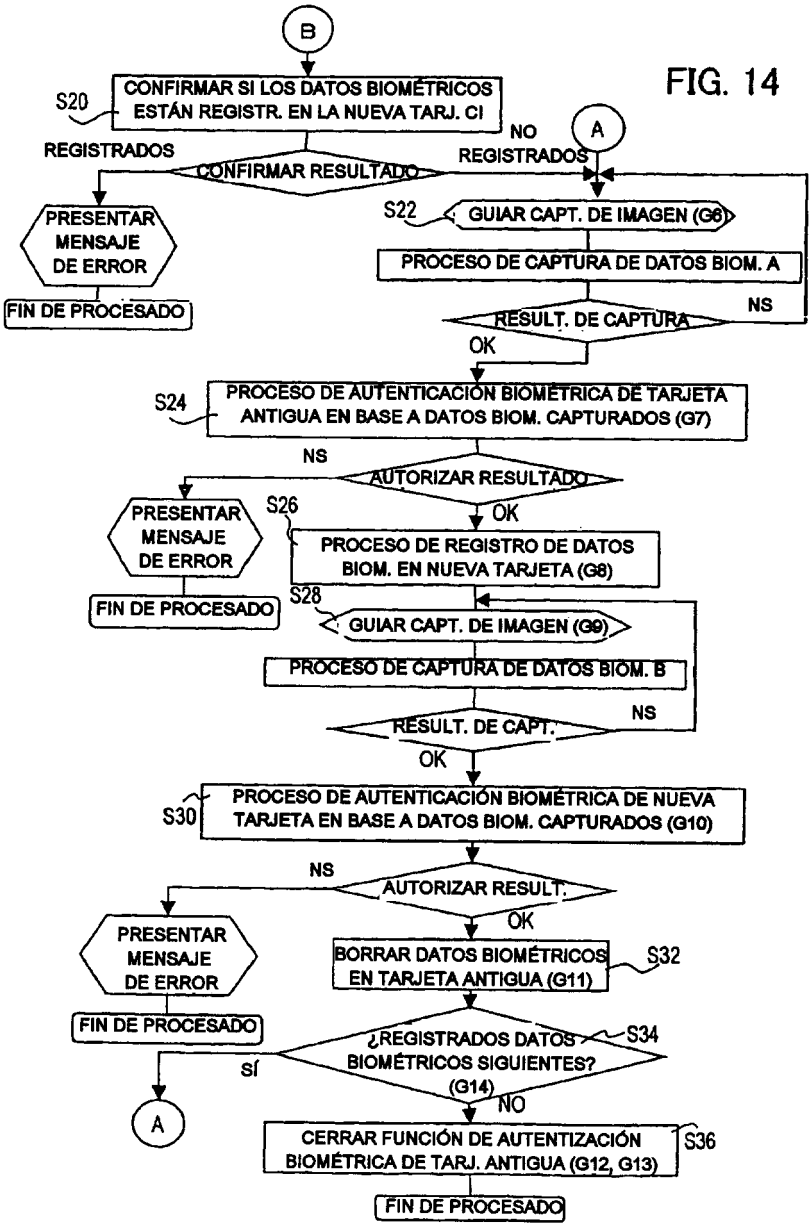

S10
INICIO (G1)
GUIAR INTRODUCCIÓN DE TARJETA CI ANTIGUA EN DISP. LECT/ESC. DE T. CI
INTROD. TARJETA CI ANT. EN D. I/E DE T. CI 1
SUPERVISAR EXTRACCIÓN DE TARJ. CI ANTIGUA (G3)
S12
GUIAR INTROD. DE TARJ. CI NUEVA EN DISP. DE LECT/ESC. DE . CI (G4)
INTROD. T. CI NUEVA EN D. LECT/ESC. T. CI 2
SUPERVISAR EXTRACCIÓN DE TARJ. CI NUEVA (G5)
S14
AUTORIZACIÓN DE TARJETA CI ANTIGUA
NS
AUTORIZAR RESULTADO
OK
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
AUTORIZACIÓN DE TARJETA CI NUEVA
S16
NS
AUTORIZAR RESULTADO
OK
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
LEER INFORMACIÓN DE CLIENTE DE TARJETAS ANTIGUA Y NUEVA. CONFIRMAR QUE LA FECHA DE CADUCIDAD DE LA TARJETA ANT. ESTÁ PRÓXIMA. CONFIRMAR QUE LA NUEVA TARJETA ES T. DE RENOVACIÓN DE LA TARJETA ANTIGUA
S18
NS
AUTORIZAR RESULTADO
OK
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
A B EN FIG. 14

FIG. 14


B
S20
CONFIRMAR SI LOS DATOS BIOMÉTRICOS ESTÁN REGISTR. EN LA NUEVA TARJ. CI
REGISTRADOS
CONFIRMAR RESULTADO
NO REGISTRADOS
A
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
S22
GUIAR CAPT. DE IMAGEN (G6)
PROCESO DE CAPTURA DE DATOS BIOM. A
RESULT. DE CAPTURA
NS
OK
S24
PROCESO DE AUTENTICACIÓN BIOMÉTRICA DE TARJETA ANTIGUA EN BASE A DATOS BIOM. CAPTURADOS (G7)
NS
AUTORIZAR RESULTADO
OK
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
S26
PROCESO DE REGISTRO DE DATOS BIOM. EN NUEVA TARJETA (G8)
S28
GUIAR CAPT. DE IMAGEN (G9)
PROCESO DE CAPTURA DE DATOS BIOM. B
RESULT. DE CAPT.
NS
OK
S30
PROCESO DE AUTENTICACIÓN BIOMÉTRICA DE NUEVA TARJETA EN BASE A DATOS BIOM. CAPTURADOS (G10)
NS
AUTORIZAR RESULT.
OK
PRESENTAR MENSAJE DE ERROR
FIN DE PROCESADO
BORRAR DATOS BIOMÉTRICOS EN TARJETA ANTIGUA (G11)
S32
¿REGISTRADOS DATOS BIOMÉTRICOS SIGUIENTES? (G14)
S34
SÍ
NO
A
CERRAR FUNCIÓN DE AUTENTIZACIÓN BIOMÉTRICA DE TARJ. ANTIGUA (G12, G13)
S36
FIN DE PROCESADO

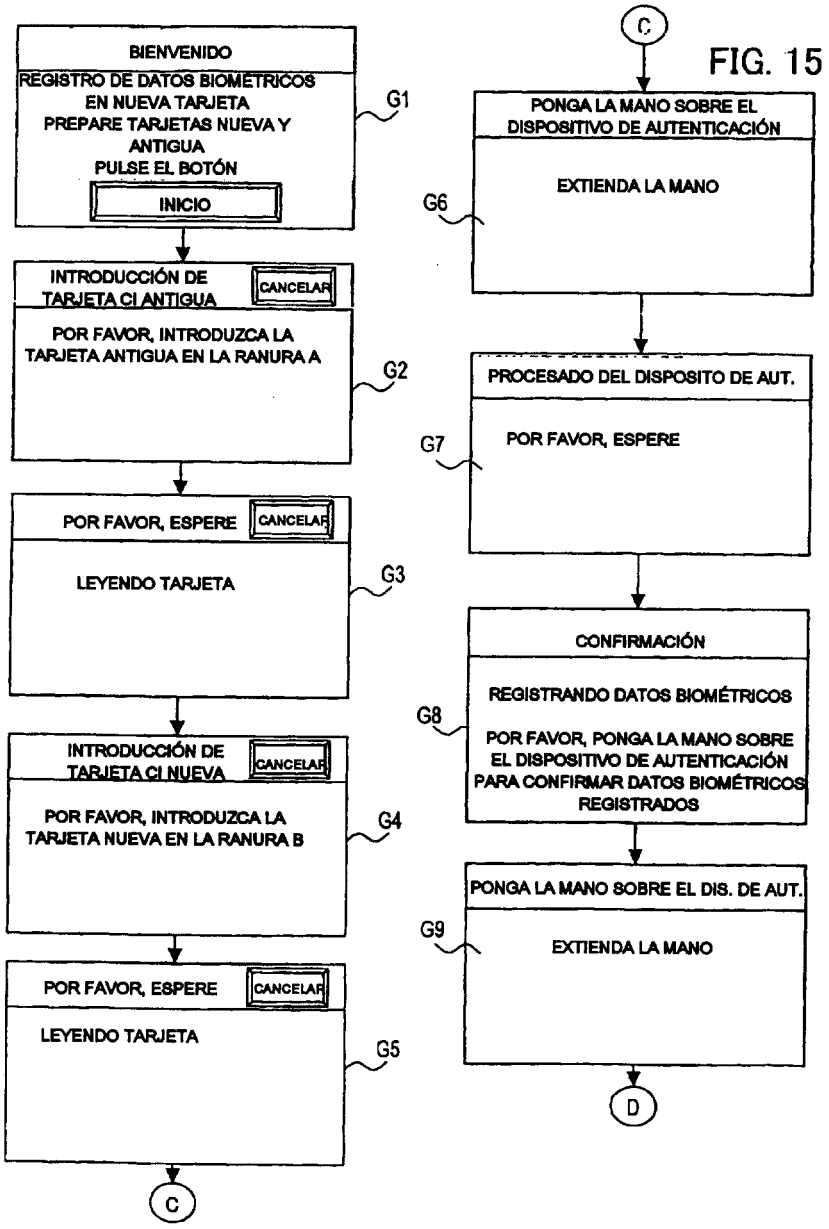
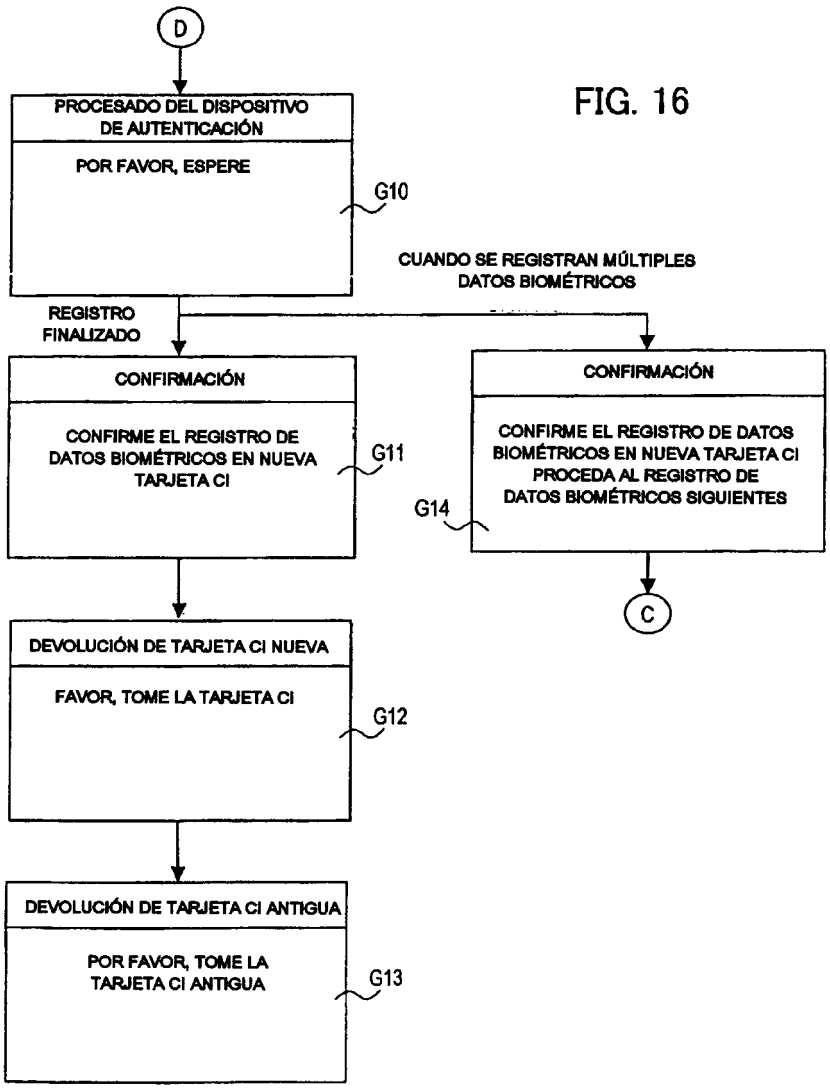

BIENVENIDO
REGISTRO DE DATOS BIOMÉTRICOS EN NUEVA TARJETA
PREPARE TARJETAS NUEVA Y ANTIGUA
PULSE EL BOTÓN
INICIO
G1
INTRODUCCIÓN DE TARJETA CI ANTIGUA
CANCELAR
POR FAVOR, INTRODUZCA LA TARJETA ANTIGUA EN LA RANURA A
G2
POR FAVOR, ESPERE
CANCELAR
LEYENDO TARJETA
G3
INTRODUCCIÓN DE TARJETA CI NUEVA
CANCELAR
POR FAVOR, INTRODUZCA LA TARJETA NUEVA EN LA RANURA B
G4
POR FAVOR, ESPERE
CANCELAR
LEYENDO TARJETA
G5
C
C
PONGA LA MANO SOBRE EL DISPOSITIVO DE AUTENTICACIÓN
EXTIENDA LA MANO
G6
PROCESADO DEL DISPOSITO DE AUT.
POR FAVOR, ESPERE
G7
CONFIRMACIÓN
REGISTRANDO DATOS BIOMÉTRICOS
POR FAVOR, PONGA LA MANO SOBRE EL DISPOSITIVO DE AUTENTICACIÓN PARA CONFIRMAR DATOS BIOMÉTRICOS REGISTRADOS
G8
PONGA LA MANO SOBRE EL DIS. DE AUT.
EXTIENDA LA MANO
G9
D

FIG. 15

FIG. 16


D
PROCESADO DEL DISPOSITIVO DE AUTENTICACIÓN
POR FAVOR, ESPERE
G10
CUANDO SE REGISTRAN MÚLTIPLES DATOS BIOMÉTRICOS
REGISTRO FINALIZADO
CONFIRMACIÓN
CONFIRME EL REGISTRO DE DATOS BIOMÉTRICOS EN NUEVA TARJETA CI
G11
CONFIRMACIÓN
CONFIRME EL REGISTRO DE DATOS BIOMÉTRICOS EN NUEVA TARJETA CI PROCEDA AL REGISTRO DE DATOS BIOMÉTRICOS SIGUIENTES
G14
C
DEVOLUCIÓN DE TARJETA CI NUEVA
FAVOR, TOME LA TARJETA CI
G12
DEVOLUCIÓN DE TARJETA CI ANTIGUA
POR FAVOR, TOME LA TARJETA CI ANTIGUA
G13

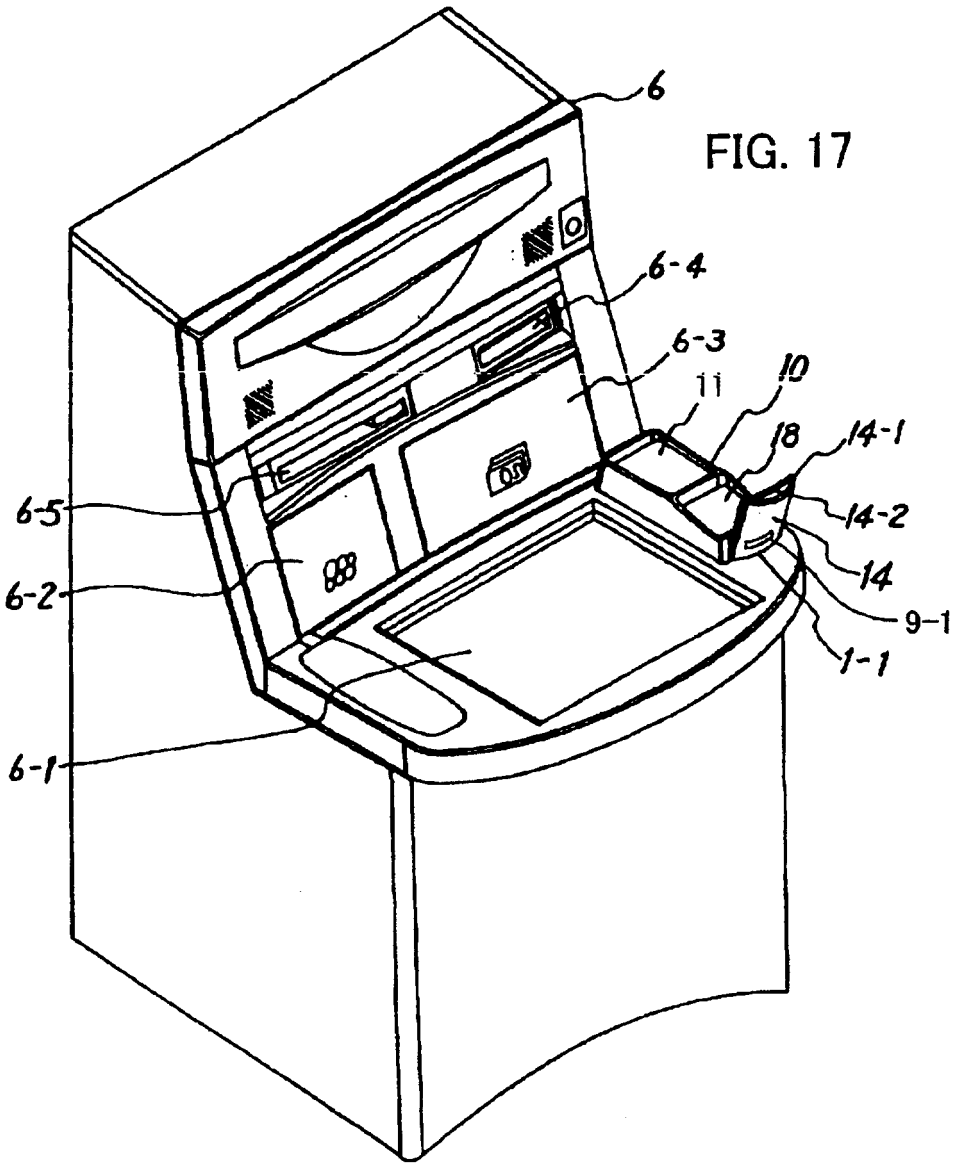
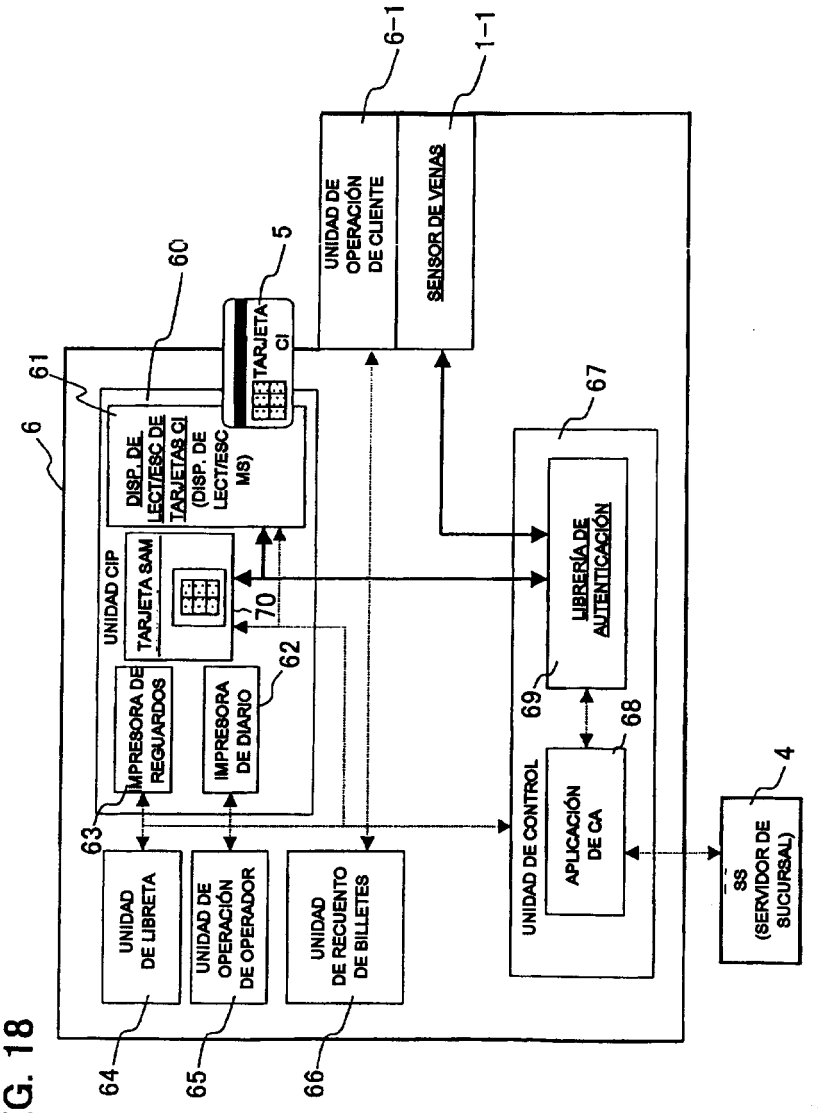


FIG. 17

FIG. 18


6-1
1-1
UNIDAD DE OPERACIÓN DE CLIENTE
SENSOR DE VENAS
5
TARJETA CI
60
61
6
DISP. DE LECT/ESC DE TARJETAS CI (DISP. DE LECT/ESC MS)
UNIDAD CIP
TARJETA SAM
70
67
LIBRERÍA DE AUTENTICACIÓN
62
IMPRESORA DE REGUARDOS
IMPRESORA DE DIARIO
69
68
63
UNIDAD DE CONTROL
APLICACIÓN DE CA
4
SS (SERVIDOR DE SUCURSAL)
UNIDAD DE LIBRETA
UNIDAD DE OPERACIÓN DE OPERADOR
UNIDAD DE RECUENTO DE BILLETES
64
65
66

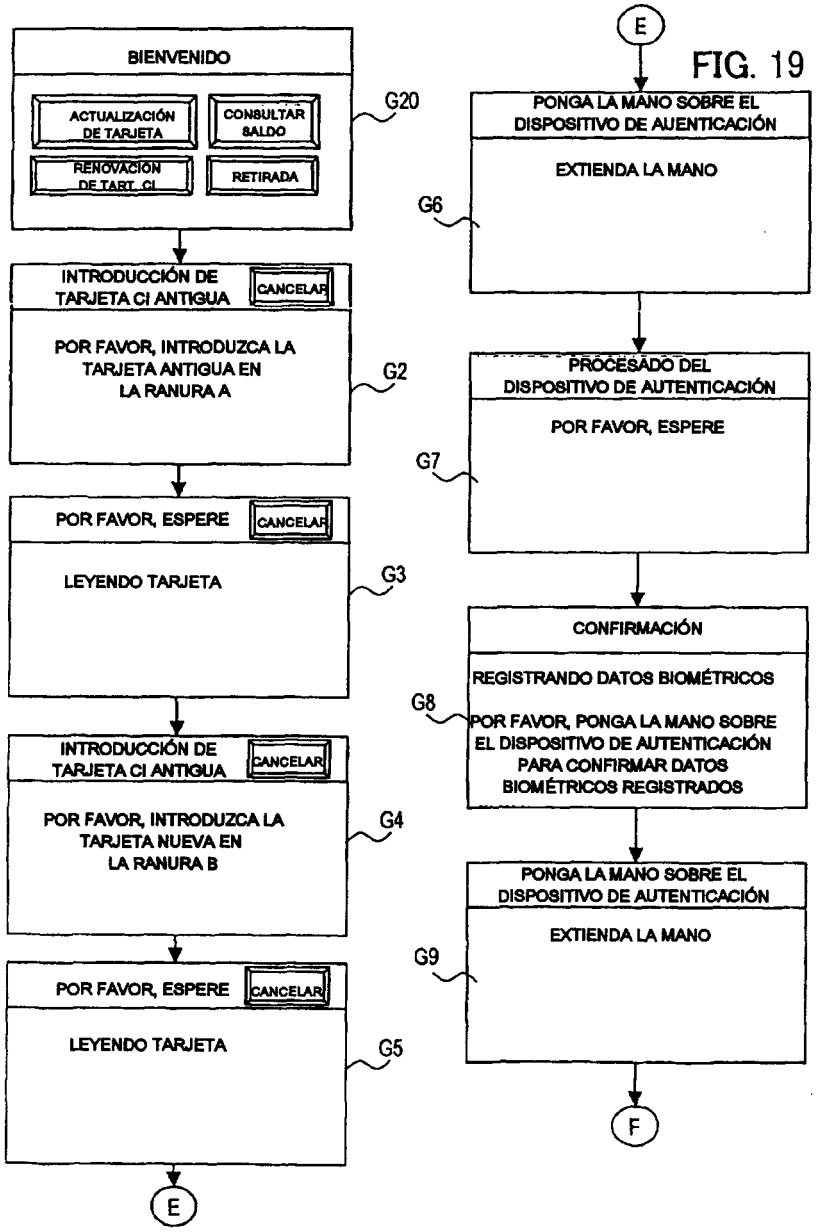

BIENVENIDO
ACTUALIZACIÓN DE TARJETA
CONSULTAR SALDO
RENOVACIÓN DE TART. CI
RETIRADA
G20
INTRODUCCIÓN DE TARJETA CI ANTIGUA
CANCELAR
POR FAVOR, INTRODUZCA LA TARJETA ANTIGUA EN LA RANURA A
G2
POR FAVOR, ESPERE
CANCELAR
LEYENDO TARJETA
G3
INTRODUCCIÓN DE TARJETA CI ANTIGUA
CANCELAR
POR FAVOR, INTRODUZCA LA TARJETA NUEVA EN LA RANURA B
G4
POR FAVOR, ESPERE
CANCELAR
LEYENDO TARJETA
G5
E
E
PONGA LA MANO SOBRE EL DISPOSITIVO DE AUENTICACIÓN
EXTIENDA LA MANO
G6
PROCESADO DEL DISPOSITIVO DE AUTENTICACIÓN
POR FAVOR, ESPERE
G7
CONFIRMACIÓN
REGISTRANDO DATOS BIOMÉTRICOS
POR FAVOR, PONGA LA MANO SOBRE EL DISPOSITIVO DE AUTENTICACIÓN PARA CONFIRMAR DATOS BIOMÉTRICOS REGISTRADOS
G8
PONGA LA MANO SOBRE EL DISPOSITIVO DE AUTENTICACIÓN
EXTIENDA LA MANO
G9
F

FIG. 19

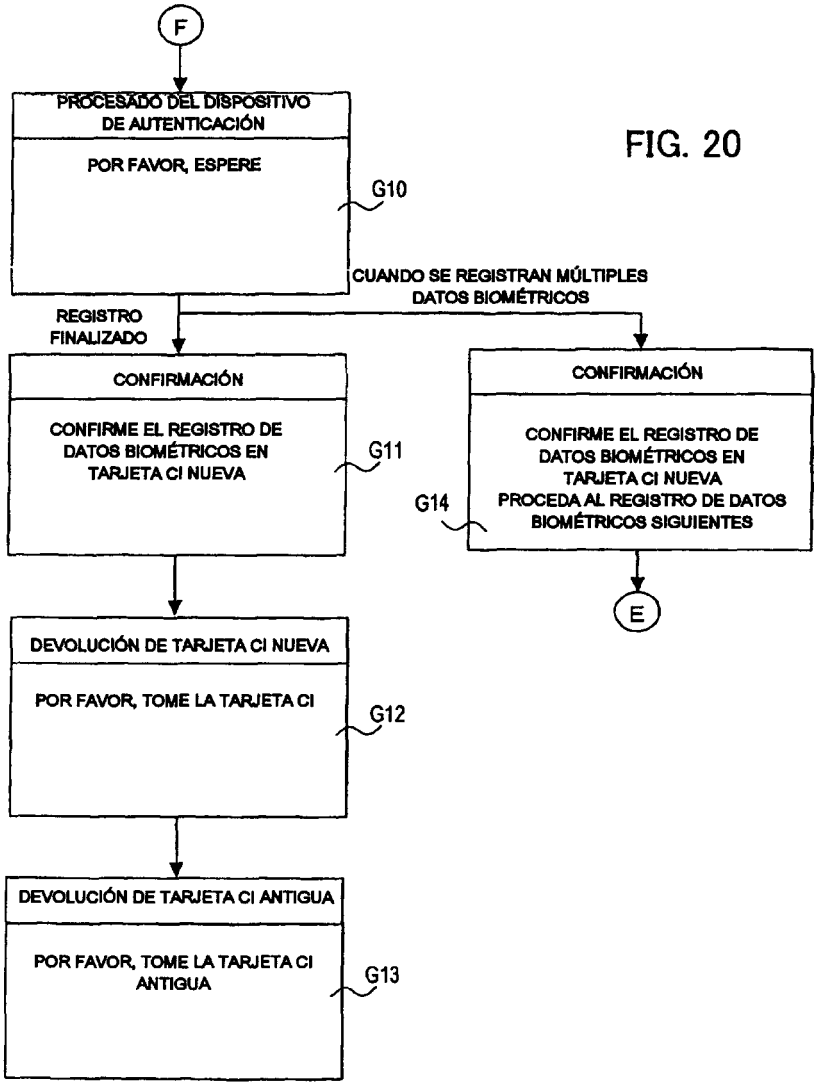

F
PROCESADO DEL DISPOSITIVO DE AUTENTICACIÓN
POR FAVOR, ESPERE
G10
CUANDO SE REGISTRAN MÚLTIPLES DATOS BIOMÉTRICOS
REGISTRO FINALIZADO
CONFIRMACIÓN
CONFIRME EL REGISTRO DE DATOS BIOMÉTRICOS EN TARJETA CI NUEVA
G11
CONFIRMACIÓN
CONFIRME EL REGISTRO DE DATOS BIOMÉTRICOS EN TARJETA CI NUEVA PROCEDA AL REGISTRO DE DATOS BIOMÉTRICOS SIGUIENTES
G14
E
DEVOLUCIÓN DE TARJETA CI NUEVA
POR FAVOR, TOME LA TARJETA CI
G12
DEVOLUCIÓN DE TARJETA CI ANTIGUA
POR FAVOR, TOME LA TARJETA CI ANTIGUA
G13

FIG. 20