(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 336 983**

(21) Número de solicitud: 200550016

(51) Int. Cl.:

G06K 19/073 (2006.01)

H04L 9/32 (2006.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación: **10.09.2003**

(30) Prioridad: **10.09.2002 US 60/409,715**
10.09.2002 US 60/409,716
27.11.2002 US 60/409,919
13.12.2002 US 60/433,254
03.07.2003 US 60/484,692

(43) Fecha de publicación de la solicitud: **19.04.2010**

(43) Fecha de publicación del folleto de la solicitud: **19.04.2010**

(71) Solicitante/s: **IVI SMART TECHNOLOGIES, Inc.**
1810 Old Oakland Road
San Jose, California 95131, US

(72) Inventor/es: **Saito, Tamio;**
Aida, Takashi y
Drizin, Wayne

(74) Agente: **Carpintero López, Francisco**

(54) Título: **Verificación de identidad biométrica segura.**

(57) Resumen:
Verificación de identidad biométrica segura.
Una tarjeta de identificación de alta seguridad incluye una memoria incorporada para almacenar datos biométricos y un sensor incorporado para capturar datos biométricos en vivo. Un procesador incorporado sobre la tarjeta realiza una operación de concordancia para verificar que los datos biométricos capturados concuerdan con los datos biométricos localmente almacenados. Unicamente si hay una concordancia positiva hay algún dato transmitido desde la tarjeta para su verificación adicional y/o procesado adicional. Preferiblemente, la tarjeta es compatible con una tarjeta inteligente ISO. En otra realización, la tarjeta inteligente ISO funciona como un cortafuegos para proteger el procesador de seguridad usado para almacenar y procesar los datos biométricos protegidos de un acceso malicioso externo vía la interfaz de la tarjeta inteligente ISO. En otra realización, el procesador de Seguridad se inserta entre la interfaz de la tarjeta inteligente ISO y un procesador de la tarjeta inteligente ISO sin modificar y bloquea cualquier comunicación externa hasta que la huella dactilar del usuario ha concordado con una huella dactilar previamente grabada.

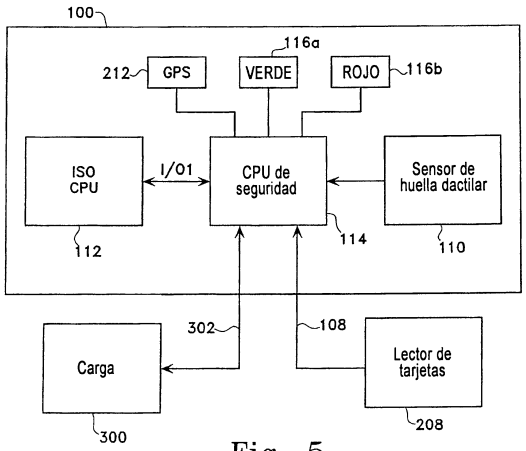


Fig. 5

ES 2 336 983 A2

DESCRIPCIÓN

Verificación de identidad biométrica segura.

Referencia cruzada a solicitudes relacionadas

Esta solicitud se basa en, y reivindica prioridad de las solicitudes provisionales 60/409.716 presentada el 10 de septiembre de 2002 (número de expediente 7167-102P1), 60/409.715 presentada el 10 de septiembre de 2002 (número de expediente 7167-103P), 60/429919 presentada el 27 de noviembre de 2002 (número de expediente 7167-104P), 60/433.254 presentada el 13 de diciembre de 2002 (número de expediente 7167-105P) y 60/484.692 presentada el 3 de julio de 2003 (número de expediente 7167-106P), que se incorporan en la presente memoria como referencia en su totalidad.

Antecedentes

La informatización y especialmente la tecnología de NTERNET ha estado proporcionando acceso a datos cada vez mayor, incluyendo datos financieros, datos médicos, datos de personas y medios para dar curso a transacciones financieras y de otro tipo en las cuales se actualizan o intercambian datos confidenciales.

Habitualmente se usan contraseñas para mantener la confidencialidad de tales datos; sin embargo, las contraseñas se basan frecuentemente en una fecha de cumpleaños o en un número de teléfono que es fácil de averiguar, y esto no es seguro en absoluto. Además, incluso una contraseña complicada generada aleatoriamente a menudo puede ser fácilmente robada. Los sistemas de acceso a datos basados en contraseñas son, pues, vulnerables a ataques delictivos con el riesgo resultante y daños en la industria y la economía, e incluso las vidas de la gente. En consecuencia, existe la necesidad de un procedimiento mejorado para asegurar datos y proteger estos datos accesos no autorizados.

Los datos biométricos pueden incluir detalles precisos que son difíciles de capturar pero fáciles de analizar (tales como una secuencia de pequeños detalles de huellas dactilares) o patrones de conjunto que son fáciles de capturar pero difíciles de analizar (tales como las características espaciales de espirales de huellas dactilares).

Existen algoritmos de encriptado que requieren una clave digital únicamente disponible para usuarios autorizados. Sin la clave adecuada, los datos encriptados únicamente se pueden desencriptar en un formato utilizable con una sustancial inversión de tiempo y de recursos de procesado, e incuso entonces, únicamente si se conocen ciertas características de los datos sin encriptar (o al menos son predecibles).

La Solicitud de Patente japonesa publicada JP 60-029868 fechada el 25 de febrero de 1985 a nombre de Tamio SAITO, describe un sistema de identificación individual que emplea una tarjeta de identidad con una memoria integrada para registrar datos biométricos cifrados obtenidos a partir del poseedor de la tarjeta. Los datos biométricos pueden incluir el espectrograma de la voz, huellas dactilares, aspecto físico y/o un ensayo biológico. Durante el uso, el dato de la tarjeta se lee y descifra por comparación con el dato correspondiente capturado de la persona que presenta la tarjeta. Un sistema como éste permite que un individuo registrado sea identificado positivamente con un alto grado de precisión. Sin embargo, como los datos biométricos se obtienen y procesan por un equipo externo, es difícil proteger la información almacenada en la tarjeta contra la posible modificación y/o robo de identidad.

Se ha propuesto una tarjeta mejorada de identificación que, en la tarjeta, incluye una lasca multiprocesadora controlada por datos para proporcionar un cortafuegos que tanto encripta como aísla los datos biométricos almacenados en la tarjeta, proporcionando, de este modo, sustancialmente mayor protección contra la modificación no autorizada de los datos almacenados. Sin embargo, el proceso real de concordancia se realizó en el mismo terminal lector externo que capturó los datos biométricos vivos y era, por ello, aún potencialmente vulnerable a la manipulación externa fraudulenta.

Sumario

Una primera realización de una tarjeta de identificación de alta seguridad incluye no solamente una memoria incorporada para los datos biométricos almacenados, sino también un sensor incorporado para capturar los datos biométricos vivos. Un sistema remoto de autentificación mantiene una base de datos segura que incluye los datos biométricos. Un procesador incorporado sobre la tarjeta realiza una operación preliminar de concordancia para verificar que el dato biométrico capturado concuerda con el dato biométrico almacenado localmente. Únicamente si hubiera una concordancia local positiva, cualquier dato capturado o dato almacenado sensible se transmite al sistema remoto de autentificación para la verificación adicional y procesado adicional. Como protección adicional contra ataques maliciosos, el dato localmente almacenado es preferiblemente diferente del dato almacenado a distancia, y la concordancia local y la concordancia remota se realizan, preferiblemente, utilizando algoritmos diferentes de concordancia. De este modo, incluso si la tarjeta, el dato localmente almacenado y/o el terminal local al cual está conectada la tarjeta aún está en una trasacción, hay una alta probabilidad de que el sistema remoto de autorización aún sea capaz de detectar la intrusión intentada.

Una segunda realización también incluye una memoria incorporada para el dato biométrico almacenado un sensor incorporado para capturar el dato biométrico vivo y un procesador incorporado; sin embargo, en esta realización todo el

proceso de concordancia es realizado por el procesador incorporado y tanto el dato biométrico originalmente capturado como cualquier otra información "privada" almacenada en la memoria incorporada no están disponibles para ningún proceso externo. En cambio, únicamente se genera un mensaje de verificación en respuesta a una concordancia con éxito entre el dato biométrico recientemente capturado y el dato biométrico previamente capturado. El mensaje de verificación hace que la tarjeta funcione de una forma similar a una tarjeta inteligente o chip ISO (SmartCard ISO) al introducir con/sin éxito un Número de Identificación Personal (PIN), pero con la seguridad adicional permitida por un proceso de verificación más seguro. En cualquiera de estas realizaciones, los datos biométricos almacenados y cualquier algoritmo de encriptado asociado localmente almacenado o clave de encriptado se carga preferentemente en la tarjeta en el momento de la emisión original al poseedor de la tarjeta de una forma que desanima cualquier acceso externo posterior, potenciando más, por lo tanto, la integridad de los datos biométricos almacenados y de todo el proceso de verificación.

En una realización, la tarjeta inteligente ISO funciona como un cortafuegos para proteger el procesador de seguridad usado para almacenar y procesar los datos biométricos protegidos de maliciosos ataques externos vía la interfaz de la tarjeta inteligente ISO. En otra realización, el procesador de seguridad se inserta entre la interfaz de la tarjeta inteligente ISO y un procesador de tarjeta inteligente ISO y bloquea cualesquiera comunicaciones externas hasta que huella dactilar del usuario ha coincidido con una huella dactilar previamente registrada.

En una realización preferida de una tarjeta de identificación de alta seguridad con capacidad incorporada para concordar huellas dactilares, se proporciona retroalimentación en tiempo real mientras el usuario está manipulando su dedo sobre el sensor de huella dactilar facilitando, por lo tanto, una colocación óptima del dedo sobre el sensor. Esta retroalimentación no solamente reduce la complejidad de cálculo, sino que también proporciona un medio adicional para discriminar entre un usuario sin experiencia y un usuario fraudulento, reduciendo más, de este modo, la probabilidad de negativos falsas y/o de positivos falsos. En otra realización preferida, el sensor de huella dactilar está retenido en un portador que proporciona rigidez adicional.

En una aplicación ejemplar, los datos biométricos capturados y/o una indicación de la identidad del poseedor de la tarjeta está encriptada e introducida en una red transaccional que incluye una institución financiera y un servidor de autentificación por separado, previo a cualquier concesión de acceso vía telefónica a datos confidenciales o a cualquier proceso automatizado para finalizar una transacción con seguridad. En otra aplicación ejemplar, la salida de la tarjeta se usa para obtener acceso físico a una zona segura. En cualquier aplicación, en la tarjeta o en un servidor externo de seguridad, o en ambos, se puede llevar un registro de intentos de acceso con éxito y sin éxito.

Dibujos

La figura 1 muestra una realización de una tarjeta inteligente con verificación biométrica incorporada de la identidad de la persona que presenta la tarjeta.

La figura 2 es un diagrama de flujo que muestra un proceso ejemplar para ayudar al usuario a una colocación óptima de un dedo sobre el sensor de huella dactilar.

La figura 3 es un diagrama de bloques por funciones de un sistema de verificación biométrica capaz de realizar tanto la verificación local como remota de la identidad de una persona que presenta una tarjeta de identificación segura.

La figura 4 es un diagrama de bloques por funciones de una tarjeta ejemplar de verificación biométrica con diferentes trayectorias de datos físicos para usar durante la carga inicial de los datos biométricos del portador de la tarjeta y durante la verificación de la identidad del portador de la tarjeta respecto de una aplicación remota.

La figura 5 muestra una realización alternativa a la tarjeta ejemplar de verificación biométrica de la figura 4, que se pretende usar con una CPU para ISO SmartCartd sin modificar.

La figura 6 es un diagrama de flujo que muestra la comunicación entre una aplicación ejemplar y una tarjeta ejemplar de verificación en la cual únicamente se realiza la identidad del poseedor de la tarjeta.

La figura 7 es similar al diagrama de flujo de la figura 6, pero modificado para usarse con la tarjeta ejemplar de verificación biométrica de la figura 5.

La figura 8 muestra una segunda realización de una tarjeta inteligente con verificación biométrica incorporada que se puede conectar a un terminal local tanto de forma inalámbrica como por medio de un conector eléctrico.

La figura 9 es una sección transversal por de la tarjeta de la figura 8.

La figura 10 es un diagrama de circuito de un sensor ejemplar de huella dactilar.

La figura 11 muestra una realización de un conjunto portador para el sensor de la figura 10.

Descripción detallada

Tarjeta inteligente

La expresión "tarjeta inteligente" se usa en la presente memoria en un sentido genérico para referirse a cualquier objeto físico que sea lo bastante pequeño como para ser contenido en la mano, enroscado alrededor del cuello, o portado de cualquier otro modo por la persona, y que incluye un microprocesador que sea capaz de almacenar, procesar y comunicar información codificada digitalmente relativa o relacionada de cualquier otro modo con un poseedor individual de tarjeta. Un ejemplo bien conocido de una tarjeta inteligente como ésta es la ISO (*International Standards Organization*) SmartCard, que tiene el mismo tamaño y forma físicos que una tarjeta de crédito convencional, pero que incluye memoria de poca duración para almacenar datos específicos de usuario y un microprocesador que se puede programar con un potente algoritmo de encriptado que indica si un PIN (*Personal Identification Number*) recibido desde una terminal de usuario concuerda o no con un PIN encriptado almacenado en la tarjeta, proporcionando, por lo tanto, un mayor grado de confianza de que la persona que presenta la tarjeta es el poseedor auténtico de la tarjeta, de lo que sería posible en un sistema de verificación que simplemente confía en una comparación visual de firmas y/o en similitud física.

Ahora se hará referencia a la figura 1, que muestra una realización de una tarjeta inteligente con verificación biométrica incorporada. La tarjeta 100 está genéricamente fabricada en plástico y tiene el aspecto en conjunto, de una tarjeta de crédito convencional, de dimensiones aproximadas, según se especifica en ISO 7816, de aproximadamente 53,98 x 85,6 mm y un grosor de aproximadamente 0,76 mm o más.

Similar a una tarjeta de crédito convencional, la tarjeta 100 incluye una región 102 superior libre que se extiende a lo largo de toda la anchura transversal de la tarjeta para sustentar una banda magnética (como especifica ISO 7811-2 & 7801-6) sobre la superficie trasera de la tarjeta, sobre la cual se puede almacenar información alfanumérica codificada convencionalmente relativa al poseedor de la tarjeta y a cualquier cuenta asociada, permitiendo, de este modo, que la tarjeta 100 sea usada en un lector convencional de banda magnética. Sin embargo, como cualquier dato incrustado en la banda magnética se puede alterar fácilmente, una banda magnética como ésta únicamente se pretende para usarse en ciertas aplicaciones donde la necesidad de compatibilidad hacia atrás con terminales más antiguos basados en banda magnética pesa más que la potencial degradación de seguridad que una banda magnética aporta al sistema.

La región 102 superior también se puede usar para soportar diversas medias de prevención del fraude, tales como una fotografía coloreada resistente material reflecor del poseedor de la tarjeta y/o un logotipo hológrafo del emisor de la tarjeta. La región 104 inferior de tarjeta 100 se puede usar de forma convencional para la información estampada en relieve (según especifica ISO 7811-1) tal como el nombre del poseedor de la tarjeta, un identificador numérico de cuenta (o tarjeta), una fecha de caducidad, para permitir el uso de la tarjeta 100 en un impresor convencional de tarjeta.

La región 102 superior y la región 104 inferior están separadas por una región 106 media, en la cual está incrustado un conjunto visible de 8 puntos 108 de contacto de la tarjeta inteligente ISO, que proporcionan una conexión eléctrica adecuada entre la tarjeta y los contactos correspondientes sobre un lector de tarjeta. Por este medio, no solamente datos, sino también, señales de energía eléctrica, temporización y control se pueden intercambiar entre el lector y la tarjeta como se especifica en ISO 7816-3.

Sobre el lado derecho de la región 106 un punto de conexión 110 de sensor es visible, el cual se usa para capturar datos de huella dactilar del dedo del poseedor de la tarjeta. La tarjeta está dotada, preferiblemente, de un código ID que es exclusivo para el sensor 110 u otro componente electrónico incrustado en la tarjeta; por ejemplo, un código en el formato de una dirección convencional IP y/o MAC.

También, indicado esquemáticamente en la figura 1, hay diversos componentes electrónicos adicionales que colaboran con el punto 108 de contacto y con el sensor 110 para proporcionar más funcionalidad, y en particular mejor seguridad, de la que de otro modo sería posible.

En una realización, el procesador 112 compatible con una tarjeta inteligente ISO está directamente conectado a puntos 108 de contacto para proporcionar una conexión eléctrica con un lector (no mostrado) de tarjeta externo y compatible con ISO para, de este modo, proporcionar no solamente energía eléctrica a los componentes electrónicos incorporados, sino también un medio para comunicar datos entre la tarjeta y cualquier aplicación informática de comunicación externa, aplicación informática de seguridad, aplicación informática de transacción y/o otra aplicación informática de aplicación que funcionan sobre el lector de tarjeta o cualesquiera dispositivos informáticos asociados dispuestos en red con el lector de tarjeta.

Aunque en la realización descrita la trayectoria de los datos entre la tarjeta 100 y el lector externo de tarjeta está en forma de una conexión cableada que usa una disposición de contacto SmartCard específicamente ISO, se debe sobrentender que en otras realizaciones, también se pueden usar otras tecnologías de transmisión tales como conexiones USB o RS 232C o SPI (serie), posiblemente sobre enlaces de comunicaciones de RF (Radio Frecuencia) inalámbrica, microondas y/o IR (Infra Rojos).

Además, aunque la realización descrita recibe energía eléctrica del lector de tarjeta, otras realizaciones preferidas podrían tener una fuente de alimentación incorporada tal como una célula solar o una batería. Una fuente de energía eléctrica incorporada como ésta, puede ser ventajosa, por ejemplo, si la interfaz mecánica entre la tarjeta 100 y un tipo de lector de tarjeta es tal que el sensor 110 de huella dactilar no es accesible al usuario cuando los contactos 108 están conectados a las correspondientes conexiones dentro del lector de tarjeta y, por ello, el dato de la huella dactilar de usuario se debe captura cuando la tarjeta 100 no está directamente unida mediante cables con el lector de tarjeta.

Procesador de seguridad

Como se ilustra, el procesador 114 de Seguridad está conectado entre el procesador 112 ISO y el sensor 110 para proporcionar procesado seguro y almacenado de los datos capturados, así como un "cortafuegos" seguro para proteger los datos y programas almacenados en su memoria específica de cualquier intento de acceso inadecuado vía el procesador 112 ISO, como se describirá en la presente memoria en lo que sigue. Un cortafuegos como éste, puede estar diseñado para dejar pasar únicamente datos encriptados que usan una clave de encriptado que esté basada en una dirección de red asignada de forma exclusiva o que, en cambio, sea exclusiva para la tarjeta particular, tal como datos extraídos de un patrón de huella dactilar previamente almacenado, o un número de dispositivo asignado de forma exclusiva, tal como un número de CPU, o un número de sensor de huella dactilar. En otra realización, el cortafuegos únicamente deja para datos que contiene datos exclusivos de identificación procedentes de una transmisión, o de datos, previa. Aún en otras realizaciones, el cortafuegos mantiene diferentes claves para diferentes aplicaciones, y usa aquellas claves para enrutar los datos hasta un procesador diferente o partición de memoria correspondiente.

En otra realización (no ilustrada), el procesador 114 de Seguridad está directamente conectado a los contactos 108 ISO y actúa como un portero seguro entre el procesador 112 ISO y los contactos 108 ISO. Una disposición alternativa como ésta tiene la ventaja de proporcionar la seguridad adicional permitida por el procesador 114 de Seguridad y el sensor 110, sin ningún compromiso posible de cualesquiera características de seguridad que ya puedan estar incorporadas en el procesador 112 ISO.

El procesador 114 de Seguridad incluye preferiblemente una memoria no volátil de semiconductor o de no semiconductor, tal como FRAM, OTP, E^2PROM, MRAM, MROM para almacenar un patrón de huella dactilar previamente inscrito y/o la otra información personal biométrica. En otras realizaciones, algunas o todas las funciones del procesador 114 de seguridad se podrían implantar en un procesador 112 ISO y/o algunas o todas las funciones del procesador 112 ISO se podrían implantar en un procesador 114 de seguridad. Una implantación combinada como ésta aún podría mantener un cortafuegos mediante aplicación informática entre las diversas funciones, lo que podría ser especialmente ventajoso si el dispositivo se implantó con un procesador que no permitía ninguna modificación posterior en las aplicaciones informáticas almacenadas. Alternativamente, ambos procesadores 112, 114 podrían ser procesadores diferentes en un único dispositivo multiprocesador diseñado para proteger cada proceso de cualquier interferencia procedente de otro proceso que se esté ejecutando en un procesador diferente. Un ejemplo de un dispositivo multiprocesador como ésta es el DDMP (*Data Driven Múltiple Processor*) de Sharp de Japón.

Aunque estos diversos sensores, contactos y otros componentes electrónicos, así como los circuitos impresos u otro cableado eléctrico con el cual están interconectados, están, preferiblemente, todos completamente incorporados dentro del cuerpo de la tarjeta 100 de tal forma que están protegidos de la abrasión y de contaminantes externos, la ubicación preferida dentro de la región 106 media entre la región 102 superior y la región 104 inferior les protege, además, de posibles daños procedentes de los lectores convencionales de banda magnética, incrustadores y equipo de impresores que mecánicamente tienen interfaces con estas otras regiones.

Retroalimentación de LED

Los LED 116a, 116b están controlados por el procesador 114 de seguridad y proporcionan retroalimentación visible al usuario. En la realización ilustrada, están ubicados en la región 104 inferior, preferiblemente en una ubicación en el borde lateral de la tarjeta alejado de los puntos 108 de contacto. En cualquier caso, los LED 116a, 116b, están preferiblemente ubicados allí donde no resulten dañados durante cualquier proceso de incrustación, y donde sean visibles cuando la tarjeta se inserte en un lector convencional de tarjetas inteligentes ISO y/o mientras el dedo del usuario se coloque sobre el sensor 110 de huella dactilar. Por ejemplo:

En Modo verificar.

- ROJO parpadeante: esperando al dedo
- El parpadeo se detiene: dedo colocado sobre el sensor
- ROJO parpadea de nuevo: incapaz de concordar, conformidad para que desplace el dedo.
- VERDE parpadeo prolongado de nuevo: concuerda, conformidad para que retire el dedo.

En Modo inscripción:

- VERDE parpadeante: espere al dedo
- El parpadeo se detiene: dedo colocado sobre el sensor
- ROJO parpadea de nuevo: incapaz de inscribir, conformidad para que desplace el dedo.
- VERDE parpadeo de nuevo: inscrito, conformidad para que retire el dedo.

En Modo Borrar:

- VERDE y ROJO parpadeante: preparado para borrar
- VERDE parpadea de nuevo: borrado.

Preferiblemente, al usuario se le dan múltiples oportunidades para posicionar su dedo para obtener una Concordancia o Inscripción con éxito antes de que se transmita cualquier informe negativo. En una realización, se transmite un informe negativo al Servidor de Autentificación únicamente si el Usuario ha retirado su dedo antes de recibir la indicación verde de conformidad, o si ha superado un tiempo I imite predeterminado. Un proceso como éste no solamente adiestra al Usuario a hacer una colocación óptima de su dedo sobre el sensor, lo que no solamente reduce la complejidad de cálculo, sino que también permite el uso de más umbrales de discriminación. Esta retroalimentación visible también proporciona una base psicológica para discriminar entre un usuario sin experiencia (que típicamente seguirá intentando hasta que consiga la colocación adecuada) y un usuario fraudulento (que típicamente no querrá llamar la atención y abandonará antes de que sus maliciosas intenciones sean descubiertas). El resultado neto es una reducción significativa en la probabilidad de negativos falsas y/o de positivos falsos.

La figura 2 ilustra un proceso ejemplar para ayudar a que el Usuario coloque su dedo sobre el sensor 110. En el bloque 150, el LED 116b ROJO está parpadeando. Una vez que se ha detectado un dedo (bloque 152), el LED deja de parpadear y se hace un test (bloque 154) para tener calidad de imagen (regiones alargadas definidas que se corresponden con las montañas y valles de la piel del dedo). Si la calidad es inadecuada (rama 156 NO), un parpadeo sencillo del LED 116b ROJO instruye al Usuario a desplazar su dedo a una posición diferente (bloque 158); en caso contrario (rama 160 SÍ) se realiza un segundo test (bloque 162) para determinar si se ha colocado el mismo dedo la misma posición que se usó para inscribir al Usuario, de tal forma que un sencillo algoritmo de Concordancia pueda verificar el dato vivo que se corresponde con el dato almacenado dentro de un umbral predeterminado, verificando, de este modo, que el dedo vivo es el mismo que el dedo que estaba originalmente inscrito (rama 164 SÍ), y el LED 116a VERDE se activa (bloque 166) durante un tiempo suficiente (bloque 168) para verificar que se ha realizado una concordancia con éxito, y que el Usuario ahora puede retirar su dedo. Alternativamente, si el umbral de concordancia no se cumple (rama 170 NO), un parpadeo sencillo del LED 116b ROJO (bloque 158) instruye al Usuario a desplazar su dedo hasta una posición diferente y el proceso se repite.

Arquitecturas ejemplo de red

Ahora se hará referencia a la figura 3 que ilustra una posible realización de un sistema biométrico de verificación capaz de realizar la verificación tanto local como remota de la identidad de una persona que presenta una tarjeta de identificación segura. El sistema incluye tres componentes principales: un terminal 200 de cliente, un servidor 202 de aplicación y un servidor 204 de autentificación. El terminal 200 de cliente incluye funcionalidad para la captura en vivo y el procesado local de la huella dactilar de un usuario, para encriptar los datos procesados localmente y para tener comunicación segura con el servidor de aplicación y con el servidor de autentificación, preferiblemente a través de INTERNET usando el protocolo de transmisión y esquema de direccionamiento IP/TCP, estando dotado de protección ante el acceso malicioso por cortafuegos 206 convencionales IP. En otras realizaciones los cortafuegos 206 pueden estar dotados de Filtros y de Codificador/Decodificador de Encriptado que codifica los datos transmitidos una vez que se ha verificado ser datos Autorizados y que decodifican los datos recibidos antes de decidir si, de hecho, es un dato Autorizado, usando, por ejemplo, un algoritmo de encriptado tal como DES 128. Por este medio, el cortafuegos 206 puede clasificar datos como Autorizados o potencialmente Malicioso en función no solamente del encabezado del mensaje, sino también en función del contenido del mensaje.

El Terminal 200 de Cliente se puede implantar como un artefacto específico de red telefónica, o se puede implantar en una aplicación informática instalada en un ordenador de sobremesa programable, agenda electrónica u otro puesto de trabajo u ordenador personal controlado por un sistema operativo con fin genérico, tal como Windows XXX, OS X, Solaris XX, Linux o Free BSD. El Terminal 200 de Cliente incluye, preferiblemente, bases de datos "negativas" actualizadas (por ejemplo, identidades de tarjetas perdidas o robadas, o restricciones sobre una tarjeta particular o grupo de tarjetas) que permiten una medida de seguridad adicional.

El servidor 202 de aplicación incluye funcionalidad para realizar una transacción o, sino, responder a instrucciones del usuario remoto en el terminal 200 de cliente una vez que se ha verificado la identidad del cliente por el servidor 204

de autentificación. El servidor 204 de autentificación incluye funcionalidad para tener comunicación segura tanto con el terminal 200 de cliente como con el servidor 202 de aplicación, para almacenar datos auténticos de huella dactilar y otra información relativa a usuarios previamente registrados, para comparar los datos almacenados con los datos vivos codificados recibidos desde el terminal 200 de cliente, y para advertir al servidor 202 de aplicación si los datos de la huella dactilar viva específica concuerdan o no con los datos de la huella dactilar específica almacenada.

Más particularmente, el Terminal 200 de Cliente comprende, además, dos componentes principales: un componente fijo de lector 208 de tarjeta que incluye un terminal 210 examinador de INTERNET, y una interfaz 108a de lector de tarjeta (que puede ser un sencillo cable USB que termina en un conjunto de contactos eléctricos para formar la correspondiente conexión eléctrica con puntos 108 de contacto de tarjeta inteligente ISO) y un componente 100' portátil de tarjeta inteligente. En una realización, el componente 100' portátil puede ser la tarjeta 100 inteligente previamente descrita que incluye el sensor 110 de huella dactilar, el procesador 114 de seguridad y el procesador 112 de tarjeta inteligente ISO.

El Servidor 202 de Aplicación comprende, además, una interfaz de servidor de INTERNET que incluye el cortafuegos 206 y el examinador 213 de INTERNET, así como un módulo 216 de aplicación de transacción y un módulo 218 de validación. En caso de que el servidor de aplicación y el módulo 216 de aplicación sean dispositivos heredados que no hubieran sido diseñados para comunicarse externamente por medio del protocolo IP/PCT, el cortafuegos 206 se puede sustituir por un convertidor de protocolo adecuado que incorpore el módulo 218 de validación y que tenga una dirección IP fija. El Servidor de Servicio de la Aplicación puede ser operado, por ejemplo, por una tercera parte que esté deseando proporcionar servicio a través de INTERNET a un Usuario autorizado.

El Servidor 204 de Autentificación comprende, además, una interfaz 220 de servidor de INTERNET, un módulo 222 de procesado que incluye un algoritmo 224 de concordancia de huella dactilar, y una base de datos 226 para almacenar huella dactilar y otra información auténtica recogida de individuos en el momento en que estos individuos se registraron en el sistema y su identidad se garantizó a satisfacción del operador del sistema. Como una mejora adicional a la seguridad, los datos almacenados por cualquier individuo particular preferiblemente no se almacenan en el Servidor de Aplicación como una simple secuencia de información, sino que cada asunto se almacena por separado y cualesquiera índices o relaciones requeridos que conectan estos asuntos son accesibles únicamente por medio de una clave correspondiente que se mantiene como parte de esos datos privados individuales en el Servidor de Autentificación.

Ubicación

En ciertas realizaciones, el lector 208 fijo y/o la tarjeta 100" también puede estar dotada de un receptor 212 integral por satélite de posicionamiento global ("GPS") que puede proporcionar información útil sobre la ubicación actual del lector y de la tarjeta en o en aproximadamente el momento en que está teniendo lugar una transacción particular. En particular, los datos de ubicación procedentes del receptor 212 GPS se pueden usar para deshabilitar (tanto permanente como temporalmente) el receptor y/o la tarjeta en el caso de cualquiera sea llevado a una ubicación en la cual su uso no está autorizado. También se puede determinar automáticamente la posición por medio diferente al GPS, por ejemplo, usando tecnología PHS (*Japanese Cellular Telephone*) de ubicación de quien llama, o sensores de ubicación que actúan ante variaciones locales en los campos electromagnéticos de la tierra. En el caso particular de una tarjeta equipada de GPS, los diversos componentes de GPS que incluyen antenas; amplificación de señal, convertidor de c.a. y circuitos de muestra y de retención; y procesador digitar para calcular la posición son preferiblemente todos parte de un sencillo circuito integrado o de dispositivos discretos montados sobre una placa de circuito sencilla, que está integrada con, estampada en relieve en, o laminada en el cuerpo de la tarjeta.

Arquitectura de tarjeta para tarjeta ISO con interfaces de concordancia incorporados del procesador ISO

La figura 4 es un diagrama funcional de bloques de una tarjeta 100 ó 100' ejemplar biométrica de verificación, compatible con una tarjeta inteligente ISO con diferentes trayectorias físicas de datos para usarse durante la carga inicial de los datos biométricos del poseedor de la tarjeta y durante la verificación de la identidad del poseedor de la tarjeta hasta una aplicación remota.

En particular, además del Procesador 112 ISO, el procesador 114 de seguridad, el sensor 110 de huella dactilar, los LED 116a, 116b y el receptor 212 GPS opcional previamente descritos, estando directamente conectado únicamente el procesador 112 ISO al lector 208 de tarjeta vía puntos 108 de contacto de una tarjeta inteligente ISO, se muestra un módulo 300 de carga diferente y la conexión 302 asociada temporal, que se proporciona para realizar la comunicación directa con el procesador 114 de seguridad durante el Registro inicial del Usuario. Es de destacar que el procesador 112 ISO se comunica con el procesador 114 de seguridad por medio de puertos 304, 306 de E/S, mientras la conexión 302 temporal de carga se conecta a un puerto 308 de E/S diferente. El procesador de seguridad se programa preferiblemente de tal forma que cualesquiera datos o aplicaciones informáticas sensibles relacionados con la seguridad son accesibles únicamente desde el puerto 308 y no desde los puertos 304 y 306, evitando, por lo tanto, cualquier posibilidad de acceso malicioso a estos datos sensibles una vez que la conexión 302 se haya deshabilitado.

La mayoría de los procesadores ISO disponibles comercialmente tienen al menos dos puertos de E/S y algunos tienen al menos tres. Únicamente uno de estos puertos (E/S 1) está diseñado para la conexión 108 de datos en serie

de tarjeta inteligente ISO hasta el lector 208 de tarjeta compatible externo ISO. El puerto extra o los dos puertos E/S extra proporcionan, preferiblemente, una comunicación específica por medio de dispositivos entre el procesador 112 ISO y el Procesador 114 de Seguridad que actúa con un dispositivo cortafuegos para bloquear cualquier intento malicioso de reprogramar el Procesador 114 de Seguridad o de obtener acceso a cualquier información sensible que pueda haber sido capturada previamente por el sensor 110 o que se pueda haber sido almacenada por otro medio dentro del procesador 114. En el caso particular de un Procesador ISO con más de dos líneas de E/S, se pueden presentar más de dos estados de información estática de estado en el trayecto específico de comunicación entre el Procesador ISO y el Procesador de Seguridad, tal como 1) Listo, 2) Ocupado, 3) Fallo y 4) Pasar incluso cuando el Procesador de Seguridad esté completamente sin energía eléctrica. Por supuesto, incluso si únicamente un puerto de E/S está disponible esas cuatro condiciones se pueden transmitir dinámicamente como datos en serie.

Entre las posibles instrucciones y datos que se pueden transmitir entre la CPU ISO y la CPU de Seguridad a través de las interfaces ISO de E/S 2 e E/S 3 son las siguientes:

• Órdenes para inscribir o autentificar a un Usuario, al cual la CPU de Seguridad enviará resultado de la inscripción o el resultado de la autentificación para el almacenamiento local y/o la transmisión hasta una aplicación remota.

• Se puede enviar información de huella dactilar como una plantilla (referencia) desde la CPU de Seguridad hasta la CPU ISO para almacenarse en la memoria de la tarjeta inteligente ISO para realizar la transmisión hasta aplicaciones remotas. Para seguridad aumentada de información sensible personal, el dato de referencia puede ser encriptado por la CPU de Seguridad antes de que sea enviado a la CPU ISO.

La conexión 302 de carga proporciona una conexión directa hasta la CPU 114 de Seguridad que contornea cualquier protección de cortafuegos, permitida la conexión ISO y los puertos 304 y 306 de E/S asociados específicos, mientras mantiene posiblemente la comunicación entre la CPU 112 ISO y el lector 208 ISO de forma que la energía eléctrica también estará disponible para la CPU 114 de Seguridad. Se usa primariamente durante el registro inicial de la tarjeta para un usuario particular, y se debería proteger contra el acceso no autorizado.

La figura 5 muestra una realización alternativa a la tarjeta biométrica ejemplar de verificación de la figura 4, que se pretende usar con una CPU de tarjeta inteligente ISO sin modificar. En particular, la CPU 112' ISO ya no debe realizar ninguna de las funciones de puerta entre el Lector 208 de tarjeta y la CPU 114' de Seguridad, tanto durante el uso normal como durante la carga y, por ello, puede ser cualquier lasca aprobada por la ISO, no modificado en modo alguno, y usado únicamente de una forma que sea absolutamente transparente tanto al lector 208 de tarjeta como a cualquier aplicación externa. En una realización alternativa como ésta, la CPU 114' de Seguridad actúa como un cortafuegos transparente entre la CPU 112' ISO y cualquier aplicación externa, si la huella dactilar capturada concuerda con la huella dactilar almacenada, y bloquea toda esta comunicación si la huella dactilar capturada no concuerda con la huella dactilar almacenada.

Inicialización de tarjeta y protección de datos almacenados

Guillotina

En una realización, la tarjeta originalmente fabricada tiene una extensión sobresaliente de circuito impreso que proporciona una conexión directa con la CPU de Seguridad, así como con al menos partes de la interfaz ISO y/o de cualquier memoria discreta incorporada. Esta interfaz de conexión directa se usa únicamente para hacer una prueba a la tarjeta e inscribir los datos de huella dactilar, e incluye la señal que permite el proceso de inscripción. Una vez finalizada la inscripción, esta extensión de circuito se interrumpe mecánicamente de forma que no sea posible ninguna inscripción adicional, y la memoria de la CPU de Seguridad es accesible únicamente a través de la CPU ISO y el cortafuegos previamente mencionado entre la CPU ISO y la CPU de Seguridad.

Fusible

En otra realización, la CPU de Seguridad tiene un tipo de memoria que una vez se ha inscrito el patrón de huella dactilar, entonces, se hará inaccesible. Un ejemplo de una memoria como ésta es una PROM de una vez ("OTP"), que es similar en construcción a EEPROM, pero es opaca a los UV y, por lo tanto, no puede ser borrada. Otro ejemplo es Flash ROM que se convierte en de solo lectura una vez que ha finalizado la inscripción, por ejemplo aplicando suficiente corriente a una parte de la trayectoria de la señal Habilitar o Dirección o Datos para formar una rotura física ("fusible") en esta trayectoria de señal.

Procesos ejemplo de autentificación

En una realización, un proceso ejemplar de autentificación incluye los datos de captura física de huella dactilar, por ejemplo, usando tecnologías ópticas o de presión o conductoras o capacitivas o acústicas o elásticas o fotográficas en el Terminal de Cliente usado por la persona que accede para conectarse al Servidor de Servicio de la Aplicación, que, entonces, se envían (preferiblemente en forma encriptada) a un Servidor de Autentificación de huella dactilar. El Servidor de Autentificación de huella dactilar compara los datos capturados de la huella dactilar con un Archivo de huellas dactilares, que incluye los datos de huella dactilar registrados del usuario, usando Aplicación informática de

autentificación, y si el dato concuerda, el Servidor de Autentificación envía una instrucción de habilitación hasta el Servidor de Servicio de la Aplicación.

En otra realización, el Usuario accede al examinador asegurada de red telefónica del Servidor de Autentificación de huella dactilar, que contiene archivos de huellas dactilares, donde están prerregistradas todas las huellas dactilares junto con los datos individuales, tales como nombre,- dirección y fecha de nacimiento. El Servidor asegurado de Autentificación de huella dactilar, cuyo Usuario está accediendo a través de un protocolo seguro tal como el formato HTTPS, envía entonces una instrucción al Terminal de Cliente para capturar la impresión del dedo del Usuario en el Terminal de Cliente. En respuesta a instrucciones visualizadas por el examinador del Terminal de Cliente, el Usuario coloca su dedo seleccionado sobre el Sensor de huella dactilar y la aplicación informática de captura de huella dactilar que reside en el Terminal de Cliente captura una huella dactilar digital, por ejemplo, una imagen basada en píxeles con un paso de resolución de 25 micrómetros hasta 70 micrómetros y un área de 12,5 mm por 25 mm cuadrados, y teniendo, además, una escala de grises de 8 bit.

El Servidor seguro de Autentificación de huella dactilar recibe los datos de la huella dactilar junto con la ID del usuario así como la dirección del IP de INTERNET y/o el código individual del sensor de huella dactilar (dirección MAC) y/o una secuencia de datos que envía el servidor al programa navegador (*cookie*) y/o cualquier otro código exclusivo u otra información que identifique al individuo o al terminal particular (por ejemplo, detalles de una conversación previa entre el Terminal de Cliente y el Servidor seguro de Autentificación de huella dactilar), sobre la cual compara los datos recibidos de la huella dactilar con un Archivo de huellas dactilares, el cual son los datos prerregistrados de la huella dactilar junto con la ID de usuario, información individual tal como nombre, dirección, fecha de nacimiento, certificado de penales, permiso de conducir, número de la seguridad social, etc., usando Aplicación informática de autentificación, que puede ser de comparación minuciosa y/o de comparación rápida con transformada de Fourier.

Al comienzo del proceso de autentificación, el servidor 214 de la red telefónica para la aplicación relevante, da instrucciones visual o audiblemente al Usuario para que coloque su dedo sobre el sensor 110 de captura de huella dactilar, y para que pulse su botón del ratón o tecla del teclado para, de este modo, intimar la aplicación informática de captura de huella dactilar en el procesador 114 de seguridad. Los datos de la huella dactilar capturados del Usuario se envían en formato encriptado (por ejemplo, usando el protocolo RSA de transmisión encriptada HTTPS), hasta el Servidor 220 de red telefónica del Servidor 204 de Autentificación de huella dactilar vía el procesador 112 ISO y el examinador 210 de red telefónica del Terminal 200 de Cliente. Si los datos capturados concuerdan con éxito con los datos correspondientes en su base de datos 226, el Servidor 204 de Autentificación de huella dactilar válida, entonces, la identidad del Usuario tanto al Terminal 200 de Cliente como al servidor 202 de aplicación.

Ahora se describirá una realización ejemplar preferida que utiliza un protocolo de autentificación de tres vías y una contraseña de una vez como una secuencia de codificación de carácter parásito, haciendo referencia a la figura 3:

• El examinador 210 de red telefónica de Terminal 200 de Cliente accede a la correspondiente Interfaz 214 de red telefónica de servidor 202 de aplicación con una solicitud para acceder al proceso 216 de aplicación.

• La interfaz 214 de red telefónica del servidor 202 de aplicación responde con información de pantalla de acceso a sesión e instrucciones relacionadas para acceder al proceso 216 de aplicación.

• Terminal 200 de Cliente da instrucciones al procesador 112 ISO para activar el procesador 114 de seguridad.

• El procesador 112 ISO dispara el procesador 114 de seguridad.

• El procesador 114 de seguridad espera los datos de la huella dactilar procedentes del sensor 110 de huella dactilar y, cuando se reciben los datos válidos, extrae un patrón digital de huella dactilar que se reenvía al examinador 210 de red telefónica vía el procesador 112 ISO.

• El examinador 210 de red telefónica envía una versión encriptada del patrón extraído de huella dactilar al servidor 202 de autentificación acompañado por (o encriptado con) información relacionada sobre la tarjeta 100' implicada y el lector 208 de tarjeta, tal como una ID de Usuario, dirección IP o Terminal 200 de Cliente, y/o código ID con dispositivos (dirección MAC) del sensor 110.

• La interfaz 220 de red telefónica del servidor 202 de autentificación, al recibir el patrón extraído de huella dactilar junto con otra información procedente del Terminal 200 de Cliente, reenvía esta información al Procesador 222 de concordancia de huella dactilar.

• Ante el control de la Aplicación informática 224 de concordancia, el Procesador 222 de concordancia de huella dactilar usa la ID de Usuario recibida u otra información relacionada específica de Usuario para recuperar un patrón de huella dactilar referencia de la base de datos 226, y compara el patrón capturado de huella dactilar con el patrón referencia de huella dactilar.

• El resultado (concordado o sin concordar) se almacena en un registro histórico de acceso con la información relacionada que identifica el terminal 200, la tarjeta 100' de ID de Usuario y la Aplicación 216 de solicitud, y el control se devuelve a la Interfaz 220 de la red telefónica del servidor de autentificación.

• Si el resultado es que concuerda, la Interfaz 220 de la red telefónica del servidor de autentificación genera entonces una contraseña de una vez en forma de secuencia de carácter de tentativa que se transmite el Terminal 200 de Cliente, y usa esta secuencia de carácter de tentativa como un código parásito para encriptar la información relacionada la cual se guarda como la respuesta tentativa correspondiente para una posible futura referencia.

• El Terminal 200 de Cliente usa la secuencia de carácter de tentativa como un código parásito para encriptar una copia sin encriptar previamente almacenada de la información relacionada presentada, la cual se envía entonces hasta la Interfaz 214 de red telefónica del servidor 202 de aplicación como parte de su respuesta al proceso de aplicación de inicio de sesión.

• La Interfaz 214 de red telefónica del servidor 202 de aplicación al recibir la información relacionada convertida en parásita, la reenvía hasta el servidor 216 de aplicación que la asocia con un intento de inicio de sección en proceso desde ese servidor de cliente, y con la finalidad de confirmar el resultado concordado, reenvía la información relacionada recibida que fue parasitada por el Terminal de Cliente usando la secuencia de tentativa facilitada por el servidor de autentificación como respuesta a la tentativa.

• La Interfaz 214 de red telefónica del servidor 204 de autentificación al recibir la respuesta de tentativa del servidor de aplicación, reenvía esta respuesta al proceso 222 de autentificación que la compara con la copia de referencia guardada de la Respuesta de tentativa esperada para determinar si la Identidad de Usuario ha sido de hecho autenticada.

• Cualquier información autentificada de identidad de Usuario resultante de esa comparación se devuelve, a continuación, al proceso 216 de aplicación vía la Interfaz 220 de la red telefónica del servidor de autentificación y la Interfaz 218 de validación del servidor 202 de aplicación.

• La Interfaz 218 de validación usa la autentificación para confirmar que la identidad del Usuario como se estableció en el intento original de inicio de sesión se ha validado.

• Una vez que la identidad de Usuario se ha confirmado, el proceso 216 de aplicación prosigue, a continuación, para comunicar directamente con el examinador 210 de red telefónica del Terminal 200 de Cliente vía Interfaz 214 de red telefónica del servidor 202 de aplicación.

La figura 6 ilustra un proceso alternativo de autentificación en el cual toda la concordancia se realiza sobre la tarjeta compatible ISO de la figura 4 por la CPU 114 de Seguridad y ningún servidor 204 externo de autentificación se utiliza. El lado izquierdo de la figura 6 muestra las funciones realizadas por el servidor 202 de aplicación, mientras que el lado derecho muestra las funciones realizadas sala de bombas la ISO 100 SmartCard.

Cuando se inserta una SmartCard 100 en el lector 208 de tarjeta, se envía una señal RST reinicio desde el lector de tarjeta tanto hasta la CPU ISO (bloque 502 INICIO) como a la CPU 114 de huella dactilar (bloque 504 verificación de huella dactilar), y ambos reciben energía eléctrica VCC desde el lector 208 de tarjeta. La CPU ISO responde, entonces, con mensaje ATR (Respuesta al reinicio) y comunica PPS (Selección de protocolo y parámetros) según las necesidades (bloque 506). Al mismo tiempo, la CPU de huella dactilar pasa al estado de espera para recibir datos de huella dactilar y cuando se reciben datos del sensor 110, realiza el proceso de autentificación (bloque 504).

Cuando se envía una orden de solicitud inicial por la aplicación 216 hasta la CPU 112 ISO (bloque 508), la CPU ISO (bloque 510) pregunta a la CPU de seguridad sobre el estatus de autentificación. Si la respuesta es positiva, la CPU ISO responde a la aplicación ejecutando la orden requerida (bloque 512). En caso contrario (bien un mensaje de error o ninguna respuesta de la CPU 114 de seguridad) no se da ninguna repuesta al comando solicitado, sino que en cambio, espera una nueva solicitud (bloque 508b).

Suponiendo que la huella dactilar se verificó y que la primera respuesta se recibió a tiempo y se determinó era respondida por la Aplicación 216 (bloque 514), el proceso de Solicitud/Respuesta continua (bloques 516, 518, 520) hasta que se haya expirado un tiempo de verificación predeterminado durante el cual no se recibieron Solicitudes procedentes de la Aplicación (bloque 522), o la Aplicación no recibió una respuesta esperada (bloque 524).

La figura 7 es similar al diagrama de flujo de la figura 6, pero modificado para usarse con la tarjeta ejemplar de verificación biométrica de la figura 5. El lado alejado izquierdo de la figura 7 muestra las funciones realizadas por el servidor 202 de aplicación, la siguiente columna corresponde al Lector 208, la siguiente columna representa los contactos 108 ISO, la siguiente columna muestra las funciones realizadas por la CPU 114 de Seguridad, mientras que el lado derecho alejado muestra las funciones realizadas por una CPU 112 de tarjeta inteligente ISO sin modificar.

• Cuando se inserta una SmartCard en un lector de tarjeta o la aplicación informática inicia la operación del dispositivo de lector de tarjeta, desde el lector 208 de tarjeta se envía una señal 550 de reinicio hasta la CPU 114 de Seguridad.

• Poco después de que la CPU de Seguridad reciba la señal 550 de reinicio, envía una correspondiente señal 552 de reinicio a la CPU 112 ISO. Concurrentemente, la CPU de Seguridad espera los datos de huella dactilar desde el sensor de huella dactilar.

• Al recibo de la señal 552 de reinicio, la CPU ISO hace una respuesta 554 ATR (Repuesta a reinicio) y, a continuación, comunica PPS (Selección de protocolo y parámetros), según las necesidades.

• Tan pronto como la CPU 114 de Seguridad recibe ATR (Respuesta a reinicio) de la CPU ISO, la transfiere al Lector de tarjeta (bloque 556), incluyendo cualesquiera órdenes PPS asociadas.

• Mientras tanto, si la CPU de Seguridad recibe datos de la huella dactilar, ejecuta el proceso de autentificación previamente descrito. En el caso de que el test de autentificación dé como resultado un PASA, el estatus pasa se mantiene durante un período específico. Si el resultado es FALLO, la CPU 114 de Seguridad espera nuevos datos de huella dactilar.

• Tras la ejecución de la aplicación, una solicitud 558 de orden se envía a la CPU de Seguridad, que transfiere una solicitud 560 de orden a la CPU ISO y también transfiere su respuesta 562 correcta al lector de tarjeta, únicamente si la CPU de Seguridad aún está en el estatus PASA previamente mencionado, o si la última respuesta correcta tenía más juegos de bit (bloque 564 de test).

• En caso contrario (rama 566 NO) la CPU de huella dactilar genera una solicitud 568 sin sentido y la transfiere a la CPU ISO y también transfiere la respuesta ERR resultante al lector 216 de tarjeta, manteniendo de este modo, la correcta sincronización entre los números de secuencia en las solicitudes y respuestas.

Encriptado y seguridad

Antes de la transmisión a través de cualquier red externa, cualquier dato sensible y/o el resultado de la autentificación está preferiblemente encriptado, posiblemente usando encriptado DES o Two Fish. La clave de encriptado se puede basar en datos de la huella dactilar capturados o encriptados, código ID de usuario, código de sensor asignado exclusivamente, dirección de memoria, datos contiguos en la memoria, otros datos relacionado con funcionalidad, una conversación previa (transacción), dirección IP, código de terminal o una contraseña asignada. Alternativamente, el dato sensible se puede enviar a través de INTERNET usando el protocolo seguro HTTPS.

Para proporcionar aún más seguridad, una puerta privada Virtual, tal como encriptado y desencriptado DES de dispositivo, se puede insertar entre el Servidor de Autentificación de huella dactilar y la conexión de red, y, correspondientemente, entre el Servidor de Servicio de la Aplicación y la conexión de red. Al actuar así, una puerta Virtual o Red Privada virtual ("VPN"), el dato sensible se protege adicionalmente por una capa adicional de encriptado, por ejemplo, ambos DES 128 (usados típicamente en el VPN) y RSA (usados por HTTPS).

Para aplicaciones especialmente seguras, todas las comunicaciones se pueden envolver con capas adicionales de seguridad. En particular, los encabezados de mensaje en una capa inferior se pueden encriptar en una capa superior.

Comunicación inalámbrica

Otras realizaciones pueden incluir una interfaz dual tanto para la operación con contacto (ISO 7816) como inalámbrica (ISO 1443 A o B), y preferiblemente incorpora una unidad de energía multifrecuencia que permite la interoperabilidad entre el contacto ISO 7816, ISO 1443 A, ISO 1443 B, ISO 15693 y sistemas inalámbricos HID heredados (entre otros) todos en una tarjeta. Alternativamente, la tarjeta puede incluir disposición para otras tecnologías de comunicación inalámbrica, tales como Bluetooth (onda corta) o Cellular (onda media) o microondas (onda grande).

Se debe hacer ahora referencia a la figura 8 que muestra una tarjeta inteligente con verificación biométrica incorporada que se puede conectar a una terminal local bien sin hilos o por medio de un conector eléctrico. En su mayor parte es similar en construcción y arquitectura a la realización previamente descrita de la figura 1, y números similares (posiblemente distinguidos por una sola comilla) indican elementos similares. En particular, CPU 112 ISO se muestra en una ubicación diferente (más bien hacia un lado de los contactos 108), pero tiene funcionalidad similar a la descrita previamente.

La antena 132 ISO comprende dos bucle generalmente ubicados alrededor de la periferia de la tarjeta 100 y proporciona una interfaz inalámbrica compatible con ISO para la CPU 112 ISO, tanto para datos como para energía eléctrica similar a la permitida por la interfaz 108 eléctrica con cables. Además, una antena 134 de Seguridad (en el ejemplo representado, la antena 132 interna y consta de únicamente un bucle) proporciona una fuente de alimentación separada para la CPU 114 de Seguridad vía el regulador 120 de energía C.C.- C.C. Puesto que no hay conexión directa para datos inalámbricos salvo a través de la CPU 112 ISO, el dato sensible almacenado en la CPU 114 de Seguridad no está comprometido por dicha interfaz inalámbrica. Alternativamente, como se mencionó previamente en relación con la realización que tiene únicamente conexiones cableadas con el lector externo y con la red externa, la funcionalidad de los dos procesadores se podría combinar, o la interfaz externa podría ser a través de la CPU 114 de Seguridad en lugar de a través de la CPU 112 ISO, en la cual las medidas de seguridad inalámbricas adecuadas se podrían haber incorporado en la arquitectura así modificada.

La figura 9 es una sección transversal a través de la tarjeta de la figura 8. Observe que la mayor parte de los componentes descritos están contenidos dentro de un núcleo central, 126, con únicamente puntos 108 de contacto que se extienden a través de una capa 122 superior protectora. El área operativa del sensor 110 es accesible a través de

una ventaja superior en la capa 122 superior y de una ventana inferior en PCB 134, que está situada entre la capa 122 superior y el núcleo 126 central y que proporciona las conexiones eléctricas necesarias entre los diversos componentes electrónicos, así como un contacto con tierra de descarga electrostática que rodea la región activa del sensor 110.

También visible hay una capa 124 inferior y una banda 128 magnética.

Sensor de huella dactilar

La figura 109 es un diagrama ejemplar de circuito esquemático para sensor 110, en el cual una formación 400 ordenada de células 402 de sensor están dispuestas en filas 404 y en columnas 406. Como se representa, cada célula 402 incluye una puerta 410 de activación y un transductor 412. Una huella dactilar está formada por los valles y cordilleras de la piel sobre un dedo. Cada transductor 412 de célula de sensor experimenta un cambio mecánico 77 eléctrico cuando una de estas cordilleras toca la vecindad inmediata de la célula 402 dentro de la formación 400, que en efecto proporciona una imagen de huella dactilar basada en variaciones de micro presión por toda la superficie del sensor ocasionada por las cordilleras y valles sobre la punta del dedo. Observe que aunque cada transductor 412 se ha descrito como un condensador variable sencillo, hay diversos tipos de transductores que pueden responder a la presencia de estas cordilleras en la piel humana: en el ejemplo particular de un transductor de película a delgada piezo sensible a la presión, la película se deforma en la vecindad de la célula y genera una carga que se almacena en un condensador almacenado en esta célula. La tensión sobre el condensador es, por ello, una función de la tensión mecánica formada por la deformación del material piezo, que a su vez es una función de si una montaña o un valle está por encima de la célula. Cuando una señal procedente del controlador 414 de columna asociado conmuta esta puerta 410 de célula ON y el controlador 416 asociado de fila está a tierra, esta tensión aparece sobre la línea 418 de salida de la fila, y se convierte en una señal digital de 8 bit en el controlador 420 de salida. Para maximizar la detección de deformación del material piezo, el material piezo eléctrico se puede formar sobre material elástico, tal como poliamida, o puede ser simplemente un material piezo eléctrico poliimida. Otras tecnologías ejemplares de transductor analógico que se pueden implantar con una organización en formación ordenadas similares incluye resistencia variable y capacitancia variable. Alternativamente, cada célula podría constar de un sencillo conmutador digital que proporcionar únicamente un bit de información; en este caso, los bits adicionales de información se pueden generar proporcionando más células en el mismo área o muestreando cada célula a una frecuencia mayor. Una realización alternativa como ésta evita la necesidad de cualquier convertidor A/D.

En una realización ejemplar, el sensor es únicamente de 3,3 mm grueso y es lo suficientemente duradero como para ser incrustado en una SmartCard y no se ve afectado por la electricidad estática, los elementos o condición (húmedo, seco, caliente, frío) de la piel de usuario. Un tamaño típico de célula unidad de sensor 110 es de 25 micrómetros a 70 micrómetros, y un paso típico de 25 micrómetros hasta 70 micrómetros. El sensor ejemplar tiene un área de detección de 12,5 mm por 25 mm cuadrados, y un multinivel de sensibilidad de 8 bit. Dicho sensor pueda ser fabricado con una formación ordenada de TFT (*Thin Film Transistor*) y condensador sensible a la presión, tal como el formado por material piezo eléctrico de película delgada, tal como Óxido de Bario titanio u Óxido de Bario estroncio, e incluye un electrodo superior que cubre y protege toda la zona de detección. Si se aplica tensión mecánica, se generan una carga correspondiente y se almacena en el Condensador piezo de película delgada. Alternativamente, un sensor basado en presión se puede fabricar como una formación ordenada de TFT (*Thin Film Transistor*) junto con condensador de película delgada, y condensador sensible a la presión, tal como el formado por hojas de material conductor de presión, tal como hojas de caucho dispersado de fibra de carbono, metal (tal como Cobre o latón o plata), papel basado en fibra de carbono o fibra de vidrio chapada, o metal material elástico disperso (tal como silicona) y una hoja de electrodo superior, que cubre toda la zona de detección.

Los controladores de fila 416, 414 cuyo elemento 402 de detección de huella dactilar específico particular es dar salida a los datos eléctricos hasta la circuitería 420 de salida, convirtiendo de este modo la entrada física representativa de la huella dactilar del usuario en datos analógicos eléctricos. El convertidor A/D en la circuitería 420 de salida convierte, a continuación, la señal analógica eléctrica en señal eléctrica digital. Cada transistor de película delgada conmuta selectivamente una interconexión de fila compartida a la tensión sobre su condensador asociado, así la tensión sobre cada condensador se puede leer y de este modo, cada deformación de célula se puede medir Toda una columna de transistores de película delgada se conmuta preferiblemente, y por ello un cierto número de células (por ejemplo 8) en una columna seleccionada se puede leer en paralelo sobre diferentes interconexiones de fila. La interconexión de múltiples puertas y filas y columnas reduce el número de interconexiones, mientras la lectura en paralelo de múltiples células de diferentes filas de la misma columna reduce el tiempo de lectura de toda la formación ordenada. La tensión de salida del sensor se puede amplificar por una amplificación diferencial. La salida de dicho amplificador puede ser muestreada y recogida por la Conversión de Analógica a digital (convertidor A/D).

El sustrato puede ser Vidrio (tal como vidrio no alcalino), acero inoxidable, aluminio, cerámica (tal como óxido de aluminio), papel, resina epoxi vítrea, pero se prefiere una delgada hoja de Silicio cristalino. El material semiconductor de película delgada puede ser Silicio amorfo, polisilicona, diamante, o cualquier otra película delgada de semiconductor. El material piezo eléctrico puede ser una cerámica piezoeléctrica, tal como películas delgadas de zirconato-titanato (PZT), que preferiblemente vas de un grosor de 0,1 a 50,0 micrómetros, o un material de película delgada de poliimida piezoeléctrico polímero. El material de interconexión puede ser: Ti/Ni/Cu, Al, Cr/Ni/Au, Al/Au, W/Cu, W/Au, W/Au.

La figura 11 muestra un conjunto de portador para un sensor formado sobre un sustrato delgado de silicio cristalino. El silicio cristalino tiene excelentes propiedades eléctricas, y facilita la integración de la formación ordenada de sensor con el controlador requerido y los circuitos de salida, sin embargo una hoja relativamente grande y delgada de silicio flexará y se fracturará al ser sometida a una presión localizada en la superficie. El portador ilustrado proporciona una estructura mucho más rígida de la que se proporcionaría con una hoja de silicio del mismo grosor en conjunto.

Como se muestra, la hoja monolítica de silicio 430 es de aproximadamente 0.1 mm de grosor, y está rodeada por un bastidor 432 igualmente grueso de resina epoxi vítrea, que está montado sobre una placa 434 de respaldo también de construcción vítrea de resina epoxi y de aproximadamente 0,05 mm de grosor. El bastidor 432 y la placa 434 de respaldo se pueden construir fácilmente usando tecnología convencional de panel de circuito impreso (PCB). En particular, las superficies superior e inferior de la placa 434 de respaldo están cubiertas por una delgada capa 436 de cobre por un núcleo de vidrio de resina epoxi. El bastidor 432 incluye un cierto número de puntos 440 de contacto soldados alrededor de su periferia externa, para conectarse al procesador 114 de seguridad. La delgada lasca 430 de silicio está unido por resina de epoxi al bastidor 432 y placa 434, y las regiones activas están eléctricamente acopladas a las correspondientes trazas eléctricas en el bastidor 432 por uniones 442 convencionales con hilo en las partes 444 de los bordes externos expuestos del silicio 430 que rodea el electrodo 446 superior protector.

Algoritmos de concordancia

Para un procesado local incorporado d onde la potencia de procesado está limitada y únicamente se consigue una sencilla concordancia 1:1 con una única muestra referencia, la aplicación informática de concordancia de la huella dactilar se puede basar en una comparación relativamente directa de pequeños detalles obtenidos de los dos patrones. Por ejemplo, la imagen en escala de grises de una huella dactilar se puede reducir a dos valores, blanco y negro, y las cordilleras en 3 dimensiones se convierten en delgadas líneas bidimensionales (vectores). La precisión del procedimiento está, por lo tanto, sujeta a, entre otros problemas, emborronado, conglutinado, distorsión, ausencia parcial de segmentos de línea y otros efectos. Aunque el procedimiento de pequeños detalles es en principio menos preciso, requiere menos recursos de cálculo y ofrece la posibilidad de compatibilidad con muchas bases de datos existentes.

Para un procesado en un servidor de autentificación remoto donde se dispone de mayor potencia de procesado y se requiere mayor precisión en la discriminación, por ejemplo, un algoritmo de concordancia "POC" (*Phase Only Correlation*). POC es un algoritmo de identificación basado en la concordancia macroscópica del conjunto de la imagen. POC, a la inversa, concuerda información estructural en un amplio intervalo -desde detalles hasta la imagen total. Por ello, POC es capaz de proporcionar una precisión robusta contra ruidos tales como conglutinación e hiato parcial. En principio, el procedimiento POC está no tiene los efectos adversos de cambio de posición y diferencias en brillo, es rápido (aproximadamente 0,1 segundos para concordar una línea desviada) y es muy preciso. Por ejemplo, la aplicación informática POC puede realizar una comparación de frecuencias espacios de los dos patrones de huella dactilar utilizando una primera transformada de Fourier en dos dimensiones ("2DFFT"). 2DFFT convierte una formación ordenada de datos digitalizados que representa una distribución de huella dactilar en dos dimensiones, en el espacio de frecuencias, con otras palabras, la distribución inversa del espacio, donde el patrón de mayor densidad tiene la mayor frecuencia espacial. Una transformación rotacional se puede usar para hacer que casen la concordancia de patrón de espacio de frecuencias. La concordancia del patrón POC tiene la ventaja adicional de que la concordancia del vector pequeños detalles, pues no se pierde con defectos comunes en el patrón de huella dactilar grabado pues POC reconocería como ruido pero un análisis minucionso los interpretaría como datos con significado.

Para aplicaciones particularmente exigentes, un enfoque híbrido puede ofrecer una mayor precisión y seguridad que el método en solitario. Por ejemplo, se puede usar una metodología de pequeños detalles en el punto de captura, mientras que se puede usar una metodología POC en un servidor remoto. Como otro ejemplo, el proceso de concordancia puede analizar tanto las relaciones de pequeños detalles como las espaciales para producir una puntuación combinada que tiene en cuenta los resultados de ambos.

Aplicaciones

La tecnología descrita en lo que antecede proporciona un alto nivel de seguridad para múltiples aplicaciones, tanto comerciales como gubernativas. En función de los requisitos de cada aplicación, pueden coexistir múltiples aplicaciones de seguridad y operar sobre la misma tarjeta y/o el mismo servidor de autentificación. En una realización, una única tarjeta puede contener hasta 24 aplicaciones independientes y seguras. Por ejemplo, la tecnología permitirá acceder/denegar (física y/o lógica), identificar la ubicación precisa y/o movimiento de personal y/o partes de una lista mientras al mismo tiempo opera sobre aplicaciones seguras y completamente aislados con seguridad una de otra.

Entre las aplicaciones habitualmente contempladas están las siguientes:

- Acceso/ID a aeropuertos
- Seguridad de edificios
- Acceso a habitación de hotel y pago de facturas

- Hospitales
- Apuestas en línea
- Descarga de juegos
- Certificado de nacimiento
- Acceso informático
- Permiso de conducir-TWIC
- Monedero electrónico
- Información médica de emergencia
- Licencia de explosivos
- Acceso a instalaciones del gobierno & militares
- Licencia HAZMAT
- Tarjeta médica & prestación de servicios
- Acceso a parking
- Pasaporte
- Licencia de vuelo
- Acceso/ID a puertos
- Justificante de estar asegurado
- Tarjeta de la seguridad social
- Tarjeta de viajero fidedigno
- Visado o pase de entrada/salida
- Tarjeta de registro de votación
- Tarjeta de cartilla & sello de alimentación.

Para muchas de estas aplicaciones, la memoria incorporada de la tarjeta también proporciona preferiblemente almacenamiento seguro de diferentes tipos de información privada personal, que únicamente es accesible cuando el poseedor de la tarjeta registrado ha demostrado su identidad y autorizado dicho acceso. Ejemplos de dicha información privada son:

• Información administrativa tal como nombre, dirección, fecha de nacimiento, lugar de nacimiento, nacionalidad, religión, socios organizativos, número de seguridad social, número de permiso de conducir, número de pasaporte, e información de inmigración tal como tipo de visado, caducidad del visado, ciudadanía, etc.

• Información financiera, tal como monedero electrónico, Visa, MasterCArd, American Express, etc. información de la tarjeta de crédito, información del banco tal como nombre del banco, saldo, información de transferencia bancaria, número IRS, registro de bancarrota, información de transferencia de dinero, etc.

• Información psicológica o de salud tal como: información biométrica para identificar individuos tale como altura, peso, huella dactilar, iris, retina tamaño de la mano, estructura ósea, voz, DNA; tipo de sangre, resultados de pruebas médicas, historial médico; medicaciones; información del seguro; respuestas psicológicas y fisiológicas a ciertos estímulos, etc.

• Información ocasionar tal como antecedentes penales, felonía, delincuencia, infracciones.

• Información de emergencia tal como cementerio, parientes y otra información de contacto, información del abogado, información religiosa.

• Estudios, historial de trabajo, incluyendo colegio en el que estuvo, licenciatura, empresa para la que trabajo relacionada con FDD.

• Historial de acceso de datos (almacena los datos de historial de acceso para entrar y salir de la tarjeta).

• Información relacionada con ID tal como patrón de huella dactilar, patrón de huella dactilar procesado, resultado de patrón de huella dactilar.

• Contraseña tal como contraseña permanente, una contraseña temporal, y/o una palabra de paso de un solo uso.

• Calves de encriptado tal como una clave pública, una clave personal, y/o una clave de una vez.

Ahora se describirá un sistema de inscripción ejemplar de tarjeta.

El solicitante: rellena una solicitud y la presenta, incluyendo preferiblemente una fotografía y huella dactilar. Para la mayoría de los solicitantes, una inspección de sus documentos de identificación y un simple cotejo de la información presentada con una de las bases de datos del gobierno o comercialmente disponibles será suficiente para establece la verdadera identidad del individuo.

Una vez que esta identidad has sido verificada, el solicitante prosigue hasta un centro de emisión donde cualquier información considerada necesaria por el emisor d e la tarjeta se carga sobre la tarjeta. El solicitante coloca su huella dactilar sobre el sensor de la tarjeta. Una vez que la huella dactilar está colocada satisfactoriamente sobre el sensor y cargada sobre la tarjeta, la pestaña sobre la tarjeta se le da una descarga de electricidad que quema algunos fusibles e impide que nadie escriba en ciertas zonas de la tarjeta nunca más. A continuación, la pequeña pestaña se corta/guillotina (como un cordón umbilical). En este punto, la tarjeta sólo puede ser escrita o leída a través del lector de contacto ISO o sistema inalámbrico ISO.

En el caso de un servidor de autentificación en red, alguno o todos de los mismos datos que se cargan en la tarjeta también se transmiten en forma encriptada al servidor remoto, posiblemente suplementados con datos adicionales que no se almacenan normalmente en una tarjeta pero que pueden ser necesarios para aplicaciones de alta seguridad.

REIVINDICACIONES

1. Una tarjeta inteligente de identificación **caracterizada** porque comprende:

una memoria incorporada para almacenar datos de referencia,

un sensor incorporado para capturar datos biométricos en vivo,

un microprocesador incorporado para comparar los datos biométricos capturados con los correspondientes datos referencia almacenados dentro de un umbral predeterminado y para generar un mensaje de verificación, únicamente si hay una concordancia con un umbral predeterminado, y

medios para comunicar el mensaje de verificación a una red externa.

2. La tarjeta de identificación de la reivindicación 1, **caracterizada** porque el mensaje de verificación incluye al menos extractos de los datos referencia almacenados.

3. La tarjeta de identificación de la reivindicación 2, **caracterizada** porque el mensaje de verificación incluye al menos extractos de los datos biométricos capturados.

4. La tarjeta de identificación de la reivindicación 3, **caracterizada** porque el mensaje de verificación se transmite a un sistema de autentificación remoto para su verificación adicional.

5. La tarjeta de identificación de la reivindicación 4, **caracterizada** porque el sistema de autentificación remoto incluye datos referencia almacenados remotamente que son diferentes de los datos referencia almacenados localmente.

6. La tarjeta de identificación de la reivindicación 4, en la cual el microprocesador incorporado usa un algoritmo de concordancia diferente que el usado en el sistema remoto de autentificación.

7. La tarjeta de identificación de la reivindicación 2, **caracterizada** porque todo el proceso de concordancia es realizado por el procesador incorporado y ninguno de los datos biométricos capturados se transmite a la red.

8. La tarjeta de identificación de la reivindicación 2, **caracterizada** porque tanto los datos biométricos capturados originalmente como cualquier otra información "privada" almacenada en la memoria incorporada no están disponibles para procesos externos.

9. La tarjeta de identificación de la reivindicación 2, **caracterizada** porque la tarjeta es compatible con una tarjeta inteligente (o chip) ISO (ISO SmartCard).

10. La tarjeta de identificación de la reivindicación 9, que comprende, además, un procesador de tarjeta inteligente ISO.

11. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque el procesador de seguridad usado para almacenar y procesar los datos biométricos está funcionalmente separado de la tarjeta inteligente ISO por un cortafuegos.

12. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque todos los datos externos hacia y desde el procesador de seguridad pasan a través del procesador de la tarjeta inteligente ISO.

13. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque todos los datos externos hacia y desde el procesador de la tarjeta inteligente ISO pasan a través del procesador de seguridad.

14. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque el procesador de seguridad tiene una primera conexión usada para cargar datos durante un proceso de carga y una segunda conexión conectada a una red externa.

15. La tarjeta de identificación de la reivindicación 14 **caracterizada** porque la primera conexión está permanentemente deshabilitada una vez que el proceso de carga ha sido deshabilitado.

16. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque el procesador de seguridad usado para almacenar y procesar los datos biométricos protegidos está funcionalmente separado de la tarjeta inteligente ISO por un cortafuegos.

17. La tarjeta de identificación de la reivindicación 10, **caracterizada** porque:

la tarjeta comprende una región de banda magnética superior y una región estampada en relieve inferior;

el sensor biométrico es un sensor de huella dactilar; y

el procesador de seguridad, el procesador de la tarjeta inteligente ISO y el sensor de huella dactilar están ubicados en una región media entre la región superior y la región inferior.

18. La tarjeta de identificación de la reivindicación 2, **caracterizada** porque los datos biométricos incluyen datos de la huella dactilar y el sensor es un sensor de huella dactilar que captura datos a partir de un dedo de usuario colocado sobre el sensor.

19. La tarjeta de identificación de la reivindicación 18, **caracterizada** porque se proporciona retroalimentación en tiempo real mientras el usuario está manipulando su dedo sobre el sensor de huella dactilar, por lo que se facilita una colocación óptima del dedo sobre el sensor.

20. La tarjeta de identificación de la reivindicación 18, **caracterizada** porque el proceso de concordancia utiliza un algoritmo de concordancia híbrido que tiene en cuenta relaciones espaciales tanto de detalle como de conjunto en los datos biométricos capturados.

21. La tarjeta de identificación de la reivindicación 18, **caracterizada** porque el sensor de huella dactilar comprende una hoja de silicio cristalino soportado por una placa de respaldo.

22. La tarjeta de identificación de la reivindicación 21, **caracterizada** porque la placa de respaldo comprende una capa vítrea de resina epoxi dispuesta a modo de sándwich entre dos capas de metal.

23. La tarjeta de identificación de la reivindicación 18, **caracterizada** porque la placa de respaldo está reforzada por un bastidor de soporte que rodea la hoja de silicio.

24. La tarjeta de identificación de la reivindicación 1, **caracterizada** porque la tarjeta comprende, además, medios para restringir el uso de la tarjeta a una ubicación predeterminada, al menos alguna de las capturadas.

25. La tarjeta de identificación de la reivindicación 1, **caracterizada** porque al menos algunos de los datos biométricos capturados y de los datos referencia se transmiten hasta un servidor de autentificación separado para la verificación segura de una identidad de usuario antes de conceder cualquier acceso vía teléfono a un servidor de aplicación para procesar las transacciones financieras seguras relacionadas con este usuario.

26. La tarjeta de identificación de la reivindicación 25, **caracterizada** porque como repuesta a una solicitud de concordancia para un intento de iniciar una sesión particular en un servidor de aplicación particular que produce una concordancia positiva en el servidor de autentificación, se ejecuta un protocolo de autentificación de tres vías en el cual se envía una secuencia de carácter de tentativa desde el servidor de autentificación hasta la tarjeta de identificación pues, la tarjeta de identificación usa, entonces, la secuencia de carácter de tentativa y la solicitud de concordancia para generar una respuesta de tentativa que se envía, entonces, hasta el servidor de aplicación, el servidor de aplicación envía entonces la respuesta de tentativa al servidor de autentificación, el cual verifica, a continuación que la respuesta de tentativa es válida.

27. La tarjeta de identificación de la reivindicación 1, **caracterizada** porque se usa la salida desde la tarjeta para obtener acceso físico a una zona segura.

28. La tarjeta de identificación de la reivindicación 27, **caracterizada** porque se mantiene un registro de intentos de acceso con éxito y sin éxito en la tarjeta.

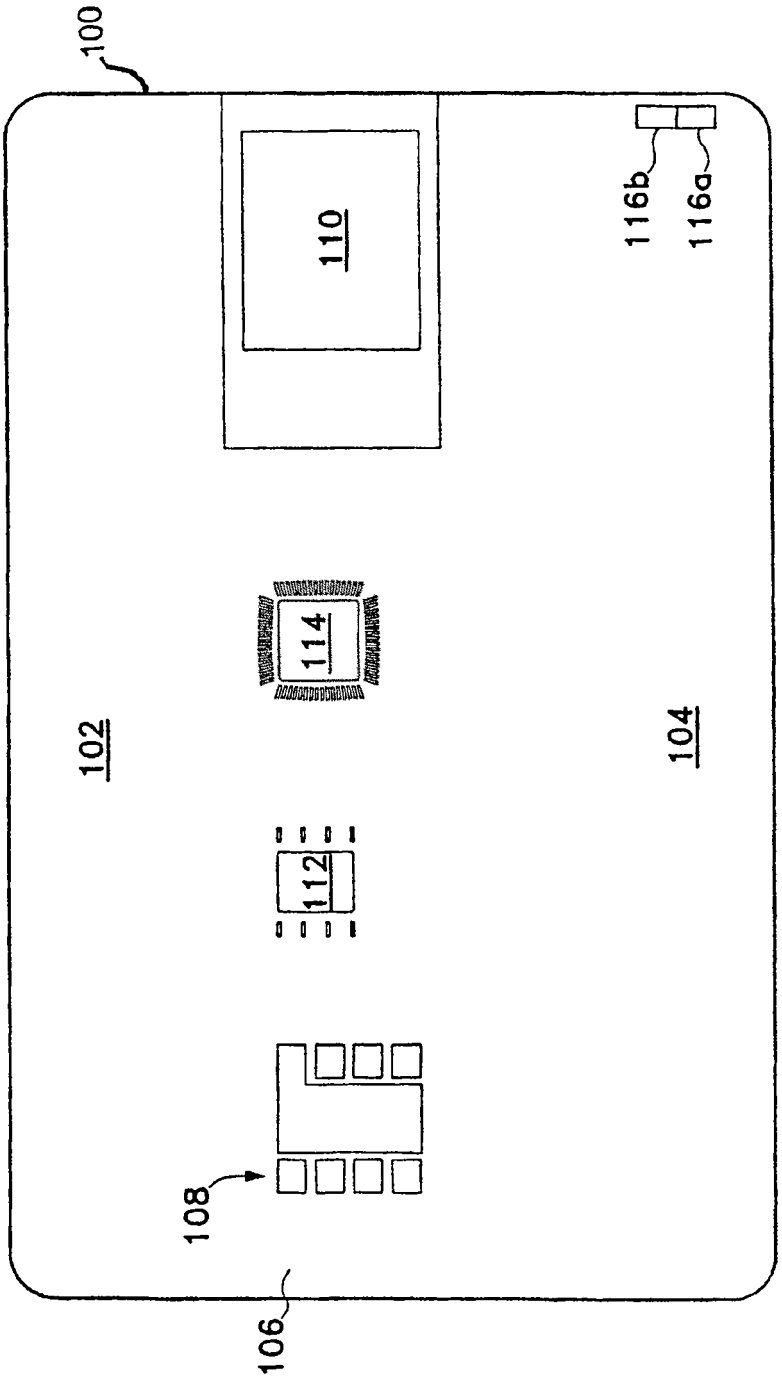


Fig. 1

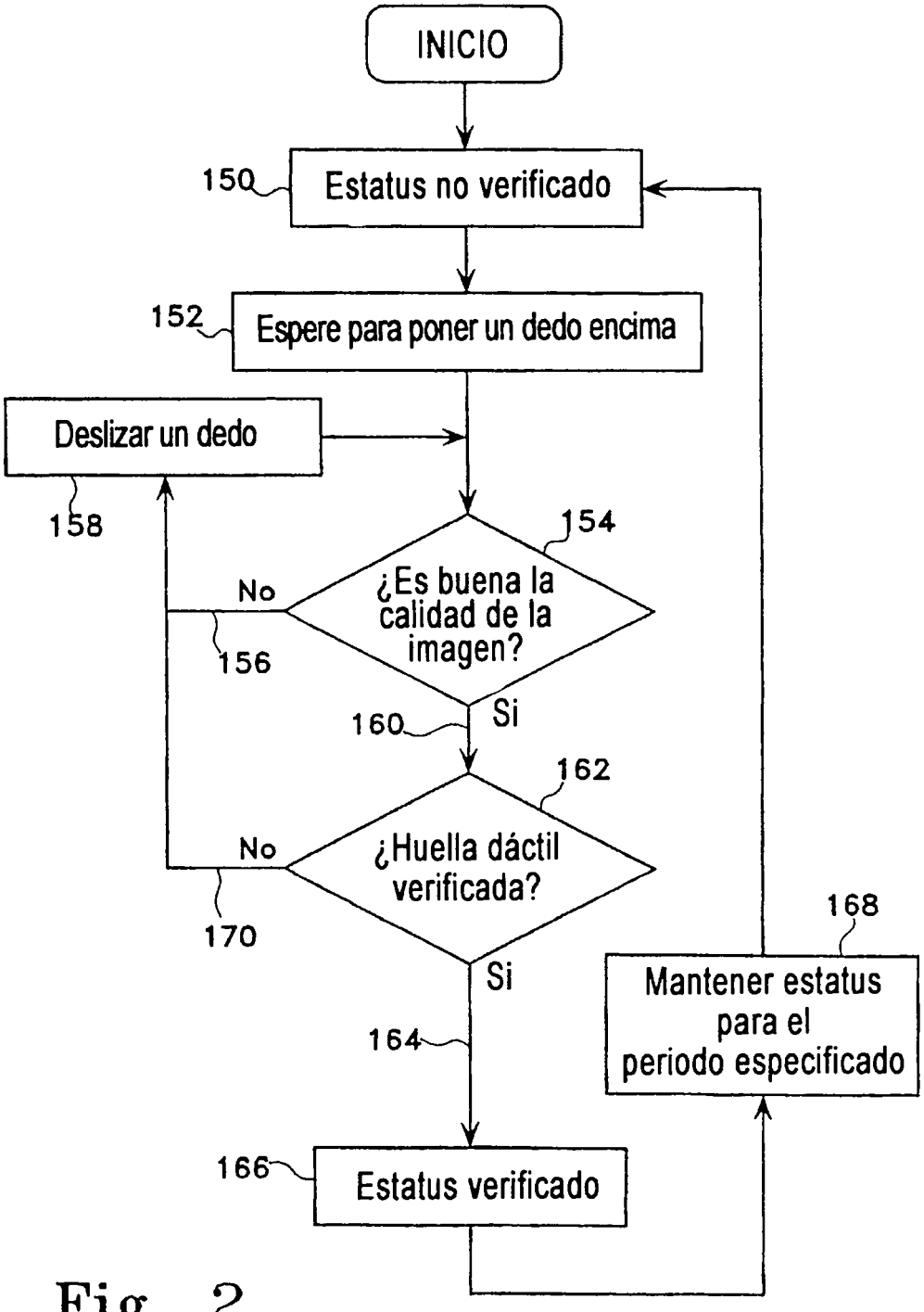

INICIO
150
Estatus no verificado
152
Espere para poner un dedo encima
Deslizar un dedo
158
154
¿Es buena la calidad de la imagen?
No
156
Si
160
162
¿Huella dáctil verificada?
No
170
Si
168
Mantener estatus para el periodo especificado
164
166
Estatus verificado

Fig. 2

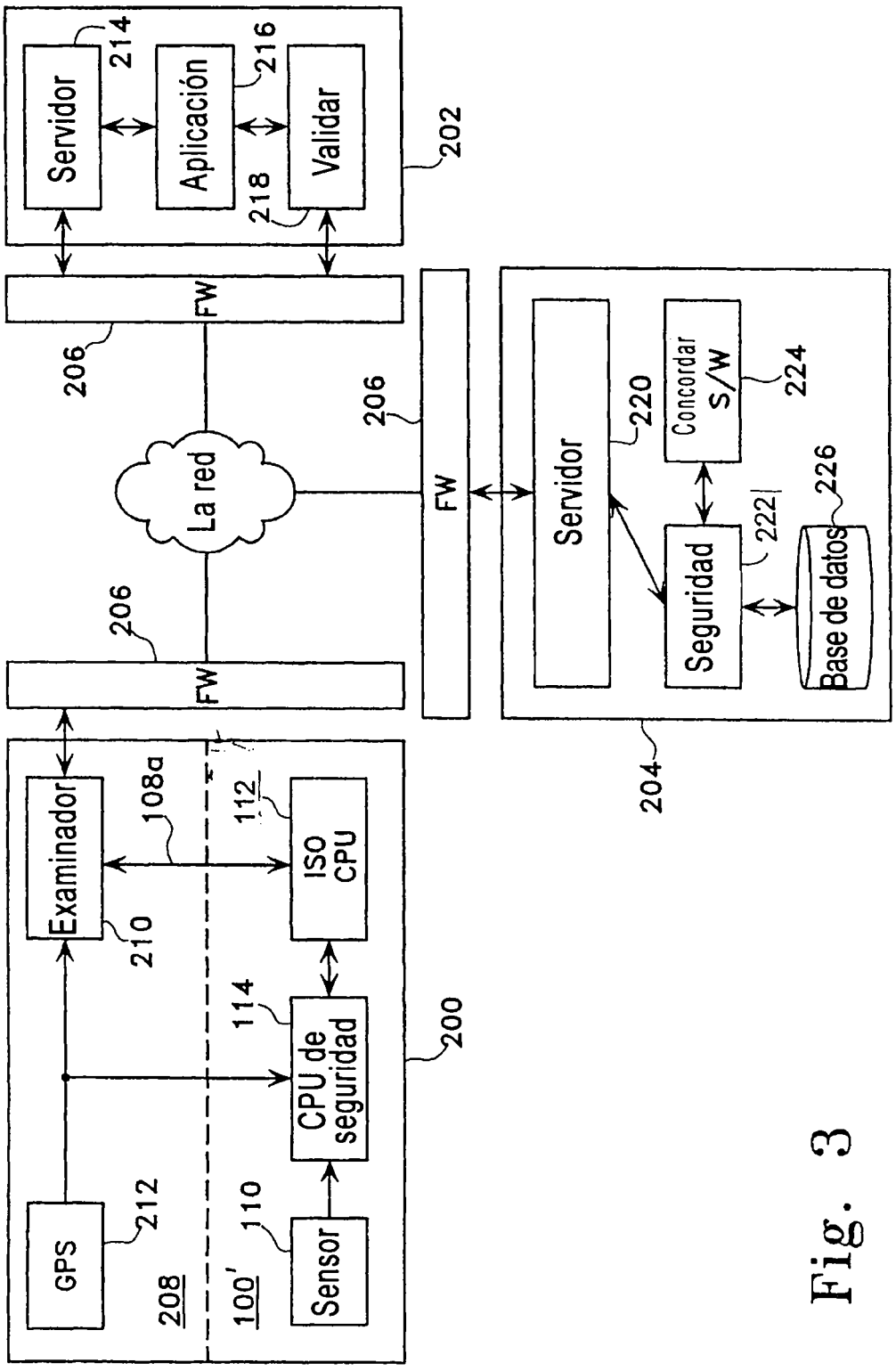

Servidor
214
Aplicación
216
Validar
218
202
FW
206
La red
FW
206
FW
206
Servidor
220
Concordar S/W
224
Seguridad
222
Base de datos
226
204
Examinador
108a
112
ISO CPU
210
114
CPU de seguridad
200
GPS
212
208
100'
110
Sensor

Fig. 3

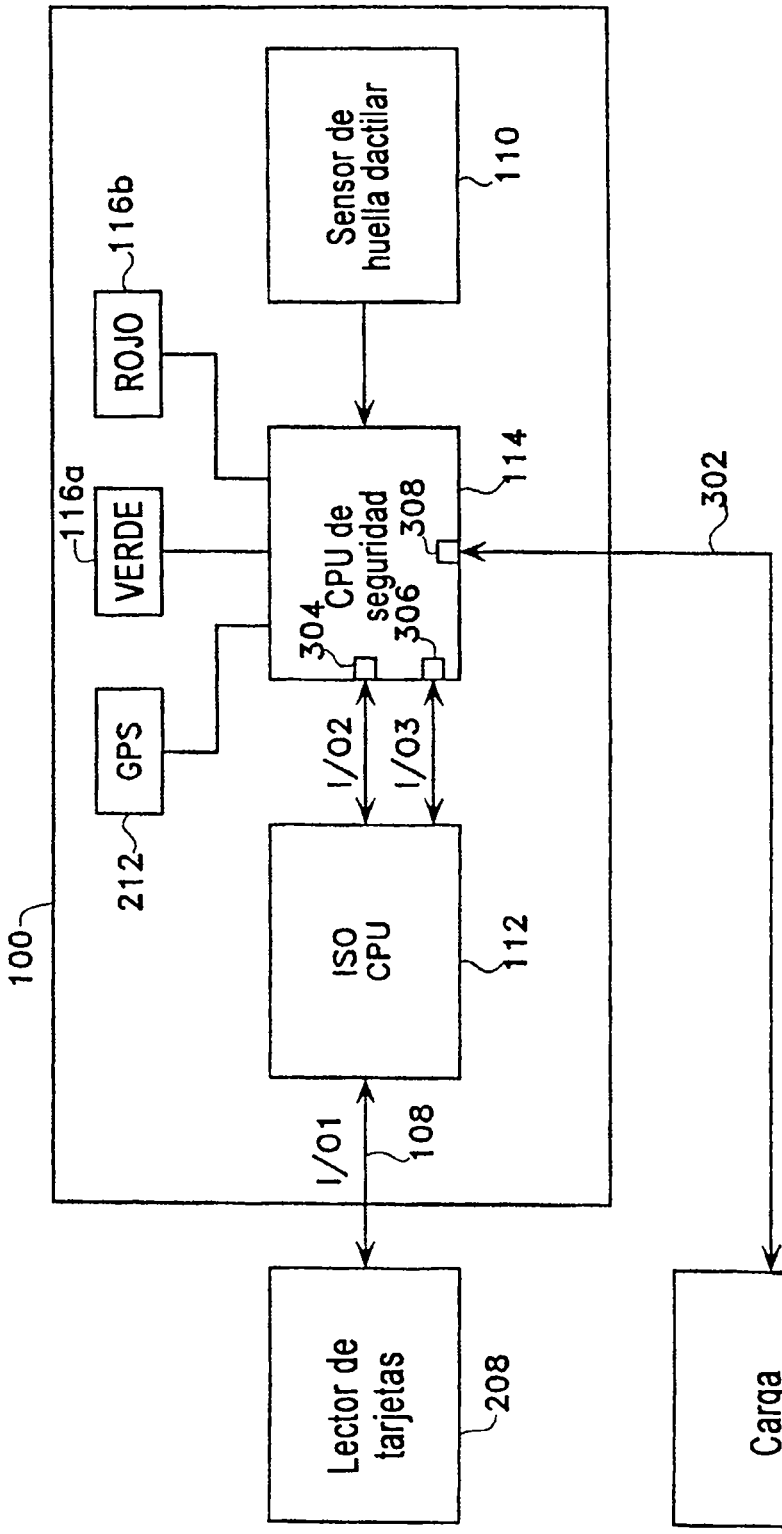

Sensor de huella dactilar
110
116b
ROJO
116a
VERDE
GPS
212
CPU de seguridad
114
308
304
306
302
I/O2
I/O3
ISO CPU
112
100
I/O1
108
Lector de tarjetas
208
Carga
300

Fig. 4

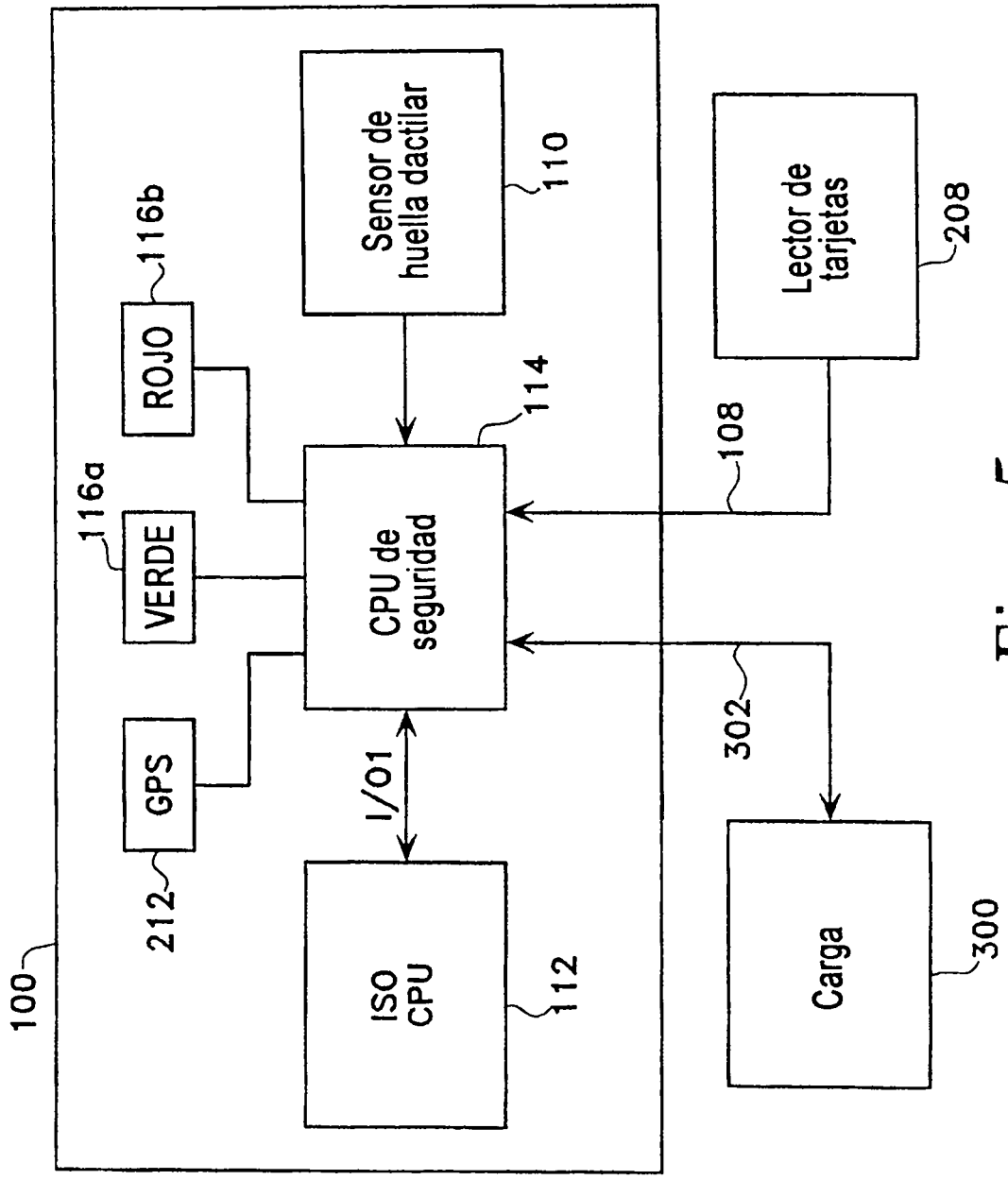

100
Sensor de huella dactilar
110
Lector de tarjetas
208
116b
ROJO
116a
VERDE
GPS
212
CPU de seguridad
114
108
I/O1
ISO CPU
112
302
Carga
300

Fig. 5

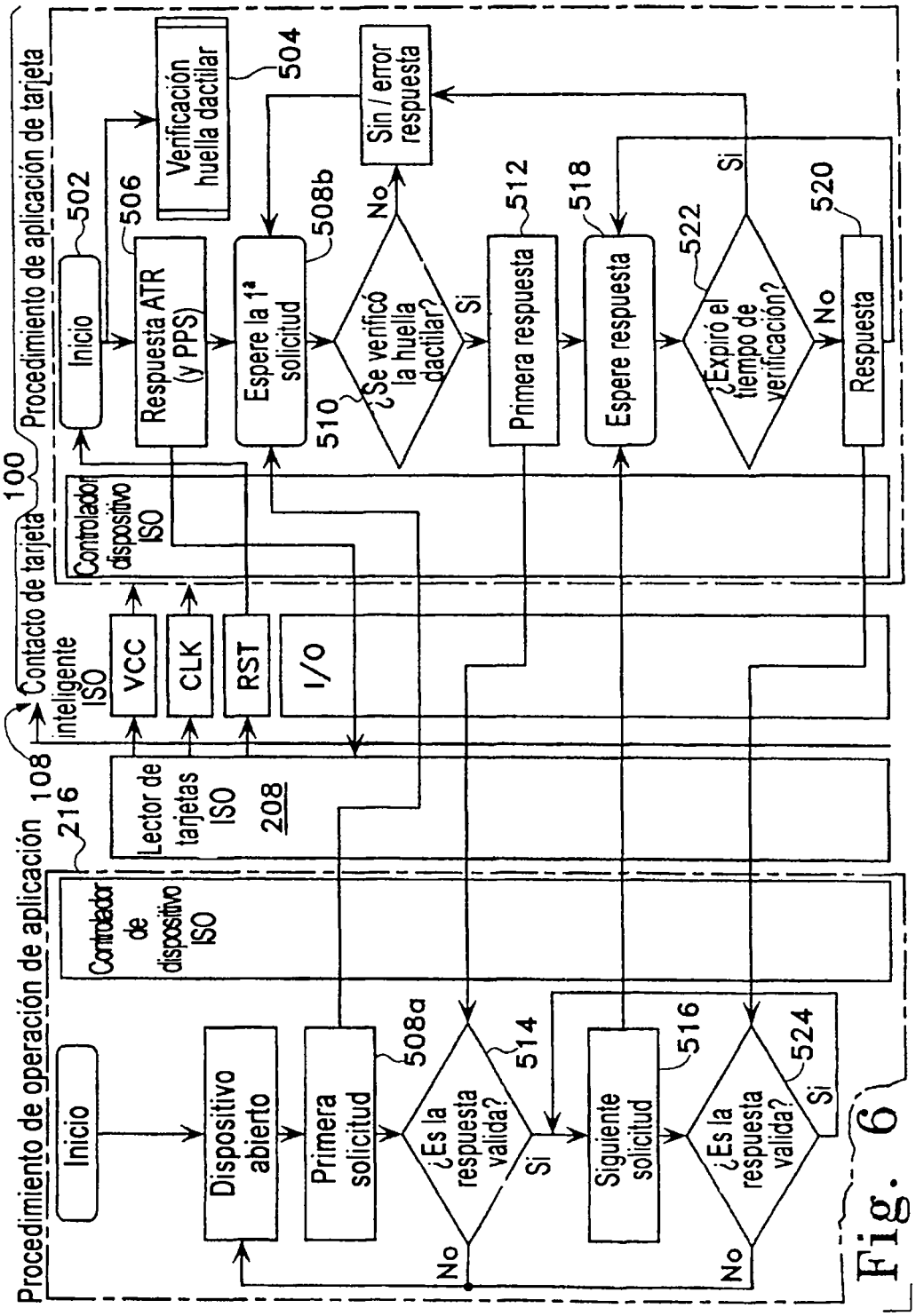

Procedimiento de operación de aplicación
Procedimiento de aplicación de tarjeta
Contacto de tarjeta inteligente ISO
Lector de tarjetas ISO
Controlador de dispositivo ISO
Controlador dispositivo ISO
Inicio
Dispositivo abierto
Primera solicitud
¿Es la respuesta valida?
Siguiente solicitud
¿Es la respuesta valida?
Inicio
Respuesta ATR (y PPS)
Espere la 1ª solicitud
¿Se verificó la huella dactilar?
Primera respuesta
Espere respuesta
¿Expiró el tiempo de verificación?
Respuesta
Verificación huella dactilar
Sin / error respuesta
VCC
CLK
RST
I/O
Si
No
100
108
208
216
502
504
506
508a
508b
510
512
514
516
518
520
522
524

Fig. 6

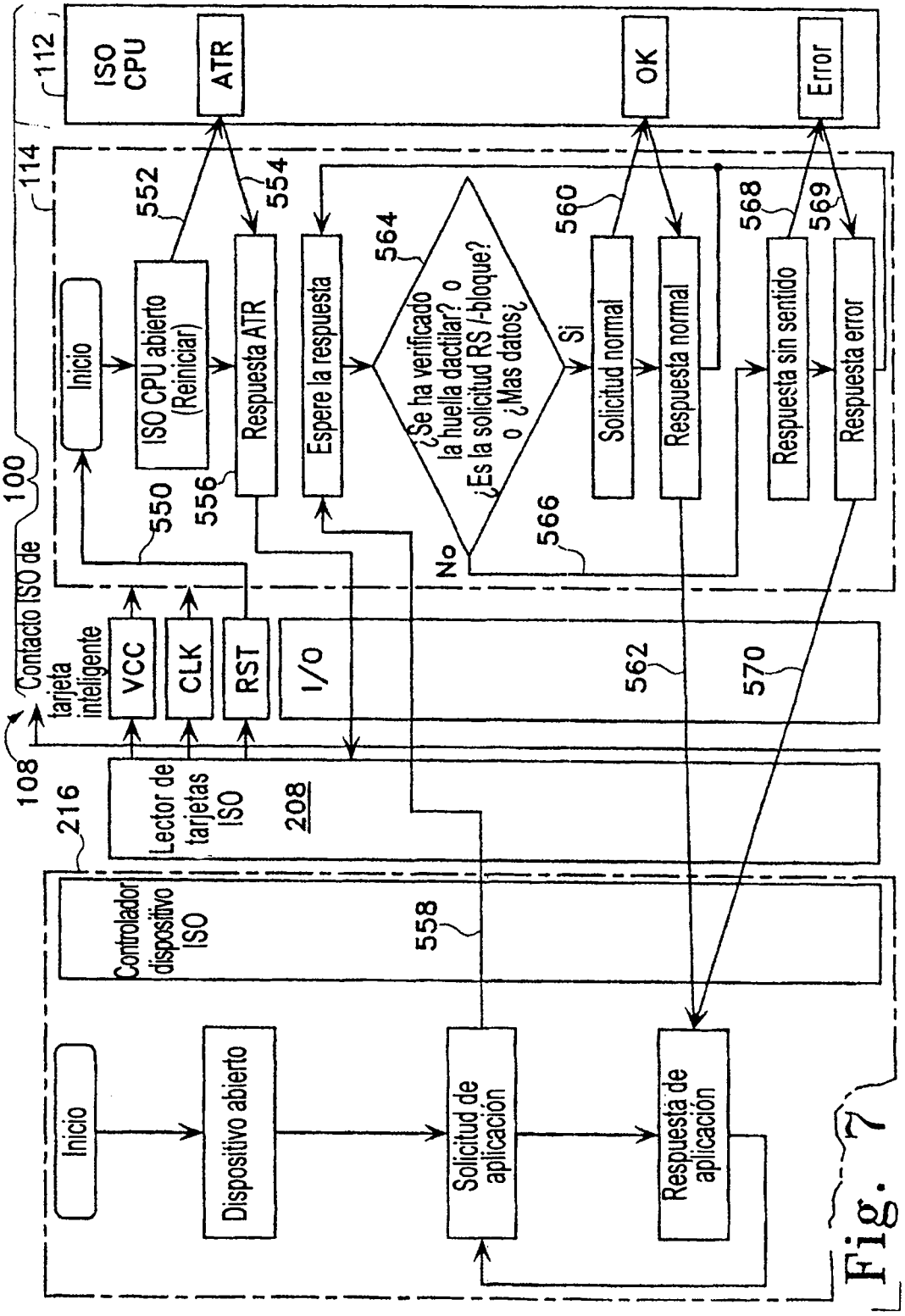

ISO CPU
112
ATR
OK
Error
114
552
554
564
560
568
569
Inicio
ISO CPU abierto (Reiniciar)
Respuesta ATR
Espere la respuesta
¿Se ha verificado la huella dactilar? o ¿Es la solicitud RS /-bloque? o ¿Mas datos¿
Si
Solicitud normal
Respuesta normal
Respuesta sin sentido
Respuesta error
100
550
556
No
566
Contacto ISO de tarjeta inteligente
VCC
CLK
RST
I/O
562
570
108
216
Lector de tarjetas ISO
208
Controlador dispositivo ISO
558
Inicio
Dispositivo abierto
Solicitud de aplicación
Respuesta de aplicación

Fig. 7

Fig. 8

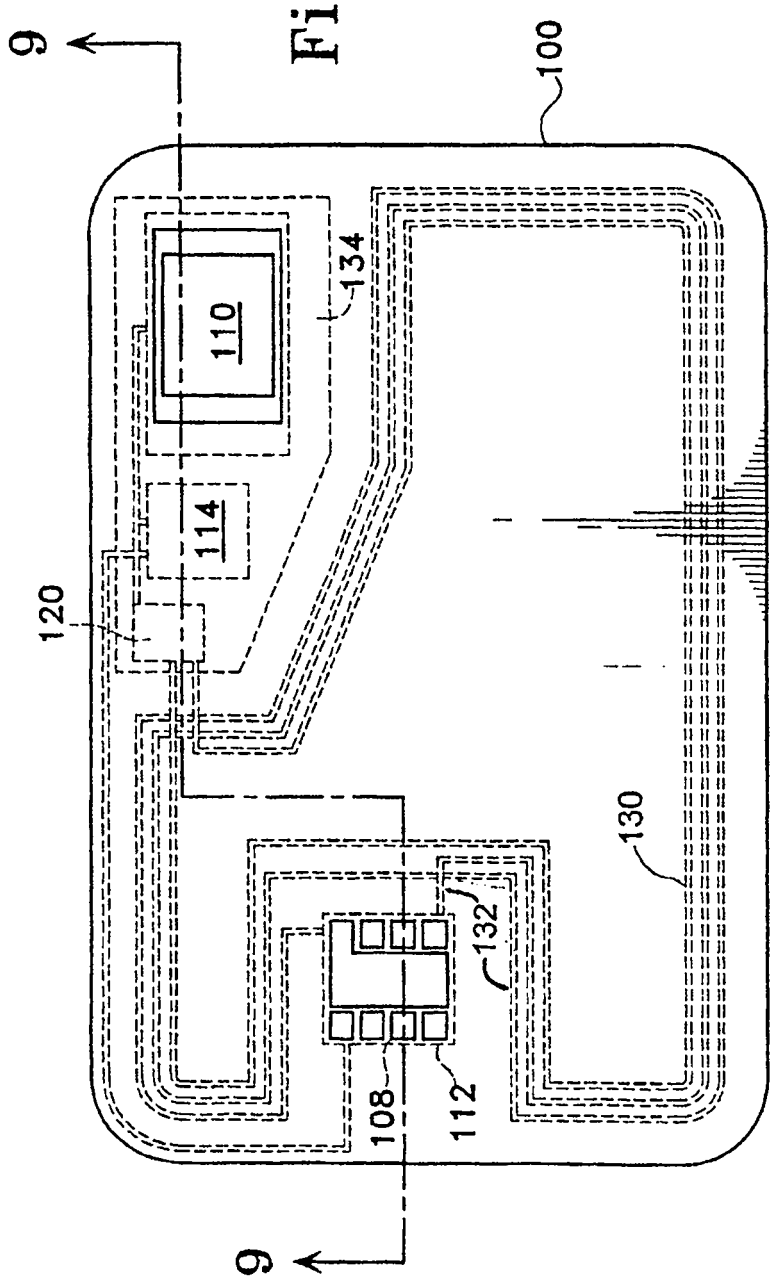
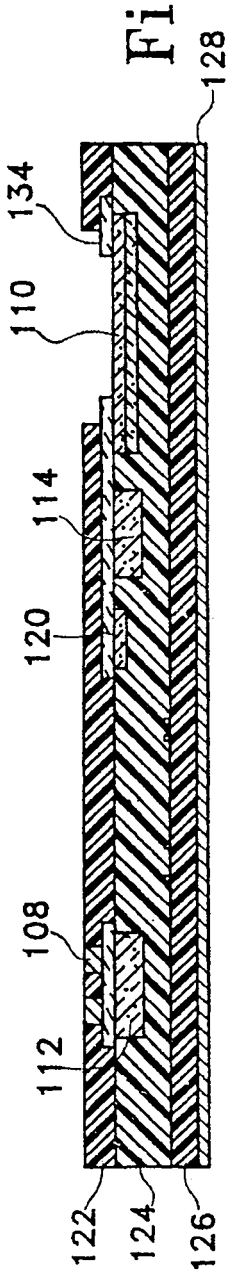

9
100
134
110
114
120
130
132
108
112
9

Fig. 9


128
134
110
114
120
108
112
122
124
126

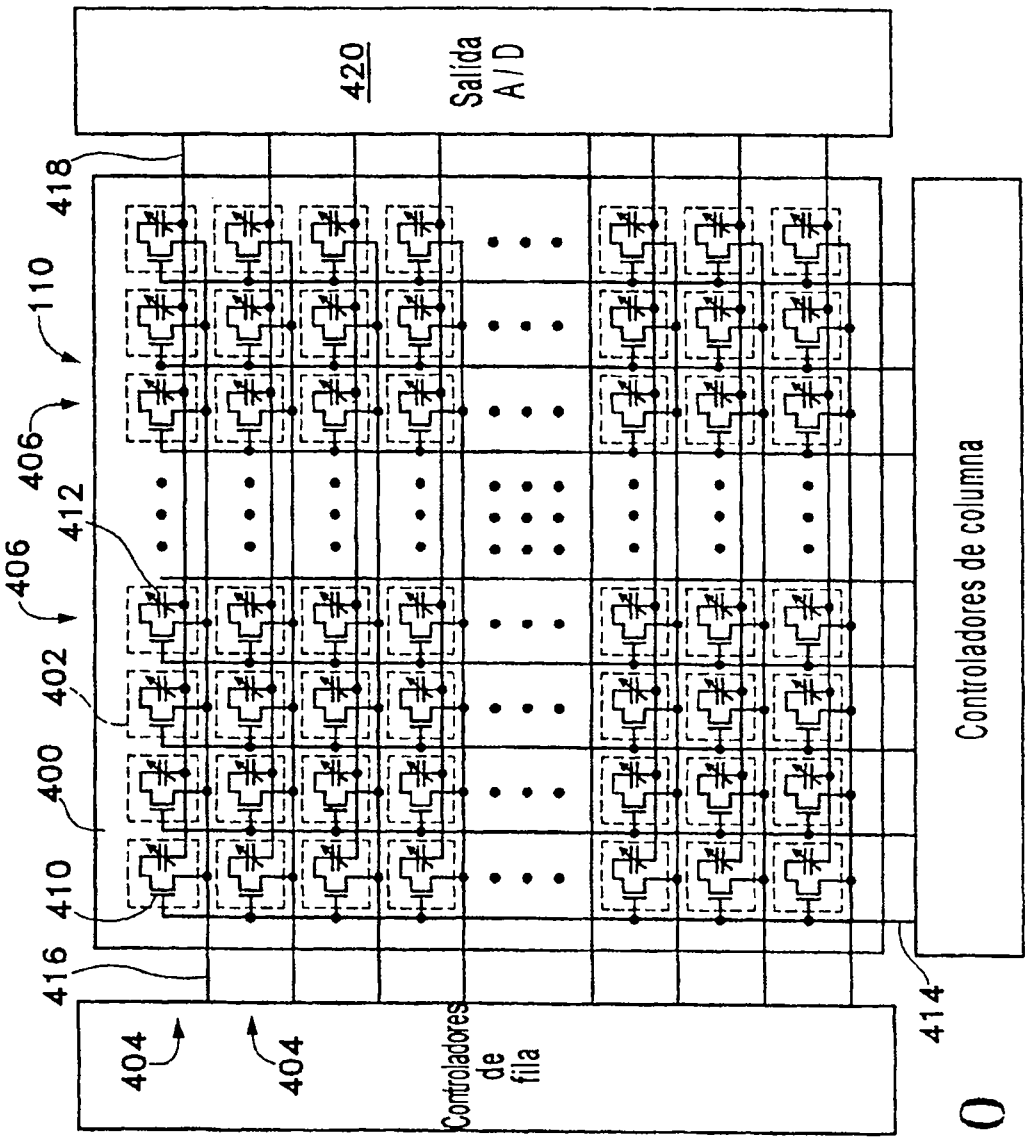

420
Salida A/D
418
110
406
412
406
402
400
410
416
404
404
Controladores de fila
414
Controladores de columna

Fig. 10

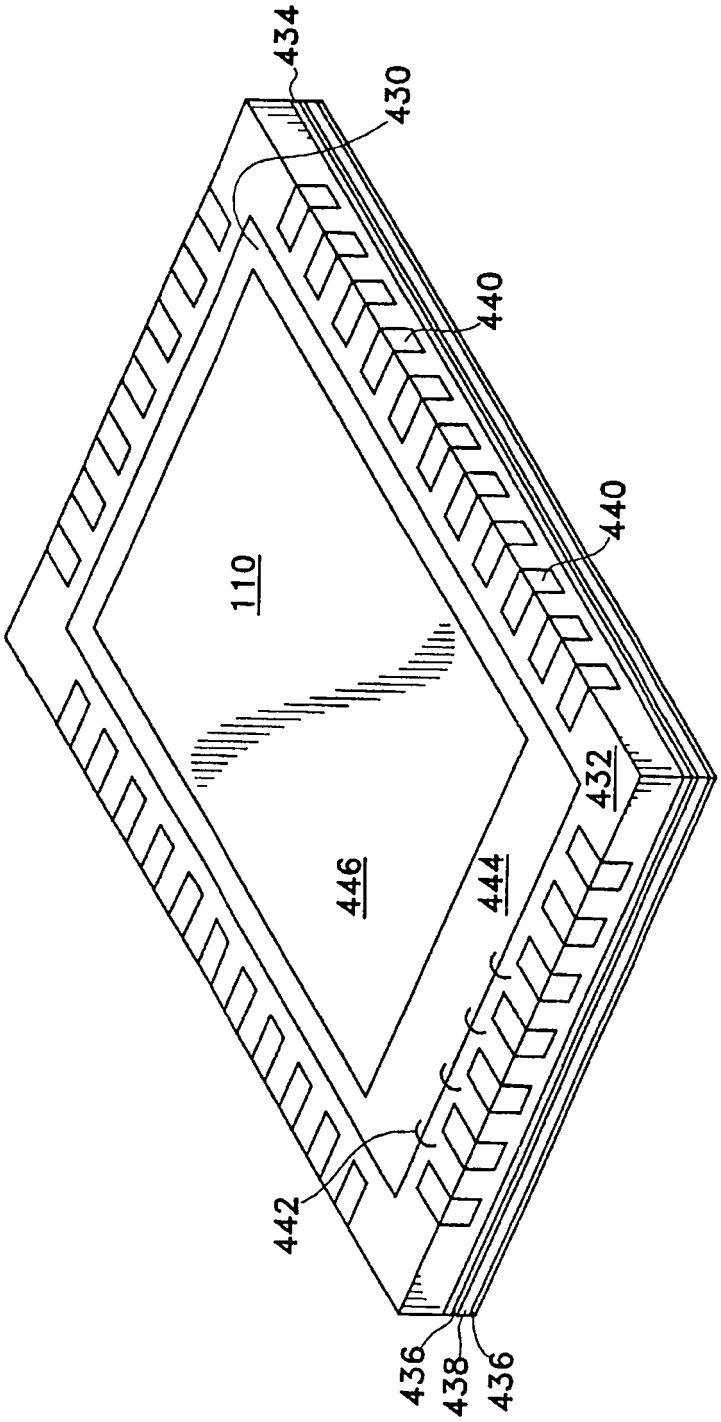


Fig. 11