(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 320 823**

(21) Número de solicitud: 200602306

(51) Int. Cl.:
G06K 19/07 (2006.01)
G06K 9/00 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **08.09.2006**

(43) Fecha de publicación de la solicitud: **28.05.2009**

Fecha de la concesión: **15.02.2010**

(45) Fecha de anuncio de la concesión: **25.02.2010**

(45) Fecha de publicación del folleto de la patente: **25.02.2010**

(73) Titular/es: **FUNDACIÓN ROBOTIKER**
Parque Tecnológico, Edif. 202
48170 Zamudio, Vizcaya, ES

(72) Inventor/es: **Garrote Contreras, Estíbaliz;**
Rentería Bilbao, Silvia;
Picón Ruiz, Artzai y
Isasi Andreu, Alberto

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

(54) Título: **Dispositivo electrónico de identificación biométrica.**

(57) Resumen:
Dispositivo electrónico de identificación biométrica.
El dispositivo se constituye como una llave/tarjeta electrónica con activación biométrica y de alimentación autónoma, teniendo integrados al menos un lector biométrico, medios de almacenamiento informático capacitados para almacenar al menos unos datos de referencia del usuario, unos medios de procesamiento informático programables para al menos realizar una extracción de datos del lector biométrico, una comparación entre los datos extraídos de los datos biométricos y los datos de referencia, y el control del transmisor de señales. Con respecto a las llaves/tarjetas electrónicas identificativas clásicas la mejora está en la activación con las características biométricas del usuario. Y con los sistemas biométricos actuales, la diferencia radica en que la captura del dato biométrico, su procesamiento, el modelo de datos de referencia y la comparación entre el dato biométrico y los de referencia se realiza todo en un único dispositivo.

ES 2 320 823 B1

DESCRIPCIÓN

Dispositivo electrónico de identificación biométrica.

Objeto de la invención

La invención que se describe tiene aplicabilidad en diversos sectores, entre los que principalmente pueden citarse los relacionados con los servicios financieros, las transacciones electrónicas en compra-venta y subastas, la seguridad en informática y telecomunicaciones, el control de acceso a edificios y recursos privados o públicos, para el área gubernamental, policial, en aduanas u otros puntos de tránsito controlados, aeroportuarios, peajes de autopistas, etc. servicios de la domótica e inmótica (en viviendas y grandes edificios) y, en general, aplicable a todos aquellos ámbitos donde es requerida la autenticación e identificación de usuarios para acceder a una determinada zona o a cierto servicio.

Más particularmente, la presente invención se refiere a un dispositivo para la identificación biométrica de personas o animales, es decir, basándose en alguna característica fisiológica o de comportamiento del individuo, con la peculiaridad de que la captura de los datos biométricos, su procesamiento, la comparación con unos datos identificativos de referencia del usuario y el almacenamiento de dichos datos identificativos de referencia se realiza en el mismo dispositivo, sin la necesidad de transmitir información al exterior que podría comprometer la seguridad de las operaciones.

Es pues objeto de la invención proveer al usuario con un dispositivo autónomo y portátil para su autenticación e identificación, que integra un lector biométrico asociado a medios de procesamiento y almacenamiento informático para efectuar todas las operaciones implicadas en dicha identificación y/o autenticación.

Antecedentes de la invención

Son muchas las ocasiones en las que se requiere un control del acceso a instalaciones o recursos y cada día son más frecuentes las operaciones sobre medios digitales donde se necesitan identificar a los agentes involucrados, como ocurre en aplicaciones como el comercio electrónico, las librerías electrónicas y la firma remota. Los elementos más habituales para llevar a cabo este control son el uso de llaves, contraseñas, certificados digitales o tarjetas identificativas personales (ejemplo: Patente ES 2114488). Si bien estos dispositivos confieren seguridad durante la realización de tales operaciones, no garantizan la legitimidad del usuario. Ya que, con mayor o menor facilidad, alguien puede ilegalmente hacerse con el dispositivo o replicarlo y, así, usurpar la identidad del verdadero propietario y con ello sus derechos haciendo un uso fraudulento del dispositivo de identificación.

Las tecnologías biométricas vienen por ello a complementar los dispositivos de seguridad tradicionales (ejemplo: Patente ES 2166321), al vincular inequívocamente al usuario con su identidad mediante diferentes métodos: reconocimiento facial, del ojo, de huellas dactilares, de la mano, de voz, etc.

Los primeros dispositivos biométricos constan de un lector que no está en poder del usuario: cuando se trata de acceder a zonas restringidas, el lector suele encontrarse en el propio punto de acceso o, en caso de que sirva para realizar transacciones electrónicas, está en poder del vendedor. El lector biométrico está asociado generalmente a un procesador informático de datos (ejemplo: Solicitud de Patente ES 2224838 y Certificado de Adición ES 2102307). Estos sistemas presentan el inconveniente de que tanto los datos biométricos del usuario capturados por el lector (por ejemplo, el escaneado de una huella o la fotografía de la retina) como el dato de referencia del usuario quedan en manos del prestador de los servicios. De tal manera que personas no autorizadas podrían tener acceso a esos datos (datos de múltiples usuarios) si violan la seguridad del procesador informático.

Una solución que evita el problema de la centralización de los datos es almacenar los datos de referencia del usuario en una tarjeta personal que porta el usuario y es leída por un sistema biométrico (ejemplo: Patente ES 2140322). En el momento de la identificación, el usuario utiliza el lector biométrico y conecta la tarjeta con sus datos almacenados al sistema, que los compara y valida o deniega el acceso requerido. Sin embargo, aunque los datos identificativos de referencia no se encuentran en el sistema, para la comparación con los datos adquiridos por el lector biométrico, es necesaria una transmisión de datos desde la tarjeta al sistema y durante la transmisión la información corre el riesgo de ser interceptada para su uso fraudulento.

Para salvar la seguridad de los datos identificativos sin tener que enviarlos fuera de la tarjeta del usuario, hay sistemas en los que la comparación se realiza en la propia tarjeta (sistemas “match-on card”). En estos sistemas el prestador del servicio dispone del lector biométrico, el usuario introduce la tarjeta en el sistema y recibe del lector el nuevo dato del usuario, para compararlo con el que tiene de referencia en dicha tarjeta.

En resumen todos estos sistemas presentan dos problemas importantes:

- Los datos biométricos del usuario son transmitidos entre dos o más equipos, con el riesgo que esto supone.

- Al existir una gran diversidad de lectores biométricos, surgen muchas dificultades de estandarización de la información que debe entregar cada lector para la comparación con los datos de referencia.

Descripción de la invención

La invención que aquí se describe viene a resolver la problemática anteriormente expuesta, en todos y cada uno de los diferentes aspectos comentados, concibiendo un dispositivo de identificación biométrica, en especial de aplicación para acceder a un recurso, constituido a partir de un soporte electrónico, tal como una tarjeta, una llave o equivalentes, que comprende los siguientes elementos integrados todos en un único soporte electrónico:

- Al menos un lector biométrico, dotado de los medios de captura de datos biométricos del usuario apropiados, por ejemplo, un sensor de huellas digitales o un escáner de línea para la lectura de dichas huellas, o bien, una microcámara de fotografía o vídeo para registrar el iris del ojo.

- Medios de almacenamiento informático, donde se guardan al menos los datos de referencia de dicho usuario que han de ser comparados con los datos resultantes de la captura realizada por el lector biométrico, pudiendo incluir otra información involucrada en la autenticación e identificación del usuario, tal como un código personal, una contraseña, firma digital, unas claves públicas y/o privadas para encriptar la información, datos específicos para acceder a un servicio informático concreto, etc.

- Al menos un transmisor de señales electromagnéticas, preferiblemente inalámbrico, siendo la señal transmitida, o de salida, portadora de una información que determina el permiso o la denegación del acceso al recurso.

- Medios de procesamiento informático, asociados al (o a los) lector(es) biométrico(s), a los medios de almacenamiento y al transmisor inalámbrico, estando programados para ejecutar al menos el control del transmisor de señales y la comparación entre los datos de referencia del usuario con los resultantes de la captura realizada por el lector biométrico.

Los medios de procesamiento, que pueden consistir en un procesador de señal digital (DSP), un microprocesador o chip integrado en el dispositivo conformando una tarjeta inteligente ("smart card"), están configurados para realizar:

- la extracción de los datos, a partir de los obtenidos por el lector biométrico, a comparar con los datos de referencia del usuario (por ejemplo, una representación discreta de las características de un iris fotografiado) y

- la comparación entre datos extraídos y almacenados tanto para las operaciones de autenticación/verificación de identidad como para la identificación del usuario.

El transmisor inalámbrico, que puede ser de radiofrecuencia para una comunicación a largo alcance o de tecnología inalámbrica de cortoalcance (infrarrojos, Bluetooth, etc.), está configurado para generar un simple mensaje de autenticación "usuario correcto/incorrecto" o enviar información más compleja de identificación digital.

En cuanto a los medios de almacenamiento informático, se trata de al menos un elemento de memoria integrada, no volátil, el cual puede estar complementado mediante otros dispositivos de almacenamiento magnético u óptico, dependiendo de la capacidad de almacenamiento de información que requiere la aplicación para la que se emplea este dispositivo.

Para la alimentación de los elementos electrónicos descritos, el dispositivo puede integrar una fuente de energía eléctrica (pilas o batería recargable y sustituibles) o bien una fuente de energía renovable (pequeñas placas fotovoltaicas insertadas en el soporte de plástico con el que se construye el dispositivo en forma de tarjeta o llave) para conferirle suficiente autonomía y portabilidad.

Las ventajas que ofrece el dispositivo propuesto a los hasta ahora conocidos y comentados en los antecedentes son:

- Frente a las llaves/tarjetas electrónicas clásicas de identificación con o sin código de acceso: dichas llaves/tarjetas no están directamente vinculadas al usuario, lo que favorece los casos de usurpación de la identidad o la negación de autoría del uso fraudulento de una llave o tarjeta. En cambio el dispositivo que se propone, integrando un lector de datos biométricos, permite una vinculación unívoca de los datos que contiene este dispositivo de identificación personal con una característica única del propietario.

- Frente a los dispositivos biométricos convencionales, tiene las siguientes propiedades ventajosas:

* Ni los datos biométricos en bruto, los resultantes del procesado de su lectura, ni los datos de referencia se centralizan en una base de datos ni salen en ningún momento del dispositivo en posesión del usuario, siendo tratados exclusivamente por los medios informáticos integrados en el propio dispositivo.

* Es posible utilizar diferentes sensores o lectores biométricos, ya que cada usuario siempre trabaja con el incluido en su dispositivo personal, el cual independientemente del tipo de lector con el que se han obtenido los datos biométricos emite una señal de salida válida, legible por cualquier sistema: ordenador, procesador... asociado a un receptor inalámbrico adecuado al enlace con el transmisor de cada dispositivo identificador, que establece finalmente el permiso o la prohibición del acceso.

* Permite garantizar la privacidad en la identidad puesto que la información ("tag" identificativo, código identificativo, firma del usuario) que transporta la señal de salida generada por el dispositivo no es de carácter biométrico.

Realización preferente de la invención

Puede describirse como una realización práctica de la invención un dispositivo electrónico portátil, por ejemplo una tarjeta dotada de un microprocesador DSP, que cuenta con una fuente de alimentación que le confiere funcionamiento autónomo y tiene integrados los siguientes elementos:

- Un escáner lineal de lectura de huella dactilar, que supone un mínimo espacio y consumo en la tarjeta, con la mejora sobre el sensor biométrico de huella digital que es evitar el efecto de huella latente, es decir, que al poner el dedo y deslizar la huella por el escáner se autoborra en vez de permanecer sobreimpresa en el sensor, además de que permite extraer datos correspondientes tanto a los rasgos de la huella como al modo de deslizamiento del dedo.

- Una memoria integrada con posibilidad de almacenamiento protegido de la información mediante un algoritmo de encriptación.

- Un transmisor inalámbrico configurado para emitir un código identificativo del usuario, generado por el microprocesador tras la comparación entre los datos extraídos de la lectura de la huella y unos datos de referencia guardados en la memoria.

A fin de aumentar el grado de seguridad, en lugar de un código identificativo, el dispositivo puede hacer uso de la firma digital del usuario, que lleva una codificación más compleja y, por tanto, supera los peligros de copia del código identificativo.

Una alternativa más sencilla consiste en habilitar un "tag" identificativo, lo cual implica que únicamente cuando el usuario ha sido autenticado, por medio del lector biométrico integrado en la tarjeta (es decir, se sabe a través de su huella si es un usuario válido o no), se activa la tarjeta, pudiendo sólo entonces (tras una autentificación positiva) realizarse la identificación y el acceso a los recursos.

Los algoritmos de extracción y comparación de datos que ejecutan esos medios de procesamiento pueden variar en función del tipo de lector biométrico utilizado, de las características del usuario que pueden dar lugar a unos datos biométricos más fáciles de captar o extraer que otros, o para el cambio de algoritmos si el dispositivo identificativo anterior se ha perdido o ha sido robado.

REIVINDICACIONES

1. Dispositivo electrónico de identificación biométrica, que se constituye a partir de un soporte electrónico, tal como una tarjeta electrónica, una llave electrónica o similar, es portátil y está configurado para ser utilizado por un usuario, **caracterizado** porque comprende:

al menos un lector biométrico dotado de medios de captura de unos datos biométricos del usuario,

unos medios de almacenamiento informático capacitados para almacenar al menos unos datos de referencia del usuario,

al menos un transmisor de señales electromagnéticas,

unos medios de procesamiento informático asociados al lector biométrico, a los medios de almacenamiento informático y al transmisor de señales electromagnéticas, programables para al menos realizar una extracción de datos del lector biométrico, una comparación entre los datos extraídos de los datos biométricos y los datos de referencia, así como un control del transmisor de señales;

y porque dichos medios de procesamiento y almacenamiento informático, transmisor de señales electromagnéticas y lector biométrico están integrados en un mismo soporte electrónico.

2. Dispositivo según reivindicación 1, **caracterizado** porque adicionalmente comprende una fuente de energía autónoma, integrable en el soporte electrónico, que se selecciona entre energía eléctrica y energía solar.

3. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el transmisor de señales es inalámbrico.

4. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el transmisor de señales está configurado para emitir datos firmados digitalmente por el usuario.

5. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el transmisor de señales está configurado para emitir un código identificativo del usuario.

6. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque el transmisor de señales está configurado para emitir un mensaje de autenticación.

7. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque los medios de almacenamiento informático comprenden al menos un elemento de memoria.

8. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque los medios de procesamiento informático comprenden al menos un procesador de señal digital.

9. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque los medios de procesamiento informático comprenden al menos un chip.

10. Dispositivo según cualquiera de las reivindicaciones anteriores, **caracterizado** porque los medios de captura del lector biométrico se seleccionan entre un sensor de huella dactilar, un escáner lineal de lectura de huella dactilar, una microcámara fotográfica y una microcámara de vídeo.

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 320 823

(21) Nº de solicitud: 200602306

(22) Fecha de presentación de la solicitud: **08.09.2006**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***G06K 19/07*** (2006.01)
G06K 9/00 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
X	EP 1074949 A1 (SHEN MING SHIANG) 07.02.2001, resumen; párrafos [1-4],[6-15]; figura 1.	1-10
X	WO 2004025545 A2 (IVI SMART TECHNOLOGIES INC; SAITO TAMIO; AIDA TAKASHI) 25.03.2004, resumen; párrafos [24-33],[48-55],[61-64],[66-74]; figuras 1,4,6,8,9.	1-10
X	US 6325285 B1 (BARATELLI et al.) 04.12.2001, resumen; columna 2, línea 50 - columna 6, línea 16; figuras 1A-5C.	1-10

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
05.05.2009	A. Figuera González	1/1