(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 353 720**

(51) Int. Cl.:

G06K 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04741709 .2**

(96) Fecha de presentación : **02.06.2004**

(97) Número de publicación de la solicitud: **1634220**

(97) Fecha de publicación de la solicitud: **15.03.2006**

(54) Título: **Procedimiento y dispositivo de identificación biométrica adaptados a la verificación de tarjetas inteligentes.**

(30) Prioridad: **05.06.2003 FR 03 06789**

(45) Fecha de publicación de la mención BOPI: **04.03.2011**

(45) Fecha de la publicación del folleto de la patente: **04.03.2011**

(73) Titular/es: **GEMALTO S.A.**
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es: **Coron, Jean-Sébastien;**
Naccache, David;
Cardonnel, Cedric y
Barral, Claude

(74) Agente: **Isern Cuyás, María Luisa**

ES 2 353 720 T3

DESCRIPCIÓN

Procedimiento y dispositivo de identificación biométrica adaptados a la verificación de tarjetas inteligentes.

La invención concierne la identificación biométrica del usuario de un sistema. Está adaptada para comprobar la identidad en un objeto portátil de tipo tarjeta chip.

Un método habitualmente utilizado para la identificación de un usuario se basa en un código de identificación secreto, igualmente llamado PIN (por Personal Identification Number en inglés). En un sistema que utiliza tarjetas chip, un usuario entra su código PIN en un terminal de transacción, que transfiere entonces el código PIN que se ha entrado a la tarjeta chip, la cual efectuará la comprobación del código PIN comparándolo con un código PIN de referencia. La seguridad de este tipo de sistema está garantizada por el hecho de que el código PIN de referencia está memorizado en la propia tarjeta chip, de por sí asegurada, y no se revela nunca durante el procedimiento de comprobación de identidad, puesto que la comprobación final la efectúa la tarjeta. El inconveniente de este sistema radica en el hecho de que el propietario de la tarjeta debe memorizar un secreto y en el hecho de que otro usuario puede hacer un fraude al robar dicho secreto.

La biometría consiste en adquirir, medir y reconocer características físicas de un usuario. Permite identificar directamente a un usuario, cuando el método por código PIN permite una identificación indirecta, debido al hecho de comprobar que el usuario conoce un secreto. Entre las técnicas conocidas en biometría, denotamos los métodos de reconocimiento de las características vocales, características propias a la forma del rostro o al iris del ojo, o en el caso más frecuente, características de huellas dactilares.

Todos los procedimientos y sistemas de comprobación de identidad biométrica que existen se dividen en tres fases:

- la primera fase consiste en una captura de datos biométricos a partir de un sensor. Frecuentemente, estos datos biométricos obtenidos son imágenes, por ejemplo en el caso de huellas dactilares, iris o forma del rostro. Pero también puede tratarse de secuencias sonoras en el caso de reconocimientos vocales.

- la segunda fase es una fase de análisis o de extracción, que permite extraer una firma biométrica a partir de datos biométricos capturados durante la primera fase, esta firma se compone de un conjunto más limitado de datos biométricos particulares. Esta segunda fase es extremadamente compleja y necesita una gran potencia de cálculo.

- la tercera fase consiste en comparar la firma biométrica obtenida durante la segunda fase con una firma de referencia definida anteriormente durante un procedimiento denominado enrolamiento.

Los objetos electrónicos portátiles de tipo tarjetas chip están provistos de microprocesadores, cuya potencia de cálculo sigue siendo limitada. Esta es la razón por la que un sistema biométrico del arte anterior que utiliza tarjetas chip funciona del siguiente modo.

- en la fase de enrolamiento, se almacena una firma biométrica de referencia del usuario de la tarjeta en una memoria asegurada de la tarjeta chip.

- en la fase de comprobación de identidad, un terminal captura los datos biométricos del usuario y seguidamente extrae una firma biométrica. Entonces existen dos soluciones:

- sea la firma biométrica de referencia se transfiere de la tarjeta al terminal para comprobar la identidad, mediante comparación de las dos firmas, en el terminal: este método presenta el inconveniente que la firma de referencia corre el riesgo de ser interceptada, lo que representa un fallo de seguridad. Una identificación clásica por código PIN no tiene este inconveniente;

- sea la firma biométrica extraída se transfiere hacia la tarjeta para una comprobación en la tarjeta. La tarjeta posee una pequeña capacidad de cálculo y la comprobación es una operación significativa que necesita bastante tiempo de tratamiento. Esto representa un inconveniente con respecto a la utilización clásica del código PIN.

Un objeto de la presente invención consiste en proponer una solución de identificación biométrica a la vez segura y sencilla, adaptada a una comprobación de identidad en un objeto de tipo tarjeta chip.

La solución se basa en un procedimiento de enrolamiento que comprende la captura de datos biométricos; la extracción de una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares, caracterizada por comprender las siguientes etapas:

- elaboración de falsos datos biométricos particulares;

- generación de la firma biométrica oscurecida al combinar los falsos datos biométricos particulares con los verdaderos datos biométricos particulares,

- elaboración de un código de autentificación que indica cuales son los falsos y verdaderos datos biométricos particulares de la firma biométrica oscurecida.

Los falsos datos biométricos particulares pueden elaborarse de manera coherente con los verdaderos datos biométricos particulares. Para ello, puede elaborarse por lo menos un falso dato biométrico particular transformando ligeramente un verdadero dato biométrico;

- en el caso de los puntos de minutia que corresponden a datos de huellas dactilares de un primer dedo, por lo menos un falso punto de minutia puede elaborarse a partir de los puntos de minutia de un segundo dedo;

- un falso dato biométrico particular también pude elaborarse al detectar un verdadero dato biométrico que posea una geometría relativamente semejante a un verdadero dato biométrico particular y al transformar este verdadero dato biométrico para crear el falso dato biométrico particular.

El código de autentificación puede establecerse según las siguientes etapas:

- los datos biométricos particulares de la firma biométrica oscurecida están ordenados;

- el código de autentificación está compuesto de una serie de bits, de longitud igual al número total de verdaderos y falsos datos biométricos particulares de la firma biométrica oscurecida, cada bit indica respectivamente si el dato biométrico particular correspondiente es verdadero o falso.

La firma biométrica oscurecida y el código de autentificación pueden registrarse en una memoria asegurada de un objeto personal de tipo tarjeta chip.

La solución propone igualmente un procedimiento de comprobación de identidad biométrica que comprende la captura de datos biométricos, la extracción de una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares, y que comprende las siguientes etapas:

- comparación de la verdadera firma biométrica con una firma biométrica oscurecida,
- elaboración de un código que indique los verdaderos y los falsos datos biométricos basándose en la comparación anterior con la verdadera firma biométrica,
- comparación de este código con un código de autentificación que indique los verdaderos y los falsos datos biométricos particulares de la firma biométrica oscurecida.

En este procedimiento, el código de autentificación puede almacenarse en una memoria asegurada de un objeto personal y la comparación del código y del código de autentificación puede tener lugar en el propio objeto personal.

El procedimiento de comprobación de identidad biométrica para acceder a un servicio por mediación de un terminal de servicio, basado en un objeto personal de tipo tarjeta chip para almacenar el código de autentificación y la firma biométrica oscurecida puede comprender las siguientes etapas:

- transferencia de la firma biométrica oscurecida del objeto personal hacia el terminal de servicio para la comparación de la verdadera firma biométrica con la firma biométrica oscurecida y elaboración del código en el propio terminal de servicio;
- transferencia del código desde el terminal de servicio hacia el objeto personal para comparación del código con el código de autentificación en el objeto personal.

La invención se basa asimismo en un dispositivo de enrolamiento que emplea un software de extracción de firma biométrica con el fin de obtener una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares a partir de datos biométricos capturados, empleando un software de oscurecimiento que consiste, por una parte, en elaborar falsos datos biométricos particulares y combinarlos con los verdaderos datos biométricos particulares con el fin de obtener una firma biométrica oscurecida, y por otra parte en elaborar un código de autentificación que permita indicar los verdaderos y falsos datos biométricos particulares de la firma biométrica oscurecida.

El dispositivo de enrolamiento puede comprender un dispositivo de comunicación con un objeto personal de tipo tarjeta chip apta a la transferencia de la firma biométrica oscurecida y del código de autentificación en el objeto personal.

La invención propone igualmente un objeto personal que incluye una memoria asegurada y un medio de comunicación y que comprende en su memoria asegurada una firma biométrica oscurecida que incluye falsos datos biométricos combinados a verdaderos datos biométricos, un código de autentificación para indicar cuales son los falsos y los verdaderos datos biométricos, y que comprende un medio de comparación de un código transferido por el medio de comunicación con el código de autentificación. Este objeto personal puede ser un soporte chip de tipo tarjeta chip.

La invención propone también un terminal de servicio que emplea un software de extracción con el fin de obtener una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares a partir de datos biométricos capturados y que emplea un software de elaboración de un código a partir de una comparación entre la verdadera firma biométrica y una firma biométrica oscurecida, el código indica los verdaderos y falsos datos biométricos sobre la base de la verdadera firma biométrica calculada por el terminal de servicio.

Este terminal puede comprender un dispositivo de comunicación para comunicar con un objeto personal de tipo tarjeta chip, apto a la transferencia desde el objeto personal de la firma biométrica oscurecida y hacia el objeto personal del código elaborado.

Otras características y ventajas de la presente invención aparecerán cuando se lea la siguiente descripción de ejemplos particulares de realización, que se dan a titulo ilustrativo y no limitativo, y los dibujos en anexo en los que:

- la figura 1 representa ejemplos de los puntos de minutia de huellas dactilares;
- la figura 2 representa ejemplos de creación de falsos puntos de minutia;
- la figura 3 representa un ejemplo simplificado de creación de una firma oscurecida y del código de autentificación según la invención;

Pasaremos a describir un modo de realización de la invención descrita en el marco de una identificación por huella digital en una aplicación bancaria.

Un usuario posee una tarjeta chip con una memoria asegurada y una función de comprobación de identidad biométrica que detallaremos a continuación.

Durante la fase de enrolamiento, que consiste en memorizar la firma biométrica de referencia en la tarjeta, el usuario se presenta en un lugar seguro como una agencia bancaria por ejemplo, donde se captura su huella digital en un terminal particular. Un algoritmo de extracción del art. anterior, cuyo principio consiste en seleccionar datos biométricos particulares de la huella digital capturada, llamados puntos de minutia, deduce de ello la firma biométrica compuesta de puntos de minutia. Para facilitar la comprensión del resto de la descripción, llamaremos verdaderos puntos de minutia y verdadera firma biométrica a estos datos obtenidos según el cálculo del arte anterior. Estos verdaderos puntos de minutia se identifican por ejemplo por dos datos que indican su posición, más un dato que indica su tipo. La figura 1 muestra dos ejemplos de tipos de puntos de minutia, una bifurcación de líneas (fig. 1a) y un final de línea (fig. 1b). El número de puntos de minutia que debe seleccionar el algoritmo de extracción se define previamente con objeto de obtener un buen compromiso entre la seguridad y la complicación del cálculo.

Según el procedimiento de la invención, antes del registro de la firma en la tarjeta chip, el terminal de enrolamiento emplea un software de oscurecimiento para transformar la verdadera firma biométrica anterior. Este software de oscurecimiento emplea un procedimiento de oscurecimiento que consiste en reunir los verdaderos puntos de minutia extraídos anteriormente y que componen la verdadera firma biométrica con falsos datos que se llamarán puntos de minutia, de manera a obtener una firma biométrica oscurecida.

Una característica del procedimiento de oscurecimiento consiste en definir falsos puntos de minutia que sean coherentes con los verdaderos puntos de minutia, con el fin de que resulte difícil o imposible la operación que consiste en descubrir la verdadera firma biométrica a partir de la firma oscurecida. Para ello, se pueden utilizar los siguientes procedimientos:

- según una primera variante, el sensor del terminal bancario introduce mayor número de puntos de minutia que el número predefinido. A continuación, los puntos de minutia suplementarios se transforman ligeramente con el fin de obtener falsos puntos de minutia. Esta transformación podrá consistir en una modificación de los datos de los puntos de minutia por una rotación o una translación, o modificando su tipo;

- según una segunda variante semejante a la anterior, se pueden obtener falsos puntos de minutia transformando los puntos de minutia obtenidos durante la captura de la huella dactilar de otro dedo. Seguidamente, nos arreglaremos para conservar únicamente falsos puntos de minutia no muy semejantes a los verdaderos puntos de minutia seleccionados con objeto de conservar una coherencia global. La ventaja de esta variante radica en que puede aplicarse en los casos en que el número de los puntos de minutia de una sola huella dactilar es bajo;

- según una tercera variante, se detectan entre los datos biométricos capturados geometrías relativamente semejantes a verdaderos puntos de minutia y se transforman con el fin de crear falsos puntos de minutia coherentes con la geometría global de la huella dactilar. Esta transformación se ilustra en la figura 2. La figura 2a1 representa una verdadera geometría que se transforma en falsos puntos de minutia de tipo bifurcación representados en la figura 2a2. La figura 2b1 representa una verdadera geometría que se transforma en falsos puntos de minutia de tipo final de línea representados en la figura 2b2.

La agrupación de los falsos y verdaderos puntos de minutia permite obtener la firma biométrica oscurecida. Al mismo tiempo, el procedimiento de oscurecimiento genera un código de autentificación, cuyo contenido indica los puntos de minutia que son verdaderos y falsos en la firma oscurecida. Para elaborar este código de autentificación, los puntos de minutia se ordenan en primer lugar según un orden bien determinado, eligiendo por ejemplo un origen geométrico, y después clasificando los puntos de minutia en función de su posición con relación a este origen. Seguidamente, el código de autentificación se establece en forma de una lista de 0 y de 1, los 0 indican que los puntos de minutia son falsos y los 1 que los puntos de minutia son justos, o al contrario. Este código de autentificación tiene como dimensión un número de bits igual al número total de los puntos de minutia de la firma oscurecida. La figura 3 ilustra un ejemplo simplificado de elaboración de una firma oscurecida y del código de autentificación asociado. La figura 3a representa una huella dactilar, la figura 3b representa los dos verdaderos puntos de minutia (representada por un redondo lleno) extraídos de la huella dactilar por el algoritmo de extracción, la figura 3c representa la firma oscurecida, que fue elaborada añadiendo dos falsos puntos de minutia (representadas por un redondo vacío), la figura 3d representa los mismos puntos de minutia ordenados y la figura 3e representa el código de autentificación asociado.

La fase de enrolamiento se termina por la memorización en la memoria no volátil (E2PROM, FLASH...) de la tarjeta chip de la firma biométrica oscurecida y del código de autentificación. Estos datos requieren un espacio memoria relativamente pequeño, limitado a unas decenas de byte.

Después del enrolamiento, la tarjeta bancaria puede utilizarse para realizar pagos, acceder a los servicios bancarios... Cada operación exige una fase de comprobación de la identidad del usuario, que comprende las siguientes etapas:

- el terminal de servicio, por ejemplo un distribuidor de monedas, captura la huella dactilar del usuario;

- el terminal calcula la verdadera firma biométrica a partir de esta huella dactilar utilizando para ello el mismo algoritmo de extracción que aquel utilizado durante la fase de enrolamiento;

- la tarjeta transfiere al terminal la firma biométrica oscurecida. Podemos observar que este procedimiento presenta la ventaja, contrariamente al arte anterior, de no transferir la verdadera firma biométrica de referencia;

- el terminal compara la verdadera firma biométrica con la firma biométrica oscurecida transferida por la tarjeta y deduce de ello un código que representa las diferencias entre las dos firmas, según un cálculo similar al de la elaboración del código de autentificación descrito durante la fase de enrolamiento. Este código representa los verdaderos y falsos puntos de minutia basándose en la verdadera firma biométrica deducida de la huella dactilar capturada. Este código debe ser casi idéntico al código de autentificación si el usuario es la persona debida.

- el código obtenido se transfiere del terminal a la tarjeta chip;

- la tarjeta chip comprende un medio, en forma de software o de material, que permite comparar (por ejemplo mediante una función XOR) el código recibido y el código de autentificación, almacenado en su memoria durante la fase de enrolamiento. Si los códigos son suficientemente idénticos con respecto a la tolerancia predefinida, entonces la tarjeta envía al terminal un mensaje positivo de validación de la identidad del usuario.

Una primera ventaja de este procedimiento radica en su flexibilidad; podemos elegir un número de verdaderos y falsos puntos de minutia en función de las exigencias de seguridad y de tiempo de tratamiento deseados. Una aplicación muy fácil con una utilización de 10 verdaderos y 10 falsos puntos de minutia, y con una tolerancia que consiste en aceptar el error de un punto de minutia en el cálculo de comprobación, conlleva un porcentaje de falsa aceptación de 1 por 10000 y un tiempo de tratamiento por la tarjeta del mismo orden que la comprobación de un código PIN.

Este procedimiento presenta, además, las mismas ventajas de los sistemas del arte anterior basados en códigos PIN, puesto que por una parte ya no hay transferencia de informaciones confidenciales de la tarjeta hacia el terminal y puesto que por otra parte, el cálculo de comprobación aplicado en la propia tarjeta es muy sencillo. Observamos que el código de autentificación desempeña un papel similar en el código PIN de las soluciones de identificación por código PIN tales como se describieron anteriormente. Por otra parte, este procedimiento comprende evidentemente las ventajas de la biometría. La invención permite acumular las ventajas de la biometría y del código PIN.

La invención, tal y como se describe en este modo de realización, se aplica mediante distintos dispositivos que comprenden las siguientes funcionalidades particulares:

- un software de oscurecimiento basado en un procedimiento de elaboración de falsos puntos de minutia, combinación de falsos y verdaderos puntos de minutia para elaborar una firma biométrica oscurecida y un código de autentificación asociado, aplicado durante una fase de enrolamiento en un terminal asegurado de un proveedor de servicio, como por ejemplo un banco;

- un software de comparación de una firma biométrica extraída con una firma biométrica oscurecida, que genera un código, aplicado en un terminal de servicio durante una fase de comprobación de identidad;

- un medio de comprobación de código aplicado en la tarjeta que posee además una memoria asegurada para contener un código de autentificación y una firma biométrica oscurecida de referencia.

Los procedimientos de la invención están evidentemente adaptados a los otros campos de la biometría, con mecanismos similares basados en datos biométricos particulares, que desempeñan el papel de puntos de minutia de la huella dactilar. Añadiremos del mismo modo falsos datos biométricos particulares coherentes con los verdaderos datos biométricos particulares.

Además, la invención está particularmente bien adaptada a los sistemas basados en objetos personales, tales como las tarjetas chip, que poseen pocos recursos de material. No obstante, puede aplicarse a otros sistemas que no utilizan obligatoriamente un objeto de este tipo.

REIVINDICACIONES

1. Procedimiento de enrolamiento que comprende la captura de datos biométricos; la extracción de una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares, **caracterizada** por comprender las siguientes etapas:

- elaboración de falsos datos biométricos particulares;

- generación de una firma biométrica oscurecida al combinar los falsos datos biométricos particulares con los verdaderos datos biométricos particulares,

- elaboración de un código de autentificación que indica cuales son los falsos y verdaderos datos biométricos particulares de la firma biométrica oscurecida.

2. Procedimiento de enrolamiento según la reivindicación 1 **caracterizada** porque los falsos datos biométricos particulares se han elaborado de manera coherente con los verdaderos datos biométricos particulares.

3. Procedimiento de enrolamiento según la reivindicación 2 **caracterizado** porque por lo menos un falso dato biométrico particular se elabora transformando ligeramente un verdadero dato biométrico.

4. Procedimiento de enrolamiento según la reivindicación 3 se **caracteriza** porque los verdaderos datos biométricos particulares son los puntos de minutia que corresponden a datos de huellas dactilares de un primer objeto y en que por lo menos un falso punto de minutia se elabora a partir de los puntos de minutia de un segundo dedo.

5. Procedimiento de enrolamiento según la reivindicación 3 **caracterizada** porque se elabora por lo menos un falso dato biométrico particular que detecta un verdadero dato biométrico con una geometría relativamente semejante a un verdadero dato biométrico particular y que transforma este verdadero dato biométrico para crear el falso dato biométrico particular.

6. Procedimiento de enrolamiento según la reivindicación 1 **caracterizado** porque el código de autentificación se establece según las siguientes etapas:

- los datos biométricos particulares de la firma biométrica oscurecida están ordenados;

- el código de autentificación está compuesto de una serie de bits, de longitud igual al número total de verdaderos y falsos datos biométricos particulares de la firma biométrica oscurecida, cada bit indica respectivamente si el dato biométrico particular correspondiente es verdadero o falso.

7. Procedimiento de enrolamiento según la reivindicación 1 **caracterizado** porque los datos biométricos son aquellos de una huella dactilar y los datos biométricos particulares de puntos de minutia.

8. Procedimiento de enrolamiento según una de las reivindicaciones anteriores **caracterizado** porque la firma biométrica oscurecida y el código de autentificación están registrados en una memoria asegurada de un objeto personal de tipo tarjeta chip.

9. Procedimiento de comprobación de identidad biométrica que comprende la captura de datos biométricos, la extracción de una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares, **caracterizado** porque comprende las siguientes etapas:

- comparación de la verdadera firma biométrica con una firma biométrica oscurecida,

- elaboración de un código que indique los verdaderos y los falsos datos biométricos basándose en la comparación anterior con la verdadera firma biométrica,

- comparación de este código con un código de autentificación que indique los verdaderos y los falsos datos biométricos particulares de la firma biométrica oscurecida.

10. Procedimiento de comprobación de identidad biométrica según la reivindicación anterior **caracterizado** porque el código de autentificación está almacenado en una memoria asegurada de un objeto personal y porque la comparación del código y del código de autentificación tiene lugar en el propio objeto personal.

11. Procedimiento de comprobación de identidad biométrica según la reivindicación anterior para acceder a un servicio por mediación de un terminal de servicio, basado en un objeto personal de tipo tarjeta chip para almacenar el código de autentificación y la firma biométrica oscurecida y que comprende las siguientes etapas:

- transferencia de la firma biométrica oscurecida del objeto personal hacia el terminal de servicio para la comparación de la verdadera firma biométrica con la firma biométrica oscurecida y elaboración del código en el propio terminal de servicio;

- transferencia del código desde el terminal de servicio hacia el objeto personal para comparación del código con el código de autentificación en el objeto personal.

12. Dispositivo de enrolamiento que emplea un software de extracción de firma biométrica con el fin de obtener una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares a partir de datos biométricos capturados **caracterizado** porque emplea un software de oscurecimiento que consiste por una parte en elaborar falsos datos biométricos particulares y combinarlos con los verdaderos datos biométricos particulares con el fin de obtener una firma biométrica oscurecida, y por otra parte en elaborar un código de autentificación que permita indicar los verdaderos y falsos datos biométricos particulares de la firma biométrica oscurecida.

13. Dispositivo de enrolamiento según la reivindicación anterior **caracterizado** porque comprende un dispositivo de comunicación con un objeto personal de tipo tarjeta chip apto a transferir la firma biométrica oscurecida y el código de autentificación al objeto personal.

14. Objeto personal que incluye una memoria asegurada y un medio de comunicación **caracterizado** por que comprende en su memoria asegurada:

- una firma biométrica oscurecida que incluye falsos datos biométricos combinados a verdaderos datos biométricos,

- un código de autentificación para indicar cuales son los falsos y los verdaderos datos biométricos, y que comprende un medio de comparación de un código transferido por el medio de comunicación con el código de autentificación.

15. Objeto personal según la reivindicación anterior **caracterizado** por ser un soporte chip de tipo tarjeta chip.

16. Terminal de servicio que emplea un software de extracción con el fin de obtener una verdadera firma biométrica compuesta de verdaderos datos biométricos particulares a partir de datos biométricos capturados y que emplea un software de elaboración de un código a partir de una comparación entre la verdadera

firma biométrica y una firma biométrica oscurecida, el código indica los verdaderos y falsos datos biométricos sobre la base de la verdadera firma biométrica calculada por el terminal de servicio.

17. Terminal de servicio según la reivindicación anterior porque comprende un dispositivo de comunicación para comunicar con un objeto personal de tipo tarjeta chip, apto a la transferencia desde el objeto personal de la firma biométrica oscurecida y hacia el objeto personal del código elaborado.

Fig. 1a

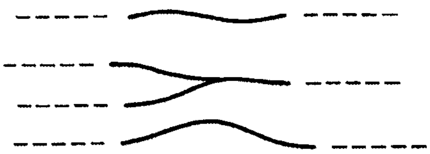


Fig. 1b

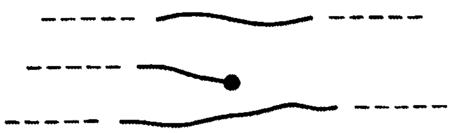


Fig. 2a1

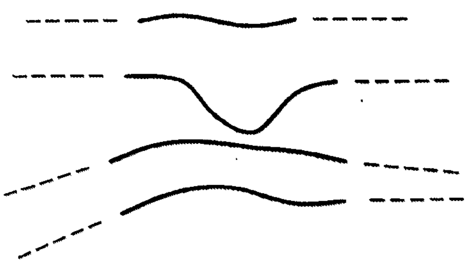


Fig. 2b1

Fig. 2a2

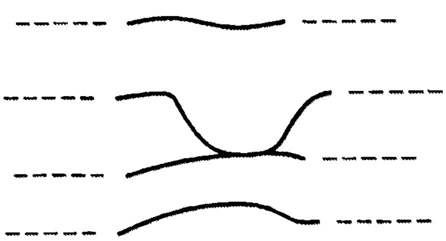
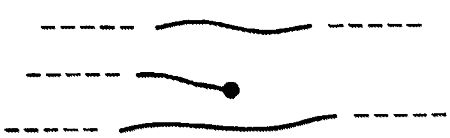


Fig. 2b2



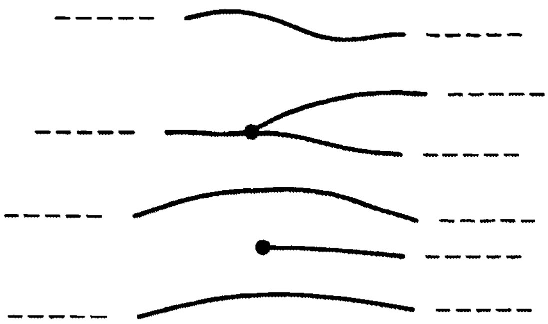


Fig. 3a

Fig. 3b

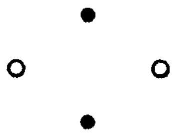


Fig. 3c

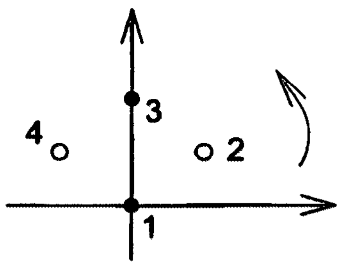


Fig. 3d

1010

Fig. 3e