(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 809**

(51) Int. CI.:

G06K 17/00 (2006.01)
G07F 7/10 (2006.01)
G06K 19/073 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.10.2009 E 09743867 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2350927**

(54) Título: **Procedimiento y sistema para personalizar un dispositivo portátil de almacenamiento de datos**

(30) Prioridad:

27.10.2008 DE 102008053366

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2013

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

EFFING, WOLFGANG;
SPITZ, STEPHAN y
MARTINI, ULLRICH

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimiento y sistema para personalizar un dispositivo portátil de almacenamiento de datos.

La invención se refiere a un procedimiento y un sistema para personalizar un soporte de datos portátil, en particular una tarjeta chip.

Para personalizar soportes de datos portátiles se utilizan hoy día frecuentemente datos biométricos, que permiten una asignación unívoca del soporte de datos a una persona correspondiente. Los datos biométricos constituyen aquí una información muy delicada específica de la persona, que, con el fin de evitar un uso indebido, no debe transmitirse a terceros sin autorización.

Por el documento WO 2005/010810 A1 se conoce el método de capturar datos biométricos de un usuario bajo la supervisión de una entidad de registro y transmitirlos a un dispositivo de personalización. El dispositivo de personalización escribe los datos biométricos en un soporte de datos portátil y el soporte de datos portátil así personalizado se devuelve a una autoridad de registro. En la autoridad de registro, el usuario presenta de nuevo sus datos biométricos, que se comparan con los datos biométricos almacenados en el soporte de datos. Si el grado de coincidencia es suficiente, se realiza una activación del soporte de datos para su uso.

En los procedimientos ya conocidos para la personalización de un soporte de datos resulta desventajoso el que los muy delicados datos biométricos se transmitan a un sistema de personalización. Los datos biométricos están así centralizados en este último, lo que abre la posibilidad de un uso indebido por terceros que se procuren acceso a los datos biométricos almacenados en el sistema de personalización.

Por lo tanto, el objetivo de la invención es crear un procedimiento y un sistema para la personalización de un soporte de datos portátil con los que se dificulte el acceso a los datos biométricos, aumentándose así la seguridad en la personalización.

Este objetivo se logra mediante el procedimiento según la reivindicación 1 o el sistema según la reivindicación 11. En las reivindicaciones dependientes se definen perfeccionamientos de la invención.

En el procedimiento según la invención se captura en una etapa a) un juego de datos biométricos de un usuario y a partir del juego de datos biométricos se calcula, con un procedimiento de cálculo predeterminado, un valor de identificación que está asignado de manera unívoca al juego de datos biométricos y a partir del cual no puede derivarse dicho juego de datos biométricos. En un sistema de personalización al que se ha transmitido el valor de identificación se almacena a continuación este último en un soporte de datos portátil. Por último, en una etapa c), una vez transferido el soporte de datos portátil del sistema de personalización al usuario o a una entidad de emisión, se captura de nuevo un juego de datos biométricos de una persona. Esta persona es en particular un usuario cuyo juego de datos biométricos se supone que ha sido capturado también en la etapa a). La persona constituye por lo tanto el supuesto usuario autorizado del soporte de datos. A partir del nuevo juego de datos biométricos capturado se calcula nuevamente, mediante el procedimiento de cálculo predeterminado, un valor de identificación, que se compara con el valor de identificación almacenado en el soporte de datos portátil, y, si existe suficiente coincidencia entre los valores de identificación, especialmente si los dos valores de identificación son idénticos, se almacena en el soporte de datos portátil el nuevo juego de datos biométricos capturado.

Así pues, la etapa c) constituye una personalización ulterior, en la que el soporte de datos portátil se personaliza con el nuevo juego de datos biométricos capturado. La etapa c) puede ser realizada directamente por el usuario, por ejemplo por medio de un sensor para el registro de los datos biométricos correspondientes en un equipo terminal del usuario. La personalización puede efectuarse también en una entidad de emisión para el soporte de datos, por ejemplo una autoridad de registro, en la que el usuario represente nuevamente su juego de datos biométricos.

El procedimiento según la invención se distingue porque se realiza una personalización del soporte de datos con datos biométricos de manera descentralizada, sin que los datos biométricos se encuentren almacenados en un sistema de personalización intermedio. El sistema de personalización sirve según la invención únicamente para efectuar una personalización previa con un valor de identificación biométrico a partir del cual no puede derivarse el juego de datos biométricos, en el que se basa el valor de identificación biométrico. Por lo tanto, según la invención se asegura que no se pongan datos biométricos de un usuario a disposición del sistema de personalización, con lo que se aumenta la seguridad en la personalización.

En una forma de realización preferida, el valor de identificación es un PIN biométrico (PIN = Personal Identification Number [número de identificación personal]) en forma de una combinación de caracteres de varias signos, especialmente de una combinación de cifras y/o letras. Puede utilizarse por ejemplo una combinación de caracteres de cuatro, cinco, seis o en caso dado incluso más posiciones.

En otra variante preferida del procedimiento según la invención, el valor de identificación calculado en la etapa a) se transfiere electrónicamente al sistema de personalización. Esta transmisión puede ser codificada. Sin embargo, la

codificación no es forzosamente necesaria, ya que a partir del valor de identificación no puede deducirse el juego de datos biométricos en el que se basa el valor de identificación.

En otra variante preferida del procedimiento según la invención, el valor de identificación calculado en la etapa a) se emite al usuario a través de un medio de emisión, en particular un dispositivo de presentación, disponiendo el usuario la transmisión al sistema de personalización del valor de identificación obtenido. De este modo se aumenta la seguridad del sistema, ya que es el propio usuario quien determina en qué momento y de qué manera se transmite al sistema de personalización el valor de identificación obtenido.

Para aumentar aun más la seguridad del procedimiento, en una variante especialmente preferida, el juego de datos biométricos capturado en la etapa a) se borra tras el cálculo del valor de identificación, de modo que no exista la posibilidad de utilización indebida del juego de datos biométricos por parte de terceras personas.

En otra forma de realización del procedimiento según la invención en el soporte de datos se almacenan otros datos del usuario junto además del valor de identificación del sistema de personalización, de modo que una vez concluida la personalización estén disponibles inmediatamente datos del usuario relevantes para el empleo del soporte de datos y no hayan de cargarse los mismos por separado en este último. En este caso, los datos del usuario pueden transmitirse al sistema de personalización junto con el valor de identificación. En caso dado, los datos del usuario pueden también transmitirse al sistema de personalización en una etapa de transmisión separada.

En otra forma de realización preferida del procedimiento según la invención, la etapa a) se repite varias veces, con lo que se obtienen varios valores de identificación, utilizándose posteriormente en la etapa b) el valor de identificación determinado con mayor frecuencia en la etapa a). De este modo, la generación del valor de identificación según la etapa a) se realiza con una redundancia múltiple, con lo que se tiene en cuenta la posible aparición de tolerancias en la captura del juego de datos biométricos y el cálculo del valor de identificación que puedan hacer que ocasionalmente se produzcan divergencias en el cálculo del valor de identificación.

En otra variante del procedimiento según la invención, si no existe suficiente coincidencia entre los valores de identificación en la etapa c), se puede repetir una cantidad predeterminada de veces la captura del juego de datos biométricos y el cálculo del valor de identificación, comparando nuevamente tras cada repetición el nuevo valor de identificación capturado con el valor de identificación almacenado en el soporte de datos y, si existe suficiente coincidencia entre los valores de identificación, almacenar en el soporte de datos portátil el nuevo juego de datos biométricos capturado a partir del cual se ha calculado el nuevo valor de identificación obtenido. Esta variante de la invención corresponde al incremento de un contador de error de manejo, con lo que de nuevo se tiene en cuenta la posible aparición de tolerancias en el nuevo cálculo del valor de identificación. Por consiguiente, en la etapa c) se determina el valor de identificación en caso dado varias veces para asegurar que una diferencia entre los valores de identificación tenga realmente su causa en que en la etapa c) se hayan representado los datos biométricos de una persona no autorizada.

En otra variante del procedimiento según la invención, el valor de identificación almacenado en el soporte de datos portátil se borra de este último durante o después de almacenar el juego de datos biométricos en la etapa c), ya que, por regla general, el valor de identificación ya no es necesario para la utilización posterior del soporte de datos portátil. En este caso lo que se hace especialmente es sobrescribir el valor de identificación con el juego de datos biométricos.

En el procedimiento según la invención se pueden capturar como juego de datos biométricos en la etapa a) o en la etapa c) cualesquiera datos biométricos y deducir a partir de éstos el juego de datos biométricos. El juego de datos biométricos se genera preferentemente a partir de una huella dactilar y/o un escáner de iris de una persona. Por regla general, el juego de datos biométricos no se trata de los datos biométricos brutos capturados, sino que han sido reprocesados adecuadamente para formar un juego de características biométricas. En el caso del registro de huellas dactilares, el juego de datos biométricos es en particular un modelo de la huella dactilar o de las minucias de la huella dactilar.

Además del procedimiento arriba descrito, la invención comprende un sistema para la personalización de un soporte de datos portátil. El sistema comprende primeros medios de captura y cálculo para capturar un juego de datos biométricos de un usuario y para calcular a partir del juego de datos biométricos, con un procedimiento de cálculo predeterminado, un valor de identificación asignado de manera unívoca al juego de datos biométricos y a partir del cual no puede derivarse el juego de datos biométricos. Además está previsto un sistema de personalización para almacenar el valor de identificación en un soporte de datos portátil tras la transmisión del valor de identificación al sistema de personalización. El sistema incluye también segundos medios de captura y cálculo para capturar nuevamente un juego de datos biométricos de una persona una vez transmitido el soporte de datos portátil del sistema de personalización al usuario o a una entidad de emisión, calculándose nuevamente con dichos segundos medios de captura y cálculo a partir del nuevo juego de datos biométricos capturado, mediante el procedimiento de cálculo predeterminado, un valor de identificación, que se compara con el valor de identificación almacenado en el soporte de datos portátil, y almacenándose el nuevo juego de datos biométricos capturado en el soporte de datos portátil si existe suficiente coincidencia entre los valores de identificación, especialmente si los valores de

identificación son idénticos. Los medios de registro y cálculo primeros y segundos pueden ser en caso dado los mismos medios de captura y cálculo o medios de captura y cálculo del mismo tipo.

El sistema según la invención está configurado preferentemente de manera que con el sistema puedan realizarse todas las variantes del procedimiento según la invención arriba descrito. Los primeros o segundos medios de captura utilizados en el sistema están en particular integrados en un equipo terminal del usuario, por ejemplo en un equipo de radiotelefonía móvil. De este modo se hace posible una personalización flexible por parte de un usuario, de forma descentralizada en un paradero cualquiera del usuario, sin que éste haya de presentar sus datos biométricos a una entidad de emisión.

El sistema de personalización empleado en el sistema según la invención es preferentemente una entidad de personalización central, prevista por ejemplo en las instalaciones del fabricante del soporte de datos portátil. A este sistema de personalización pueden transmitírsele valores de identificación de infinidad de usuarios diferentes. Aunque pueda existir una entidad de personalización central, en el sistema según la invención el juego de datos biométricos correspondiente se captura sólo de forma descentralizada y no se transmite a la entidad de personalización central.

A continuación se describe la invención detalladamente por medio de la figura 1. Esta figura muestra, en una representación esquemática, el desarrollo de una forma de realización del procedimiento según la invención para la personalización de una tarjeta chip.

En el ejemplo de realización de la figura 1, en primer lugar se captura en una primera etapa S1 la huella dactilar de un usuario, a partir de la cual se genera un vector biométrico BV1, que constituye un juego de datos biométricos en el sentido de la reivindicación 1. La captura de la huella dactilar y la generación del vector BV1 asociada a dicho registro se realizan mediante un sensor de huellas dactilares correspondiente. A partir del vector biométrico BV1 se calcula, a partir de un procedimiento de cálculo predeterminado, un PIN biométrico en forma de una primera identificación K1. En la técnica actual se conocen ya procedimientos correspondientes para la deducción de un PIN a partir de un vector biométrico y por ello no se describen éstos detalladamente. El PIN biométrico se trata de una identificación que está asignada de manera unívoca al vector biométrico BV1. Es decir que si se deduce una identificación a partir del vector biométrico de una huella dactilar capturada de otra persona, esta identificación será diferente de la identificación K1.

Una vez determinado el PIN K1 se borra el vector biométrico BV1, para evitar una utilización indebida por un uso no autorizado de este vector.

En la etapa siguiente S2 se transmite la identificación K1 a un soporte de datos portátil en forma de una tarjeta chip 1. Para ello se transmite la identificación K1 a un sistema de personalización central, que almacena el PIN en la tarjeta chip 1, sometiéndola así esta última a una personalización previa. El sistema de personalización central está dispuesto preferentemente en las instalaciones del fabricante de la tarjeta chip 1. La personalización previa tiene la gran ventaja de que ya no se transmite el vector biométrico en sí, sino un PIN de transporte biométrico deducido del mismo en forma de la identificación K1. Este PIN es considerablemente menos delicado, ya que se trata únicamente de una combinación corta de cifras, y en caso dado también letras, de la que ya no puede deducirse la información en cuanto a la huella dactilar de la que procede.

El PIN K1 puede transmitirse al sistema de personalización central de cualquier modo. Por ejemplo, la identificación K1 puede enviarse electrónicamente al sistema de personalización central mediante un enlace de comunicación correspondiente inmediatamente después de haber sido generada. También es posible que el sensor de huellas dactilares al que el usuario presenta sus datos biométricos disponga sólo de una pantalla de presentación en la que se indique al usuario el PIN biométrico. En este caso no es posible una transmisión electrónica directa del PIN. De este modo se evita el uso indebido, ya que no existe posibilidad de que el usuario transmita electrónicamente a terceras personas de manera inadvertida los datos capturados. El usuario al que se le ha presentado el PIN en el dispositivo de presentación retiene esta identificación en la memoria y la transmite él mismo al sistema de personalización, por ejemplo desde casa mediante el envío de un correo electrónico correspondiente.

A continuación se transmite al usuario la tarjeta chip 1 con la identificación K1 almacenada en ella. En una etapa S3 se realiza finalmente una personalización ulterior de la tarjeta chip. El proceso para ello es el siguiente: el usuario presenta su huella dactilar de nuevo a un sensor de huellas dactilares, que deduce a partir de la misma un vector biométrico BV2. Con el mismo algoritmo que el utilizado en la etapa S1 para el cálculo de la identificación K1 se deduce de nuevo a partir del vector biométrico BV2 una identificación K2 en forma de un PIN biométrico. Si la huella dactilar de la etapa S1 procede del mismo usuario que la huella dactilar de la etapa S3, por regla general las dos identificaciones K1 y K2 son idénticas. Por lo tanto se efectúa una comparación de las identificaciones K1 y K2. Si se comprueba que estas identificaciones se corresponden entre sí, la personalización ulterior concluye con el almacenamiento definitivo del vector biométrico BV2 en la tarjeta chip 1 y además el borrado de la identificación K1 de la tarjeta chip 1. De este modo se crea una tarjeta chip personalizada con datos biométricos de un usuario, sin que haya sido necesario presentar durante la personalización los datos biométricos del usuario de manera centralizada, por ejemplo en el sistema de personalización central arriba descrito.

Un ejemplo de aplicación del procedimiento según la invención es la personalización de una tarjeta SIM de un proveedor de radiotelefonía móvil. Para ello se captura de forma descentralizada en un establecimiento del proveedor de radiotelefonía móvil la huella dactilar de un cliente, mediante un sensor de huellas dactilares, y se calcula a partir de la misma el PIN biométrico K1. A continuación se transmite el PIN directamente al sistema de personalización central o se visualiza el PIN en un dispositivo de presentación del sensor de huellas dactilares, después de lo cual el cliente mismo transmite los datos al sistema de personalización central.

En el sistema de personalización central se almacenan en la tarjeta la identificación K1 y, en caso dado, otros datos del cliente, sometiendo así la tarjeta a una personalización previa. Después, la tarjeta se entrega de nuevo a la tienda del proveedor de radiotelefonía móvil o directamente al cliente. A continuación se realiza la personalización ulterior. Ésta puede efectuarse en el sensor de huellas dactilares empleado también para generar la identificación original K1. También existe la posibilidad de que el teléfono móvil del cliente disponga de un sensor de huellas dactilares propio con el que, basándose en el mismo algoritmo que en el cálculo de la identificación K1, se deduzca la identificación K2 correspondiente a partir de la huella dactilar del cliente. En cualquier caso, durante la personalización ulterior se compara la identificación K1 almacenada en la tarjeta chip con la identificación K2 generada. Si estas identificaciones coinciden, la personalización ulterior concluye con el almacenamiento del vector biométrico BV2 en la tarjeta chip 1.

REIVINDICACIONES

1. Procedimiento para personalización de un soporte de datos portátil (1), en particular una tarjeta chip, con datos biométricos, en el que:

a) se captura un juego de datos biométricos (BV1) de un usuario y a partir de dicho juego de datos biométricos (BV1) se calcula, con un procedimiento de cálculo predeterminado, un valor de identificación (K1) que se asigna de manera unívoca al juego de datos biométricos (BV1) y a partir del cual no puede derivarse el juego de datos biométricos (BV1);

b) tras la transferencia del valor de identificación (K1) a un sistema de personalización, dicho sistema de personalización almacena el valor de identificación (K1) en un soporte de datos portátil;

c) una vez transferido el soporte de datos portátil (1) del sistema de personalización al usuario o a una entidad de emisión, se captura de nuevo un juego de datos biométricos (BV2) de una persona, calculándose nuevamente a partir del nuevo juego de datos biométricos capturado de nuevo (BV2), mediante el procedimiento de cálculo predeterminado, un valor de identificación (K2), que se compara con el valor de identificación (K1) almacenado en el soporte de datos portátil (1), y, si existe suficiente coincidencia entre los valores de identificación (K1, K2), el nuevo juego de datos biométricos capturado (BV2) se almacena en el soporte de datos portátil (1).

2. Procedimiento según la reivindicación 1, caracterizado porque el valor de identificación (K1) es una combinación de caracteres de varios signos, en particular una combinación de cifras y/o letras.

3. Procedimiento según la reivindicación 1 ó 2, caracterizado porque el juego de datos biométricos (BV1) capturado en la etapa a) se borra después de calcular el valor de identificación (K1).

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el valor de identificación (K1) calculado en la etapa a) se transmite electrónicamente al sistema de personalización.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el valor de identificación (K1) calculado en la etapa a) se emite al usuario a través de un medio de emisión, en particular un dispositivo de presentación, en el que el usuario produce la transmisión al sistema de personalización del valor de identificación (K1) obtenido.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque en el soporte de datos portátil (1) se almacenan otros datos del usuario junto además del valor de identificación (K1) del sistema de personalización.

7. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la etapa a) se repite varias veces, con lo que se obtienen varios valores de identificación (K1), utilizándose posteriormente en la etapa b) el valor de identificación (K1) determinado con mayor frecuencia.

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque, si no existe suficiente coincidencia entre los valores de identificación (K1, K2) en la etapa c), se puede repetir una cantidad predeterminada de veces la captura del juego de datos biométricos (BV2) y el cálculo del valor de identificación (K2), comparando nuevamente tras cada repetición el nuevo valor de identificación calculado (K2) con el valor de identificación (K1) almacenado en el soporte de datos portátil y, si existe suficiente coincidencia entre los valores de identificación (K1, K2), almacenar en el soporte de datos portátil (1) el juego de datos biométricos capturado de nuevo (BV2) a partir del cual se ha calculado el nuevo valor de identificación obtenido (K2).

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el valor de identificación (K1) almacenado en el soporte de datos portátil (1) se borra de este último durante o después de almacenar el juego de datos biométricos (BV2) en la etapa c).

10. Procedimiento según una de las reivindicaciones precedentes, en el que el juego de datos biométricos (BV1, BV2) es generado en la etapa a) y/o en la etapa c) a partir de una huella dactilar y/o un escáner de iris.

11. Sistema para personalización de un soporte de datos portátil (1), en particular una tarjeta chip, con datos biométricos, que comprende:

- primeros medios de captura y cálculo para capturar un juego de datos biométricos (BV1) de un usuario y para calcular a partir del juego de datos biométricos (BV1), con un procedimiento de cálculo predeterminado, un valor de identificación (K1) asignado de manera unívoca al juego de datos biométricos (BV1) y a partir del cual no puede derivarse el juego de datos biométricos (BV1);

- un sistema de personalización para almacenar el valor de identificación (K1) en un soporte de datos portátil (1) tras la transmisión del valor de identificación (K1) al sistema de personalización;

- segundos medios de captura y cálculo para capturar nuevamente un juego de datos biométricos (BV2) de una persona una vez transmitido el soporte de datos portátil (1) del sistema de personalización al usuario o a una entidad de emisión, calculándose nuevamente con los segundos medios de captura y cálculo a partir del nuevo juego de datos biométricos capturado (BV2), mediante el procedimiento de cálculo predeterminado, un valor de identificación (K2), que se compara con el valor de identificación (K1) almacenado en el soporte de datos portátil (1), y almacenándose el nuevo juego de datos biométricos capturado en el soporte de datos portátil (1) si existe suficiente coincidencia entre los valores de identificación (K1, K2).

12. Sistema según la reivindicación 11, caracterizado porque el sistema está configurado de manera que con dicho sistema pueda llevarse a cabo un procedimiento según una de las reivindicaciones 2 a 10.

13. Sistema según la reivindicación 11 ó 12, caracterizado porque los primeros y/o los segundos medios de captura y cálculo está(n) integrado(s) en un equipo terminal, especialmente en un equipo de radiotelefonía móvil.

14. Sistema según una de las reivindicaciones 11 a 13, caracterizado porque el sistema de personalización es una entidad de personalización central a la que se transmiten valores de identificación (K1, K2) de una pluralidad de usuarios diferentes.

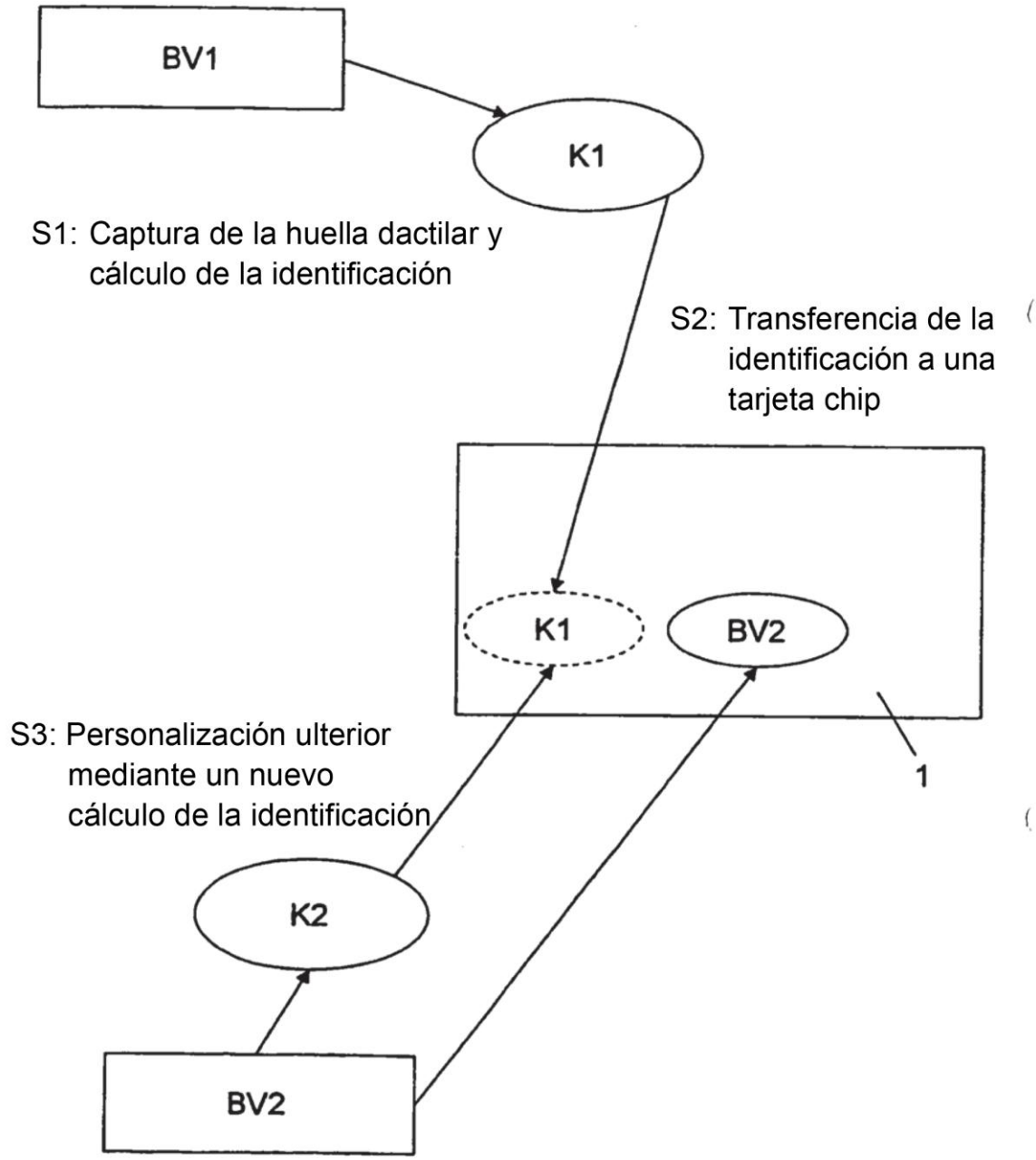
BV1
K1
S1: Captura de la huella dactilar y cálculo de la identificación
S2: Transferencia de la identificación a una tarjeta chip
K1
BV2
1
S3: Personalización ulterior mediante un nuevo cálculo de la identificación
K2
BV2

FIG. 1

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

• WO 2005010810 A1 **[0003]**