(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 798 002**

(51) Int. CI.:

H04W 12/00 (2009.01)
H04L 29/06 (2006.01)
G06F 21/00 (2013.01)
H04L 12/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.03.2008 PCT/EP2008/002494**

(87) Fecha y número de publicación internacional: **09.10.2008 WO08119515**

(96) Fecha de presentación y número de la solicitud europea: **28.03.2008 E 08734866 (0)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 2140654**

(54) Título: **Dispositivo multimedia y procedimiento de transmisión de datos por un dispositivo multimedia**

(30) Prioridad:

30.03.2007 DE 102007015788

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.12.2020

(73) Titular/es:

FM MARKETING GMBH
Huberbergstrasse 23
5162 Obertrum am See , AT

(72) Inventor/es:

MAIER, FERDINAND

(74) Agente/Representante:

IZQUIERDO BLANCO, María Alicia

DESCRIPCIÓN

Dispositivo multimedia y procedimiento de transmisión de datos por un dispositivo multimedia

[0001] La invención se refiere a un dispositivo multimedia de acuerdo con el preámbulo de la reivindicación 1 y a un método para la transmisión de datos en un dispositivo multimedia de acuerdo con el preámbulo de la reivindicación 2.

[**0002]** Un dispositivo y método de este tipo se conoce a partir del documento WO 2007/022481 A.

[**0003]** Allí, se describe un control remoto para dispositivos multimedia con un dispositivo para detectar una huella digital para autenticar a un usuario. Después de la autenticación, los dispositivos multimedia se personalizan, es decir, ciertas funciones se activan o no, dependiendo de la identidad del usuario.

[**0004]** También se conoce un dispositivo similar a partir de DE 198 58 310B4.

[**0005]** El documento EP-A-1 602 999 describe un método para la reproducción de datos con un dispositivo de usuario que contiene un sensor biométrico, tal como un lector de huellas digitales y una tarjeta SIM, en el que se almacenan los datos del usuario. Si el usuario del dispositivo se identifica correctamente, se activa una conexión a otro dispositivo o una red. Los datos de activación se transmiten en forma cifrada. La identificación completa del usuario tiene lugar en el dispositivo, lo que requiere un procesador complejo y, por lo tanto, una gran cantidad de hardware.

[**0006]** El presente dispositivo de electrónica de consumo, tales como televisores, equipos de audio, reproductores de DVD, receptores de satélite, grabadores de video, decodificadores, etc., generalmente son operados por control remoto, que generalmente se comunican de forma inalámbrica con los dispositivos correspondientes a través de un enlace infrarrojo o de radio. Todos estos dispositivos multimedia, que hoy también incluyen computadoras, se denominan a continuación "dispositivos". Todos estos dispositivos, así como, en mayor medida, otras instalaciones en los hogares, como controles de puertas de garaje, sistemas de alarma, controles de calefacción, electrodomésticos y aparatos de cocina, así como equipos de telecomunicaciones como teléfonos, faxes, acceso a Internet, están cada vez más conectados en red y, si es posible, solo un control remoto. Muchos de los dispositivos mencionados pueden configurarse individualmente para diferentes usuarios y adaptarse a las preferencias del usuario respectivo. Utilizando el ejemplo de un receptor de televisión se explican algunas adaptaciones poco conocidas:

- se puede proporcionar una "seguridad para niños" que solo permite canales de televisión seleccionados y/o solo permite la recepción de televisión en momentos predefinidos;
- los hábitos de televisión pueden preprogramarse, por ejemplo, para que un determinado usuario vea ciertos programas en ciertos canales en ciertos días de la semana en ciertos momentos;
- para cada usuario, se puede crear una lista de canales de televisión preferidos, que se muestran como favoritos en un menú de selección;
- dependiendo del usuario y el dispositivo, se puede cambiar la asignación de botones de los botones en el control remoto;
- bajo demanda, se pueden proporcionar sistemas interactivos, tales como televisión interactiva, compras en el hogar, banca en el hogar, video o fusibles similares, por ejemplo, límites para ordenar productos o películas, tipos de películas (por ejemplo, calificación “G”), etc.

[**0007]** Por las razones anteriores, es necesario adaptar automáticamente el control remoto al usuario respectivo y configurar y activar una autorización de acceso individual.

[**0008]** Para este fin, se ha propuesto varias veces proporcionar al control remoto un dispositivo de identificación que detecte automáticamente a una persona autorizada para el acceso. Por ejemplo, el documento DE 198 58 310 B4 propone un lector de huellas digitales en el control remoto, que detecta los datos biométricos del usuario por medio de sensores y activa un perfil operativo individual cuando se reconoce a una persona autorizada para acceder.

[**0009]** Ya se han propuesto también otros dispositivos de registro de datos biométricos, tales como un circuito de reconocimiento de voz, un dispositivo de detección del iris y un dispositivo de reconocimiento facial (ver. WO 02/17627 A2).

[**0010]** La huella digital de una persona se utiliza particularmente con frecuencia para la identificación, por ejemplo en US 2001/007592 A1, US 2005/0149870 A1, US 5,758,257, US 5,771,307, US 5,920,642, US 6,020,882, US 6,130,726, US 6,137,539, US 6,914,517 B2, US 6,968,565 B1 o WO 01/56213 A1.

[**0011]** En todos estos mandos a distancia con reconocimiento de personas, existen los siguientes problemas:

- se ha de asegurar un alto nivel de seguridad, lo que implica que un dispositivo no puede ser operado por un control remoto extraño y que no se puede crear un nuevo usuario "sin autorización";
- la complejidad del hardware del control remoto debe ser lo más baja posible;

- el consumo de energía del control remoto debe ser lo más bajo posible;

- la comunicación entre el control remoto y el dispositivo debe ser "a prueba de golpes", por lo que es especialmente importante porque hay una variedad de controles remotos programables en el mercado, los cuales registran, graban y vuelven a emitir señales emitidas desde un control remoto original.

[**0012]** Para aumentar la seguridad, se han realizado varias propuestas. Por ejemplo, el documento US 2001/0007592 A1 sugiere consultar una secuencia de varias huellas digitales de diferentes dedos.

[**0013]** El documento EP 1 286 518 A2 propone equipar al menos un botón del control remoto con un lector de huellas digitales para que cada vez que se invoquen ciertas funciones, tales como cambiar canales, botón de confirmación o similares, se verifique al usuario autorizado.

[**0014]** Para aumentar la seguridad de acceso, se recomienda al solicitante en la solicitud de la anterior patente alemana 10 2006 042 014, no publicada anteriormente, proporcionar otro dispositivo de hardware adicional, además de un dispositivo de lectura de datos biométricos, en particular un lector de huellas digitales, con el fin de identificar el control remoto como tal, lo cual se realiza en la forma de realización ejemplar específica mediante una llamada tarjeta SIM. Esto significa que al menos la creación de un nuevo perfil de usuario o la modificación de un perfil de usuario existente solo es posible si la tarjeta SIM está insertada en el control remoto.

[**0015]** El objeto de la invención es mejorar el dispositivo multimedia mencionado anteriormente y el método para la transmisión de datos en un dispositivo multimedia del tipo mencionado de tal manera que con baja complejidad de hardware del control remoto, el dispositivo garantiza una alta seguridad de transmisión de los datos desde el control remoto.

[**0016]** Este objetivo se consigue para el dispositivo multimedia por la reivindicación 1 y para el método por las características indicadas en la reivindicación de patente 2.

[**0017]** Se describen realizaciones ventajosas y desarrollos adicionales de la invención en las reivindicaciones dependientes.

[**0018]** Brevemente, el objeto de la pieza de hardware reducido se logra en el sentido de que los datos biométricos del control remoto son detectados, transferidos al dispositivo y solo luego evaluados. La evaluación de los datos biométricos requiere una potencia de procesador relativamente alta, que ya está presente en el dispositivo, mientras que la adquisición de los datos biométricos, por ejemplo con un lector de huellas digitales, requiere solo una potencia de cálculo comparativamente menor, de modo que se puede utilizar un procesador más simple y, por lo tanto, menos costoso en el control remoto, que también tiene un menor requisito de potencia. La mayor seguridad de la transmisión de datos se garantiza mediante un cifrado especial de los datos transmitidos desde el control remoto al dispositivo, incluidos los datos almacenados en la tarjeta SIM.

[**0019]** A continuación, se explica en más detalle la invención en base a un modo de realización adjunto.

[**0020]** Se muestra:

Fig. 1	un diagrama de bloques de un dispositivo multimedia con control remoto y dispositivo multimedia;
Fig. 2	un diagrama de flujo de los pasos del procedimiento en la inicialización de una conexión entre el control remoto y el dispositivo;
Fig. 3	un diagrama de flujo de los pasos del procedimiento en un proceso de identificación

[**0021]** La figura 1 muestra un control remoto 1 que opera un dispositivo 2, en el que el dispositivo 2 puede operar, a su vez, una pluralidad de otros dispositivos, como se indicó anteriormente. En la Fig. 1 solo se muestran los módulos relevantes para el control.

[**0022]** El controlador remoto 1 incluye un microprocesador 3, una memoria 4, un lector de tarjetas SIM 5, un teclado 6 y un dispositivo 7 para la detección de los datos biométricos, en particular los medios para detectar una huella digital. Además, el control remoto contiene un transceptor 8, preferiblemente para enviar y recibir señales infrarrojas. Los módulos 4-8 mencionados están conectados al microprocesador 3.

[**0023]** La memoria 4 puede estar dividida en varios subgrupos y, por ejemplo, tiene una memoria de sólo lectura para los programas, y una memoria de trabajo. Una tarjeta SIM para ser insertada en el lector de tarjetas SIM 5 también contiene una o más memorias de una manera conocida per se. La unidad de transmisión/recepción 8 está conectada al dispositivo 2 a través de una conexión de radio inalámbrica bidireccional 9. El dispositivo 2 también contiene un microprocesador 10, una memoria 11, que también contiene una memoria de programa y una memoria de trabajo, y

otra memoria, que se denomina aquí la base de datos de usuario 12, y finalmente una unidad transmisora/receptora 13, que está conectada a la unidad transmisora/receptora 8 el control remoto está en conexión inalámbrica 9.

[**0024]** El microprocesador 10 tiene una salida 14, que está en conexión a través de una interfaz 15 con uno o más dispositivos que han de ser controlados.

[**0025]** En la interfaz 15, se pueden conectar cualquier número de diferentes dispositivos de control con medios de conexión conocidos, por ejemplo cable "SCART", terminal "USB" o similares.

[**0026]** Se puede hacer hincapié en que el microprocesador 3 del mando a distancia 1 tiene una potencia de cálculo más baja que el microprocesador 10 del dispositivo. También tiene un menor consumo de energía y es más barato.

[**0027]** Con referencia a la figura 2, ahora se describe la fase de inicialización. Primero, la tarjeta SIM debe insertarse en el lector de tarjetas SIM 5 de la figura 1 en un paso 20. La tarjeta SIM contiene los siguientes datos almacenados:

1. Un número de identificación personal (llamado PIN),
2. Datos personales de un usuario, como nombre, fecha de nacimiento, sexo, número de tarjeta de crédito, etc.,
3. una primera clave privada (PrivK 1), por la cual los datos mencionados en 2 y 3 solo son accesibles después de ingresar el PIN mencionado en 1.

[**0028]** Además, la tarjeta SIM contiene los siguientes datos de libre acceso:

4. una segunda clave privada (PrivK 2),
5. un código de identificación personal (PIC),
6. una primera clave pública (PubK 1) y
7. una segunda clave pública (PubK 2).

[**0029]** Como se explica en más detalle a continuación, las teclas PubK 1 y PrivK 1 formarán un primer par y las teclas PubK 2 y PrivK 2 un segundo par de claves utilizadas para el cifrado y el descifrado. Se usa una llamada criptografía asimétrica, en donde se usa una clave de uno de los pares mencionados, generalmente la llamada clave pública, para cifrar datos y la otra clave del par, generalmente la llamada clave privada, se usa para descifrado. Por lo tanto, se utilizan diferentes claves para el cifrado y descifrado. No es posible descifrar datos con la clave que se usó para el cifrado. Los algoritmos para el cifrado y descifrado son conocidos en principio. Por ejemplo, se hace referencia a los algoritmos de cifrado asimétrico RSA, el criptosistema Rabin o el criptosistema Elgamal. Después de insertar la tarjeta SIM, primero se consulta el PIN (Paso 21), que se ingresa a través del teclado 6 (Fig. 1) y generalmente es un número de cuatro dígitos. La tarjeta SIM ahora está desbloqueada y se puede acceder a los datos personales mencionados anteriormente mediante el PIN y la primera clave privada PrivK 1.

[**0030]** El control remoto transmite entonces la primera clave privada PrivK 1 (Paso 22) y la segunda clave pública PubK 2 (Paso 24) al dispositivo 2 a través del dispositivo de transmisión/recepción 8, en donde son recibidas por la unidad de emisión/recepción 13 y son almacenadas en la memoria 11 a través del microprocesador 10 (pasos 22-25). A continuación, los datos biométricos del usuario se leen a través del dispositivo de lectura de huellas dactilares 7 (Paso 27) y se transmiten al dispositivo 2 (Paso 28), donde se cifran con la clave pública PubK 2 recibida y almacenada previamente (Paso 29). Del mismo modo, el código de identificación personal PIC se consulta desde la tarjeta SIM y se transmite al dispositivo 2 (Paso 30), donde también se cifra con la clave pública PubK 2 (Paso 31). Los datos personales del usuario se consultan desde la tarjeta SIM o se ingresan a través del teclado y se transmiten al dispositivo 2 (Paso 32), donde también se cifran con la segunda clave pública PubK 2 en el paso 33.

[**0031]** La segunda clave pública PubK 2, que se ha registrado en la unidad 2 en el paso 25, es borrada en el paso 34 después de esta operación. A partir de los datos almacenados y parcialmente encriptados, se crea un perfil de usuario y se almacena en la base de datos de usuarios 12, que inicialmente contiene los siguientes datos:

- la primera clave privada no encriptada PrivK 1,
- los datos biométricos del usuario encriptados con la clave PubK 2,
- los códigos de identificación personal (PIC) encriptados y los datos personales encriptados, cada uno encriptado con PubK 2.

[**0032]** Además, el usuario puede añadir datos adicionales a los datos personales, tales como la lista de canales de canales de televisión preferidos, asignaciones de las teclas de los botones del mando a distancia, canales de televisión bloqueados, tiempos de televisión, etc.

[**0033]** El proceso de inicialización descrito es hasta ahora clasificado como crítico, ya que la primera clave privada PrivK 1 se transmite de forma inalámbrica y, por lo tanto, se puede "escuchar" si un dispositivo receptor adecuado está dentro del alcance. Sin embargo, en el caso de la transmisión infrarroja, el riesgo es muy pequeño de que un dispositivo receptor adecuado esté dentro del alcance, ya que el alcance es muy limitado y se requiere una línea de visión sin obstáculos.

[**0034]** Posteriormente, sin embargo, existe alta seguridad, porque el resto de los datos se cifran con la clave pública PubK 2, la cual se elimina después de la inicialización en el dispositivo 2 y estos datos no pueden ser descifrados con la primera clave privada PrivK 1.

[**0035]** Para aumentar aún más la seguridad, también se puede eliminar la clave PrivK 1 en la tarjeta SIM para que pueda configurarse como "privada", ya que será la única disponible con esta unidad.

[**0036]** En relación con la Fig. 3, se describirá ahora el proceso de identificación normal con el que se construye una conexión entre el controlador remoto 1 y el aparato inicializado 2. Se supone que el control remoto 1 está listo para enviar y el dispositivo 2 está listo para recibir.

[**0037]** En un Paso 35, se leen los datos biométricos del usuario, por ejemplo, cuando el usuario pone un dedo en el lector de huellas digitales 7, el cual lee los conjuntos de datos de imagen correspondientes. Estos datos de imagen se pueden comprimir en un paso 35, lo cual tiene lugar de acuerdo con métodos de compresión de datos conocidos, como p. ej. el código Huffman.

[**0038]** En un Paso 37, el código de identificación personal PIC se agrega a estos datos de imagen comprimidos y se lee desde la tarjeta SIM o la memoria 4 (Fig. 1). En el Paso 38, también se agrega la segunda clave privada PrivK 2, que también se lee desde la tarjeta SIM o la memoria 4. Este conjunto de datos consta de los datos biométricos comprimidos, el PIC y la clave PrivK 2. Este conjunto de datos se cifra con la primera clave pública PubK 1 en un Paso 39. Además, se puede llevar a cabo una codificación de bloque y una llamada corrección de errores hacia adelante (FEC para abreviar) (Paso 40).

[**0039]** A continuación, los datos así generados se transmiten a la unidad 2 a través del enlace de radio 9 (Paso 41) y son recibidos por el dispositivo 2 (Paso 42). Allí, estos datos se descifran primero con la clave privada PrivK 1 almacenada en la base de datos del usuario (Paso 43), de la que se obtiene un registro de datos con PrivK 2, PIC y los datos biométricos (bloque 44), de los cuales en el paso 45 se obtiene la segunda clave privada PrivK 2. Los datos biométricos y el PIC se almacenan temporalmente en la memoria de trabajo 11. Con la segunda clave privada ahora descifrada y extraída PrivK 2, los datos son almacenados en la base de datos de usuario 12 y cifrados con la clave pública PubK 2 antes de almacenarse, es decir, el PIC, los datos biométricos y los datos personales, se descifran y, en el paso siguiente 47, los datos ahora descifrados de la base de datos del usuario y los datos recibidos se comparan entre sí. Por conveniencia, el PIC se compara primero. Si no hay coincidencia, los datos recibidos no provienen de un control remoto autorizado, por lo que se pueden interrumpir otros pasos de trabajo. Si es necesario, se puede generar una solicitud de transmisión repetida, que se muestra, por ejemplo, en una pantalla del televisor o se transmite como una señal de retorno a través del enlace de radio 9 al control remoto 1 y se muestra allí.

[**0040]** Cuando un control remoto autorizado realiza una comparación de la PIC, los datos biométricos se comparan (Paso 47) y, si coinciden, el microprocesador 10 emite una señal de habilitación a su salida 14 a la interfaz 15 (Paso 48). El control remoto 1 puede llevar a cabo una operación segura y autorizada del dispositivo 2 y los otros dispositivos conectados a él. Además, la asignación de teclas de las teclas 6 del control remoto 1 también se puede determinar de acuerdo con el usuario identificado a través del enlace de radio 9. Además, una señal de reconocimiento para un inicio de sesión exitoso a través del enlace de radio 9 del control remoto transmitido, borra la información sensible en el control remoto en la memoria 4, en particular los datos biométricos detectados. De manera similar, los datos que se comparan entre sí también se eliminan en la memoria 11 del dispositivo, de modo que las memorias 11 y 4 del control remoto 2 y el dispositivo 1 vuelven a su estado inicial después del registro exitoso. El funcionamiento normal entre el control remoto 1 y el dispositivo 2 se puede iniciar, lo que también puede ser bidireccional.

[**0041]** Por razones de seguridad, también puede estar previsto que la conexión autorizada después de un tiempo predeterminado se interrumpa y un nuevo registro se realice de acuerdo con los pasos descritos en relación con la Fig. 3. También se puede prever la realización de una nueva identificación para ciertos procesos de control relacionados con la seguridad, por ejemplo, cuando se transmite el nombre, la dirección o el número de tarjeta de crédito a través de dispositivos de comunicación conectados.

[**0042]** En la inicialización descrita en los pasos descritos anteriormente en relación con la Fig. 2, pueden también asignarse derechos de usuario con los datos personales del usuario, por ejemplo, con respecto a la introducción o modificación de los perfiles de usuario, de modo que por ejemplo, sólo ciertas personas, identificadas en los datos biométricos del usuario estén autorizadas para crear nuevos usuarios en la base de datos de usuarios o para cambiar los derechos asignados a usuarios individuales específicos. Se puede también realizar determinaciones con respecto a otros datos, que también se almacenan en los datos personales, de tal manera que el usuario individual pueda cambiarlos después de la identificación, p. ej., la asignación de teclas del control remoto, lista de favoritos de canales de TV individuales, en la medida en que se lanzan.

[**0043]** En resumen, la invención logra un nivel muy alto de seguridad. Incluso si el dispositivo llega a manos de personas no autorizadas sin una tarjeta SIM, no es posible acceder a los datos biométricos protegidos ni a los datos personales protegidos. Solo si una persona no autorizada tiene el dispositivo y la tarjeta SIM disponibles, teóricamente

es posible descifrar los datos protegidos almacenados en la base de datos del usuario con la primera clave PubK 1 almacenada en la tarjeta SIM. Para hacer esto, el usuario debe tener acceso directo a la base de datos de usuarios, lo que requiere un alto nivel de esfuerzo técnico. El fabricante puede prever aquí que la memoria correspondiente esté protegida de tal manera que no es posible el acceso externo o que su contenido se elimina automáticamente cuando se intenta expandir la memoria. En cualquier caso, es recomendable borrar la memoria que contiene la base de datos del usuario antes de entregar el dispositivo a terceros.

REIVINDICACIONES

1. Un dispositivo multimedia con un control remoto (1), que comprende:

- un primer microprocesador (3),
- un primer dispositivo de hardware (5) para identificar el control remoto (1),
- un segundo dispositivo de hardware (7) para detectar datos biométricos de una persona, y
- un dispositivo de transmisión (8) para transmitir datos, y con un aparato multimedia (2) que comprende
- un dispositivo de recepción (13) para recibir los datos,
  una memoria (11, 12) y
  un segundo microprocesador (10),

caracterizado porque
el primer dispositivo de hardware es una tarjeta SIM (5) en donde se almacenan los siguientes datos:

- un primer par de códigos digitales (PubK 1, PrivK 1),
- un segundo par de códigos digitales (PubK 2, PrivK 2),
- un código de identificación personal (PIC),

y los datos personales de al menos un usuario, porque la memoria (12) del aparato multimedia (2) lleva a cabo los siguientes datos almacenados después de una primera inicialización:

- solo un código (PrivK 1) del primer par de códigos digitales,
- solo un código (PubK 2) del segundo par de códigos digitales, datos biométricos y datos personales de un usuario, así como el código de identificación personal (PIC) codificado con el único código (PubK 2) del segundo par de códigos digitales,

porque el segundo dispositivo de hardware (7) lee en los datos biométricos del usuario una conexión establecida entre el control remoto (1) y el aparato multimedia (2),
les agrega el código de identificación personal (PIC) y el otro código (PrivK 2) del segundo par de códigos digitales,
codifica un paquete de datos formado de esta manera con el otro código (PubK 1) del primer par de códigos digitales y transmite el conjunto de datos codificado de esta manera al dispositivo multimedia (2),
porque el dispositivo multimedia (2) decodifica el conjunto de datos codificado recibido con el código almacenado (PrivK 1) del primer par de códigos digitales,
extrae de él el otro código (PrivK 2) del segundo par de códigos digitales, el código de identificación personal (PIC) y los datos biométricos,
extrae de la memoria (12) los datos biométricos codificados, los datos personales codificados y el código de identificación personal (PIC) codificado y los decodifica con el otro código (PrivK 2) del segundo par de códigos digitales, compara el código de identificación personal recibido y decodificado y el código de identificación personal almacenado y decodificado entre sí y, si se acuerda, compara los datos biométricos decodificados recibidos y los datos biométricos decodificados almacenados entre sí y solo borran el aparato multimedia (2) previo acuerdo.

2. Un proceso para la transmisión de datos en un dispositivo multimedia de acuerdo con la reivindicación 1 con los siguientes pasos del proceso:

Almacenamiento de un primer código (PrivK 1) de un primer par de códigos digitales en una memoria de un dispositivo multimedia, almacenamiento de datos de usuario codificado con un primer código (PubK 2) de un segundo par de códigos digitales cuyos datos contienen datos biométricos, un código de identificación personal (PIC) y datos personales,
Lectura en datos biométricos de un usuario en un control remoto,
Agregar un código de identificación personal (PIC) desde una memoria, además de agregar un segundo código (PrivK 2) del segundo par de códigos digitales para formar un conjunto de datos, codificando este conjunto de datos con el segundo código del primer par de códigos digitales,
Transmitir el conjunto de datos codificado de esta manera a un dispositivo multimedia,
Decodificar el conjunto de datos recibidos con el primer código almacenado (PrivK 1) del primer par de códigos digitales,
Extraer componentes (PrivK 2, PIC, datos biométricos) del conjunto de datos codificados,
Decodificar los datos codificados almacenados en la memoria del dispositivo multimedia con el segundo código extraído y decodificado del segundo par de códigos digitales,
Comparar el código de identificación recibido y decodificado con el código de identificación personal almacenado y decodificado y, previo acuerdo,

Comparar los datos biométricos decodificados recibidos con los datos biométricos decodificados almacenados y
Borrar el dispositivo multimedia si la comparación de los datos biométricos resulta en un acuerdo.

3. El proceso de acuerdo con la reivindicación 2, **caracterizado porque** los datos biométricos leídos en el control remoto se comprimen antes de la formación del conjunto de datos.

4. El proceso de acuerdo con la reivindicación 3, **caracterizado porque** la compresión tiene lugar de acuerdo con el código Huffman.

5. El proceso de acuerdo con una de las reivindicaciones 2 a 4, **caracterizado porque** el conjunto de datos a transmitir desde el control remoto al dispositivo multimedia está codificado en bloque.

6. El proceso de acuerdo con una o más de las reivindicaciones 2 a 5, **caracterizado porque** el conjunto de datos que se transmitirá desde el control remoto al dispositivo multimedia está provisto de una corrección de errores hacia adelante.

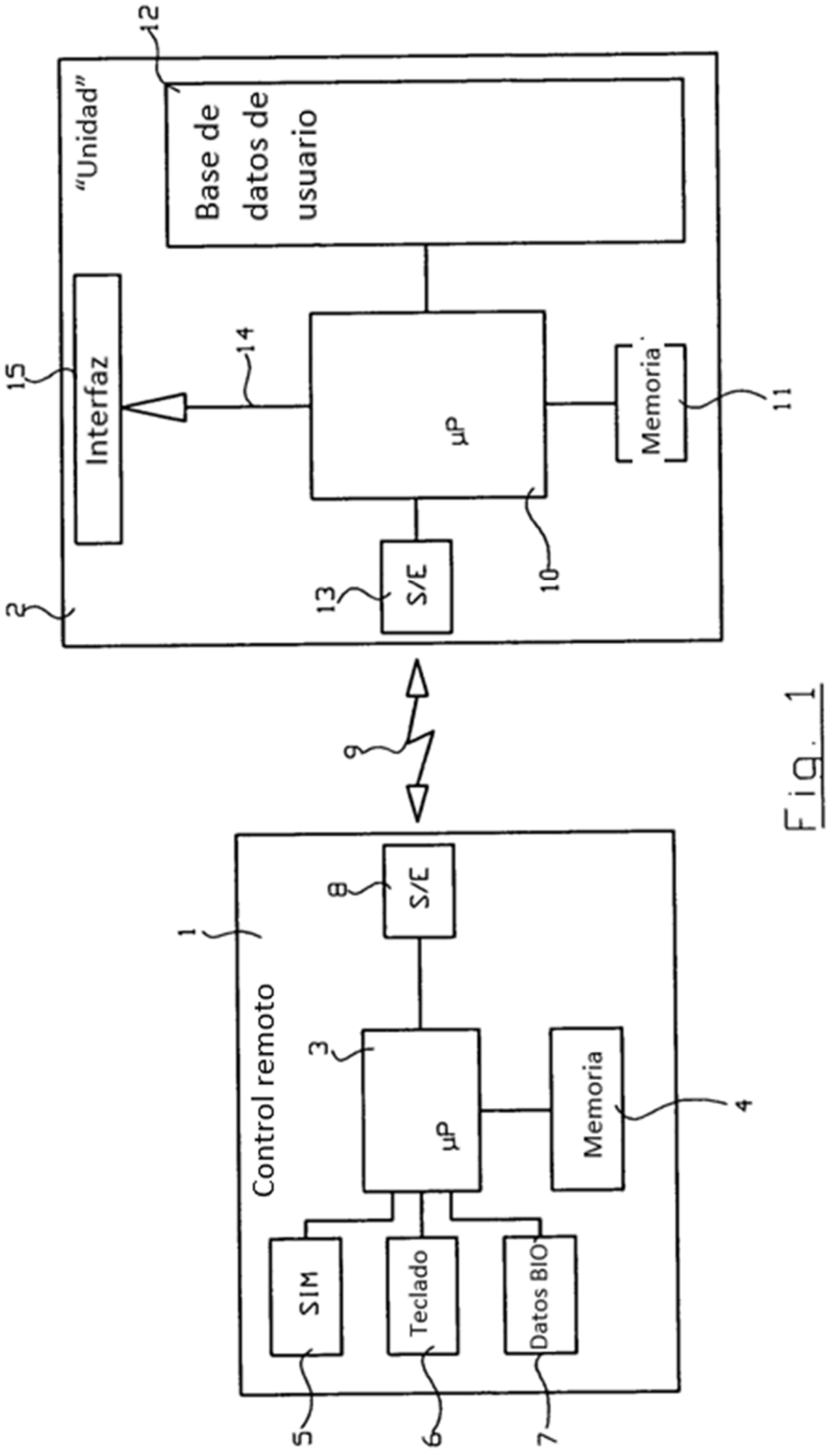
"Unidad"
Base de datos de usuario
Interfaz
μP
Memoria
S/E
Control remoto
μP
Memoria
S/E
SIM
Teclado
Datos BIO
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Fig. 1

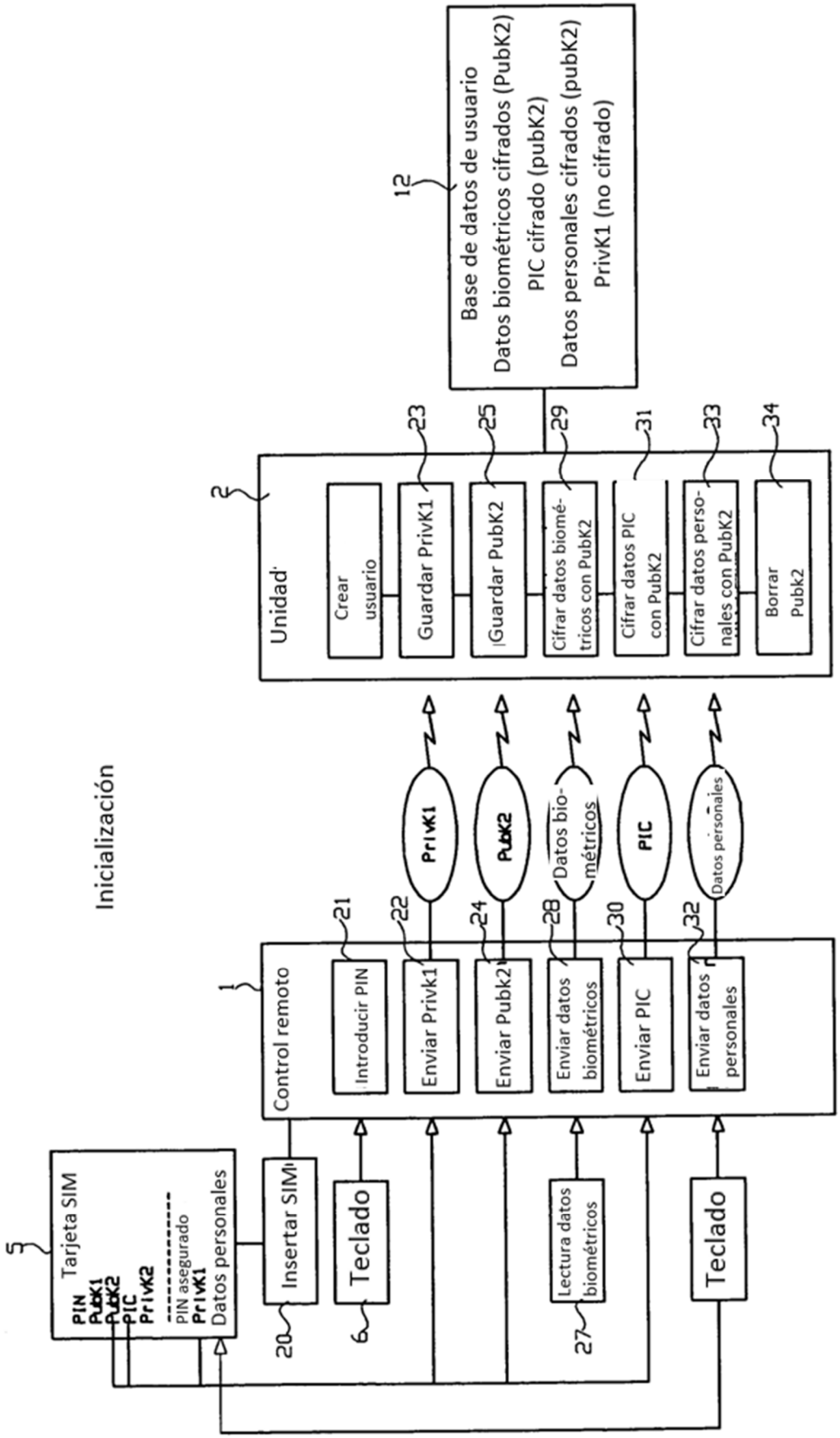
Inicialización
5
Tarjeta SIM
PIN
PubK1
PubK2
PIC
PrivK2
PIN asegurado
PrivK1
Datos personales
Insertar SIM
20
Teclado
6
1
Control remoto
21
Introducir PIN
22
Enviar Privk1
24
Enviar Pubk2
28
Enviar datos biométricos
30
Enviar PIC
32
Enviar datos personales
PrivK1
PubK2
Datos biométricos
PIC
Datos personales
Lectura datos biométricos
27
Teclado
2
Unidad
Crear usuario
23
Guardar PrivK1
25
Guardar PubK2
29
Cifrar datos biométricos con PubK2
31
Cifrar datos PIC con PubK2
33
Cifrar datos personales con PubK2
34
Borrar Pubk2
12
Base de datos de usuario
Datos biométricos cifrados (PubK2)
PIC cifrado (pubK2)
Datos personales cifrados (pubK2)
PrivK1 (no cifrado)

Fig.2

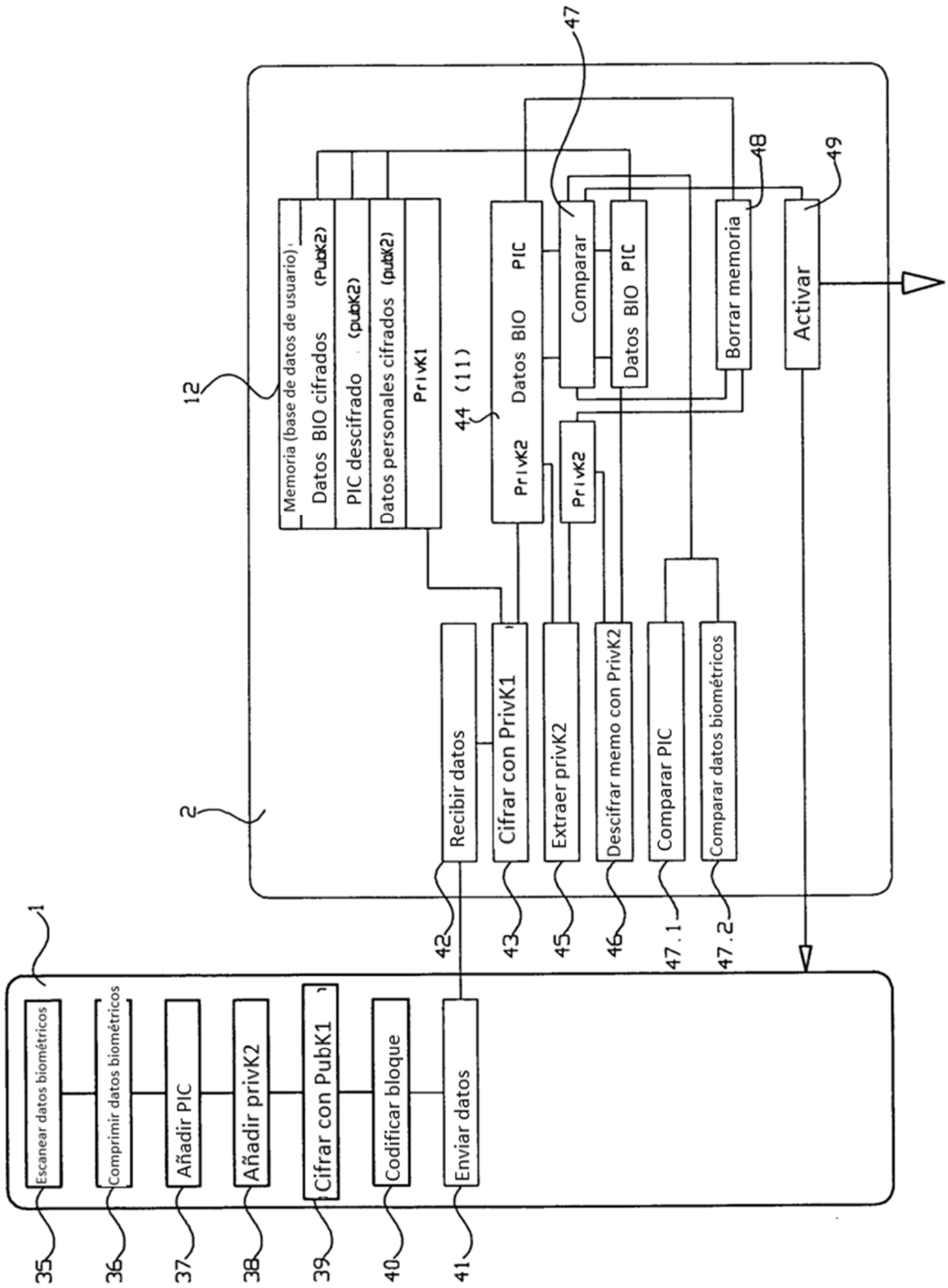
1
2
12
Escanear datos biométricos
Comprimir datos biométricos
Añadir PIC
Añadir privK2
Cifrar con PubK1
Codificar bloque
Enviar datos
35
36
37
38
39
40
41
Recibir datos
Cifrar con PrivK1
Extraer privK2
Descifrar memo con PrivK2
Comparar PIC
Comparar datos biométricos
42
43
45
46
47.1
47.2
Memoria (base de datos de usuario)
Datos BIO cifrados (PubK2)
PIC descifrado (pubK2)
Datos personales cifrados (pubK2)
PrivK1
44 (11)
PrivK2
Datos BIO PIC
PrivK2
47
Comparar
Datos BIO PIC
48
Borrar memoria
49
Activar

Fig. 3