(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 550 366**

(51) Int. CI.:

***H04W 12/02*** (2009.01)
***H04W 12/04*** (2009.01)
***H04L 29/06*** (2006.01)
***G07F 7/10*** (2006.01)
***G06Q 20/32*** (2012.01)
***G06Q 20/34*** (2012.01)
*H04W 8/20* (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.11.2009 E 09175772 (4)**

(97) Fecha y número de publicación de la concesión europea: **01.07.2015 EP 2190232**

(54) Título: **Procedimiento para proporcionar datos en al menos una zona de una tarjeta electrónica**

(30) Prioridad:

**14.11.2008 DE 102008057464**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**06.11.2015**

(73) Titular/es:

**VODAFONE HOLDING GMBH (100.0%)**
**MANNESMANNUFER 2**
**40213 DÜSSELDORF, DE**

(72) Inventor/es:

**LINDEN, HOLGER;**
**MÜLLER, FRANK;**
**DOHMANN, DIERK y**
**VARELMANN, KERSTIN**

(74) Agente/Representante:

**LÓPEZ CAMBA, María Emilia**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Procedimiento para proporcionar datos en al menos una zona de una tarjeta electrónica.

La invención se refiere a un procedimiento para proporcionar datos en al menos una zona de una tarjeta electrónica, principalmente en una tarjeta SIM, y preferiblemente segura.

En los sistemas de telecomunicaciones modernos, los accesos a los recursos de comunicación disponibles están administrados por distintos usuarios desde distintas redes de comunicación mediante el uso de tarjetas SIM (SIM: Subscriber Identity Module, Módulo de Identidad de los Suscriptores).
Si otras partes, por ejemplo, operadores de red distintos, quieren tener acceso a la tarjeta SIM, entonces deben proporcionarse mecanismos mediante los cuales se garantice la seguridad ante las escuchas. Por tanto, para la siguiente generación de tarjetas SIM se prevén diferentes zonas en la tarjeta SIM.

Una posible división podría ser la siguiente: una primera zona es la llamada zona TSD (Trusted Third Party Security Domain). Esta zona podrían utilizarla los llamados Terceros de Confianza (Trusted Third Parties, TTP), por ejemplo las empresas, que hayan firmado un contrato con un operador de red y por ello hayan obtenido derecho de acceso. Una segunda zona es la llamada zona ISD (Issuer Security Domain), a la que solo puede tener acceso el operador de la red. Es de suponer que en el futuro habrá más TSD en una tarjeta SIM, para que puedan coexistir más TTP. Además, la zona TSD puede dividirse en subzonas SPSD (Service Provider Security Domain), por lo que puede haber más subzonas similares por TSD. La SPSD está pensada para proveedores de servicios, es decir, empresas, que disponen de aplicaciones, como la llamada banca electrónica, en su tarjeta SIM.
Por eso es necesario cumplir con determinadas condiciones de seguridad.

Varios comités de normalización, como la GSMA (Asociación GSM) dan diversas recomendaciones, por ejemplo, que el acceso a una zona aislada debe realizarse de un modo seguro. Cuando una de las partes de la zona, por ejemplo, un operador de la red en la zona ISD o un TTP en la zona TD o un proveedor de servicios en la zona SPSD quiera participar, entonces debe garantizarse que las partes no pueden interceptarse unas a otras. El consejo que da la GSMA al respecto es que cada parte obtenga una clave directamente de un fabricante de tarjetas SIM, con la que pueda acceder a su zona asignada. Técnicamente hablando, esto quiere decir que el fabricante de tarjetas SIM, junto a la interfaz existente actualmente, debe mantener al operador de red aún más interfaces a los TTP y a los proveedores de servicios. Como cada tarjeta SIM está provista de una clave, se deben preparar, por ejemplo, para una ISD, 5 TSD y 10 SPSD por TSD unas 56 claves para cada tarjeta SIM. Para un aproximado de 30 millones de usuarios, de deben preparar, gestionar y distribuir 1,68 mil millones de claves independientes entres sí, lo que va unido a unos costes muy elevados.

Por ejemplo, los documentos US 2008/0162715 y EP 1 860 840 A2 muestran procedimientos para la personalización de un módulo de seguridad.

Por tanto, la tarea de la invención es la de desvelar un procedimiento para proporcionar datos en al menos una zona de una tarjeta electrónica, principalmente en una tarjeta SIM, que no presenta el inconveniente mencionado anteriormente, particularmente eficaz, sencillo y que se activa con una cantidad mínima de claves independientes.

Esta tarea se resuelve mediante la característica de la reivindicación independiente 1. En las reivindicaciones dependientes se muestran otras formas de realización ventajosas de la invención.

El procedimiento objeto de la invención para proporcionar datos en al menos una zona de una tarjeta electrónica, principalmente en una tarjeta SIM, y preferiblemente segura se caracteriza por las siguientes etapas:

- Entrega de un código de encriptación desde una primera posición a una segunda posición,
- Entrega de un código de descodificación correspondiente al código de encriptación desde la primera posición a la tarjeta electrónica,
- Utilización del código de encriptación para la generación de un registro encriptado de un registro,
- Entrega del registro encriptado en una tercera posición,
- Transferencia del registro encriptado a la al menos una zona de una tarjeta electrónica,
- Utilización del código de descodificación para descodificar el registro encriptado del registro a la tarjeta electrónica.

La parte esencial del procedimiento objeto de la invención es que un código de encriptación se transmite desde la primera posición exclusivamente a una segunda posición, que a su vez encripta un registro. La transferencia de dicho registro encriptado a la tarjeta electrónica se llevará a cabo entonces desde la tercera posición.
Por lo tanto se realiza una separación entre la encriptación y la transmisión de los datos encriptados en la tarjeta electrónica. En el contexto de la invención, el término "Código de encriptación" denota una clave criptográfica creada de forma arbitraria.
En el caso del código de descodificación puede tratarse de una regla de descodificación criptográfica. Mediante el código de descodificación se generará el registro encriptado a partir del registro, por ejemplo, con la ayuda de una función o un algoritmo matemáticos. Con la ayuda del código de descodificación se produce una transformación

inversa del registro encriptado en el registro, que puede leer cualquier usuario y/o puede procesarse en la tarjeta electrónica. Mediante el procedimiento objeto de la invención se puede proporcionar el código de encriptación a la primera posición, por ejemplo, un fabricante de tarjetas electrónicas, y hasta a una segunda posición, por ejemplo, un proveedor de servicios.

Este código de encriptación permite que la segunda posición encripte las informaciones que le gustaría tener almacenadas en la tarjeta electrónica.

Mediante la transmisión del registro encriptado, la tercera posición, que puede tratarse de un tercero de confianza (TTP) o un operador de red, no podrá cambiar ni leer este registro. Más bien, la tercera posición se utiliza para la transmisión del registro encriptado a la al menos una zona de la tarjeta electrónica. La tercera posición incluso puede acceder a la tarjeta electrónica, pero no al registro. Por el contrario, la segunda posición puede encriptar el registro mediante el código de encriptación, pero no puede acceder a la tarjeta electrónica. De este modo se produce una reducción del número de aquellas claves gracias a la invención. La tarjeta electrónica puede ser, principalmente, una tarjeta SIM (SIM: Subscriber Identity Module). El procedimiento objeto de la invención se ha encontrado especialmente ventajoso en su uso en las tarjetas SIM de los teléfonos móviles.

Una realización ventajosa del procedimiento objeto de la invención se caracteriza por el siguiente paso:

- Entrega de una primera clave de acceso desde la primera posición hasta la tercera posición.

En el marco de las reivindicaciones de la presente invención se entregará una clave de la primera posición a la tercera. Al contrario que el código de encriptación, se trata de una clave de acceso. Esta clave de acceso, por lo tanto, no sirve para encriptar un registro. La ventaja es que esta clave de acceso se usará para el siguiente paso del procedimiento:

- Utilización de la primera clave de acceso para acceder a una primera zona segura de la tarjeta electrónica mediante la transferencia del registro encriptado.

La clave de acceso permite a la tercera posición grabar el registro encriptado en una primera zona segura de la tarjeta electrónica. Esta primera zona segura solo puede abrirse mediante la clave de acceso. De ese modo, la segunda posición no puede colocar el registro encriptado directamente en la tarjeta electrónica. Más bien, es necesario que la tercera posición, que posee la primera clave de acceso, guarde el registro encriptado en la primera zona segura. La primera zona segura puede ser parte de estas zonas de la tarjeta electrónica, en la que los datos se almacenan, de acuerdo con la invención.

Otra realización ventajosa del procedimiento objeto de la invención se caracteriza por el siguiente paso:

- Entrega de una segunda clave de acceso desde la primera posición a la segunda posición.

En el marco de los pasos de este procedimiento, la segunda posición se preparará una segunda clave de acceso. De nuevo, no se trata, al igual que el caso de la primera clave de acceso, de un código de encriptación.

En el marco de otra realización ventajosa, se prevé el siguiente paso en el procedimiento:

- Adición de la segunda clave de acceso al registro antes de la utilización del código de encriptación para la generación de un registro encriptado.

En el marco de este paso, la segunda clave de acceso se trasladará con el registro tras la utilización del código de encriptación en el registro encriptado. El registro encriptado ya no incluye exclusivamente el registro, sino también la segunda clave de acceso. El registro encriptado conseguido de este modo puede ser transmitido desde la tercera posición a la tarjeta electrónica. Aún así, mediante la encriptación con el código de encriptación, la tercera posición no puede acceder a la segunda clave de acceso.

En el marco de otra realización ventajosa, se prevé el siguiente paso en el procedimiento:

- Utilización de la segunda clave de acceso para acceder a una segunda zona segura de la tarjeta electrónica tras la utilización del código de descodificación para descodificar el registro encriptado por el registro en la tarjeta electrónica.

La segunda clave de acceso transmitida mediante el registro encriptado a la tarjeta electrónica sirve así para acceder a la segunda zona segura de la tarjeta electrónica. Esta segunda zona segura puede estar ubicada en la primera zona segura o en la zona de la tarjeta electrónica. Por lo tanto, se necesita la primera clave de acceso para que la tercera posición pueda transmitir el registro encriptado en la primera zona segura. Ahí puede darse una descodificación del registro encriptado mediante el código de descodificación. La segunda clave de acceso extraída permite la apertura de la segunda zona segura, para transmitir el registro en esta segunda zona segura. Después de la descodificación del registro encriptado en la tarjeta electrónica, la tercera posición sigue sin poder introducirse en

la segunda zona segura, a pesar de poseer la primera clave de acceso, ni puede conseguir el registro desencriptado.

Otra realización ventajosa del procedimiento objeto de la invención se caracteriza por el siguiente paso:

- Entrega de un único código de encriptación y el código único de descodificación correspondiente al código de encriptación para una pluralidad de tarjetas electrónicas.

Este paso del procedimiento presenta la ventaja de que se puede reducir claramente el número de códigos de encriptación y de descodificación. Solo se necesita un único o una pequeña cantidad de códigos de encriptación que se transmitirían a la segunda posición o se depositarían en la tarjeta electrónica. De este modo se reduce significativamente el número total de códigos de encriptación y descodificación necesarios para facilitar los datos a al menos una zona preferiblemente segura de una tarjeta electrónica. En lo sucesivo, no es necesario poner para cada tarjeta electrónica un par único de códigos de encriptación y descodificación.

Para elevar la seguridad del procedimiento objeto de la invención, se ha destacado el siguiente paso en el procedimiento como ventajoso:

- Entrega de una primera clave de acceso asignada exclusivamente a una tarjeta electrónica y/o una segunda clave de acceso asignada exclusivamente a una tarjeta electrónica.

Al contrario que el código de encriptación, la primera y/o segunda claves de acceso se adjudicarán individualmente a una tarjeta electrónica. De este modo cada parte puede acceder únicamente a la tarjeta electrónica o a la zona segura de la que poseen la clave de acceso correspondiente.

Una realización ventajosa de la invención se caracteriza porque la tarjeta electrónica se trata de una tarjeta SIM.

Otras ventajas, características y detalles de la invención se presentan en la siguiente descripción, que se explica con la referencia a los dibujos de los ejemplos de realización de la invención. Las características mencionadas en las reivindicaciones y en la descripción pueden considerarse de forma individual o en combinaciones esenciales para la invención. Las figuras muestran lo siguiente:

Figura 1 una representación esquemática de una tarjeta electrónica,
Figura 2 una representación esquemática de los pasos del procedimiento para la facilitación de los datos en la tarjeta electrónica,
Figura 3 otra realización del procedimiento objeto de la invención y
Figura 4 una realización adicional del procedimiento objeto de la invención.

El procedimiento objeto de la invención sirve para proporcionar datos en al menos una zona de una tarjeta electrónica, principalmente en una tarjeta electrónica, y preferiblemente segura. En el marco de la siguiente descripción se asume que la tarjeta electrónica es una tarjeta SIM (SIM: Subscriber Identity Module). En consecuencia, los términos tarjeta electrónica y tarjeta SIM se utilizarán como sinónimos. Sin embargo, esto no debe considerarse como una limitación, sino como una aclaración de la invención.

En la Figura 1 se representa una tarjeta SIM 10. Esta tarjeta SIM (10) puede utilizarse, por ejemplo, en un teléfono móvil 11. La tarjeta SIM 10 sirve en ese caso para la identificación del usuario del teléfono móvil 11 en una red móvil terrestre. En el ejemplo de la realización, la tarjeta SIM 10 presenta una zona 45 en la que los datos y/o códigos se pueden depositar y/o consultar. Una parte de esta zona 45 presenta una primera zona segura 50, así como cuatro segundas zonas seguras 55. En el marco del procedimiento objeto de la invención se prepararán los datos en la primera zona segura 50 y/o en la segunda zonta segura 55. El procedimiento objeto de la invención así aprovechado se explica en la Figura 2.

Una primera posición 20 pone a disposición de una segunda posición 30 un código de encriptación c1.
La primera posición 20 puede tratarse de un fabricante de tarjetas SIM, que distribuye el código de encriptación c1 a la segunda posición 30. Esta segunda posición 30 puede tratarse de un proveedor de servicios que quiere ofrecer a determinados clientes la tarjeta SIM 11. Así, se puede pensar, por ejemplo, que la segunda posición 30 sea un fabricante de tarjetas de crédito y/o una empresa ferrocarrilera, que distribuyen su aplicación en la tarjeta SIM 10 y quieren transmitir los datos correspondientes a esta última. En el marco del primer paso del procedimiento, esta segunda posición 30 solo transmitirá la clave c1.
De forma paralela, la primera posición 20 puede transmitir un código de encriptación c2 correspondiente a la tarjeta SIM 10. Si la primera posición 20 se trata del fabricante de tarjetas SIM, es posible integrar directamente el código de encriptación c2 en la tarjeta SIM 10.

Con la ayuda del código de encriptación c1, la segunda posición 30 puede realizar una encriptación 100 de un registro DS. El registro DS puede tratarse, por ejemplo, de información que la segunda posición 30 necesite para su

aplicación en la tarjeta electrónica 10. Mediante la encriptación 100 del registro DS con el código de encriptación c1 se generará un registro encriptado VDS.
Este registro encriptado VDS se transmitirá a una tercera posición 40. La tercera posición 40 puede tratarse de un operador de red o de otra posición de confianza, que sirva como transmisor del registro encriptado VDS de la segunda posición 30 a la tarjeta electrónica 10. En el marco del procedimiento que se muestra en la Figura 2, la tercera posición 30 sirve así como transmisora del registro encriptado VDS a la al menos una zona 45 de la tarjeta electrónica 10. En la tarjeta electrónica 10 se puede proporcionar de forma automática y/o mediante una señal externa una descodificación 110 del registro encriptado VDS mediante la clave c2. Después de la utilización del código de descodificación c2, en la tarjeta electrónica 10 se encuentra el registro DS en forma encriptada.

Otra realización ventajosa del procedimiento objeto de la invención se muestra en la Figura 3.
De nuevo, la primera posición 20 transmite el código de encriptación c1 a la segunda posición 30. Este código sirve para encriptar 100 el registro DS. El registro encriptado VDS conseguido de este modo se transmitirá a la tercera posición 40. Como complemento al paso del procedimiento que se muestra en la Figura 2, la primera posición 20 transmite una primera clave de acceso k1 a la tercera posición 40. Esta primera clave de acceso k1 permite a la tercera posición 40 acceder a una primera zona segura 50 de la tarjeta electrónica 10. Esta primera zona segura 50 puede coincidir o ser una parte de la zona 45. En el ejemplo mostrado, la primera zona segura 50 comprende la totalidad de la zona 45 de la tarjeta SIM 10. Sin la primera clave de acceso k1 no es posible la transmisión del registro encriptado VDS a la tarjeta electrónica 10. Entonces, la tercera posición 40 solo puede acceder mediante la primera clave de acceso k1 a la primera zona segura 50. De este modo, queda garantizada una mayor protección de la información y/o los registros encriptados y/o los registros depositados en la primera zona 50. En cambio, se produce de forma automática y/o mediante una señal externa la activación de una descodificación 110 del registro encriptado VDS con la ayuda del código de descodificación c2. El registro descodificado DS resultante puede almacenarse a continuación en la primera zona segura 50. Esta realización se caracteriza porque, por un lado, la segunda posición 30 permite la encriptación 100 del registro DS mediante el código de encriptación c1, pero por otro lado no se integra el registro encriptado VDS en la primera zona segura 50. Además, la tercera posición 40 puede transmitir el registro encriptado VDS con la ayuda de la primera clave de acceso k1 a la primera zona segura 50. Sin embargo, la tercera posición 40 no puede descodificar el registro encriptado VDS, ya que la tercera posición 40 no posee el código de descodificación c2.

En la Figura 4 se muestra otra adición al procedimiento objeto de la invención que ilustra otros pasos ventajosos del procedimiento. En el marco de este procedimiento, la primera posición 20 no solo transmitirá el código de encriptación c1 a la segunda posición 30, sino que también le pasará una segunda clave de acceso k2.
Esta segunda clave de acceso k2 servirá más adelante para acceder a una segunda zona segura 55 de la tarjeta SIM.

La segunda posición 30 combina el registro DS con la segunda clave de acceso k2 y encripta 100 ambos con el código de encriptación c1. El registro encriptado VDS así obtenido contiene así tanto el registro DS como la segunda clave de acceso k2. Este registro encriptado VDS se traspasará a la tercera posición 40. Así, la tercera posición 40 posee la primera clave de acceso k1, transmitida por la primera posición 20. Mediante la primera clave de acceso k1, la tercera posición 40 podrá acceder a la primera zona segura 50 de la tarjeta electrónica 10. En la tarjeta electrónica 10 se produce entonces de forma automática y/o mediante una señal externa la activación de una descodificación 110 del registro encriptado VDS con la ayuda del código de descodificación c2. Como resultado, en la primera zona segura 50 se encuentran tanto el registro DS como la segunda clave de acceso k2.

Mediante la segunda clave de acceso k2 se puede acceder entonces a la segunda zona segura 55.
La apertura de esta segunda zona de acceso segura 55 mediante la segunda clave de acceso k2 puede activarse de forma automática o mediante una señal externa.

Después de la apertura de la segunda zona segura 55, puede importarse el registro DS. La particularidad de este procedimiento objeto de la invención radica en que la tercera posición 40, aunque posea la primera clave de acceso k1, esta le permite acceder a la primera zona segura 50. Aunque se posponga el registro DS después de la descodificación 110 de la primera zona segura 50 con la ayuda de la segunda clave de acceso k2 en la segunda zona segura 55, la tercera posición 40 no puede acceder al registro DS. Más bien, la tercera posición debe poseer para ello la clave k2. Sin embargo, tal como está planteada la invención, este no es el caso.

Lista de referencia

10 Tarjeta electrónica, tarjeta SIM
11 Aparato de radio móvil
20 Primera posición
30 Segunda posición
40 Tercera posición
45 Zona de la tarjeta electrónica 10
50 Primera zona asegurada
55 Segunda zona asegurada

c1 Código de encriptación
c2 Código de descodificación
k1 Primera clave de acceso
k2 Segunda clave de acceso
DS Registro
VDS Registro encriptado
100 Encriptación
110 Descodificación

**REIVINDICACIONES**

**1.** Procedimiento para proporcionar datos en al menos una zona segura (45) de una tarjeta SIM (10), con las siguientes etapas:
- la entrega de un código de encriptación (c1) desde una primera posición (20) a una segunda posición (30),
- la entrega de un código de descodificación (c2) correspondiente al código de encriptación (c1) de la primera posición (20) a la tarjeta SIM (10), **caracterizado por**
- la utilización del código de encriptación (c1) para producir un registro encriptado (VDS) desde un registro (DS) **mediante** la segunda posición (30),
- la entrega del registro encriptado (VDS) desde la segunda posición (30) a una tercera posición (40),
- la transmisión del registro encriptado (VDS) desde la tercera posición (40) a la al menos una zona (45) de la tarjeta SIM (10),
- la aplicación del código de descodificación (c2) para descodificar el registro encriptado (VDS) al registro (DS) en la tarjeta SIM (10),
- la entrega de una primera clave de acceso (k1) desde la primera posición (20) hasta la tercera posición (40) y transmite la primera clave de acceso (k1) desde la tercera posición (40) a la tarjeta SIM (10).

**2.** Procedimiento según la reivindicación 1, **caracterizado por**
- la utilización de la primera clave de acceso (k1) para acceder a una primera zona segura (50) de la tarjeta SIM (10) mediante la transferencia del registro encriptado (VDS).

**3.** Procedimiento según una de las reivindicaciones anteriores, **caracterizado por**
- la entrega de una segunda clave de acceso (k2) desde la primera posición (20) a la segunda posición (30).

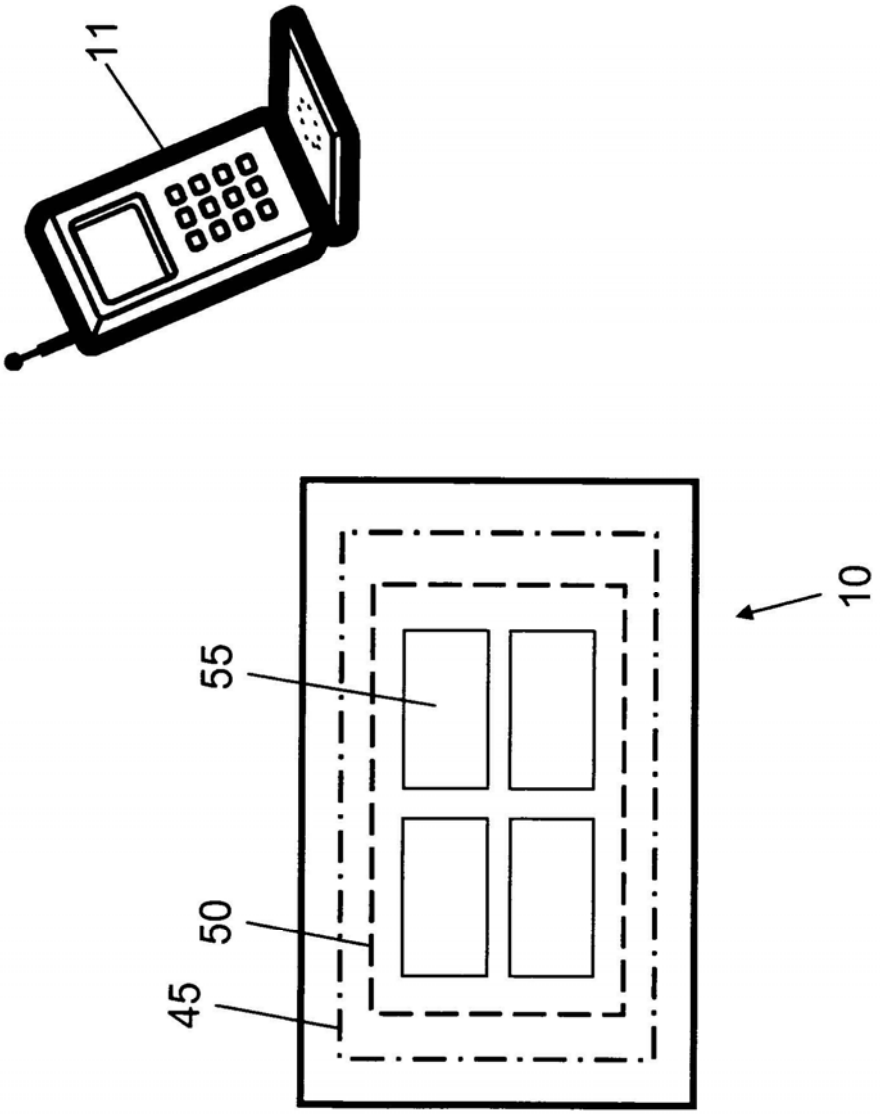
**4.** Procedimiento según la reivindicación 3, **caracterizado por**
- la adición de la segunda clave de acceso (k2) al registro (DS) antes de la utilización del código de encriptación (c1) para la generación de un registro encriptado (VDS).

**5.** Procedimiento según la reivindicación 4, **caracterizado por**
- la utilización de la segunda clave de acceso (k2) para acceder a una segunda zona segura (55) de la tarjeta SIM (10) tras la utilización del código de descodificación (c2) para descodificar el registro encriptado (VBS) por el registro (DS) en la tarjeta SIM (10).

**6.** Procedimiento según una de las reivindicaciones anteriores, **caracterizado por**
- la entrega de un único código de encriptación (c1) y el código único de descodificación (c2) correspondiente al código de encriptación (c1) para una pluralidad de tarjetas SIM (10).

**7.** Procedimiento según una de las reivindicaciones 3 a 6, **caracterizado por** la entrega de una primera clave de acceso (k1) asignada exclusivamente a una tarjeta SIM (10) y/o una segunda clave de acceso (k2) asignada exclusivamente a una tarjeta SIM (10).

Fig. 1



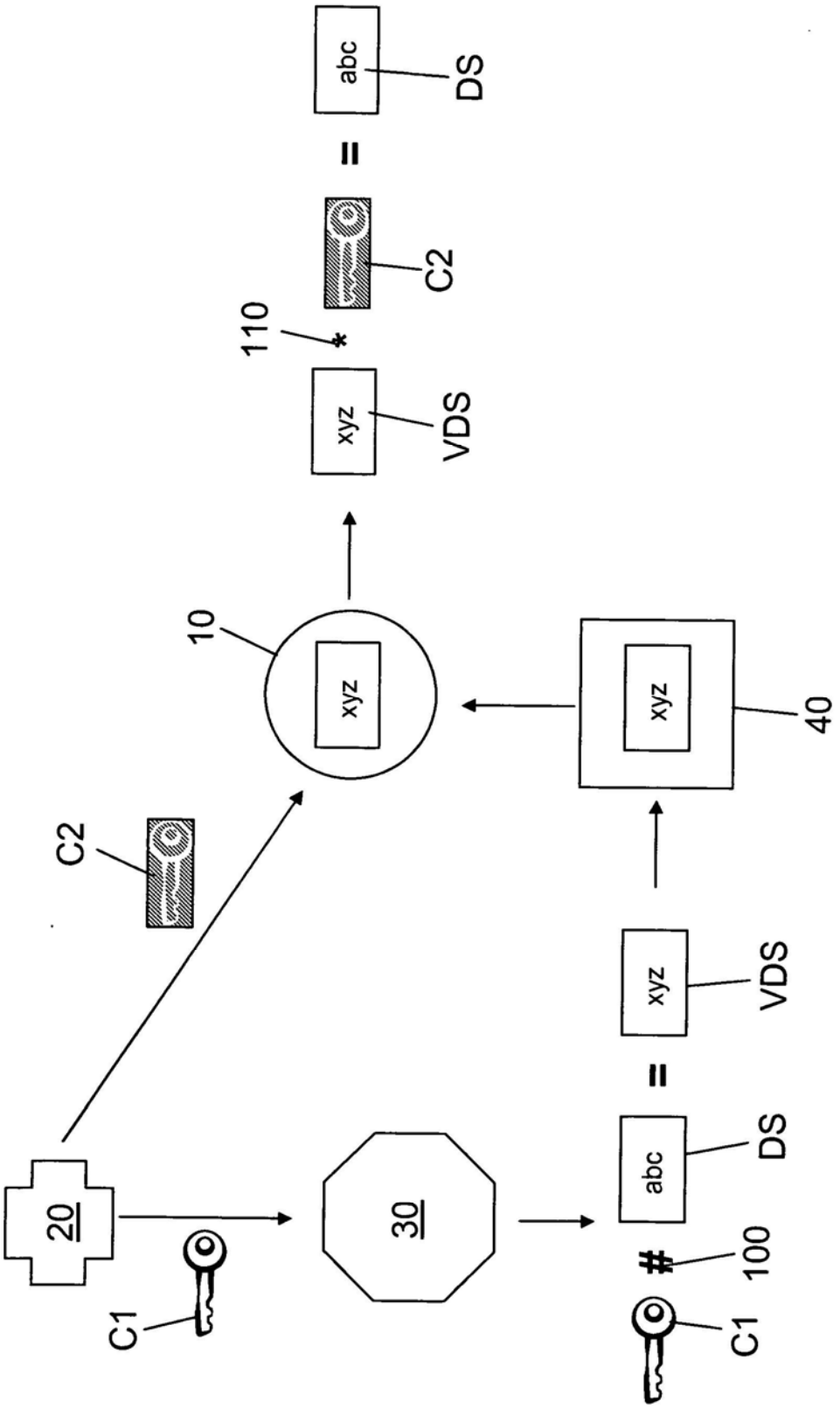

abc
DS
=
C2
110
*
xyz
VDS
10
xyz
xyz
40
C2
xyz
VDS
=
20
30
abc
DS
#
100
C1
C1

Fig. 2

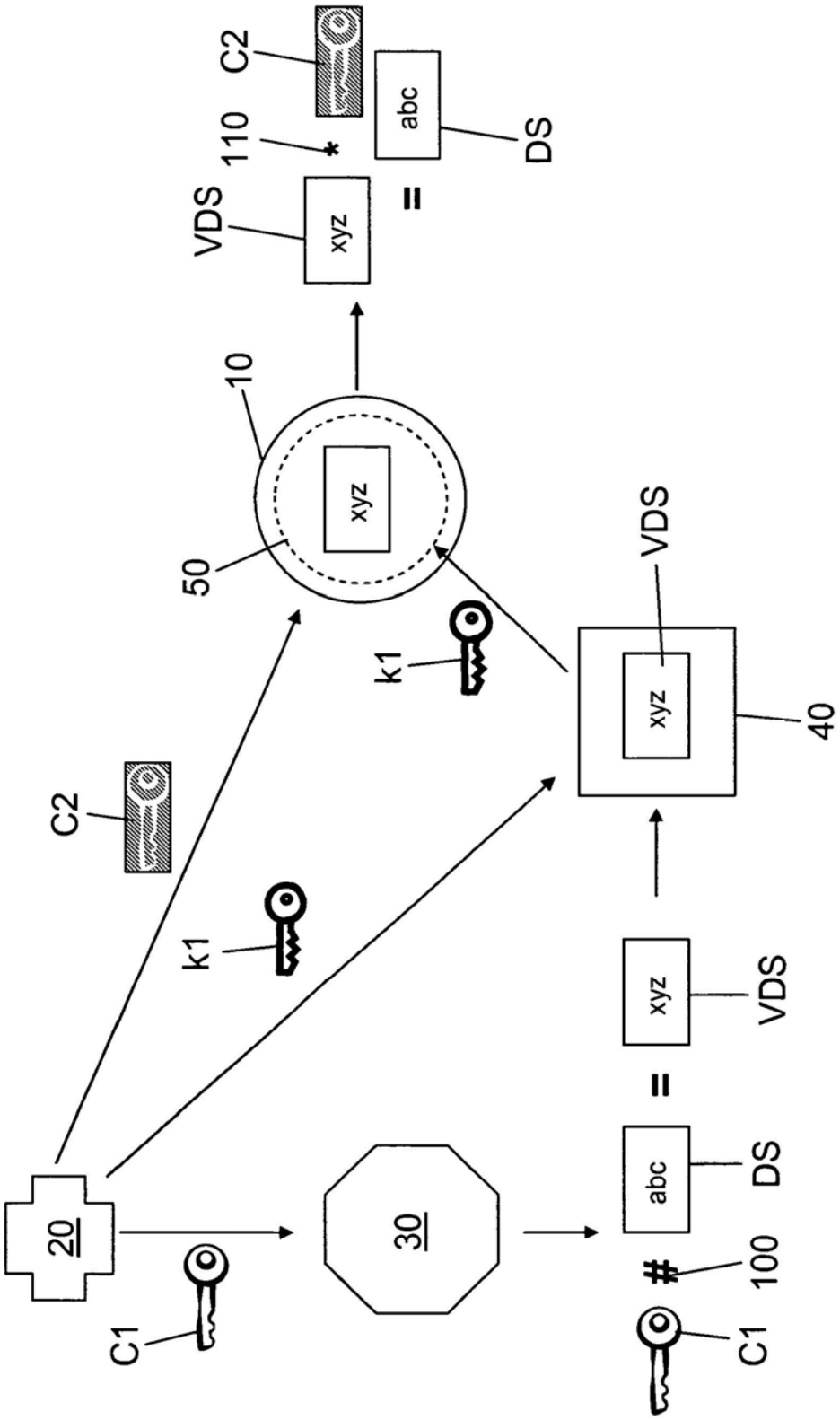

C2
110
abc
DS
VDS
xyz
=
10
xyz
50
k1
VDS
xyz
40
C2
k1
xyz
VDS
=
20
30
abc
DS
#
100
C1
C1

Fig. 3

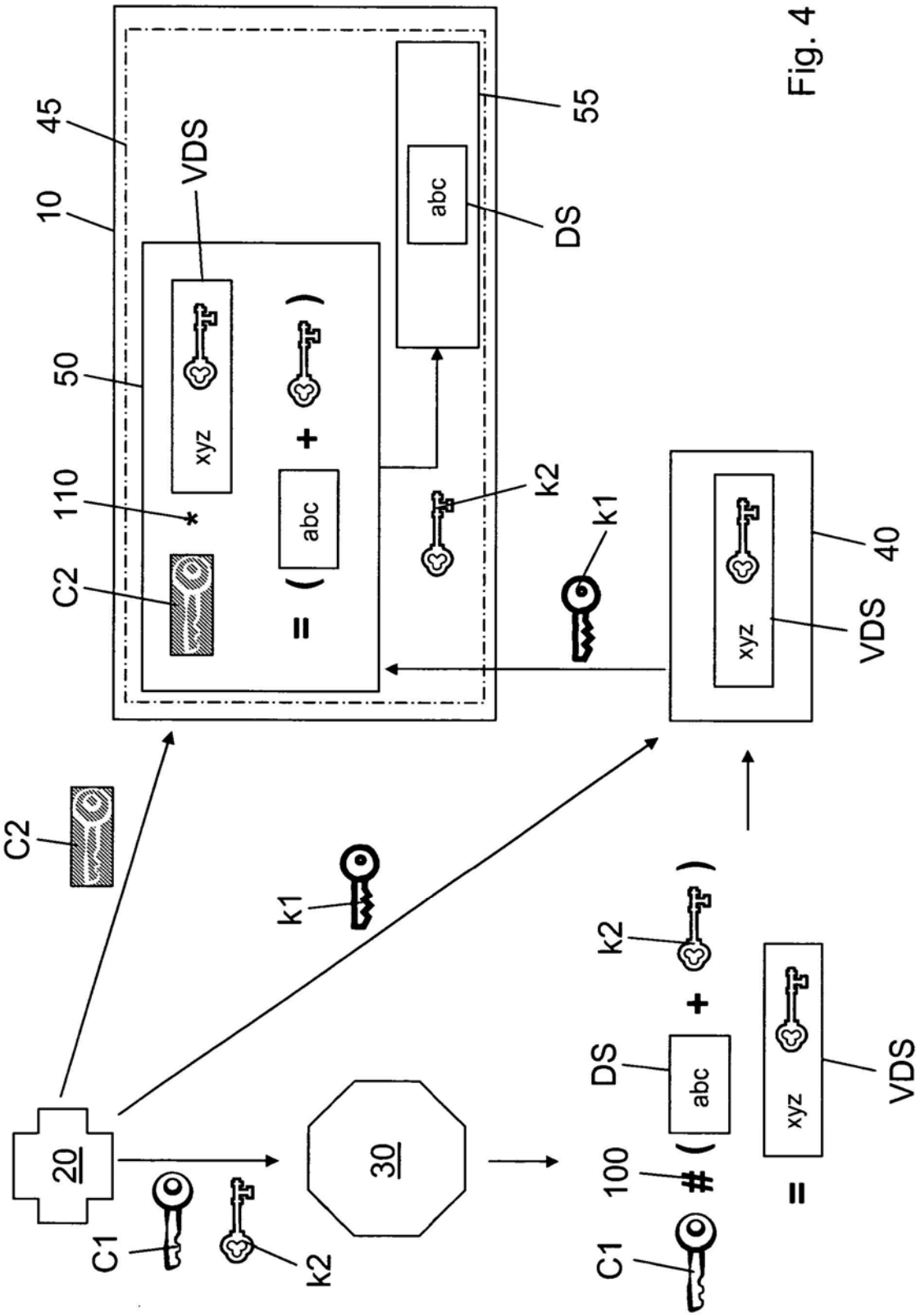

45
10
VDS
50
110
C2
xyz
abc
55
DS
k2
k1
40
VDS
C2
k1
20
C1
k2
30
k2
DS
100
C1
abc
xyz
VDS

Fig. 4