(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 754 624**

(51) Int. CI.:

H04W 4/50 (2008.01)
H04L 9/08 (2006.01)
H04W 4/00 (2008.01)
H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/04 (2009.01)
H04W 8/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.07.2017 E 17001284 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3277005**

(54) Título: **Personalización de un elemento de seguridad**

(30) Prioridad:

29.07.2016 DE 102016009259

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2020

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

SCHUSTER, HELMUT

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Personalización de un elemento de seguridad

La presente invención está orientada a un procedimiento para personalizar un elemento de seguridad, por ejemplo, una tarjeta SIM o una tarjeta de chip para teléfonos móviles, que permita proporcionar datos de personalización al elemento de seguridad con poco esfuerzo técnico. La invención también está orientada a un sistema de personalización que esté configurado según el procedimiento descrito. Además, se propone un producto de programa informático con comandos de control que implementen el procedimiento u operen el sistema de personalización propuesto.

La Patente WO 2012/ 076421 A1 muestra una personalización de un elemento de seguridad utilizando componentes físicos, es decir, una llave electrónica («dongle»). En este caso, los datos de personalización se ponen a disposición por medio del hardware y el usuario inserta la llave electrónica en un ordenador, tras lo cual se personaliza el elemento de seguridad. Para hacerlo posible, en un paso de preparación debe fabricarse o distribuirse la llave electrónica física.

La Patente WO 2015/052422 A1 muestra una personalización de un eUICC para un operador de red mediante un script de personalización que es transferido a un dispositivo de telefonía móvil «over the air» (OTA) y luego se ejecuta dentro del eUICC para instalar datos de personalización en el eUICC.

Se conocen elementos de seguridad que, por ejemplo, se ponen a disposición para un dispositivo móvil. Estos elementos de seguridad pueden proporcionarse en forma de una tarjeta SIM o un eUICC. Estos elementos de seguridad sirven, por ejemplo, para que un usuario pueda autenticarse ante un operador de red. Para lograr una autentificación lo más segura posible, típicamente se requieren otros procedimientos criptográficos.

Por tanto, se conocen procedimientos criptográficos que presuponen una parte de datos pública y una secreta. En este caso, una parte pública es una identificación generalmente conocida, por ejemplo, un número de teléfono o, en general, una dirección de correo electrónico. Una parte privada o secreta es un número PIN o también una contraseña.

En este sentido, siempre es especialmente crítico para la seguridad proporcionar datos de personalización a un dispositivo móvil. Mediante los datos de personalización es posible que, por ejemplo, el dispositivo móvil asuma una determinada identidad. De este modo, es posible ofrecer precisamente a esta identidad datos sensibles o servicios sensibles. Por esta razón existe la necesidad de proporcionar un procedimiento especialmente seguro, que permita justamente una personalización de un elemento de seguridad.

Los procedimientos conocidos presentan la desventaja de que, para personalizar elementos de seguridad, deben proporcionarse equipos físicos. Esto representa un esfuerzo técnico considerable y ofrece otra posibilidad adicional de ataque en caso de que, potencialmente, la llave física llegue a las manos equivocadas, es decir, que sea hurtada. Por ejemplo, si un elemento de seguridad se personaliza con una llave electrónica, entonces es posible que justamente esta llave electrónica se pierda y sea utilizada por un usuario no autorizado.

Típicamente, un eUICC de un terminal se personaliza sin acceso a una red. Esto también puede tener lugar a través de una de dichas llaves electrónicas que disponga de un elemento de seguridad. Los datos de la llave electrónica son transferidos entonces a través del terminal al eUICC, y de este modo se personaliza el eUICC. En este caso resulta especialmente desventajoso que, puesto que la propia llave electrónica presenta un elemento de seguridad, es decir, debe formar un entorno seguro, no puede llenarse con datos de personalización en cualquier equipo, sino que requiere por sí mismo un entorno seguro. En caso contrario, la seguridad de la llave electrónica podría verse comprometida. O bien la llave electrónica se dota de datos en un entorno seguro o en un comercio existe un entorno seguro. Ambos aspectos representan un esfuerzo innecesariamente elevado. Además, se genera un esfuerzo adicional porque debe asegurarse la llave electrónica en sí.

Por lo tanto, un objetivo de la invención consiste en proporcionar un procedimiento para personalizar un elemento de seguridad, que permita personalizar el elemento de seguridad de un modo también seguro y sin generar un esfuerzo técnico innecesario. También es objetivo de la presente invención proporcionar un sistema correspondiente, así como un producto de programa informático configurado para operar el sistema propuesto o implementar el procedimiento propuesto.

El objetivo se consigue mediante un procedimiento de personalización con las características de la reivindicación 1. Otras realizaciones preferentes se indican en las reivindicaciones dependientes.

Por tanto, se propone un procedimiento para personalizar un elemento de seguridad con el paso de proporcionar datos de personalización al elemento de seguridad mediante comandos de control de personalización. Además, tiene lugar una personalización del elemento de seguridad mediante escritura de los datos de personalización

proporcionados en una memoria de datos del elemento de seguridad, tal que los comandos de control de personalización están configurados para proporcionar una única vez los datos de personalización.

En la presente, un elemento de seguridad es cada elemento que es adecuado para proporcionar un servicio especialmente crítico para la seguridad, por ejemplo, una autenticación, una autentificación o también una autorización. El elemento de seguridad puede estar configurado para dar una indicación de un usuario, por ejemplo, proporcionado una identificación de usuario en base a la cual el usuario puede identificarse ante un proveedor de servicios. Por ejemplo, el elemento de seguridad puede ser una denominada tarjeta SIM, mediante la cual se puede determinar cuántas unidades de volumen ha consumido un usuario. En función de ello puede realizarse un cálculo de las llamadas o conexiones de datos mediante un elemento de seguridad personalizado.

Sin embargo, un elemento de seguridad también puede montarse en cualquier dispositivo móvil y debe asegurar que los datos que son puestos a disposición mediante el elemento de seguridad no pueden falsificarse. Para ello, el experto con conocimientos medios conoce algoritmos, por ejemplo, algoritmos criptográficos que realizan una codificación de conexiones de datos o datos.

Una personalización del elemento de seguridad tiene lugar de forma que, por ejemplo, un usuario guarda su identificación inequívoca en el elemento de seguridad. Pero también es posible calcular otros datos en función de los datos proporcionados de forma que tenga lugar una personalización. En general, la personalización representa una introducción de información en un elemento de seguridad de forma que justamente este un elemento de seguridad se diferencia de otros elementos de seguridad. Para ello es especialmente ventajoso que el elemento de seguridad se diferencie inequívocamente de otros elementos de seguridad de forma que un servicio sensible, por ejemplo, datos sensibles, solo puedan ponerse a disposición de este un elemento de seguridad en función de la personalización.

La personalización en sí misma tiene lugar mediante escritura de los datos de personalización proporcionados en el elemento de seguridad o en una memoria de datos del elemento de seguridad. En este sentido es posible no escribir los datos en sí en la memoria de datos del elemento de seguridad, sino más bien realizar una personalización mediante datos que fueron calculados en función de los datos de personalización proporcionados. Por ejemplo, se proporciona una clave de personalización en forma de datos de personalización, en base a la cual se generan a su vez datos que sirven para la personalización. De este modo, los datos de personalización pueden servir también indirectamente para una personalización. Tras la personalización del elemento de seguridad, justamente este elemento de seguridad se diferencia de otros elementos de seguridad en al menos una característica. Esto puede ser, por ejemplo, un identificador de usuario o una referencia a una identidad de usuario.

Por ejemplo, una memoria de datos del elemento de seguridad puede estar asegurada por medio del hardware de forma que sea especialmente segura. Esto puede realizarse, por ejemplo, de forma que la memoria esté asegurada mediante otros procedimientos conocidos, por ejemplo, procedimientos criptográficos, de forma que tenga lugar una escritura especialmente segura de forma que esté garantizada una integridad de los datos y que incluso también solo personas autorizadas escriban en esta memoria de datos. Para ello pueden estar previstas, por ejemplo, características físicas que aseguran que la memoria de datos no es atacada de forma que los datos de personalización sean modificados por un usuario no autorizado o incluso también se introduzcan datos de personalización modificados. También es posible configurar la memoria de datos de forma que esta no pueda ser accesible por otras unidades funcionales del elemento de seguridad. Si la memoria de datos fuera accesible por otras características estructurales, es decir, si se trata de una memoria de datos dividida o de uso común, entonces debe preverse que otros comandos de control o unidades físicas no puedan acceder a la memoria de datos de forma no autorizada. Típicamente, este tipo de mecanismos de aseguramiento ya está previsto en los elementos de seguridad conocidos. Por tanto, los elementos de seguridad conocidos deben equiparse según la invención únicamente de forma que proporcionen una posibilidad de almacenamiento especialmente segura para datos de personalización.

Los comandos de personalización están configurados para un ajuste único de datos de personalización, tal que estos datos de personalización pueden generarse o bien de forma dinámica en relación a la ejecución o también estar integrados de un modo especialmente asegurado en los comandos de control de personalización. Una integración debe realizarse de forma que, también en caso de que un atacante pueda obtener información sobre la implementación de los comandos de control de personalización, los datos de personalización proporcionados no sean legibles. Para ello se puede prever, por ejemplo, una interfaz asegurada, para que los comandos de control de personalización proporcionen los datos de personalización. En este sentido es especialmente ventajoso que los datos de personalización proporcionados una única vez no puedan volver a utilizarse. Esto tiene lugar, por ejemplo, mediante una invalidación de los datos de personalización que ya fueron utilizados. En este caso, en comparación con los procedimientos conocidos, es especialmente ventajoso que incuso también los comandos de control de personalización solo puedan utilizarse una vez.

Puesto que, a fin de cuentas, los comandos de control de personalización sirven para la personalización del elemento de seguridad, estos pueden generarse una única vez para cada usuario individual o para cada característica de personalización individual. Es decir, que los comandos de control de personalización, si han

proporciona una vez datos de personalización, son borrados o invalidados. Una invalidación denomina en este caso el proceso de caracterizar los comandos de control de personalización y/o datos de personalización como «utilizados». De este modo, es posible una personalización especialmente segura, ya que los comandos de control de personalización y los datos de personalización pueden utilizarse exactamente para un único elemento de seguridad.

Según un aspecto de la presente invención, los comandos de control de personalización se descartan tras proporcionar los datos de personalización. Esto tiene la ventaja de que no solo se utilizan una única vez los datos de personalización, sino incluso también los comandos de control de personalización. Por ejemplo, en comparación con los procedimientos conocidos, puede realizarse una personalización de elementos de seguridad únicamente mediante comandos de control. Esto es ventajoso porque no debe ponerse a disposición ningún elemento de hardware físico. No obstante, para aumentar la seguridad en este caso, los comandos de control de personalización y/o los datos de personalización se descartan. De este modo, una sustracción de comandos de control de personalización y datos de personalización no resulta crítico para la seguridad, ya que un usuario autorizado simplemente no utiliza los datos de personalización y, por tanto, el atacante no puede cometer un hurto de identidad. En este caso, el usuario autorizado sería capaz de identificarse simplemente mediante otros datos de personalización que son proporcionados mediante otros comandos de control de personalización y de utilizar por tanto estos nuevos datos de personalización y comandos de control de personalización. El atacante, por el contrario, tendría únicamente los comandos de control y datos antiguos, que entonces el usuario autorizado no va a utilizar.

Según otro aspecto de la presente invención, los datos de personalización presentan una Identidad Internacional de Abonado Móvil («International Mobile Subscriber Identity»), abreviado IMSI. Esto tiene la ventaja de que, por ejemplo, en una red GSM, una red UMTS o una red LTE, puede tener lugar una identificación inequívoca de un abonado de red. Por ejemplo, la presente invención puede utilizarse en una red de telecomunicación, tal que al menos una parte de los datos de personalización puede realizarse mediante la Identidad Internacional del Abonado Móvil, abreviado IMSI. Por ejemplo, es posible proporcionar los datos de personalización mediante comandos de control de personalización a través de una red de telecomunicación. Para ello pueden volver a utilizarse parámetros ya existentes.

Según otro aspecto de la presente invención, los datos de personalización presentan una clave de autentificación. Esto tiene la ventaja de que pueden utilizarse algoritmos criptográficos conocidos que, por ejemplo, prevén una clave secreta y una clave pública, por ejemplo, una clave de autentificación.

Según otro aspecto de la presente invención, la puesta a disposición de los datos de personalización tiene lugar a través de un ordenador central. Esto tiene la ventaja de que un ordenador central puede asumir pasos de cálculo intensivo y que puede realizarse en un entorno especialmente seguro. Por ejemplo, el ordenador central está presente como un servidor que genera los datos de personalización y los comandos de control de personalización correspondientes. Por ejemplo, los comandos de control de personalización pueden distribuirse como una aplicación, tal que la aplicación presenta datos de personalización o al menos los genera. En este caso, el ordenador central puede proporcionar los datos de personalización directamente al elemento de seguridad. Pero también pueden preverse otros componentes intermedios. Un componente intermedio de este tipo puede ser, por ejemplo, un dispositivo móvil.

Según otro aspecto de la presente invención, la puesta a disposición de los datos de personalización tiene lugar a través de un dispositivo móvil. Esto tiene la ventaja de que el usuario puede cargar los comandos de control de personalización en su dispositivo móvil, por ejemplo, desde el ordenador central propuesto. De este modo, el usuario puede realizar una personalización del elemento de seguridad utilizando únicamente su dispositivo móvil. El dispositivo móvil puede a su vez recibir los comandos de control de personalización del ordenador central y reenviarlos al elemento de seguridad o bien reenviar los datos de personalización.

Según otro aspecto de la presente invención, los datos de personalización se guardan junto con los comandos de control de personalización en una memoria de un dispositivo móvil. Esto tiene la ventaja de que los datos de personalización, junto con los comandos de control de personalización, pueden guardarse, por ejemplo, en una tarjeta SD que se introduce luego en el espacio de memoria previsto del dispositivo móvil. No obstante, no tiene por qué tratarse de una tarjeta SD, sino que también puede preverse que los comandos de control de personalización se descarguen del ordenador central al dispositivo móvil y se guarden en una memoria instalada en el dispositivo móvil. De este modo, la memoria del dispositivo móvil puede ser una memoria extraíble o también una memoria de instalación fija. De forma general, también es posible disponer la memoria del dispositivo móvil de forma remota, de forma que los datos de personalización, junto con los comandos de control de personalización, se descargan de un ordenador remoto o que esté prevista una interfaz segura a través de la cual pueden transferirse los datos de personalización.

Según otro aspecto de la presente invención, los comandos de control de personalización están configurados para calcular los datos de personalización. Esto tiene la ventaja de que los datos de personalización no deben estar integrados en los comandos de control de personalización, sino que estos pueden generarse más bien dinámicamente mediante otros parámetros y algoritmos a través de los comandos de control de personalización.

Esto es especialmente ventajoso porque los comandos de control de personalización solo se utilizan una vez y por tanto proporcionan un valor previamente desconocido que luego puede proporcionarse, por ejemplo, con otros valores, como datos de personalización. De este modo, los datos de personalización pueden calcularse exactamente en el momento en que realmente se necesitan y no están disponibles previamente, lo que a su vez representaría un riesgo de seguridad.

Según otro aspecto de la presente invención, los comandos de control de personalización están configurados para reconocer automáticamente si el elemento de seguridad ya está personalizado. Esto tiene la ventaja de que, si un equipo que realiza la personalización, por ejemplo, un dispositivo móvil, detecta un elemento de seguridad, también puede realizar inmediatamente una personalización. Por ejemplo, el elemento de seguridad es conectado a través de la red, o acoplado para establecer una comunicación, con un dispositivo final de personalización. De este modo, es posible que el elemento de seguridad pueda ser analizado automáticamente de modo que se detecten datos de personalización o características de personalización. Si estos datos de personalización no están presentes, entonces el equipo de personalización puede iniciar automáticamente la personalización.

Según otro aspecto de la presente invención, los datos de personalización se integran de tal forma en los comandos de control de personalización, que no sean legibles. En este sentido, ya se conocen procedimientos relevantes para la seguridad, que permiten que los datos de personalización no sean guardados como parámetros, por ejemplo, en un código fuente de forma que estos sean leídos durante una descompilación. En este sentido, se conoce, por ejemplo, el uso de una denominada criptografía White-Box. Gracia a ella, los datos tampoco pueden ser leídos aunque se conozcan los correspondientes comandos de control de personalización. En este caso, por ejemplo, los datos de personalización no son conocidos previamente, sino que se generan, por ejemplo, a partir de los comandos de control de personalización.

Según otro aspecto de la presente invención, la puesta a disposición de los datos de personalización tiene lugar a través de una interfaz aérea. Esto tiene la ventaja de que los datos de personalización, junto con los comandos de control de personalización, pueden ser puestos a disposición, por ejemplo, por un ordenador central. Esto puede tener lugar, por ejemplo, a través de internet o también a través de cualquier LAN. No obstante, también es posible realizar la personalización del elemento de seguridad mediante un dispositivo móvil. En este caso, es posible utilizar las interfaces aéreas conocidas de forma que la puesta a disposición de los datos de personalización mediante comandos de control de personalización tenga lugar a través de Bluetooth, infrarrojos y/o WLAN. De este modo pueden volver a utilizarse los protocolos de transmisión tradicionales.

Según otro aspecto de la presente invención, el elemento de seguridad está presente a modo de tarjeta SIM, tarjeta Secure-SD, una UICC y/o un chip de hardware. Esto tiene la ventaja de que pueden volver a utilizarse componentes de hardware conocidos como elemento de seguridad y que los procedimientos proporcionados pueden tenerlos en cuenta. De este modo, también los elementos de seguridad tradicionales pueden ser accesibles según la invención de forma que sea posible una personalización segura y sencilla de justamente estos elementos de seguridad.

El objetivo también se consigue mediante un sistema de personalización para personalizar un elemento de seguridad, con un ordenador central que está configurado para proporcionar datos de personalización al elemento de seguridad mediante comandos de control de personalización. Además, está prevista una unidad de personalización que está configurada para personalizar el elemento de seguridad mediante escritura de los datos de personalización proporcionados en una memoria de datos del elemento de seguridad, tal que los comandos de control de personalización están configurados para proporcionar una única vez los datos de personalización.

Según la invención es especialmente ventajoso que el sistema de personalización propuesto también pueda implementarse como un dispositivo de personalización. Este dispositivo puede estar acoplado, por ejemplo, a un ordenador central y proporcionar los datos de personalización, junto con los comandos de control de personalización. Este dispositivo se comunica entonces con el ordenador central y comprende la unidad de personalización.

El objetivo también se consigue mediante un producto de programa informático con comandos de control que implementan el procedimiento propuesto u operan el dispositivo de personalización propuesto o el sistema de personalización propuesto.

Según la invención es especialmente ventajoso que los pasos de procedimiento en el sistema de personalización sean aplicados de forma que este proporcione respectivamente características estructurales que permitan la ejecución de los pasos de procedimiento. Según la invención, también es posible implementar las características estructurales del sistema de personalización de forma que estas proporcionen respectivamente un paso de procedimiento. En particular, el procedimiento propuesto está configurado para operar el dispositivo de personalización o el sistema de personalización. El sistema de personalización o el dispositivo de personalización están configurados a su vez para ejecutar el procedimiento propuesto.

Otras realizaciones ventajosas se explican en detalle en base a las figuras. Muestran:

La figura 1: comandos de control de personalización con datos de personalización según un aspecto de la presente invención;
La figura 2: el sistema de personalización propuesto para personalizar un elemento de seguridad según un aspecto de la presente invención; y
La figura 3: un diagrama de desarrollo esquemático de un procedimiento para personalizar un elemento de seguridad según un aspecto de la presente invención.

La figura 1 muestra comandos de control de personalización que también pueden denominarse como aplicación de personalización. En este caso se representa que los datos de personalización codificados están integrados en la aplicación de personalización. Estos pueden codificarse, por ejemplo, mediante una clave de transporte («Transport Key»). En este caso, también se puede utilizar otra clave, por ejemplo, la previamente denominada «Transport Key». Los datos de personalización están integrados en la aplicación de personalización de forma que estos no son legibles allí. Por consiguiente, se utiliza la denominada criptografía White-Box.

De este modo se evita, según la invención, que tenga lugar una personalización fuera de línea de un eUICC, mediante lo cual se evita, por ejemplo, una llave electrónica («dongle»). Una llave electrónica requiere un entorno seguro, lo que significa un mayor esfuerzo.

En este caso, es posible que los datos de personalización y la aplicación de personalización se encuentren en una aplicación. Los datos de personalización están integrados según una criptografía White-Box en la aplicación de personalización, es decir, para cada juego de datos de personalización se pone a disposición una aplicación de personalización propia. Por tanto, los datos de personalización pueden transmitirse o proporcionarse sin medidas de seguridad, por ejemplo, a través de un soporte de almacenamiento de datos portátil. Para personalizar el eUICC, el usuario instala, por ejemplo, los datos de personalización que la personalización ejecuta automáticamente. Para una protección contra un uso indebido de los datos de personalización, los componentes de los mismos críticos para la seguridad son transmitidos durante el primer contacto con una red de telefonía móvil y los datos de personalización anteriores ya no son válidos.

De este modo se logra un ahorro de costes, ya que no se requiere ningún otro componente físico como, por ejemplo, una llave electrónica. Por tanto, para la personalización solo debe instalarse la aplicación de personalización. En consecuencia, se crea una posibilidad de elusión para los procedimientos conocidos.

La figura 2 muestra un aspecto de la presente invención en el que se personaliza un elemento de seguridad con la ayuda de un teléfono inteligente. Este teléfono inteligente obtiene una aplicación de personalización de un ordenador central, TSM, y pone esta aplicación de personalización, junto con los datos de personalización, a disposición del elemento de seguridad. En este caso es ventajoso que el teléfono inteligente controle la aplicación de personalización de forma que el Transport Key se elimine de los datos de personalización.

Los datos de personalización según la invención están compuestos, entre otros, por dos componentes, en concreto componentes públicos como, por ejemplo, la IMSI, así como componentes críticos para la seguridad, es decir, secretos, por ejemplo, la clave de autenticación Ki.

Según un aspecto, el procedimiento propuesto según la invención prevé no guardar los datos de personalización en una llave electrónica con elemento de seguridad, sino en un soporte de almacenamiento de datos portátil sin medidas de seguridad especiales. Se trata preferentemente de una tarjeta SD, por ejemplo, una tarjeta de memoria micro-SD, que se coloca en el teléfono inteligente a personalizar. No obstante, también son posibles otros soportes de almacenamiento de datos habituales como, por ejemplo, una memoria USB. También es posible una transmisión de los datos de personalización de un teléfono inteligente (del comerciante) al teléfono inteligente (del cliente), por ejemplo, mediante Bluetooth o WLAN. El teléfono inteligente que pone a disposición los datos de personalización tampoco necesita presentar medidas de seguridad especiales. No obstante, para proteger los datos de personalización de un acceso no autorizado, están previstas, entre otras, dos medidas.

En primer lugar, el concepto de Seguridad basada en Software («Software-based-Security»). Los datos que vale la pena proteger se codifican con la ayuda de algoritmos de criptografía y se guardan o bien dentro de la aplicación o como bloque de datos externo, por ejemplo, en un archivo. Al contrario que en el caso de la Seguridad basada en Hardware («Hardware-based-Security»), donde los datos que vale la pena proteger se guardan dentro de un elemento de seguridad, por ejemplo, una tarjeta SIM.

De este modo, los datos de personalización y la aplicación no se tratan por separado, sino que están combinados en una aplicación de personalización única. Los datos de personalización no están presentes de forma explícita como datos, sino integrados en una aplicación de personalización según el concepto de la criptografía White-Box. Esto significa que, para cada juego de datos de personalización se pone a disposición una aplicación propia. Este tipo de aplicaciones pueden generarse de forma completamente automática.

La criptografía White-Box es un método para, por así decirlo, ocultar una clave criptográfica en una implementación pública de un algoritmo. De este modo es posible operar con datos codificados sin que la(s) clave(s) necesaria(s) para ello sea(n) legible(s) en algún momento desde el programa, por ejemplo, una imagen de memoria. Una posibilidad para integrar los datos de personalización en una aplicación con la ayuda de la criptografía White-Box es la de guardar los datos de personalización con una clave de personalización de forma codificada. Estos datos de personalización protegidos están asegurados luego adicionalmente con una clave de transporte, «Transport Key», que está presente en la aplicación de personalización como clave de White-Box («White-Box-Key»). Los datos de personalización asegurados de este modo se guardan en la aplicación.

La aplicación de personalización puede decodificar entonces la codificación de transporte de los datos de personalización antes de la personalización y enviarlos a la tarjeta/eUICC o a un subprograma («applet») que se encuentra en la misma. La aplicación de personalización puede reconocer automáticamente que la eUICC aún no está personalizada. Esto tiene lugar de forma que la eUICC o el Applet correspondiente informa, a petición, que no debe tener lugar ninguna personalización. Una eUICC puede contener diferentes Applets que pueden o deben personalizarse. Además, pueden preverse componentes de los datos de personalización críticos para la seguridad que se intercambian durante el primer contacto con una red de telefonía móvil. Por ejemplo, puede utilizarse un identificador inicial que se transmite únicamente durante el primer proceso de registro a la red de telefonía móvil. En caso contrario, se utilizan claves, configuraciones y otras informaciones que son necesarias para la eUICC del Applet en la eUICC.

Para realizar la personalización de la eUICC, el usuario del teléfono inteligente instala la aplicación de personalización, o bien desde la tarjeta micro-SD o mediante Bluetooth/WLAN desde otro teléfono inteligente/terminal Point-of-Sale. La aplicación de personalización reconoce automáticamente que la eUICC aún no dispone de una/la personalización y la realiza. Luego puede borrarse la aplicación de personalización o esta se borra por sí misma.

En segundo lugar, a diferencia de un elemento de seguridad, una aplicación de personalización puede copiarse sin que esto sea notado. Además, la Software-based-Security tampoco ofrece protección ilimitada contra un atacante. Para evitar que un atacante pueda hacer un uso indebido de datos de personalización hackeados, los componentes de los datos de personalización críticos para la seguridad se intercambian durante el primer contacto con la red de telefonía móvil. Los datos de personalización críticos para la seguridad originales ya no son válidos.

Si ahora un atacante utiliza los datos de personalización, después de que el usuario real los utiliza, estos no son válidos para el atacante. Por tanto, el atacante ya no puede hacer nada con ellos. Si un atacante utiliza los datos de personalización, antes de que el usuario real los utilice, estos no son válidos para el usuario real. Por tanto, no se puede engañar al usuario.

Si bien el último caso es incómodo para el usuario, ya que los datos de personalización ya no funcionan, un atacante al menos no puede obtener ninguna ventaja del hackeo de una aplicación de personalización. En particular, el esfuerzo técnico para ello es demasiado grande. Por este motivo, la motivación para un atacante es muy baja, por lo que la ocurrencia de justamente este último caso no es de esperar.

En resumen puede decirse que el usuario simplemente debe instalar una aplicación para la personalización, por ejemplo, a través de WLAN o desde una tarjeta micro-SD. No es necesario familiarizarse con una aplicación especial. Por lo demás, la aplicación no requiere ninguna otra acción por parte del usuario y, por tanto, es fácil de operar.

La figura 3 muestra en un primer paso de procedimiento 100 la puesta a disposición de datos de personalización mediante comandos de control de personalización. Esto puede comprender pasos parciales adicionales, por ejemplo, los datos, junto con los comandos de control, pueden ser puestos a disposición de un dispositivo móvil por parte de un ordenador central. El dispositivo móvil puede estar configurado entonces para proporcionar los datos, junto con los comandos de control, al elemento de seguridad. A continuación tiene lugar una personalización 101 del elemento de seguridad mediante escritura de los datos de personalización proporcionados. En este caso es especialmente ventajoso que los datos de personalización se proporcionen una única vez. Incluso si la puesta a disposición 100 comprende varios pasos intermedios, los datos de personalización solo se utilizan una vez. Por tanto, también los comandos de control de personalización solo se utilizan una vez, ya que para un juego de datos de personalización se dispone de un juego de comandos de control de personalización.

En un paso de procedimiento102 opcional subsiguiente tiene lugar un descarte de los datos de personalización o comandos de control de personalización. Esto asegura que estos solo se proporcionan una vez al elemento de seguridad. De este modo, también es posible realizar el paso de procedimiento de puesta a disposición 100 varias veces o realizarlo mediante estaciones intermedias, aunque la puesta a disposición de los datos de personalización mediante los comandos de control al elemento de seguridad solo tiene lugar una vez.

REIVINDICACIONES

1. Procedimiento para personalizar un elemento de seguridad con los pasos:

- Puesta a disposición (100) de datos de personalización al elemento de seguridad mediante comandos de control de personalización;
- Personalización (101) del elemento de seguridad mediante escritura de los datos de personalización puestos a disposición, en una memoria de datos del elemento de seguridad, tal que los comandos de control de personalización están configurados para poner a disposición (100) una única vez los datos de personalización,

caracterizado por que los comandos de control de personalización se descartan (102) tras la puesta a disposición (100) de los datos de personalización,
tal que los datos de personalización presentan una Identidad Internacional de Abonado Móvil, abreviado, IMSI,
tal que los comando de control de personalización están configurados para calcular los datos de personalización,
tal que los comandos de control de personalización están configurados para reconocer automáticamente si el elemento de seguridad ya está personalizado,
tal que los comandos de control de personalización están configurados para personalizar automáticamente el elemento de seguridad.

2. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** los datos de personalización presentan una clave de autentificación.

3. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** la puesta a disposición (100) de los datos de personalización tiene lugar a través de un ordenador central.

4. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** la puesta a disposición (100) de los datos de personalización tiene lugar a través de un dispositivo móvil.

5. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** los datos de personalización, junto con los comandos de control de personalización, se guardan en una memoria de un dispositivo móvil.

6. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** los datos de personalización se integran en los comandos de control de personalización de forma que no son legibles.

7. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** la puesta a disposición (100) de los datos de personalización tiene lugar mediante una interfaz aérea.

8. Procedimiento, según cualquiera de las reivindicaciones anteriores, **caracterizado por que** el elemento de seguridad está presente como una tarjeta SIM, una tarjeta Secure-SD, una UICC y/o un chip de hardware.

9. Sistema de personalización para personalizar un elemento de seguridad, según las reivindicaciones 1 a 8, que presenta:

- un ordenador central configurado para la puesta a disposición (100) de datos de personalización al elemento de seguridad mediante comandos de control de personalización;
- una unidad de personalización configurada para la personalización (101) del elemento de seguridad mediante escritura de los datos de personalización puestos a disposición, en una memoria de datos del elemento de seguridad.

10. Producto de programa informático con comandos de control que implementan el procedimiento, según cualquiera de las reivindicaciones 1 a 8.

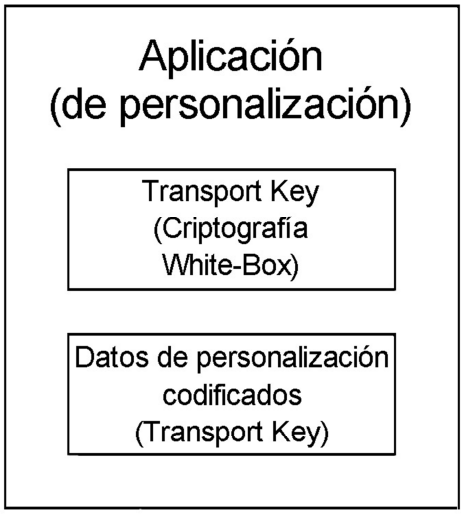
Aplicación
(de personalización)
Transport Key
(Criptografía
White-Box)
Datos de personalización
codificados
(Transport Key)

Fig. 1

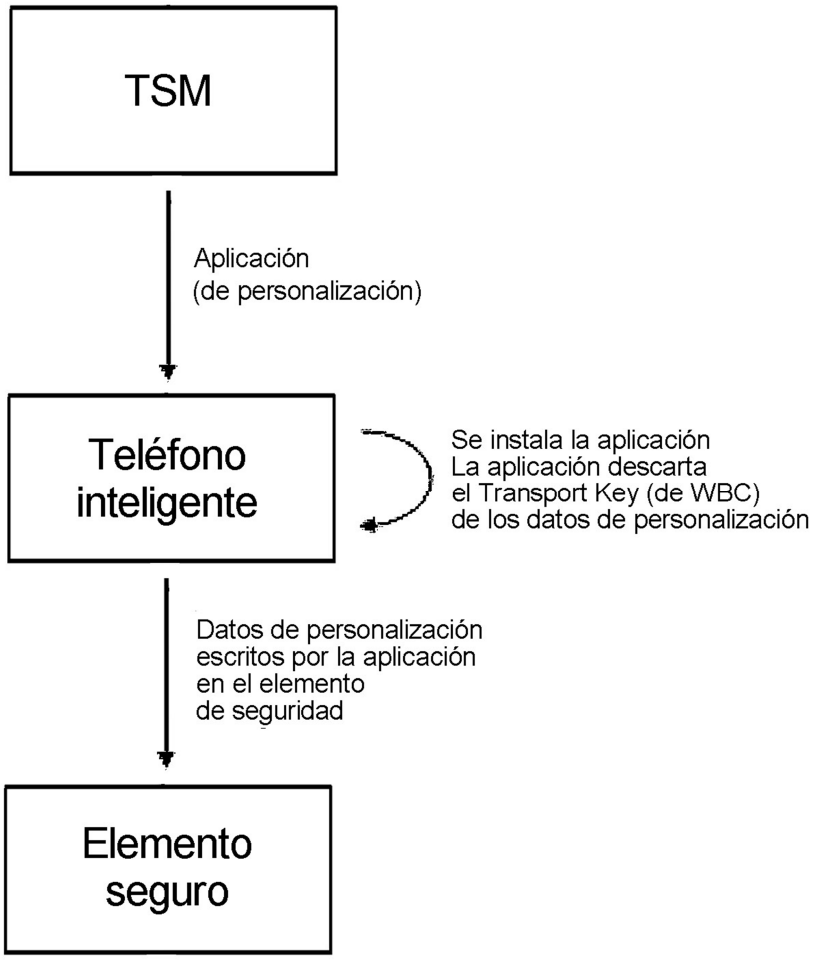
TSM
Aplicación
(de personalización)
Teléfono
inteligente
Se instala la aplicación
La aplicación descarta
el Transport Key (de WBC)
de los datos de personalización
Datos de personalización
escritos por la aplicación
en el elemento
de seguridad
Elemento
seguro

Fig. 2

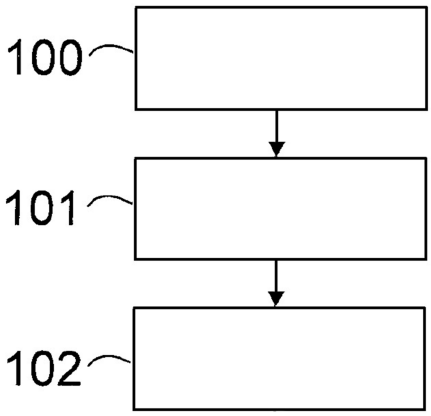

Fig. 3

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citada por el solicitante es únicamente para mayor comodidad del lector. No forman parte del documento de la Patente Europea. Incluso teniendo en cuenta que la compilación de las referencias se ha efectuado con gran cuidado, los errores u omisiones no pueden descartarse; la EPO se exime de toda responsabilidad al respecto.

Documentos de patentes citados en la descripción

- WO 2012076421 A1
- WO 2015052422 A1