(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 636 746**

(51) Int. CI.:

G06F 21/34 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.03.2011 PCT/EP2011/001107**

(87) Fecha y número de publicación internacional: **15.09.2011 WO11110318**

(96) Fecha de presentación y número de la solicitud europea: **07.03.2011 E 11707806 (3)**

(97) Fecha y número de publicación de la concesión europea: **10.05.2017 EP 2545486**

(54) Título: **Procedimiento para autentificar un soporte de almacenamiento de datos portátil**

(30) Prioridad:

10.03.2010 DE 102010010950

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2017

(73) Titular/es:

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

(72) Inventor/es:

EICHHOLZ, JAN y
MEISTER, GISELA

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimiento para autentificar un soporte de almacenamiento de datos portátil

La presente invención se refiere a un procedimiento para autentificar un soporte de almacenamiento de datos portátil ante un dispositivo terminal, así como a un soporte de almacenamiento de datos correspondientemente configurado y a un dispositivo terminal.

Un soporte de almacenamiento de datos portátil, por ejemplo, en forma de un documento de identidad electrónico, comprende un circuito integrado con un procesador y una memoria. En la memoria están almacenados datos relacionados con un usuario del soporte de almacenamiento de datos. En el procesador se puede ejecutar una aplicación de autentificación, a través de la cual el soporte de almacenamiento de datos se puede autentificar ante un dispositivo terminal, en el caso de un documento de identidad, por ejemplo, en un control fronterizo o similar.

Durante un procedimiento de autentificación de este tipo se prepara una comunicación de datos segura entre el soporte de almacenamiento de datos y el dispositivo terminal, acordando una clave de comunicación secreta para el cifrado simétrico de una comunicación de datos subsiguiente, por ejemplo, mediante el procedimiento conocido de intercambio de claves según Diffie y Hellman u otros procedimiento adecuados. Además, al menos el terminal verifica generalmente la autenticidad del soporte de almacenamiento de datos, por ejemplo, mediante un certificado.

El documento WO2006/089101 A2 muestra cómo pueden derivarse claves simétricas a partir de una clave maestra y una identidad. En el "Handbook of Applied Cryptography" de Menezes y otros se describen diversos procedimientos criptográficos, entre otros, para claves asimétricas dependientes de la identidad y para la derivación simétrica de claves.

En el artículo "Anonymous Attribute Authentication Scheme Using Self-Blindable Certificates" de Kiyomoto y otros, ISI 2008, se describe una autentificación anónima mediante el uso de una clave pública individual, modificada para la sesión, junto con un certificado individual correspondientemente modificado de la clave pública.

Para realizar un procedimiento con objeto de acordar la clave de comunicación secreta es necesario que tanto el terminal como también el soporte de almacenamiento de datos pongan a disposición respectivamente una clave secreta y una clave pública. El certificado del soporte de almacenamiento de datos puede estar relacionado, por ejemplo, con su clave pública.

Si cada soporte de almacenamiento de datos de un conjunto o grupo de soportes de almacenamiento de datos es personalizado con un par de claves individual, compuesto por una clave pública y una clave secreta, se producen problemas en cuanto al anonimato del usuario del soporte de almacenamiento de datos. Ello es debido a que sería posible asignar a cada uso del soporte de almacenamiento de datos inequívocamente el usuario correspondiente y de este modo, por ejemplo, crear un perfil de movimiento completo del usuario. Para solucionar este aspecto se ha propuesto que una pluralidad o un grupo de soportes de almacenamiento de datos estén provistos respectivamente con un par de claves denominado par de claves de grupo idéntico, compuesto por una clave de grupo pública y una clave de grupo secreta. De este modo se puede restablecer el anonimato de un usuario, al menos dentro del grupo. La desventaja de esta solución es que, en el caso de que uno de los soportes de almacenamiento de datos del grupo se vea comprometido, se debe sustituir el grupo completo de soportes de almacenamiento de datos. Si se ha interceptado, por ejemplo, la clave de grupo secreta de un soporte de almacenamiento de datos del grupo, ya no se puede continuar utilizando de forma segura ninguno de los soportes de almacenamiento de datos del grupo. El esfuerzo y los costes necesarios para la sustitución pueden ser muy elevados.

La presente invención tiene como objetivo proponer un procedimiento de autentificación que asegure el anonimato del usuario y en el que el hecho de que un soporte de almacenamiento de datos se vea comprometido no afecte negativamente a la seguridad de los demás soportes de almacenamiento de datos.

Este objetivo se consigue mediante un procedimiento, un soporte de almacenamiento de datos, un dispositivo terminal y un sistema con las características de las reivindicaciones secundarias. En las reivindicaciones dependientes se especifican realizaciones y perfeccionamientos preferentes.

Un procedimiento según la invención para autentificar un soporte de almacenamiento de datos portátil ante un dispositivo terminal comprende los siguientes pasos: En el soporte de almacenamiento de datos se deriva una clave de sesión pública de una clave pública individual del soporte de almacenamiento de datos. Esta clave pública individual del soporte de almacenamiento de datos ha sido derivada por su parte de una clave de grupo pública. Adicionalmente, en el soporte de almacenamiento de datos se deriva una clave de sesión secreta de una clave secreta individual del soporte de almacenamiento de datos, que a su vez ha sido derivada de una clave de grupo secreta. La clave pública individual del soporte de almacenamiento de datos y la clave secreta individual del soporte de almacenamiento de datos están almacenadas en el soporte de almacenamiento de datos, no así la clave de grupo secreta y la clave de grupo pública. En el marco de la autentificación del soporte de almacenamiento de datos ante el dispositivo terminal se utilizan la clave de sesión pública y la secreta. El soporte de almacenamiento de datos

utilizará su clave de sesión secreta. El soporte de almacenamiento de datos pone a disposición del dispositivo terminal la clave de sesión pública para utilizarla en el marco de la autentificación del soporte de almacenamiento de datos.

En particular, entre el soporte de almacenamiento de datos y el dispositivo terminal se puede acordar una clave de comunicación secreta. El soporte de almacenamiento de datos presenta para ello la clave de sesión pública y la secreta. Por su parte, el dispositivo terminal presenta para ello una clave de terminal pública y una clave de terminal secreta. Finalmente, el dispositivo terminal verifica la clave de sesión pública del soporte de almacenamiento de datos.

Un soporte de almacenamiento de datos portátil según la invención comprende, por tanto, un procesador, una memoria y una interfaz de comunicación de datos para la comunicación de datos con un dispositivo terminal, así como un dispositivo de autentificación. Este está configurado para derivar una clave de sesión secreta a partir de una clave secreta individual del soporte de almacenamiento de datos almacenada en la memoria. El dispositivo de autentificación está configurado además para derivar una clave de sesión pública a partir de una clave pública individual del soporte de almacenamiento de datos almacenada en la memoria. Además, dicho dispositivo puede acordar una clave de comunicación secreta con el dispositivo terminal. Para ello, el dispositivo de autentificación utiliza la clave de sesión pública y la clave de sesión secreta.

En definitiva, un dispositivo terminal según la invención está configurado para la comunicación de datos con un soporte de almacenamiento de datos portátil según la invención, así como para acordar una clave de comunicación secreta con el soporte de almacenamiento de datos utilizando una clave de terminal pública y una clave de terminal secreta. El dispositivo terminal está configurado además para verificar una clave de sesión pública del soporte de almacenamiento de datos, que ha sido derivada de una clave de grupo pública a través de una clave pública individual del soporte de almacenamiento de datos.

En el procedimiento según la invención ya no es necesario almacenar la clave de grupo secreta en el soporte de almacenamiento de datos. Por lo tanto, esta ya no puede ser interceptada en caso de ataque al soporte de almacenamiento de datos. Las claves de sesión secretas de otros soportes de almacenamiento de datos no atacados de un grupo de soportes de almacenamiento de datos se pueden seguir utilizando. El seguimiento de un usuario del soporte de almacenamiento de datos mediante la clave de sesión secreta del soporte de almacenamiento de datos, que es utilizada eventualmente en un procedimiento de desafío-respuesta (“challenge-response”) para la autentificación ante el dispositivo terminal, no es posible, ya que esta clave de sesión cambia de un uso al siguiente.

Preferentemente, el dispositivo terminal verifica la clave de sesión pública del soporte de almacenamiento de datos mediante un certificado de la clave de grupo pública que está almacenada en el soporte de almacenamiento de datos. Para ello, el dispositivo terminal comprueba en primer lugar el certificado. El dispositivo terminal es capaz entonces de derivar la clave de sesión pública a partir de la clave de grupo pública por medio de la clave pública individual del soporte de almacenamiento de datos. La información de derivación necesaria para ello es puesta a disposición por el soporte de almacenamiento de datos. De este modo, el soporte de almacenamiento de datos puede ser autentificado como un soporte de almacenamiento de datos del grupo al que está asignado el par de claves de grupo, pero no puede ser captado mediante un certificado individual del soporte de almacenamiento de datos, que no está previsto según la invención. En el soporte de almacenamiento de datos está almacenado únicamente el certificado de la clave de grupo pública idéntico para todos los soportes de almacenamiento de datos, gracias a lo cual se mantiene el anonimato del usuario del soporte de almacenamiento de datos.

Según un modo de realización preferente, la clave pública individual del soporte de almacenamiento de datos y la clave secreta individual del soporte de almacenamiento de datos son derivadas de la clave de grupo pública y la clave de grupo secreta, y almacenadas en el soporte de almacenamiento de datos, en una fase de personalización del soporte de almacenamiento de datos. También en esta fase se puede introducir y almacenar el certificado de la clave de grupo pública en el soporte de almacenamiento de datos.

Preferentemente, la clave secreta individual del soporte de almacenamiento de datos es derivada de la clave de grupo secreta utilizando un primer número aleatorio. Para ello se puede utilizar cualquier operación adecuada que acepte como datos de entrada, entre otros, la clave de grupo secreta, así como el primer número aleatorio y pueda procesarlos para generar la clave secreta individual del soporte de almacenamiento de datos. Se pueden utilizar, por ejemplo, operaciones matemáticas como multiplicación, exponenciación o similares. La clave pública individual del soporte de almacenamiento de datos se puede derivar entonces mediante la clave secreta individual del soporte de almacenamiento de datos derivada anteriormente. Esto es razonable, por ejemplo, si también la clave de grupo pública ha sido generada con ayuda de la clave de grupo secreta, por ejemplo, mediante exponenciación modular, como se conoce del procedimiento de intercambio de claves Diffie-Hellman. También es posible derivar la clave pública individual del soporte de almacenamiento de datos de otro modo a partir de la clave de grupo pública.

De forma similar, también la derivación de la clave de sesión secreta y la clave de sesión pública de la clave secreta individual del soporte de almacenamiento de datos o la clave pública individual del soporte de almacenamiento de

datos tiene lugar de forma aleatoria, es decir, en función de un segundo número aleatorio. También en este caso se pueden utilizar diferentes operaciones de derivación que permitan como datos de entrada al menos respectivamente la clave individual del soporte de almacenamiento de datos correspondiente y el segundo número aleatorio. Generalmente, la derivación de la clave de sesión secreta es distinta de la derivación de la clave de sesión pública. No obstante, para la derivación de ambas claves del par de claves de sesión se utiliza habitualmente el mismo segundo número aleatorio. Puesto que para cada uso del soporte de almacenamiento de datos, es decir, para cada autentificación ante un dispositivo terminal, se deriva un nuevo par de claves de sesión, no es posible rastrear el soporte de almacenamiento de datos mediante la clave de sesión.

De acuerdo con un modo de realización preferente del procedimiento según la invención, la clave de comunicación secreta se acuerda mediante un procedimiento conocido de intercambio de claves Diffie-Hellman. Este se basa en una raíz primitiva especificada de módulo un número primo especificado. La clave secreta individual del soporte de almacenamiento de datos es derivada de la clave de grupo secreta mediante multiplicación por el primer número aleatorio. La clave pública individual del soporte de almacenamiento de datos se calcula a partir de una exponenciación de la raíz primitiva con la clave secreta individual del soporte de almacenamiento de datos. En este caso, la clave de grupo pública está generada por exponenciación de la raíz primitiva con la clave de grupo secreta. El procedimiento según la invención, preferentemente con claves de sesión que cambian de forma aleatoria, se puede integrar por tanto sin importantes modificaciones en protocolos similares conocidos que prevén un par de claves asociado de forma fija al soporte de almacenamiento de datos y utilizan el procedimiento Diffie-Hellman.

La clave de sesión secreta se puede generar mediante multiplicación de la clave secreta individual del soporte de almacenamiento de datos por el segundo número aleatorio. Luego se deriva la clave de sesión pública mediante exponenciación de la clave individual del soporte de almacenamiento de datos con el segundo número aleatorio. De este modo resulta que la clave de sesión pública se puede calcular mediante una exponenciación de la clave de grupo pública con el producto del primer número aleatorio por el segundo.

Para que el terminal pueda verificar la clave de sesión pública del soporte de almacenamiento de datos, el soporte de almacenamiento de datos envía al dispositivo terminal la clave de sesión pública, el producto del primer número aleatorio por el segundo, y el certificado de la clave de grupo publica.

El dispositivo terminal verifica la clave de sesión pública, después de haber comprobado el certificado de la clave de grupo pública, calculando una exponenciación de la clave de grupo pública con el producto de ambos números aleatorios. El resultado de este cálculo es, tal como se ha descrito anteriormente, justamente la clave de sesión pública, siempre y cuando esta haya sido derivada del modo descrito a partir de la clave de grupo pública por medio de la clave pública individual del soporte de almacenamiento de datos. Por lo tanto, la clave de sesión pública se puede verificar exclusivamente mediante la clave de grupo pública. De este modo, el soporte de almacenamiento de datos es autentificado como correspondiente a la clave de grupo pública, manteniendo el anonimato del usuario del soporte de almacenamiento de datos y sin que sea necesario un certificado individual del soporte de almacenamiento de datos.

Por soporte de almacenamiento de datos cabe entender, por ejemplo, un documento de identidad electrónico, una tarjeta de chip, una tarjeta SIM, una tarjeta multimedia segura o un token USB seguro. El dispositivo terminal puede ser cualquier pareja de autentificación. En particular, puede ser un terminal local o remoto, un servidor remoto u otro soporte de almacenamiento de datos.

Como se ha indicado varias veces anteriormente, para derivar las claves secretas individuales del soporte de almacenamiento de datos y las claves públicas individuales del soporte de almacenamiento de datos de una pluralidad de diferentes soportes de almacenamiento de datos que forman un grupo de soportes de almacenamiento de datos, se utilizan respectivamente las mismas claves de grupo públicas o secretas. Naturalmente es posible prever varios grupos de soportes de almacenamiento de datos, que están asignados respectivamente a un par de claves de grupo propio.

A continuación se describe la invención a modo de ejemplo en relación a los dibujos adjuntos. Muestran:

La figura 1, en forma esquemática, un modo de realización preferente de un soporte de almacenamiento de datos según la invención y las

figuras 2 y 3, pasos de un modo de realización preferente del procedimiento según la invención para autentificar el soporte de almacenamiento de datos de la figura 1 ante un dispositivo terminal.

En relación a la figura 1, un soporte de almacenamiento de datos -10-, que aquí está representado como tarjeta de chip, comprende interfaces de comunicación de datos -20-, -20'-, un procesador -30-, así como diferentes memorias -40-, -50- y -60-. El soporte de almacenamiento de datos -10- también puede presentar otra forma constructiva.

Como interfaces de comunicación de datos -20-, -20'-, el soporte de almacenamiento de datos -10- comprende un conjunto de conexiones -20- para la comunicación de datos por contacto, así como una bobina de antena -20'- para

la comunicación de datos inalámbrica. Pueden estar previstas interfaces de comunicación de datos alternativas. Además es posible que el soporte de almacenamiento de datos -10- solo soporte un tipo de comunicación de datos, es decir, solo por contacto o inalámbrica.

La memoria ROM -40- no volátil de solo lectura comprende un sistema operativo (OS) -42- del soporte de almacenamiento de datos -10-, que controla el soporte de almacenamiento de datos -10-. Al menos partes del sistema operativo -42- pueden estar almacenadas en la memoria -50- no volátil de lectura y escritura. Esta puede estar presente, por ejemplo, a modo de memoria FLASH.

La memoria -50- comprende un dispositivo de autentificación -52-, mediante el cual se puede realizar una autentificación del soporte de almacenamiento de datos -10- ante un dispositivo terminal. En este caso se utilizan las claves individuales del soporte de almacenamiento de datos -54-, -56-, así como un certificado -58- digital, también almacenados en la memoria. El modo de funcionamiento del dispositivo de autentificación -52-, las claves -54-, -56- y el certificado -58-, así como su papel durante el procedimiento de autentificación se describen en detalle en base a las figuras 2 y 3. La memoria -50- puede contener otros datos, por ejemplo, datos relacionados con su usuario.

La memoria RAM -60- volátil de lectura y escritura sirve al soporte de almacenamiento de datos -10- como memoria de trabajo.

El soporte de almacenamiento de datos -10- puede comprender otras características (no mostradas), por ejemplo, si se trata de un documento de identidad electrónico. Estas pueden estar visibles sobre una superficie del soporte de almacenamiento de datos -10-, por ejemplo, impresas, y designar el usuario del soporte de almacenamiento de datos, por ejemplo, por su nombre o una foto.

Haciendo referencia a las figuras 2 y 3 se describe ahora en detalle un modo de realización del procedimiento para autentificar el soporte de almacenamiento de datos -10- ante un dispositivo terminal. En la figura 2 se muestran pasos preparativos. Estos se pueden realizar, por ejemplo, durante la fabricación del soporte de almacenamiento de datos -10-, por ejemplo, en una fase de personalización.

En un primer paso -S1- se generan una clave de grupo secreta -SK-, así como una clave de grupo pública -PK-. La clave -PK- se calcula como resultado de una exponenciación de una raíz primitiva de módulo -g- de un número primo -p- especificado. Todos los cálculos descritos a continuación se deben leer como módulo del número primo -p-, aunque no se indique siempre de forma explícita. Ambas claves -SK- y -PK- forman un par de claves de grupo y sirven de base para la arquitectura de claves descrita a continuación para un grupo de soportes de almacenamiento de datos -10- del mismo tipo.

En el paso -S2- se crea un certificado -C_{PK}- que sirve para la verificación de la clave de grupo pública -PK-.

El paso -S3- tiene lugar durante la personalización del soporte de almacenamiento de datos -10-. El soporte de almacenamiento de datos -10-, que representa un soporte de almacenamiento de datos de un grupo de soportes de almacenamiento de datos especificado, es provisto con un par de claves individuales del soporte de almacenamiento de datos -SK_i-, -PK_i-, que es derivado de forma aleatoria, es decir, en función de un primer número aleatorio -RND_i-, del par de claves de grupo -SK-, -PK-. De este modo, cada soporte de almacenamiento de datos -10- del grupo es provisto con un par propio de claves individuales del soporte de almacenamiento de datos que se diferencia del par de claves correspondiente de otro soporte de almacenamiento de datos del grupo por el componente aleatorio en la derivación de la clave. Por otro lado, todos los soportes de almacenamiento de datos -10- del grupo tienen en común que su par de claves ha sido derivado del mismo par de claves de grupo -SK-, -PK-.

En el paso parcial -TS31- se deriva una clave secreta individual del soporte de almacenamiento de datos -SK_i- mediante multiplicación de la clave de grupo secreta -SK- por el número aleatorio -RND_i-.

La clave pública individual del soporte de almacenamiento de datos -PK_i- se calcula a continuación, en el paso parcial -TS32-, como resultado de una exponenciación de la raíz primitiva -g- mencionada anteriormente con la clave secreta individual del soporte de almacenamiento de datos -SK_i- generada anteriormente.

Las claves -SK_i- y -PK_i- derivadas de este modo son almacenadas en el paso parcial -TS33- junto con el número aleatorio -RND_i- y el certificado -C_{PK}- en el soporte de almacenamiento de datos -10-. De este modo, este está configurado para realizar una autentificación ante un dispositivo terminal mediante su dispositivo de autentificación -52-, tal como se describe en detalle en relación a la figura 3.

Para preparar un acuerdo de clave con el dispositivo terminal (véase paso -S7-), el dispositivo de autentificación -52- deriva en el paso -S4- una clave de sesión secreta -$SK_{Session}$-. Esta clave de sesión secreta -$SK_{Session}$- forma junto con la clave de sesión pública -$PK_{Session}$- descrita a continuación (véase paso -S5-) un par de claves de sesión. No obstante, este par de claves es utilizado en el soporte de almacenamiento de datos por el dispositivo de autentificación -52- solo en relación a una única autentificación ante un dispositivo terminal. Para realizar cualquier autentificación adicional futura, el dispositivo de autentificación -52- deriva respectivamente un nuevo par de claves

de sesión a partir del par de claves individuales del soporte de almacenamiento de datos -SK_i-, -PK_i-, del modo descrito a continuación.

El par de claves de sesión también se genera con la ayuda de un componente aleatorio. Para ello, el dispositivo de autentificación -52- genera o pone a disposición un segundo número aleatorio -$RND_{Session}$-. La clave de sesión secreta -$SK_{Session}$- se puede calcular entonces mediante multiplicación de la clave secreta individual del soporte de almacenamiento de datos -SK_i- por el segundo número aleatorio -$RND_{Session}$-.

La clave de sesión pública -$PK_{Session}$- se deriva en el paso -S5- como resultado de la exponenciación de la clave pública individual del soporte de almacenamiento de datos -PK_i- con el segundo número aleatorio -$RND_{Session}$-. En el paso -S6-, el dispositivo de autentificación -52- envía al dispositivo terminal la clave de sesión pública -$PK_{Session}$-, el valor -RND_i*$RND_{Session}$-, que resulta de la multiplicación del primer número aleatorio por el segundo, y el certificado -C_{PK}-.

Entonces, en el paso -S7-, se acuerda una clave de comunicación -KK- entre el dispositivo de autentificación -52- del soporte de almacenamiento de datos -10- y el dispositivo terminal. Esta sirve para cifrar una comunicación de datos subsiguiente entre el soporte de almacenamiento de datos -10- y el dispositivo terminal mediante un procedimiento de cifrado simétrico. El acuerdo de clave se puede realizar con procedimientos conocidos, por ejemplo, el procedimiento de intercambio de claves Diffie-Hellman.

Finalmente, el dispositivo terminal comprueba en el paso -S8- la autenticidad del soporte de almacenamiento de datos -10-. Para ello, en un primer paso parcial -TS81- comprueba el certificado -C_{PK}- de la clave de grupo pública -PK-, que es conocida por el terminal. A continuación, el dispositivo terminal verifica la clave de sesión pública -$PK_{Session}$- del soporte de almacenamiento de datos -10-. Para ello, el dispositivo terminal calcula el resultado de la exponenciación de la clave de grupo pública con el producto -RND_i*$RND_{Session}$- de ambos números aleatorios y compara este resultado con la clave de sesión pública -$PK_{Session}$-. A través de este cálculo, el dispositivo terminal es capaz de derivar la clave de sesión pública -$PK_{Session}$- a partir de la clave de grupo pública -PK- por medio de la clave pública individual del soporte de almacenamiento de datos -PK_i-. Esto es así porque

$PK_{Session}$	$=PK_i\text{^}(RND_{Session})$	(véase paso -S5-)
	$=(g\text{^}(SK_i))\text{^}(RND_{Session})$	(véase paso parcial -TS32-)
	$=(g\text{^}(SK*RND_i))\text{^}(RND_{Session})$	(véase paso parcial -TS31-)
	$=(g\text{^}SK)\text{^}(RND_i*RND_{Session})$	(reformulación matemática)
	$=PK\text{^}(RND_i*RND_{Session})$	(véase paso -S1-)

Si el resultado coincide con la clave de sesión pública -$PK_{Session}$-, el soporte de almacenamiento de datos -10- se considera verificado. En el caso contrario, el dispositivo terminal interrumpe el procedimiento de autentificación.

Por lo tanto, el procedimiento hace posible mantener el anonimato del usuario del soporte de almacenamiento de datos -10-, al menos dentro del grupo de soportes de almacenamiento de datos asignados al mismo par de claves de grupo -SK-, -PK-. No es posible rastrear el usuario a partir del uso del soporte de almacenamiento de datos -10-, ya que, por un lado, para cada sesión se utilizan claves de sesión diferentes -$SK_{Session}$-, -$PK_{Session}$- y, por el otro lado, la verificación del soporte de almacenamiento de datos -10- tiene lugar únicamente mediante el certificado -C_{PK}- de la clave de grupo pública -PK-, que es igual para todos los soportes de almacenamiento de datos del grupo, y no mediante un certificado individual del soporte de almacenamiento de datos. También es ventajoso poder prescindir del almacenamiento de la clave de grupo secreta -SK- en el soporte de almacenamiento de datos -10- del grupo.

En el marco de la presente solución, una multiplicación puede ser cualquier multiplicación específica del grupo y una exponenciación, cualquier exponenciación específica del grupo. Las multiplicaciones y las exponenciaciones se pueden realizar en base al logaritmo discreto o en base a curvas elípticas. Además, en la derivación, por ejemplo, de la clave individual $SK_i = SK*RND_i$ se puede utilizar una derivación modificada para dificultar el cálculo de -SK-. Se puede elegir, por ejemplo: $SK_i = RND_i\text{^}\ SK$.

REIVINDICACIONES

1. Procedimiento para autentificar un soporte de almacenamiento de datos (10) portátil ante un dispositivo terminal, con los siguientes pasos:

- derivación (S5) de una clave de sesión pública ($PK_{Session}$) a partir de una clave pública individual del soporte de almacenamiento de datos (PK_i) derivada (TS32) de una clave de grupo pública (PK) y derivación (S4) de una clave de sesión secreta ($SK_{Session}$) a partir de una clave secreta individual del soporte de almacenamiento de datos (SK_i) derivada (TS31) de una clave de grupo secreta (SK), en el soporte de almacenamiento de datos (10);
- autentificación anónima (S8) del soporte de almacenamiento de datos (10) ante el dispositivo terminal utilizando la clave de sesión secreta ($SK_{Session}$) en el soporte de almacenamiento de datos (10) y un certificado (C_{PK}) de la clave de grupo pública (PK), que está almacenado en el soporte de almacenamiento de datos (10).

2. Procedimiento, según la reivindicación 1, **caracterizado por que** el dispositivo terminal verifica la clave de sesión pública ($PK_{Session}$) mediante el certificado (C_{PK}) de la clave de grupo pública (PK), dicho certificado estando almacenado en el soporte de almacenamiento de datos (10), tal que el dispositivo terminal comprueba (TS81) en primer lugar el certificado (C_{PK}) y luego reproduce (TS82) la derivación de la clave de sesión pública ($PK_{Session}$) a partir de la clave de grupo pública (PK) a través de la clave pública individual del soporte de almacenamiento de datos (PK_i).

3. Procedimiento, según la reivindicación 1 o 2, **caracterizado por que** la clave pública individual del soporte de almacenamiento de datos (PK_i) y la clave secreta individual del soporte de almacenamiento de datos (SK_i) son derivadas de la clave de grupo pública (PK) o la clave de grupo secreta (SK) y almacenadas (S3) en el soporte de almacenamiento de datos (10), en una fase de personalización del soporte de almacenamiento de datos (10).

4. Procedimiento, según cualquiera de las reivindicaciones 1 a 3, **caracterizado por que** la clave secreta individual del soporte de almacenamiento de datos (SK_i) es derivada de la clave de grupo secreta (SK) utilizando un primer número aleatorio (RND_i).

5. Procedimiento, según cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** la clave de sesión pública ($PK_{Session}$) y la clave de sesión secreta ($SK_{Session}$) son derivadas de la clave pública individual del soporte de almacenamiento de datos (PK_i) o la clave secreta individual del soporte de almacenamiento de datos (SK_i) utilizando un segundo número aleatorio ($RND_{Session}$).

6. Procedimiento, según cualquiera de las reivindicaciones 1 a 5, **caracterizado por** el acuerdo (S7) de una clave de comunicación (KK) entre el soporte de almacenamiento de datos (10) y el dispositivo terminal, utilizando la clave de sesión pública ($PK_{Session}$) y la clave de sesión secreta ($SK_{Session}$) del soporte de almacenamiento de datos (10), así como una clave de terminal pública y una clave de terminal secreta del dispositivo terminal.

7. Procedimiento, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por que** la clave de sesión secreta ($SK_{Session}$) se deriva (S4) mediante multiplicación de la clave secreta individual del soporte de almacenamiento de datos (SK_i) por el segundo número aleatorio ($RND_{Session}$) y la clave de sesión pública ($PK_{Session}$) se deriva (S5) mediante exponenciación de la clave pública individual del soporte de almacenamiento de datos (PK_i) con el segundo número aleatorio ($RND_{Session}$).

8. Procedimiento, según cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** el soporte de almacenamiento de datos (10) envía la clave de sesión pública ($PK_{Session}$), el producto (RND_i*$RND_{Session}$) del primer número aleatorio (RND_i) por el segundo ($RND_{Session}$), así como el certificado (C_{PK}) de la clave de grupo pública (PK) al dispositivo terminal.

9. Procedimiento, según cualquiera de las reivindicaciones 1 a 8, **caracterizado por que** el dispositivo terminal, para verificar la clave de sesión pública ($PK_{Session}$), calcula una exponenciación de la clave de grupo pública (PK) con el producto (RND_i*$RND_{Session}$) del primer número aleatorio (RND_i) por el segundo ($RND_{Session}$).

10. Procedimiento, según cualquiera de las reivindicaciones 1 a 9, **caracterizado por que** para derivar las claves públicas individuales del soporte de almacenamiento de datos (PK_i) y las claves secretas individuales del soporte de almacenamiento de datos (SK_i) de una pluralidad de diferentes soportes de almacenamiento de datos (10) se utilizan respectivamente las mismas claves de grupo públicas o secretas (PK; SK).

11. Soporte de almacenamiento de datos (10) portátil que comprende un procesador (30), una memoria (50) y una interfaz de comunicación de datos (20; 20') para la comunicación de datos con un dispositivo terminal, así como un dispositivo de autentificación (52), **caracterizado por que** el dispositivo de autentificación (52) del soporte de almacenamiento de datos (10) está configurado para derivar una clave de sesión pública ($PK_{Session}$) a partir de una clave pública individual del soporte de almacenamiento de datos (PK_i) almacenada en la memoria (50), para derivar una clave de sesión secreta ($PK_{Session}$) a partir de una clave secreta individual del soporte de almacenamiento de datos (SK_i) almacenada en la memoria (50) y para utilizar la clave de sesión secreta ($SK_{Session}$) en el marco de una

autentificación ante el dispositivo terminal, tal que la clave pública individual del soporte de almacenamiento de datos (PK_i) es derivada de una clave de grupo pública (PK) y la clave secreta individual del soporte de almacenamiento de datos (SK_i) es derivada de una clave de grupo secreta (SK), y tal que el soporte de almacenamiento de datos almacena un certificado (C_{PK}) de la clave de grupo pública (PK) para la autentificación.

12. Soporte de almacenamiento de datos (10), según la reivindicación 11, **caracterizado por que** el soporte de almacenamiento de datos (10) está configurado para autentificarse ante un dispositivo terminal conforme a un procedimiento, según cualquiera de las reivindicaciones 1 a 10.

13. Dispositivo terminal para la comunicación de datos con un soporte de almacenamiento de datos (10) portátil, según la reivindicación 11 o 12, tal que el dispositivo terminal está configurado para acordar una clave de comunicación (KK) con el soporte de almacenamiento de datos (10) portátil utilizando una clave de terminal pública y una clave de terminal secreta y para verificar la clave de sesión pública ($PK_{Session}$) del soporte de almacenamiento de datos (10), dicha clave de sesión pública habiendo sido derivada de la clave de grupo pública (PK) a través de la clave pública individual del soporte de almacenamiento de datos (PK_i).

14. Dispositivo terminal, según la reivindicación 13, **caracterizado por que** el dispositivo terminal está configurado para verificar la clave de sesión pública ($PK_{Session}$) del soporte de almacenamiento de datos (10) mediante el certificado (C_{PK}) de la clave de grupo pública (PK) que está almacenada en el soporte de almacenamiento de datos (10), tal que el dispositivo terminal comprueba en primer lugar el certificado (C_{PK}) y luego reproduce la derivación de la clave de sesión pública ($PK_{Session}$) a partir de la clave de grupo pública (PK) por medio de la clave pública individual del soporte de almacenamiento de datos (PK_i).

15. Sistema que comprende un soporte de almacenamiento de datos (10) portátil, según la reivindicación 11 o 12, y un dispositivo terminal, según la reivindicación 13 o 14, configurado para realizar un procedimiento, según cualquiera de las reivindicaciones 1 a 10.

FIG 1

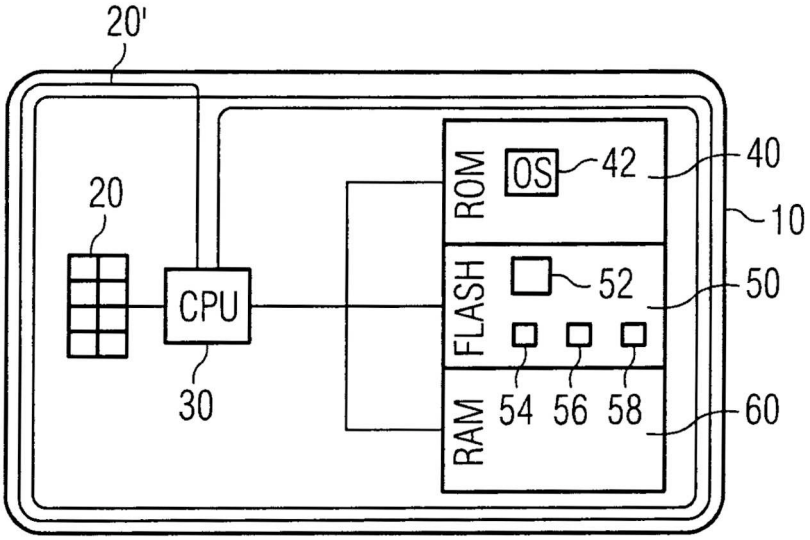


FIG 2

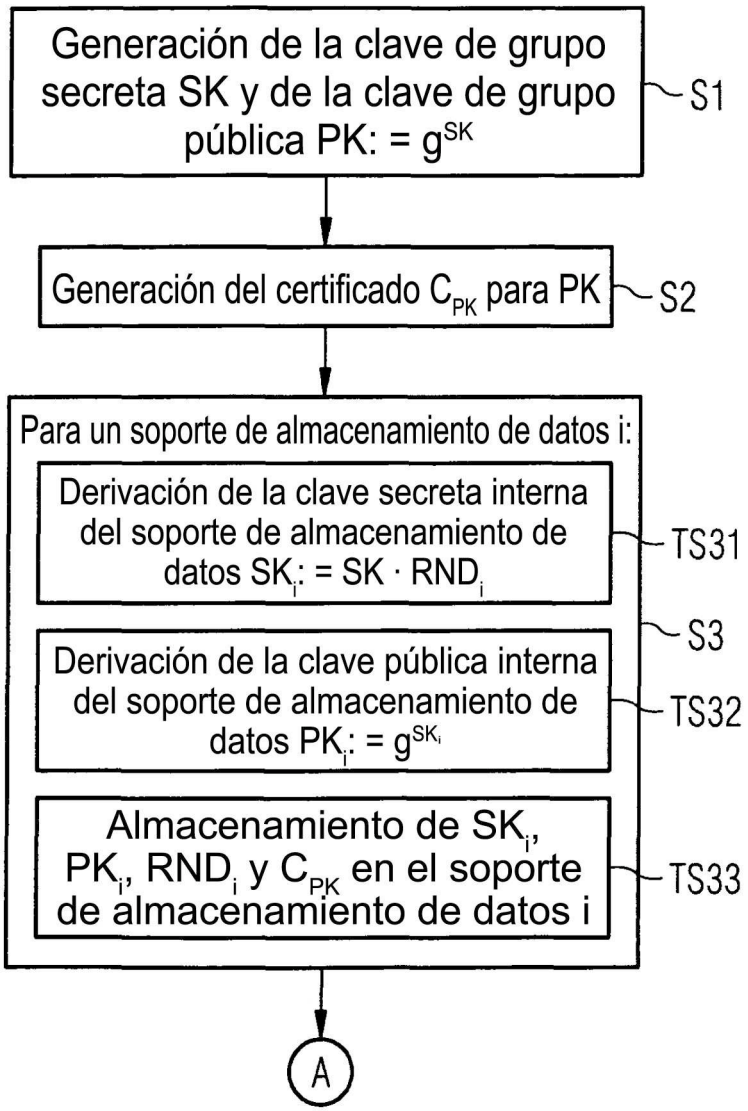
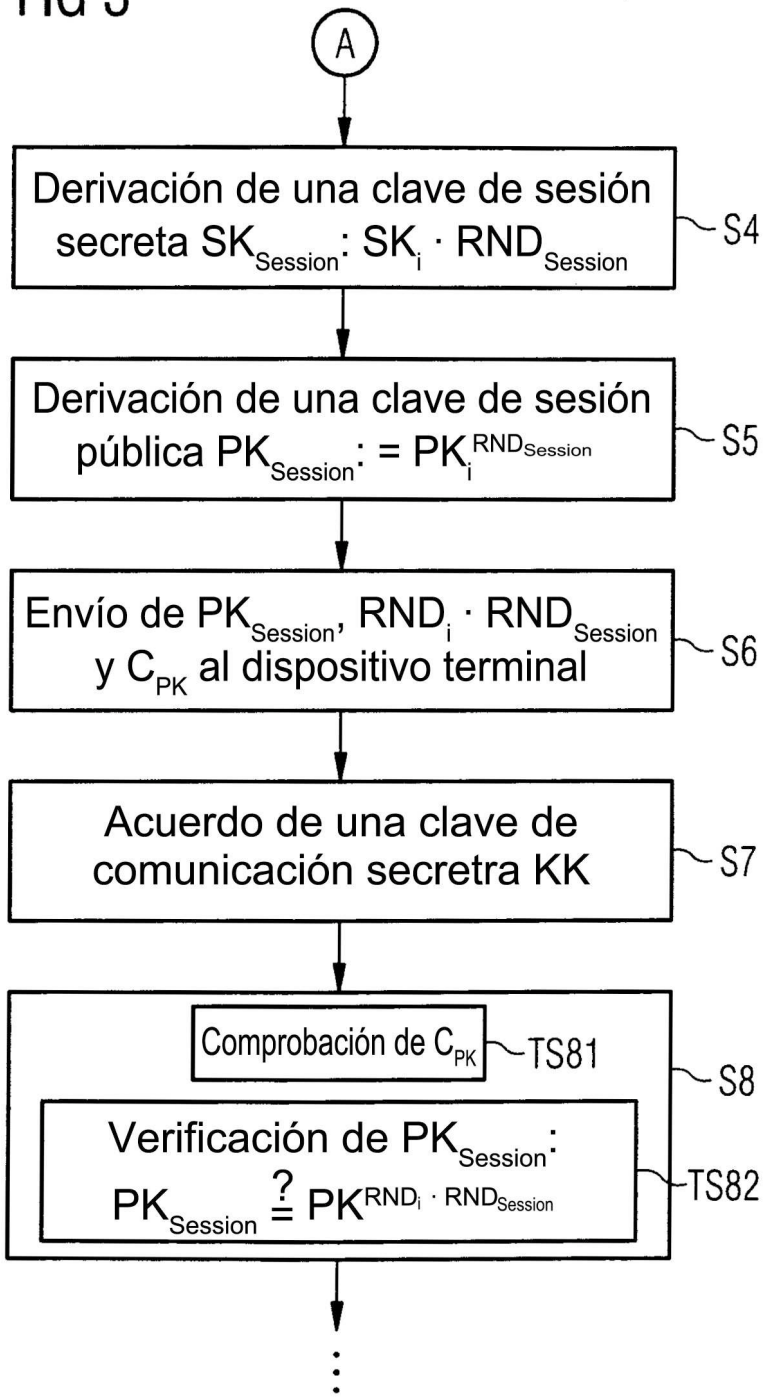

Generación de la clave de grupo secreta SK y de la clave de grupo pública PK: = g^{SK}
S1
Generación del certificado C_{PK} para PK
S2
Para un soporte de almacenamiento de datos i:
Derivación de la clave secreta interna del soporte de almacenamiento de datos SK_i: = SK · RND_i
TS31
S3
Derivación de la clave pública interna del soporte de almacenamiento de datos PK_i: = g^{SK_i}
TS32
Almacenamiento de SK_i, PK_i, RND_i y C_{PK} en el soporte de almacenamiento de datos i
TS33
A

FIG 3


A
Derivación de una clave de sesión secreta $SK_{Session}$: $SK_i \cdot RND_{Session}$
S4
Derivación de una clave de sesión pública $PK_{Session}$: = $PK_i^{RND_{Session}}$
S5
Envío de $PK_{Session}$, $RND_i \cdot RND_{Session}$ y C_{PK} al dispositivo terminal
S6
Acuerdo de una clave de comunicación secretra KK
S7
Comprobación de C_{PK}
TS81
S8
Verificación de $PK_{Session}$: $PK_{Session} \stackrel{?}{=} PK^{RND_i \cdot RND_{Session}}$
TS82