(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 328 983**

(51) Int. Cl.:
***H04L 29/06*** (2006.01)
***H04L 9/30*** (2006.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07704152 .3**
(96) Fecha de presentación : **26.01.2007**
(97) Número de publicación de la solicitud: **1980080**
(97) Fecha de publicación de la solicitud: **15.10.2008**

(54) Título: **Procedimiento y dispositivo para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones.**

(30) Prioridad: **30.01.2006 DE 10 2006 004 237**

(45) Fecha de publicación de la mención BOPI:
**19.11.2009**

(45) Fecha de la publicación del folleto de la patente:
**19.11.2009**

(73) Titular/es: **SIEMENS AKTIENGESELLSCHAFT**
**Wittelsbacherplatz 2**
**80333 München, DE**

(72) Inventor/es: **Abendroth, Jörg;**
**Cuellar, Jorge y**
**Rajasekaran, Hariharan**

(74) Agente: **Zuazo Araluze, Alexander**

## DESCRIPCIÓN

Procedimiento y dispositivo para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones.

La presente invención se refiere a un procedimiento y un dispositivo para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones.

Tales procedimientos se conocen por ejemplo por la solicitud de patente americana US 2005/0010769.

Existen múltiples posibilidades de aplicación para medios de memoria con baja capacidad de cálculo integrada, como por ejemplo lápices USB con procesadores incorporados, chips RFID, Smart Chip Cards (tarjetas con chip inteligente), etc. Los mismos pueden utilizarse por ejemplo para el control de accesos o en procesos logísticos. Otro campo de aplicación son los Digital Rights Management Systems (sistemas de gestión de derechos digitales), que se utilizan en la comercialización de DVDs y software licenciado.

Para utilizar estos aparatos de comunicaciones en tales aplicaciones críticas en cuanto a seguridad, es condición necesaria garantizar un manejo seguro de los datos sensibles, en particular en la transmisión a otro aparato de comunicaciones.

Explicaremos esto más en detalle en base a un ejemplo. El acceso a objetos de datos electrónicos protegidos frente a copiado, como por ejemplo ficheros de audio, ficheros de video o software, se regula usualmente mediante mecanismos de protección electrónicos denominados sistemas Digital Rights Management (de gestión de derechos digitales), DRM. Los mismos limitan el acceso a ofertas digitales la mayoría de las veces a usuarios registrados, es decir, de pago, o posibilitan incluso la facturación individual de cada acceso a una oferta. En la práctica esto funciona mediante formatos de ficheros especialmente desarrollados, que contienen una protección frente a copiado o bien una codificación. Estos ficheros pueden en consecuencia utilizarse sólo con programas especiales y la correspondiente clave llamada Content Encryption Key (clave de encriptado del contenido), CEK. Así no es posible acceder al contenido del objeto de datos protegido sin la correspondiente clave CEK.

Usualmente se memoriza el contenido codificado del objeto de datos a proteger sobre un medio de memoria como CDs, DVDs, lápices USB o tarjetas de memoria Memory Cards SD ("Secure Digital Memory Card", tarjeta de memoria digital segura) y la correspondiente clave CEK para la decodificación del contenido digital se distribuye separadamente. Es especialmente ventajoso suministrar la clave CEK sobre un aparato de comunicaciones con reducida capacidad de memoria y reducida capacidad de cálculo disponible.

Un ejemplo de un tal aparato de comunicaciones es un chip RFID ("Radio Frequency Identification", identificación de radiofrecuencia), que típicamente incluye un chip de silicio con un procesador integrado con capacidades de cálculo limitadas, una antena para la comunicación con un aparato lector y un pequeño espacio de memoria con unos dos Kilobytes. Estas características hacen de los chips RFID un atractivo medio para distribuir claves CEK con las que se otorga el acceso a contenidos codificados en un medio de memoria.

Al respecto es problemática la transmisión de la clave CEK o de los datos para averiguar la clave CEK al aparato de comunicaciones que debe decodificar el contenido protegido. En este caso debe quedar asegurado que la clave CEK sólo se transmite a aparatos de comunicaciones autorizados para ello y que estos aparatos de comunicaciones a su vez aceptan la clave CEK sólo de aparatos de comunicaciones autorizados para ello. Esto queda asegurado mediante un protocolo de autentificación mutuo entre el aparato de comunicaciones receptor y el aparato de comunicaciones transmisor. Los protocolos de autentificación conocidos necesitan para ello desde luego grandes capacidades de cálculo y una elevada capacidad de memoria disponible.

Con ello la invención tiene como tarea básica ofrecer un procedimiento y un dispositivo para la autentificación mutua de un primer aparato de comunicaciones y un segundo aparato de comunicaciones, así como para acordar una clave común entre el primer aparato de comunicaciones y el segundo aparato de comunicaciones, en el que frente a las soluciones hasta ahora conocidas se logre una reducción adicional de la capacidad de cálculo necesaria, así como una reducción del espacio de memoria necesario.

En el marco de la invención se resuelve esta tarea mediante un procedimiento y un dispositivo con las características de las reivindicaciones 1 y 7. Ventajosos perfeccionamiento de la invención se indican en las reivindicaciones subordinadas.

En el marco de la invención se acuerdan, en un procedimiento para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones, parámetros de seguridad entre ambos aparatos de comunicaciones. En base a los parámetros de seguridad acordados, calcula el segundo aparato de comunicaciones un primer valor de seguridad y lo transmite al primer aparato de comunicaciones. En base a los parámetros de seguridad acordados y al primer valor de seguridad transmitido, calcula el primer aparato de comunicaciones un segundo y un tercer valor de seguridad y los transmite al segundo aparato de comunicaciones. El segundo aparato de comunicaciones autentifica al primer aparato de comunicaciones cuando coinciden el segundo valor de seguridad transmitido y un cuarto valor de seguridad calculado por el segundo aparato de comunicaciones en base a los parámetros de seguridad

acordados. Cuando la autentificación ha tenido éxito, calcula el primer aparato de comunicaciones y el segundo aparato de comunicaciones en cada caso en base a los parámetros de seguridad acordados y al tercer valor de seguridad, una clave común. Al respecto es especialmente ventajoso que el protocolo de autentificación esté diseñado tal que el aparato de comunicaciones con baja capacidad integrada de cálculo no tenga que comprobar o verificar firmas ni certificados, y con ello se logre una considerable reducción del coste de cálculo necesario. Además, no se necesita ningún servidor central para la autentificación, ya que todos los valores necesarios para el proceso de autentificación pueden ya ser descargados sobre un medio de memoria accesible para el correspondiente aparato de comunicaciones.

Según otra configuración mejorada de la presente invención, se transmiten los parámetros de seguridad acordados y los valores de seguridad inalámbricamente entre el primer y el segundo aparato de comunicaciones, en particular mediante señales electromagnéticas de alta frecuencia según el estándar RFID.

Según otra configuración ventajosa de la presente invención, se incrementa un valor de contador en el primer aparato de comunicaciones tras cada acuerdo sobre una clave común y se utiliza para calcular el tercer valor de seguridad. Así se acuerda de manera ventajosa una clave común entre ambos aparatos de comunicaciones con un costo en cálculo lo más bajo posible.

Según un perfeccionamiento ventajoso de la presente invención, calcula el segundo aparato de comunicaciones en base a los parámetros de seguridad acordados y al segundo y/o tercer valor de seguridad transmitido un quinto valor de seguridad y lo transmite al primer aparato de comunicaciones. El primer aparato de comunicaciones autentifica al segundo aparato de comunicaciones cuando coinciden el quinto valor de seguridad trasmitido y un sexto valor de seguridad transmitido y un sexto valor de seguridad calculado por el primer aparato de comunicaciones en base a los parámetros de seguridad acordados. Esto tiene el efecto ventajoso de que también el segundo aparato de comunicaciones es autentificado directamente por el primer aparato de comunicaciones. Esto puede ser necesario en aplicaciones especialmente críticas para la seguridad.

Según el dispositivo correspondiente a la invención para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones, presenta el dispositivo medios que están equipados tal que pueden realizarse las siguientes etapas del procedimiento:

Entre el primer y el segundo aparato de comunicaciones se acuerdan parámetros de seguridad. En base a los parámetros de seguridad acordados, calcula el segundo aparato de comunicaciones un primer valor de seguridad y lo transmite al primer aparato de comunicaciones. El primer aparato de comunicaciones calcula un segundo y un tercer valor de seguridad en base a los parámetros de seguridad acordados y al primer valor de seguridad trasmitido y los transmite al segundo aparato de comunicaciones. El segundo aparato de comunicaciones autentifica al primer aparato de comunicaciones cuando coinciden el segundo valor de seguridad trasmitido y un cuarto valor de seguridad calculado por el segundo aparato de comunicaciones en base a los parámetros de seguridad acordados. Cuando la autentificación ha tenido éxito, calculan el primer aparato de comunicaciones y el segundo aparato de comunicaciones una clave común, en cada caso en base a los parámetros de seguridad acordados y al tercer valor de seguridad.

La presente invención se describirá a continuación más en detalle con ejemplos de ejecución en base a los dibujos. Se muestra en

figura 1 una representación esquemática de un procedimiento para autentificar y acordar una clave común para dos aparatos de comunicaciones,

figura 2 una representación esquemática de un vector de bits de datos con una ocupación del vector de bits de datos con informaciones relativas a derechos en relación con un objeto de datos,

figura 3 una representación esquemática de un procedimiento para acordar una clave común entre dos aparatos de comunicaciones,

figura 4 una representación esquemática de un procedimiento para la autentificación mutua entre dos aparatos de comunicaciones.

La figura 1 muestra esquemáticamente un procedimiento para autentificar un primer aparato de comunicaciones respecto a un segundo aparato de comunicaciones y para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones. El primer aparato de comunicaciones es en este ejemplo de ejecución un chip RFID 101 y el segundo aparato de comunicaciones un reproductor de DVD 102 que desea obtener acceso al contenido digital almacenado sobre un DVD 103. Para ello necesita el reproductor de DVD 102 del chip RFID 101 material de claves KM, para generar como función del Secret String (cadena secreta) SS y material de claves KM la clave de encriptado del contenido (Content Encryption Key CEK) para decodificar el contenido digital del DVD 103. Al comienzo del procedimiento acuerdan ambos aparatos de comunicaciones 101 y 102 parámetros de seguridad. El chip RFID 101 conoce una clave privada (Privat Key) d, una firma Sig, parámetros sobre la curva elíptica n,G y una clave pública (Public Key) D = d*G y el reproductor de DVD 102 conoce una clave de firma pública (Public Signature Key) SK, parámetros sobre la curva elíptica n,G y una clave del reproductor kp.

En una primera etapa 104 transmite el chip RFID 101 los parámetros sobre la curva elíptica n,G juntamente con la clave pública D y la firma Sig al reproductor de DVD 102. Cuando el reproductor de DVD 102 ha verificado la firma del chip RFID 101 en base a los parámetros sobre la curva elíptica n,G y de la clave de la firma pública SK, calcula el reproductor de DVD 102 un primer valor de seguridad C = c*G con $c \in_{RAND} [1,n]$ y transmite este primer valor de seguridad en una segunda etapa 105 al chip RFID 101. Este calcula en base al primer valor de seguridad C recibido y a su clave privada d un segundo valor de seguridad R = d*C. Para calcular un tercer valor de seguridad p*G, calcula el chip RFID 101 primeramente un X = d*R y transforma el valor X calculado a continuación en un número natural p. Finalmente calcula el chip RFID 101 el tercer valor de seguridad p*G. El segundo y el tercer valor de seguridad se transmiten finalmente en las etapas 106 y 107 al reproductor de DVD 102. Cuando un valor de seguridad c*D = c*d*G es igual al segundo valor de seguridad R recibido, autentifica el reproductor de DVD 102 al chip RFID 101. Ambos aparatos de comunicaciones 101 y 102 calculan a continuación la clave de sesión común c*D = p*c*G. En base a la clave común Key codifica el chip RFID 101 el material de claves KM y transmite el material de claves codificado en la etapa 108 al reproductor de DVD 102. El reproductor de DVD 102 calcula sobre el DVD 103 el correspondiente Secret String (cadena secreta) SS y calcula sobre la base del material de claves decodificado KM y del Secret String SS la clave de encriptado del contenido CEK. Con ayuda del CEK está ahora el reproductor de DVD 102 en condiciones de decodificar el contenido digital codificado que se encuentra sobre el DVD 103.

Puesto que el reproductor de DVD 102 sólo puede calcular la clave de encriptado del contenido CEK cuando ha recibido el Secret String SS utilizando una Device Key (clave del aparato) idéntica, se autentifica el reproductor de DVD 102 en este ejemplo de ejecución implícitamente frente al chip RFID 101.

La figura 2 muestra a modo de ejemplo un vector de bits de datos que está memorizado en un aparato de comunicaciones con baja capacidad de cálculo y baja capacidad de memoria disponible. Éste indica qué derechos posee un determinado usuario sobre un determinado objeto de datos. El vector de datos puede por ejemplo indicar un derecho existente en un punto 201 predefinido en el vector de bits de datos mediante un 1 y un derecho no existente mediante un 0. La correspondiente función de estado relativa al correspondiente derecho está prevista en este ejemplo en una celda del vector de bits de datos 202 contigua, que puede predeterminarse. En el ejemplo de la figura 2 puede interpretarse el vector del bits de datos en el sentido de que el objeto de datos puede reproducirse 201 tres veces 202, puede copiarse 204 dos veces 203 y a partir de una cierta fecha 205 sólo copiarse una vez 206.

La figura 3 muestra esquemáticamente un procedimiento para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones. El procedimiento de autentificación entre el chip RFID 301 y el reproductor de DVD 302 se realiza en este ejemplo de ejecución tal como en el ejemplo de ejecución antes descrito en relación con la figura 1. En este ejemplo de ejecución se prevé además un valor de contador 1, que está memorizado en el chip RFID 301 y que tras cada acuerdo cerrado sobre una clave común se incrementa en el valor 1. La clave común Key la calcula el chip RFID 301 tras realizarse la autentificación del chip RFID 301 frente al reproductor de DVD 302 en la etapa 304 como función del valor del contador 1 y de la clave privada d. A continuación se transmite el valor del contador 1 y el material de claves KM codificado con la clave Key desde el chip RFID 301 al reproductor de DVD 302 en la etapa 305. A continuación el chip RFID 301 incrementa el valor del contador 1 en el valor 1. Con ayuda del valor del contador 1 recibido, reconstruye el reproductor de DVD 302 la clave Key y decodifica a continuación el material de claves KM codificado. Tal como ya se ha descrito antes, el reproductor de DVD 302 está a continuación en condiciones de calcular sobre la base del material de claves KM decodificado y del Secret String SS la clave de encriptado del contenido CEK para decodificar el contenido digital sobre el DVD 303.

La figura 4 muestra un procedimiento para autentificar un segundo aparato de comunicaciones frente a un primer aparato de comunicaciones. En este ejemplo de ejecución se utiliza en lugar de un DVD un servidor 403, al que un usuario desea obtener acceso con ayuda de un chip RFID 401 a través de una puerta del servidor 402. La autentificación del chip RFID 401 respecto a la puerta del servidor 402 se realiza según el procedimiento descrito en la figura 2. Una vez realizada la autentificación en la etapa 404, calcula el chip RFID 401 el tercer valor de seguridad p*C y transmite el mismo en la etapa 405 a la puerta del servidor 402, que transmite el tercer valor de seguridad a su vez en la etapa 406 al servidor 403. El servidor 403 calcula ahora un quinto valor de seguridad R = w*p*C y transmite el quinto valor de seguridad en las etapas 407 y 408 a través de la puerta del servidor 402 al chip RFID 401. Si coincide el quinto valor de seguridad transmitido con un sexto valor de seguridad p*W = p*w*G calculado por el chip RFID 401, autentifica el chip RFID 401 la puerta del servidor 402. Una vez finalizada la autentificación mutua, puede transmitir el chip RFID 401 informaciones que se necesitan para recibir a través de la puerta del servidor 402 acceso al servidor 403.

La presente invención no queda limitada a los ejemplos de ejecución aquí descritos.

## REIVINDICACIONES

1. Procedimiento para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones, en el que

- entre el primer y el segundo aparato de comunicaciones se acuerdan parámetros de seguridad (104),
- en base a los parámetros de seguridad acordados, el segundo aparato de comunicaciones calcula un primer valor de seguridad y lo transmite al primer aparato de comunicaciones (105),
- en base a los parámetros de seguridad acordados y al primer valor de seguridad transmitido, el primer aparato de comunicaciones calcula un segundo y un tercer valor de seguridad y los transmite al segundo aparato de comunicaciones (106, 107),
- el segundo aparato de comunicaciones autentifica al primer aparato de comunicaciones cuando coinciden el segundo valor de seguridad transmitido y un cuarto valor de seguridad calculado por el segundo aparato de comunicaciones en base a los parámetros de seguridad acordados,
- cuando la autentificación tiene éxito, el primer aparato de comunicaciones y el segundo aparato de comunicaciones calculan en cada caso en base a los parámetros de seguridad acordados y al tercer valor de seguridad, una clave común.

2. Procedimiento según la reivindicación 1, en el que

los parámetros de seguridad acordados incluyen parámetros de una curva elíptica y parámetros para un procedimiento asimétrico criptográfico.

3. Procedimiento según la reivindicación 1, en el que

los parámetros de seguridad acordados y los valores de seguridad se transmiten inalámbricamente entre el primer y el segundo aparato de comunicaciones.

4. Procedimiento según la reivindicación 1, en el que

los parámetros de seguridad acordados y los valores de seguridad se transmiten mediante señales electromagnéticas de alta frecuencia según el estándar RFID entre el primer y el segundo aparato de comunicaciones.

5. Procedimiento según la reivindicación 1, en el que

- un valor de contador en el primer aparato de comunicaciones se incrementa después de cada acuerdo sobre una clave común,
- el valor del contador se utiliza para calcular el tercer valor de seguridad.

6. Procedimiento según la reivindicación 1, en el que

- en base a los parámetros de seguridad acordados y al segundo o tercer valor de seguridad transmitido, el segundo aparato de comunicaciones calcula un quinto valor de seguridad y lo transmite al primer aparato de comunicaciones.
- el primer aparato de comunicaciones autentifica al segundo aparato de comunicaciones cuando coinciden el quinto valor de seguridad transmitido y un sexto valor de seguridad calculado por el primer aparato de comunicaciones en base a los parámetros de seguridad acordados.

7. Dispositivo para acordar una clave común entre un primer aparato de comunicaciones y un segundo aparato de comunicaciones, en el que el dispositivo presenta medios que están equipados tal que pueden ejecutarse las siguientes etapas de procedimiento:

- entre el primer y el segundo aparato de comunicaciones se acuerdan parámetros de seguridad (104)
- en base a los parámetros de seguridad acordados, el segundo aparato de comunicaciones calcula un primer valor de seguridad y lo transmite al primer aparato de comunicaciones (105),
- en base a los parámetros de seguridad acordados y al primer valor de seguridad transmitido, el primer aparato de comunicaciones calcula un segundo y un tercer valor de seguridad y los transmite al segundo aparato de comunicaciones (106, 107),

- el segundo aparato de comunicaciones autentifica al primer aparato de comunicaciones cuando coinciden el segundo valor de seguridad transmitido y un cuarto valor de seguridad calculado por el segundo aparato de comunicaciones en base a los parámetros de seguridad acordados,

- cuando la autentificación tiene éxito, el primer aparato de comunicaciones y el segundo aparato de comunicaciones calculan en cada caso en base a los parámetros de seguridad acordados y al tercer valor de seguridad, una clave común.

FIG 1

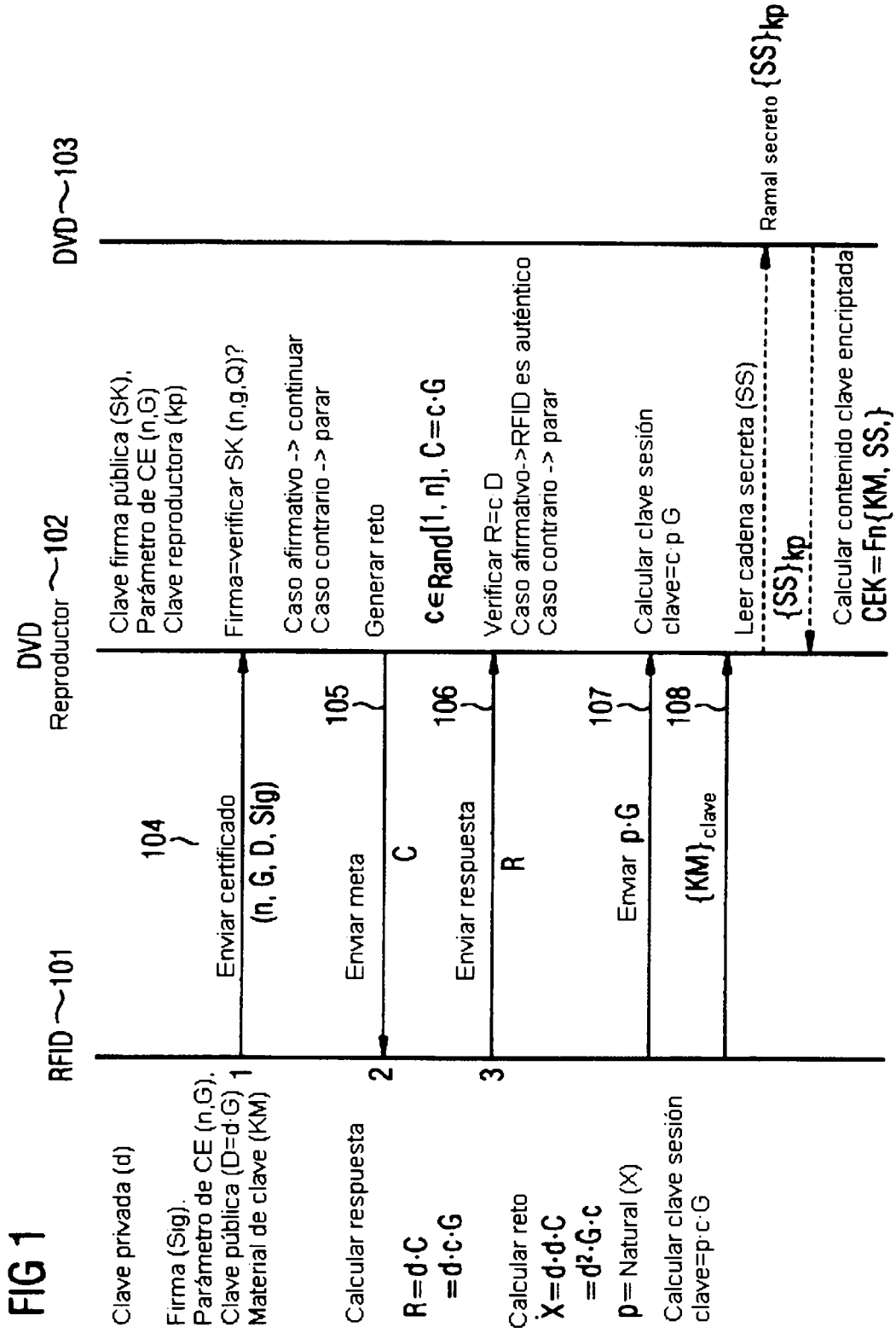

RFID ~101
DVD
Reproductor ~102
DVD ~103
Clave privada (d)
Firma (Sig).
Parámetro de CE (n,G),
Clave pública (D=d·G)
Material de clave (KM)
Calcular respuesta
R=d·C
=d·c·G
Calcular reto
X=d·d·C
=d²·G·c
p= Natural (X)
Calcular clave sesión
clave=p·c·G
1
2
3
104
Enviar certificado
(n, G, D, Sig)
Clave firma pública (SK),
Parámetro de CE (n,G)
Clave reproductora (kp)
Firma=verificar SK (n,g,Q)?
Caso afirmativo -> continuar
Caso contrario -> parar
105
Enviar meta
C
Generar reto
c∈Rand[1, n], C=c·G
106
Enviar respuesta
R
Verificar R=c D
Caso afirmativo->RFID es auténtico
Caso contrario -> parar
107
Enviar p·G
Calcular clave sesión
clave=c·p·G
108
{KM}clave
Leer cadena secreta (SS)
{SS}kp
Calcular contenido clave encriptada
CEK=Fn{KM, SS,}
Ramal secreto {SS}kp

FIG 2

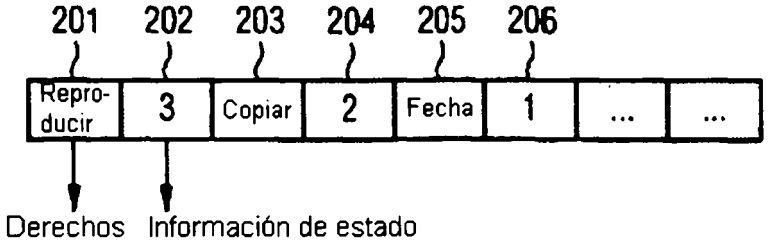

201
202
203
204
205
206
Repro-ducir
3
Copiar
2
Fecha
1
...
...
Derechos
Información de estado

FIG 3

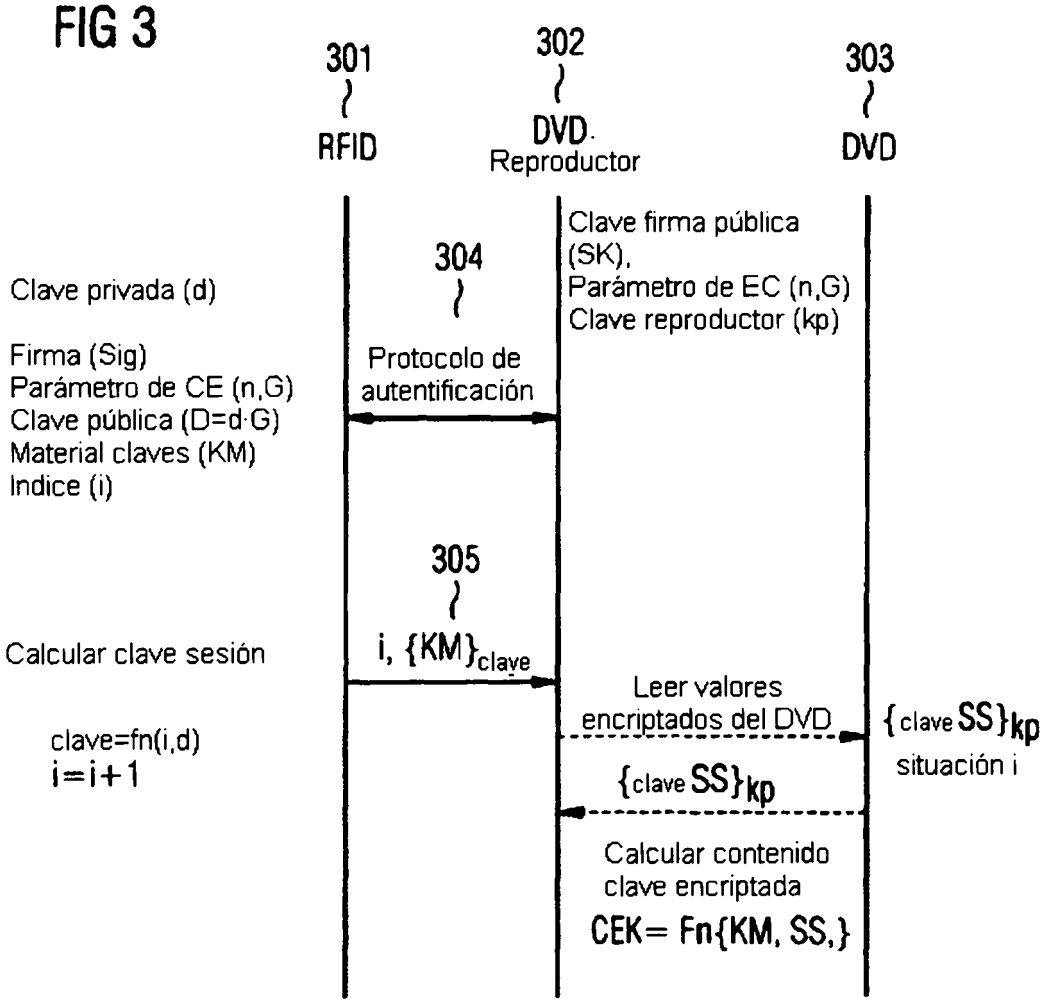
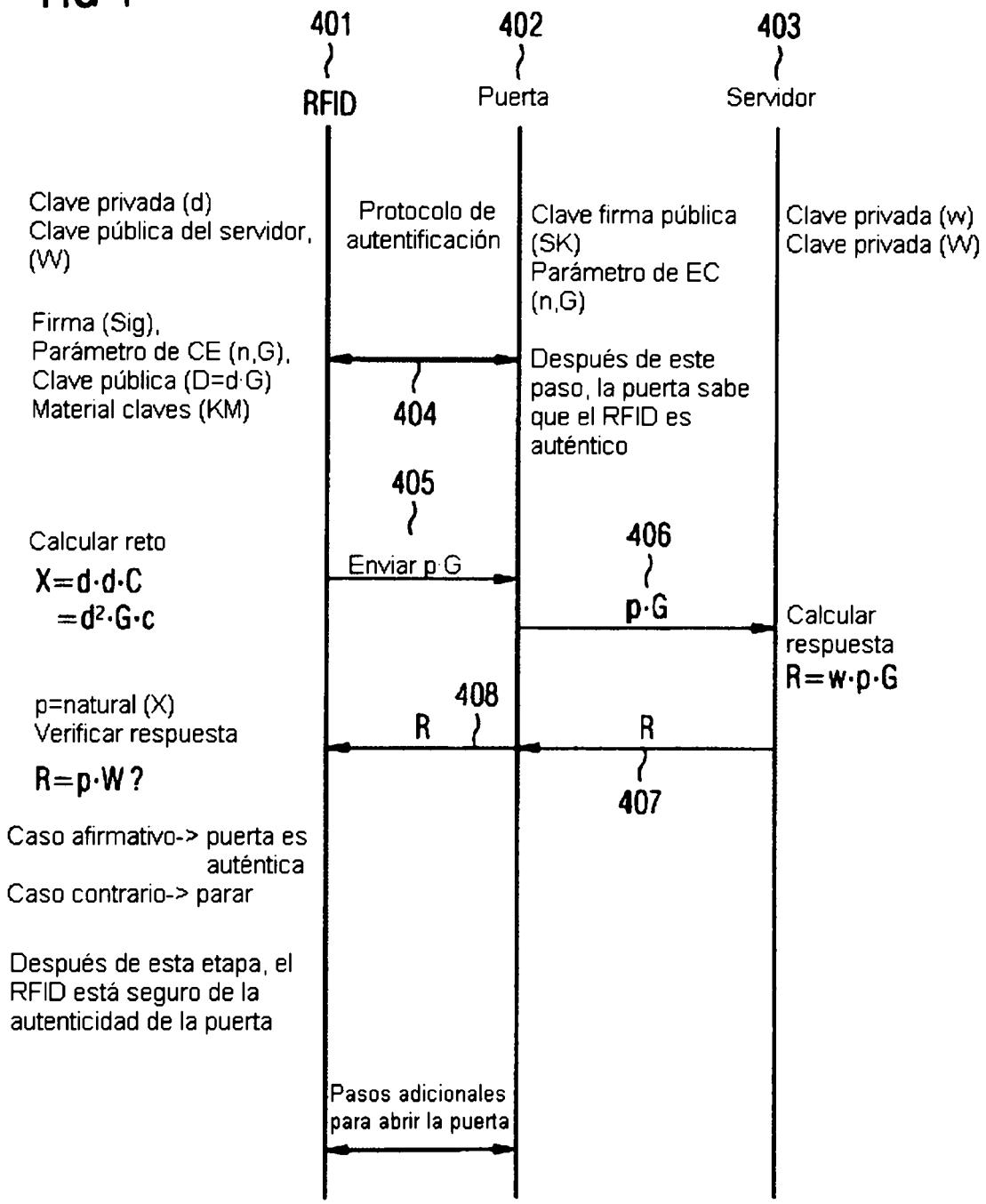

301
RFID
302
DVD-Reproductor
303
DVD
Clave privada (d)
Firma (Sig)
Parámetro de CE (n,G)
Clave pública (D=d·G)
Material claves (KM)
Indice (i)
304
Protocolo de autentificación
Clave firma pública (SK),
Parámetro de EC (n,G)
Clave reproductor (kp)
305
i, {KM}clave
Calcular clave sesión
clave=fn(i,d)
i=i+1
Leer valores encriptados del DVD
{clave SS}kp
situación i
{clave SS}kp
Calcular contenido clave encriptada
CEK= Fn{KM, SS,}

FIG 4


401
RFID
402
Puerta
403
Servidor
Clave privada (d)
Clave pública del servidor, (W)
Protocolo de autentificación
Clave firma pública (SK)
Parámetro de EC (n,G)
Clave privada (w)
Clave privada (W)
Firma (Sig),
Parámetro de CE (n,G),
Clave pública (D=d·G)
Material claves (KM)
404
Después de este paso, la puerta sabe que el RFID es auténtico
405
Calcular reto
X=d·d·C
=d²·G·c
Enviar p·G
406
p·G
Calcular respuesta
R=w·p·G
p=natural (X)
Verificar respuesta
R=p·W ?
408
R
R
407
Caso afirmativo-> puerta es auténtica
Caso contrario-> parar
Después de esta etapa, el RFID está seguro de la autenticidad de la puerta
Pasos adicionales para abrir la puerta