(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 372 780**

(51) Int. CI.:
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08160321 .9**
(96) Fecha de presentación: **27.06.2003**
(97) Número de publicación de la solicitud: **1973297**
(97) Fecha de publicación de la solicitud: **24.09.2008**

(54) Título: **MEDICIÓN DE DISTANCIA AUTENTICADA SEGURA.**

(30) Prioridad:
26.07.2002 EP 02078076

(45) Fecha de publicación de la mención BOPI:
26.01.2012

(45) Fecha de la publicación del folleto de la patente:
26.01.2012

(73) Titular/es:
KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN, NL

(72) Inventor/es:
Kamperman, Franciscus L. A. J.

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

DESCRIPCION

Medición de distancia autenticada segura.

La invención se refiere a un método para un primer dispositivo de comunicación para realizar una medición de distancia autenticada entre un primer dispositivo de comunicación y un segundo dispositivo de comunicación. La invención también se refiere a un método para determinar si contenido protegido almacenado en un primer dispositivo de comunicación debe accederse mediante un segundo dispositivo de comunicación. Además, la invención se refiere a un primer dispositivo de comunicación para realizar una medición de distancia autenticada a un segundo dispositivo de comunicación.

Los medios digitales se han convertido en portadores populares para varios tipos de información de datos. El software informático y la información de audio, por ejemplo, están ampliamente disponibles en discos compactos ópticos (CD) y recientemente también el DVD ha ganado en compartición de distribución. El CD y el DVD utilizan una norma común para la grabación digital de datos, software, imágenes y audio. Medios adicionales, tales como discos grabables, memoria de estado sólido, y similares, están realizando ganancias considerables en el mercado de distribución de software y datos.

La calidad sustancialmente superior del formato digital en comparación con el formato analógico hace que el primero sea sustancialmente más propenso a una copia no autorizada o piratería, además un formato digital es tanto más fácil como más rápido de copiar. Mediante la copia de un flujo de datos digital, ya esté comprimido, no comprimido, encriptado o no encriptado, normalmente no conduce a ninguna pérdida de calidad apreciable en los datos. Por tanto, la copia digital es esencialmente ilimitada en cuanto a copias de múltiples generaciones. Los datos analógicos con su pérdida de relación señal a ruido con cada copia secuencial, por otro lado, están limitados de manera natural en cuanto a copias de múltiples generaciones y en masa.

La llegada de la popularidad reciente en el formato digital también ha provocado bastantes sistemas y métodos de protección de copias y DRM. Estos sistemas y métodos usan tecnologías tales como encriptado, marcado de agua y descripciones correctas (por ejemplo reglas para acceder y copiar datos).

Una manera de proteger el contenido en la forma de datos digitales es garantizar que el contenido sólo se transferirá entre dispositivos si

- el dispositivo de recepción se ha autenticado como un dispositivo conforme,

- si el usuario del contenido tiene el derecho a transferir (mover, copiar) ese contenido a otro dispositivo.

Si se permite la transferencia del contenido, esto se realizará normalmente de una manera encriptada para asegurarse de que el contenido no pueda captarse ilegalmente en un formato útil.

La tecnología para realizar la autenticación de dispositivos y la transferencia de contenido encriptado está disponible y se denomina canal autenticado seguro (SAC). Aunque pueda permitirse realizar copias de contenido sobre un SAC, la industria de contenido está muy en alza en la distribución de contenido sobre Internet. Esto da como resultado un desacuerdo de la industria de contenido sobre transferir contenido sobre interfaces que coinciden bien con Internet, por ejemplo Ethernet.

Además, un usuario que visita a su vecino debe poder ver una película, que posee, en la pantalla de televisión grande del vecino. Normalmente, el propietario de contenido no permitirá esto, pero puede ser aceptable si puede probarse que un propietario de licencia de esa película (o un dispositivo que posee el propietario de la licencia) está cerca de la pantalla de televisión.

Por tanto es de interés poder incluir una medición de distancia autenticada cuando se decide si el contenido debe accederse o copiarse por otros dispositivos.

En el artículo por Stefan Brands y David Chaum, “Distance-Bounding protocols”, Eurocrypt ’93 (1993), páginas 344-359, se describe la integración de protocolos de acotamiento de distancia con esquemas de identificación de clave pública. En este caso la medición de distancia se describe basándose en la medición de tiempo usando bits de desafío y de respuesta y con el uso de un protocolo de compromiso. Esto no permite pruebas de conformidad de dispositivo autenticado y no es eficaz cuando dos dispositivos también deben autenticarse entre sí.

Un objeto de la invención es obtener una solución al problema de realizar una transferencia segura de contenido dentro de una distancia limitada.

Esto se obtiene mediante un método según la reivindicación 1. Un primer dispositivo de comunicación realiza una medición de distancia autenticada entre dicho primer dispositivo de comunicación y un segundo dispositivo de comunicación, en el que el primer y el segundo dispositivo de comunicación comparten un secreto común y dicho

secreto común se usa para realizar la medición de distancia entre dicho primer y dicho segundo dispositivo de comunicación.

Puesto que el secreto común está usándose para realizar la medición de distancia, puede garantizarse que cuando se mide la distancia desde el primer dispositivo de comunicación al segundo dispositivo de comunicación, es la distancia entre los dispositivos correctos la que está midiéndose.

El método combina un protocolo de medición de distancia con un protocolo de autenticación. Esto permite pruebas de conformidad de dispositivo autenticado y es eficaz, porque se necesita de cualquier manera un canal seguro para permitir una comunicación segura entre los dispositivos y un dispositivo puede someterse a prueba en primer lugar para determinar la conformidad antes de ejecutarse una medición de distancia.

En una realización específica, el secreto común se comparte de manera segura con el segundo dispositivo encriptando el secreto común usando una clave pública de un par de clave privada/pública.

En una realización específica adicional, la medición de distancia comprende una medición de tiempo de ida y vuelta para determinar la distancia medida. En una realización específica, la medición de distancia autenticada se realiza según las siguientes etapas,

- transmitir una primera señal desde el primer dispositivo de comunicación al segundo dispositivo de comunicación en un primer tiempo t1, estando dicho segundo dispositivo de comunicación adaptado para recibir dicha primera señal, generar una segunda señal modificando la primera señal recibida según el secreto común y transmitir la segunda señal al primer dispositivo,

- recibir la segunda señal en un segundo tiempo t2,

- comprobar si la segunda señal se ha modificado según el secreto común,

- determinar la distancia entre el primer y el segundo dispositivo de comunicación según una diferencia de tiempo entre t1 y t2.

Cuando se mide una distancia midiendo la diferencia de tiempo entre la transmisión y recepción de una señal y usando un secreto compartido entre el primer y el segundo dispositivo de comunicación, para determinar si la señal devuelta realmente se originó del segundo dispositivo de comunicación, la distancia se mide de una manera autenticada segura que garantiza que la distancia no se medirá para un tercer dispositivo de comunicación (que no conoce el secreto). El uso de un secreto compartido para modificar la señal es una manera simple de realizar una medición de distancia autenticada segura.

En una realización específica la primera señal es una señal de espectro ensanchado. Así se obtiene una resolución alta y es posible afrontar condiciones de mala transmisión (por ejemplo entornos inalámbricos con muchas reflexiones).

En otra realización la etapa de comprobar si la segunda señal se ha modificado según el secreto común se realiza mediante las etapas de,

- generar una tercera señal modificando la primera señal según el secreto común,

- comparar la tercera señal con la segunda señal recibida.

Este método es una manera fácil y sencilla de realizar la comprobación, pero requiere que tanto el primer dispositivo de comunicación como el segundo dispositivo de comunicación sepan cómo está modificándose la primera señal usando el secreto común.

En una realización específica la primera señal y el secreto común son palabras de bits y la segunda señal comprende información que se genera realizando un XOR entre las palabras de bits. Así, es una operación muy sencilla la que tiene que realizarse, dando como resultado una demanda de pocos recursos tanto por el primer como por el segundo dispositivo de comunicación cuando se realiza la operación.

En una realización el secreto común se ha compartido antes de realizar la medición de distancia, realizándose la compartición mediante las etapas de,

- realizar una comprobación de autenticación desde el primer dispositivo de comunicación en el segundo dispositivo de comunicación comprobando si dicho segundo dispositivo de comunicación es conforme con un conjunto de reglas de conformidad predefinidas,

- si el segundo dispositivo de comunicación es conforme, compartir dicho secreto común transmitiendo dicho secreto

al segundo dispositivo de comunicación.

Ésta es una manera segura de realizar la compartición del secreto, garantizando que sólo los dispositivos que son conformes con las reglas de conformidad pueden recibir el secreto. Además, el secreto compartido puede usarse después para generar un canal SAC entre los dos dispositivos. El secreto puede compartirse usando por ejemplo mecanismos de transporte clave tal como se describe en la norma ISO 11770-3. Alternativamente, puede usarse un protocolo de acuerdo de clave, que por ejemplo también se describe en la norma ISO 11770-3.

En otra realización la comprobación de autenticación comprende además comprobar si la identificación del segundo dispositivo es conforme con una identificación esperada. Así, se garantiza que el segundo dispositivo es realmente el dispositivo que debe ser. La identidad puede obtenerse comprobando un certificado almacenado en el segundo dispositivo.

La invención también se refiere a un método para determinar si datos almacenados en un primer dispositivo de comunicación deben accederse mediante un segundo dispositivo de comunicación, comprendiendo el método la etapa de realizar una medición de distancia entre el primer y el segundo dispositivo de comunicación y comprobar si dicha distancia medida está dentro de un intervalo de distancia predefinido, en el que la medición de distancia es una medición de distancia autenticada según lo anterior. Mediante el uso de la medición de distancia autenticada en relación con compartir datos entre los dispositivos, puede reducirse la distribución de contenido no autorizada.

En una realización específica los datos almacenados en el primer dispositivo se envían al segundo dispositivo si se determina que los datos almacenados en el primer dispositivo deben accederse por el segundo dispositivo.

En una realización específica el método para determinar si datos multimedia almacenados en un primer dispositivo de comunicación deben accederse mediante un segundo dispositivo de comunicación comprende la etapa de realizar una medición de distancia entre un tercer dispositivo de comunicación y el segundo dispositivo de comunicación y comprobar si dicha distancia medida está dentro de un intervalo de distancia predefinido, en el que la medición de distancia es una medición de distancia autenticada según lo anterior. En esta realización, la distancia no se mide entre el primer dispositivo de comunicación, en el que se almacenan los datos, y el segundo dispositivo de comunicación. En cambio, la distancia se mide entre un tercer dispositivo de comunicación y el segundo dispositivo de comunicación, en la que el tercer dispositivo de comunicación puede ser personal para el propietario del contenido.

La invención también se refiere a un primer dispositivo de comunicación configurado para determinar si datos multimedia almacenados en el dispositivo de comunicación deben accederse mediante un segundo dispositivo de comunicación. El primer dispositivo de comunicación realiza una medición de distancia autenticada al segundo dispositivo de comunicación, en el que el primer dispositivo de comunicación comparte un secreto común con el segundo dispositivo de comunicación y en el que el dispositivo de comunicación comprende medios para medir la distancia al segundo dispositivo usando dicho secreto común.

En una realización el dispositivo comprende,

- medios para transmitir una primera señal a un segundo dispositivo de comunicación en un primer tiempo t1, estando dicho segundo dispositivo de comunicación adaptado para recibir dicha primera señal, generar una segunda señal modificando la primera señal recibida según el secreto común y transmitir la segunda señal,

- medios para recibir la segunda señal en un segundo tiempo t2,

- medios para comprobar si la segunda señal se ha modificado según el secreto común,

- medios para determinar la distancia entre el primer y el segundo dispositivo de comunicación según una diferencia de tiempo entre t1 y t2.

El documento US5126746 da a conocer un sistema para la calibración de distancia segura entre un lector y una etiqueta, en el que la distancia entre los dos se determina a partir del tiempo entre una señal desde el lector a la etiqueta y una respuesta devuelta por la etiqueta. La etiqueta espera un periodo de tiempo variable antes de devolver la respuesta, periodo que depende de una encriptación de un número aleatorio enviado por la etiqueta usando una clave que sólo conoce el lector y la etiqueta.

El documento WO 01/93434 da a conocer un método y un dispositivo para permitir y bloquear un intercambio de datos entre un dispositivo local y uno remoto basándose en una distancia del dispositivo remoto en relación con el dispositivo local.

El documento WO 97/39553 da a conocer a sistema de autenticación inalámbrica para controlar un estado de funcionamiento de un nodo tal como un ordenador basado en la proximidad de un usuario autorizado que lleva un testigo al nodo. El nodo envía un desafío al testigo, que debe devolver una respuesta correcta dentro de un tiempo

predeterminado. Si la respuesta llega demasiado tarde o es incorrecta, se niega el acceso al nodo. En una realización el testigo encripta el desafío con una clave secreta almacenada en una memoria local.

A continuación se describirán realizaciones preferidas de la invención con referencia a las figuras, en las que

la figura 1 ilustra una medición de distancia autenticada que se usa para la protección de contenido,

la figura 2 es un diagrama de flujo que ilustra el método de realizar una medición de distancia autenticada,

la figura 3 ilustra en mayor detalle la etapa de realizar la medición de distancia autenticada mostrada en la figura 2,

la figura 4 ilustra un dispositivo de comunicación para realizar la medición de distancia autenticada.

La figura 1 ilustra una realización en la que la medición de distancia autenticada que se usa para la protección de contenido. En el centro del círculo 101 se coloca un ordenador 103. El ordenador comprende un contenido, tal como un contenido multimedia que es vídeo o audio, almacenado por ejemplo en un disco duro, DVD o CD. El propietario del ordenador es propietario del contenido y por tanto el ordenador está autorizado para acceder y presentar el contenido multimedia para el usuario. Cuando el usuario desea realizar una copia legal del contenido a otro dispositivo a través de por ejemplo un SAC, se mide la distancia entre el otro dispositivo y el ordenador 103 y sólo se permite que los dispositivos dentro de una distancia predefinida ilustrada por los dispositivos 105, 107, 109, 111, 113 dentro del círculo 101 reciban el contenido. Mientras tanto, no se permite que los dispositivos 115, 117, 119 que tienen una distancia al ordenador 101 que es más grande que la distancia predefinida reciban el contenido.

En el ejemplo un dispositivo es un ordenador, pero también puede ser por ejemplo una unidad de DVD, una unidad de CD o un vídeo, siempre que el dispositivo comprenda un dispositivo de comunicación para realizar la medición de distancia.

En un ejemplo específico puede no tener que medirse la distancia entre el ordenador, en el que se almacenan los datos, y el otro dispositivo, también puede ser un tercer dispositivo por ejemplo un dispositivo que es personal para el propietario del contenido el que está dentro de la distancia predefinida.

En la figura 2 un diagrama de flujo ilustra la idea general de realizar una medición de distancia autenticada entre dos dispositivos, 201 y 203, que comprenden cada uno dispositivos de comunicación para realizar la medición de distancia autenticada. En el ejemplo el primer dispositivo 201 comprende contenido que ha solicitado el segundo dispositivo 203. Entonces la medición de distancia autenticada es tal como sigue. En 205 el primer dispositivo 201 autentica al segundo dispositivo 203; esto puede comprender las etapas de comprobar si el segundo dispositivo 203 es un dispositivo conforme y también puede comprender la etapa de comprobar si el segundo dispositivo 203 es realmente el dispositivo identificado para el primer dispositivo 201. Entonces en 207, el primer dispositivo 201 intercambia un secreto con el segundo dispositivo 203, lo que por ejemplo puede realizarse transmitiendo una palabra de bits generada aleatoria a 203. El secreteo debe compartirse de manera segura, por ejemplo según algún protocolo de gestión de clave tal como se describe por ejemplo en la norma ISO 11770.

Entonces en 209, se transmite una señal para la medición de distancia al segundo dispositivo 203; el segundo dispositivo modifica la señal recibida según el secreto y retransmite la señal modificada de vuelta al primer dispositivo. El primer dispositivo 201 mide un tiempo de ida y vuelta entre la señal que sale y la señal que vuelve y comprueba si la señal devuelta se modificó según el secreto intercambiado. La modificación de la señal devuelta según algún secreto dependerá lo más probablemente del sistema de transmisión y la señal usada para la medición de distancia, es decir será específica para cada sistema de comunicación (tal como 1394, Ethernet, Bluetooth, ieee 802.11, etc.).

La señal usada para la medición de distancia puede ser una señal de bits de datos normales, pero también pueden usarse señales especiales distintas de para la comunicación de datos. En una realización se usan señales de espectro ensanchado para permitir conseguir una alta resolución y permitir afrontar condiciones de mala transmisión (por ejemplo entornos inalámbricos con muchas reflexiones).

En un ejemplo específico se usa una señal de espectro ensanchado de secuencia directa para la medición de distancia; esta señal puede modificarse mediante una operación con XOR de los chips (por ejemplo el código de ensanchamiento consiste en 127 chips) del código de secuencia directa mediante los bits del secreto (por ejemplo el secreto también consiste en 127 bits). Además, pueden usarse otras operaciones matemáticas como XOR.

La autenticación 205 y el intercambio de secreto 207 pueden realizarse usando los protocolos descritos en algunas normas ISO conocidas: ISO 9798 y ISO 11770. Por ejemplo el primer dispositivo 201 puede autenticar el segundo dispositivo 203 según el siguiente escenario de comunicación:

Primer dispositivo -> Segundo dispositivo: R_B||Text 1

donde R_B es un número aleatorio

Segundo dispositivo -> Primer dispositivo: CertA||TokenAB

Donde CertA es un certificado de A

$TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)$

R_A es un número aleatorio

Identificador B es una opción

sS_A es una firma establecida por A usando una clave privada S_A

Si se sustituye TokenAB por el testigo tal como se especifica en la norma as ISO 11770-3 puede realizarse al mismo tiempo un intercambio de clave secreta. Puede usarse esto sustituyendo Text2 por:

$Text2:= eP_B(A||K||Text2) ||Text3$

Donde eP_B está encriptado con clave pública B

A es un identificador de A

K es un secreto que va a intercambiarse

En este caso el segundo dispositivo 203 determina la clave (es decir tiene control de clave), esto también se denomina protocolo de transporte de clave, pero también puede usarse protocolo de acuerdo de clave. Esto puede no desearse en cuyo caso puede invertirse, de manera que el primer dispositivo determine la clave. Ahora se ha intercambiado una clave secreta según 207 en la figura 2. Nuevamente, la clave secreta puede intercambiarse por ejemplo por un protocolo de transporte de clave o un protocolo de acuerdo de clave.

Después de que se ha medido la distancia de una manera segura autenticada tal como se describió anteriormente, puede enviarse contenido, datos, entre el primer y el segundo dispositivo en 211.

La figura 3 ilustra en mayor detalle la etapa de realizar la medición de distancia autenticada. Tal como se describió anteriormente el primer dispositivo 301 y el segundo dispositivo 303 han intercambiado un secreto; el secreto se almacena en la memoria 305 del primer dispositivo y la memoria 307 del segundo dispositivo. Para realizar la medición de distancia, se transmite una señal al segundo dispositivo a través de un transmisor 309. El segundo dispositivo recibe la señal a través del receptor 311 y 313 modifica la señal usando el secreto localmente almacenado. La señal se modifica según reglas conocidas por el primer dispositivo 301 y se transmite de vuelta al primer dispositivo 301 a través de un transmisor 315. El primer dispositivo 301 recibe la señal modificada a través de un receptor 317 y en 319 se compara la señal modificada recibida con una señal, que se ha modificado localmente. La modificación local se realiza en 321 usando la señal transmitida al segundo dispositivo en 309 y luego modificando la señal usando el secreto localmente almacenado similar a las reglas de modificación usadas por el segundo dispositivo. Si la señal modificada recibida y la señal localmente modificada son idénticas, entonces la señal recibida se autentica y puede usarse para determinar la distancia entre el primer y el segundo dispositivo. Si las dos señales no son idénticas, entonces la señal recibida no puede autenticarse y por tanto no puede usarse para medir la distancia tal como se ilustra por 325. En 323 se calcula la distancia entre el primer y el segundo dispositivo; por ejemplo esto puede realizarse midiendo el tiempo, cuando la señal se transmite por el transmisor 309 desde el primer dispositivo al segundo dispositivo y la medición cuando el receptor 317 recibe la señal desde el segundo dispositivo. Entonces puede usarse la diferencia de tiempo entre el tiempo de transmisión y el tiempo de recepción para determinar la distancia física entre el primer dispositivo y el segundo dispositivo.

En la figura 4 se ilustra un dispositivo de comunicación para realizar la medición de distancia autenticada. El dispositivo 401 comprende un receptor 403 y un transmisor 411. El dispositivo comprende además medios para realizar las etapas descritas anteriormente, que puede ser mediante ejecución de software usando un microprocesador 413 conectado a la memoria 417 a través de un bus de comunicación. El dispositivo de comunicación puede colocarse entonces dentro de dispositivos tales como un DVD, un ordenador, un CD, un grabador de CD, un televisor y otros dispositivos para acceder a contenido protegido.

REIVINDICACIONES

1. Método para determinar si contenido protegido almacenado en un primer dispositivo (201) de comunicación debe accederse mediante un segundo dispositivo (203) de comunicación, comprendiendo el método la etapa de realizar una medición de distancia entre el primer (201) y el segundo dispositivo (203) de comunicación y comprobar si dicha distancia medida está dentro de un intervalo de distancia predefinido, caracterizado porque la medición de distancia es una medición de distancia autenticada y porque el primer y el segundo dispositivo de comunicación comparten un secreto común y dicho secreto común se usa para realizar la medición de distancia y en el que

- el primer dispositivo (201) autentica al segundo dispositivo (203), y

- el primer dispositivo (201) comparte de manera segura el secreto común con el segundo dispositivo (203) según un protocolo de gestión de clave.

2. Método según la reivindicación 1, en el que el secreto común se comparte de manera segura con el segundo dispositivo encriptando el secreto común usando una clave pública de un par de clave privada/pública.

3. Método según la reivindicación 1, en el que la medición de distancia comprende una medición de tiempo de ida y vuelta para determinar la distancia medida.

4. Método según la reivindicación 3, en el que la medición de tiempo de ida y vuelta se realiza según las siguientes etapas,

- transmitir (305) una primera señal desde el primer dispositivo (201) de comunicación al segundo dispositivo (203) de comunicación en un primer tiempo t1, estando dicho segundo dispositivo de comunicación adaptado para recibir (311) dicha primera señal, generar (313) una segunda señal modificando la primera señal recibida según el secreto común y transmitir (315) la segunda señal al primer dispositivo,

- recibir (317) la segunda señal en un segundo tiempo t2,

- comprobar (319) si la segunda señal se ha modificado según el secreto común,

- determinar (323) una diferencia de tiempo entre el primer tiempo t1 y el segundo tiempo t2.

5. Método según la reivindicación 4, en el que la primera señal es una señal de espectro ensanchado.

6. Método según la reivindicación 5, en el que la etapa de comprobar si la segunda señal se ha modificado según el secreto común se realiza mediante las etapas de,

- generar una tercera señal modificando la primera señal según el secreto común,

- comparar la tercera señal con la segunda señal recibida.

7. Método según la reivindicación 4, en el que la primera señal y el secreto común son palabras de bits y en el que la segunda señal comprende información que se genera realizando un XOR entre las palabras de bits.

8. Método según la reivindicación 1, en el que el secreto común se ha compartido antes de realizar la medición de distancia, realizándose la compartición mediante las etapas de,

- realizar una comprobación (205) de autenticación desde el primer dispositivo (201) de comunicación en el segundo dispositivo (203) de comunicación, comprobando si dicho segundo dispositivo (203) de comunicación es conforme con un conjunto de reglas de conformidad predefinidas,

- si el segundo dispositivo de comunicación es conforme, compartir (207) dicho secreto común transmitiendo dicho secreto al segundo dispositivo (203) de comunicación.

9. Método según la reivindicación 8, en el que la comprobación de autenticación comprende además comprobar si la identificación del segundo dispositivo (203) es conforme con una identificación esperada.

10. Método según la reivindicación 1, en el que el contenido protegido almacenado en el primer dispositivo (201) se envía al segundo dispositivo (203) si se determina que el contenido protegido almacenado en el primer dispositivo (201) debe accederse por el segundo dispositivo (203).

11. Método según la reivindicación 10, en el que el contenido protegido puede enviarse entre el primer y el segundo dispositivo después de que se ha medido la distancia de una manera segura autenticada.

12. Método según la reivindicación 1, en el que la autenticación del segundo dispositivo (203) por el primer dispositivo (201) comprende las etapas de comprobar si el segundo dispositivo (203) es un dispositivo conforme.

13. Método según la reivindicación 1, en el que la autenticación del segundo dispositivo (203) por el primer dispositivo (201) comprende la etapa de comprobar si el segundo dispositivo (203) es realmente el dispositivo identificado para el primer dispositivo (201).

14. Método según la reivindicación 1, en el que compartir de manera segura el secreto con el segundo dispositivo (203) por el primer dispositivo (201) comprende transmitir una palabra de bits generada de manera aleatoria al segundo dispositivo (203).

15. Método según la reivindicación 1, en el que el secreto común compartido se usa después para generar un canal autenticado seguro entre el primer (201) y el segundo dispositivo (203) de comunicación.

16. Primer dispositivo (201) de comunicación configurado para determinar si el contenido protegido almacenado en el primer dispositivo (201) de comunicación debe accederse mediante un segundo dispositivo (203) de comunicación, comprendiendo el primer dispositivo medios para realizar una medición de distancia entre el primer (201) y el segundo dispositivo (203) de comunicación y comprobar si dicha distancia medida está dentro de un intervalo de distancia predefinido, caracterizado porque la medición de distancia es una medición de distancia autenticada y porque el primer dispositivo comprende una memoria que almacena un secreto común también almacenado en el segundo dispositivo de comunicación, secreto común que se usa para realizar la medición de distancia, estando el primer dispositivo configurado (411, 413, 417) para autenticar al segundo dispositivo (203) y luego compartir de manera segura el secreto con el segundo dispositivo.

17. Primer dispositivo (201) de comunicación según la reivindicación 16, que comprende además

- medios dispuestos para compartir de manera segura el secreto común con el segundo dispositivo (203) encriptando el secreto común usando una clave pública de un par de clave privada/pública.

18. Primer dispositivo (201) de comunicación según la reivindicación 16, que comprende además:

- medios para transmitir (305) una primera señal desde el primer dispositivo (201) de comunicación al segundo dispositivo (203) de comunicación en un primer tiempo t1, estando dicho segundo dispositivo de comunicación adaptado para recibir (311) dicha primera señal, generar (313) una segunda señal modificando la primera señal recibida según el secreto común y transmitir (315) la segunda señal al primer dispositivo,

- medios para recibir (317) la segunda señal en un segundo tiempo t2,

- medios para comprobar (319) si la segunda señal se ha modificado según el secreto común,

- medios para determinar (323) una diferencia de tiempo entre el primer tiempo t1 y el segundo tiempo t2 para determinar la distancia medida.

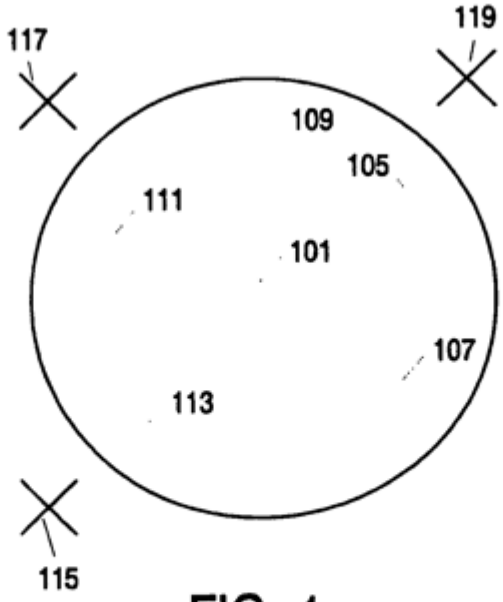
117
119
109
105
111
101
107
113
115

FIG. 1

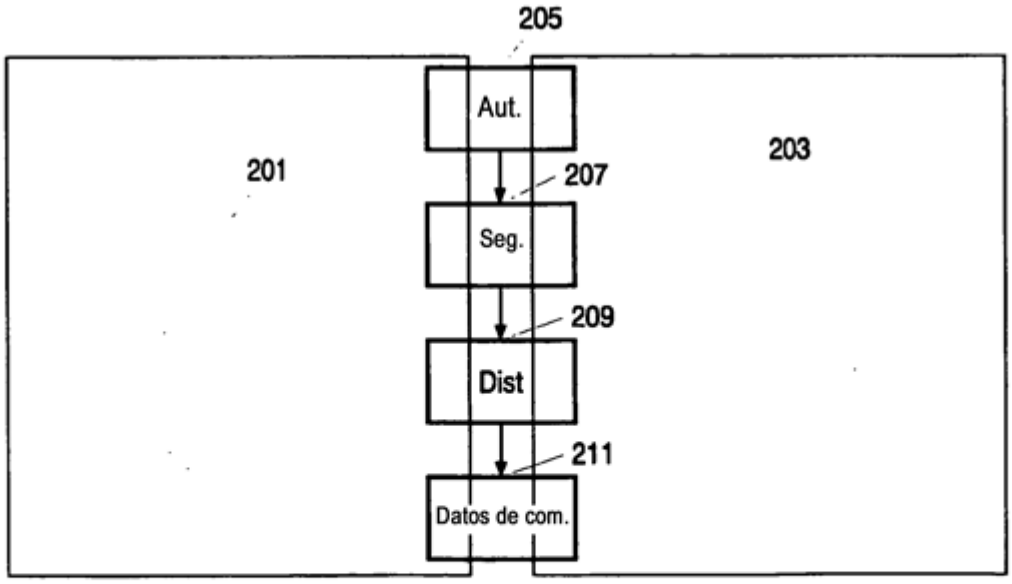
205
Aut.
201
203
207
Seg.
209
Dist
211
Datos de com.

FIG. 2

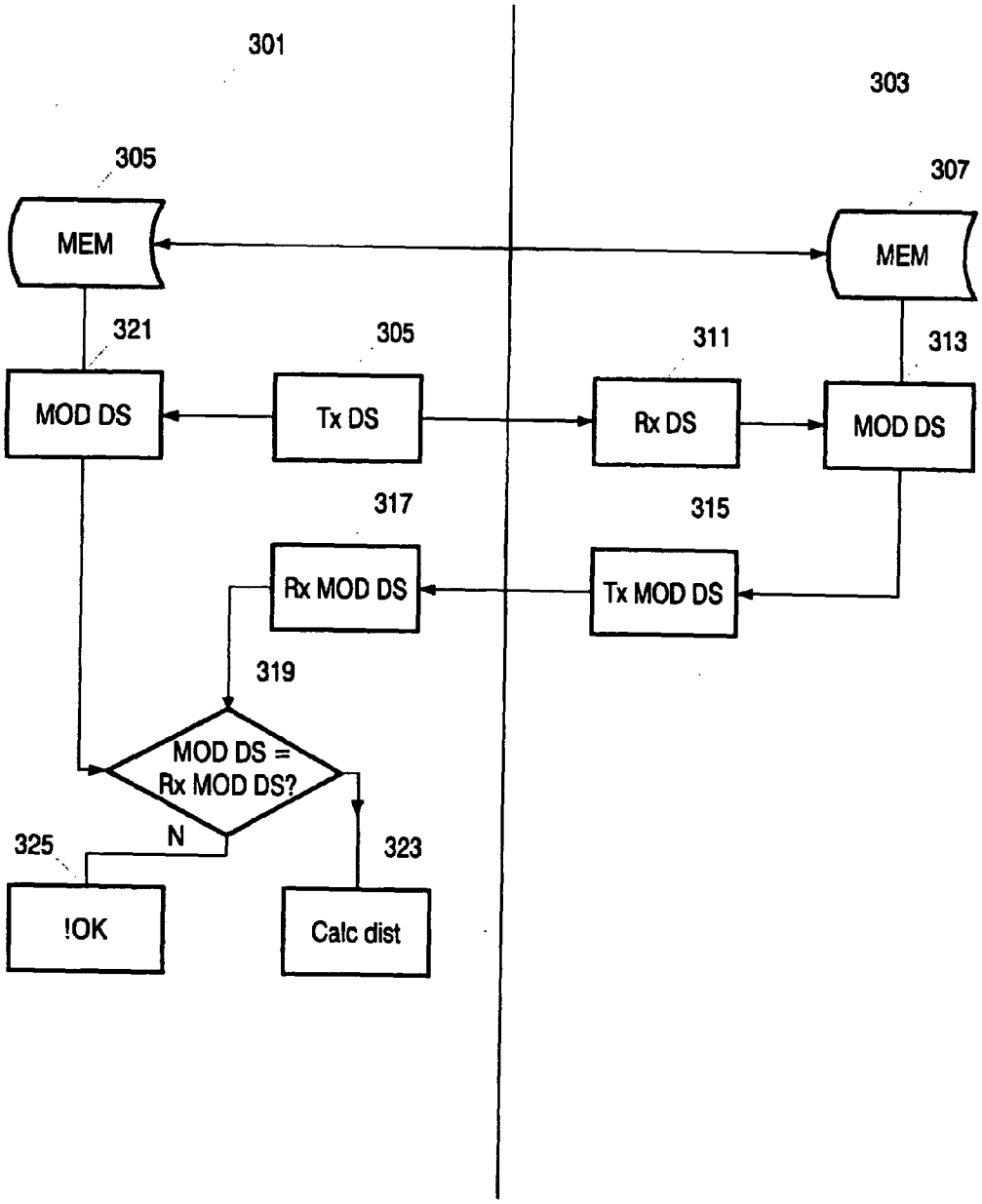
301
303
305
307
MEM
MEM
321
305
311
313
MOD DS
Tx DS
Rx DS
MOD DS
317
315
Rx MOD DS
Tx MOD DS
319
MOD DS =
Rx MOD DS?
N
325
323
!OK
Calc dist

FIG. 3

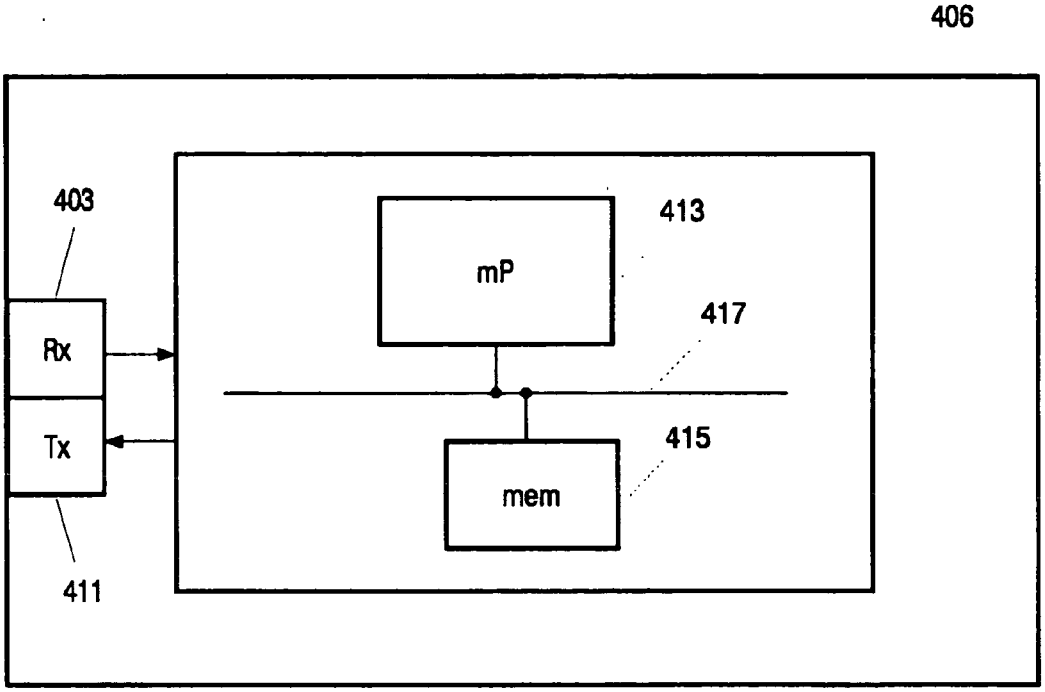

FIG. 4