(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 531 910**

(51) Int. CI.:

H04N 21/418 (2011.01)
H04N 21/4367 (2011.01)
H04N 21/443 (2011.01)
G06F 21/77 (2013.01)
H04N 7/16 (2011.01)
G06F 21/12 (2013.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.11.2006 E 06830247 (0)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 1955248**

(54) Título: **Módulo de seguridad actualizable**

(30) Prioridad:

30.11.2005 EP 05111532

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.03.2015

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
ROUTE DE GENÈVE 22-24
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

HILL, MICHAEL JOHN

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Módulo de seguridad actualizable

Dominio de la invención

[0001] La presente invención se refiere al dominio de los módulos de seguridad electrónicos, en particular a los módulos de seguridad destinados al control de acceso a las prestaciones teletransmitidas y otros medios de comunicación.

Estado de la técnica

[0002] Las operaciones de seguridad se realizan habitualmente en un módulo de seguridad asociado a la unidad multimedia o al descodificador. Tal módulo de seguridad se puede realizar en particular según cuatro formas distintas. Una de ellas es una tarjeta con microprocesador protegida habitualmente de forma ISO 7816, una tarjeta inteligente o más habitualmente un módulo electrónico (que tiene forma de llave, de etiqueta de identificación...). Tal módulo es habitualmente desmontable y conectable al descodificador. La forma con contactos eléctricos es la más utilizada, pero no excluye un enlace sin contacto por ejemplo de tipo ISO 14443 o una combinación de tipo con y sin contacto.

[0003] Una segunda forma conocida es la de un alojamiento de circuito integrado colocado, habitualmente de manera definitiva e inamovible, en el alojamiento del descodificador. Una variante está constituida por un circuito instalado sobre un zócalo o conector tal como un conector de módulo tarjeta SIM.

[0004] En una tercera forma, el módulo de seguridad está integrado en un alojamiento de circuito integrado que tiene igualmente otra función, por ejemplo en un módulo de descodificación del descodificador o el microprocesador del descodificador.

[0005] En la práctica, la evolución de estos módulos de seguridad es grande entre los primeros módulos utilizados en un parque de descodificadores y los instalados con los últimos descodificadores. Varias generaciones de módulos de seguridad pueden cohabitar en un mismo parque de un operador de distribución de medios de comunicación, por ejemplo por satélite, por cable, a través de Internet.

[0006] No hace falta decir que si se detectan fallos de seguridad, entonces se efectúa el reemplazo de antiguos módulos.

[0007] La diferencia de generación de los módulos está a menudo relacionada con los servicios que acepta la unidad de usuario que está unida a los mismos. De hecho, si una versión de módulo no contiene la función "monedero", le será imposible cargar un crédito y por lo tanto autorizar el consumo de contenido sin intercambio bidireccional con un centro de gestión.

[0008] Así, un módulo de una cierta generación ofrecerá un número de servicios limitado.

[0009] Esto es también un inconveniente para las unidades de usuarios, a saber la compatibilidad con todas las generaciones de módulo. El procedimiento utilizado hasta ahora es la identificación del módulo de seguridad por la unidad de usuario. Esta identificación puede además ser bidireccional es decir que el módulo de seguridad interrogue a la unidad de usuario con el fin de saber cuáles son sus características.

[0010] El cambio de generación de módulo de seguridad puede estar acompañado de modificaciones materiales, por ejemplo, de la disponibilidad de nuevos puertos de comunicación. Un ejemplo de tal módulo de seguridad se ilustra en la patente US 6.779.734.

[0011] Es por lo tanto importante que un módulo de seguridad pueda adaptarse a las unidades de usuario y ajustar sus funcionalidades según los medios de comunicación de la unidad de usuario.

[0012] Un tercero malintencionado podría utilizar un descodificador modificado e intentar acceder a servicios de alto valor añadido haciéndose pasar por un descodificador de última generación. Una vez en este modo, va a intentar modificar la memoria interna del módulo de seguridad para su beneficio. Además, la presencia en un módulo de medios de comunicación evolucionados tales como USB 2.0 permite a estos terceros multiplicar los ataques por estos medios de comunicación a gran velocidad con respecto a otros medios de comunicación (IS07816) mucho más lentos.

[0013] En la solicitud EP 1 486 907, un módulo de seguridad es igualmente configurable en función del entorno. El objetivo es proceder a una autoconfiguración según las señales recibidas por el dispositivo huésped. Así, si un tercero malintencionado imita un entorno particular, el módulo se va a adaptar a este entorno incluso si no está autorizado.

Breve descripción de la invención

[0014] El objetivo de la presente invención es proponer un módulo de seguridad capaz de soportar las diferentes funcionalidades y configuraciones físicas de la conectividad de la última generación y las generaciones anteriores, ofreciendo ninguna nueva posibilidad de ataque debido a esta adaptabilidad.

[0015] Este objetivo se alcanza por un módulo de seguridad que incluye primeros medios de comunicación (COM0) hacia un dispositivo huésped, primeros medios de almacenamiento (MEM0) y primeros medios de desencriptación (ENC0), al igual que un módulo de estado (ME) y segundos medios de comunicación (COM1), caracterizado por el hecho de que comprende medios de acoplamiento/desacoplamiento eléctricos (TSB) de dichos segundos medios, estos medios de acoplamiento/desacoplamiento están controlados por el módulo de estado (ME), y por el hecho de que comprende medios de recepción de un mensaje protegido que permite modificar el estado de dicho módulo de estado (ME) y controlar la activación y la desactivación de los segundos medios de comunicaciones (COM1).

[0016] Así, según el estado memorizado en la memoria de estado del módulo, los segundos medios de comunicaciones son completamente inoperantes y no se pueden utilizar por un tercero con fines deshonestos. El acoplamiento/desacoplamiento eléctrico de los medios de comunicación es controlado por unos medios materiales tales como elementos de tres estados (tri-state) o "High Voltage bidirectional MOSFETs" según el resultado de una operación criptográfica.

[0017] Es lo mismo para las otras partes del módulo de seguridad tales como una parte de la memoria. Esta memoria puede contener informaciones tales como claves o números de serie que estén completamente desactivados, por lo tanto imposibles de acceder según la memoria de estado. Esta memoria de estado envía señales materiales de bloqueo o desbloqueo de la memoria para que aunque un programa pirata funcione en tal módulo, no pueda acceder a esta memoria. El mismo mecanismo puede aplicarse a otros elementos tales como un motor de descodificación o un módulo de desencriptación asimétrica.

[0018] Existen varias variantes de realización para definir el modo de operación del módulo de seguridad.

A. Preconfiguración

[0019] En el momento de la fabricación del módulo de seguridad, o en el momento de una etapa de personalización de dicho módulo, se preconfigura para que funcione según un entorno particular. No hace falta decir que esta preprogramación podrá ser modificada durante otra etapa de preconfiguración en un entorno de inicialización.

B. Activación por mensaje

[0020] En el momento de la inicialización, el módulo está en un modo básico y sólo los medios de comunicación comunes para todos los dispositivos huéspedes están activados. Según la preconfiguración, podrá estar en un modo particular que tiene en cuenta el destino de tal módulo. Para cambiar el estado del módulo de seguridad y por lo tanto activar otras funcionalidades, el módulo espera la recepción de un mensaje protegido que autoriza tal cambio. Sólo después de haber desencriptado tal mensaje y después de verificar este mensaje el módulo va a cambiar de estado y por lo tanto a abrir los segundos medios de comunicación.

Breve descripción de las figuras

[0021] La invención se comprenderá mejor gracias a la siguiente descripción detallada y que se refiere a los dibujos anexos que se aportan a modo de ejemplo en ningún caso limitativo, a saber:

- la figura 1 ilustra un esquema global de un módulo de seguridad,

- la figura 2 ilustra el control de un puerto de entrada/salida.

Descripción detallada de una forma de realización

[0022] La figura 1 ilustra un ejemplo de un módulo de seguridad SM que comprende una forma de realización de la invención. Según este ejemplo, este módulo comprende los primeros medios de comunicaciones COM0 y los segundos medios de comunicación COM1. Igualmente, el recurso memoria disponible se divide en varias partes (aquí 2) MEM0 y MEM1, pudiendo ser utilizado para el programa del microprocesador.

[0023] Según nuestro ejemplo, el módulo dispone de un primer módulo de encriptación/desencriptación ENC0 así como de un segundo módulo de encriptación/desencriptación ENC1.

[0024] Según el ejemplo ilustrado en la figura 1, el módulo de encriptación/desencriptación está conectado a un bus de comunicación de alta velocidad COM1. Una realización posible es el descifrado del flujo audio/vídeo según la norma DVB Common Descrambler o un descodificador propietario.

[0025] Los diferentes módulos están conectados al procesador CPU que coordina las operaciones, inicializa los módulos, transmite los resultados de un módulo a otro, etcétera.

[0026] Un módulo particular llamado módulo de estado ME va a controlar la activación y la desactivación de ciertos módulos y más generalmente el funcionamiento del módulo de seguridad. Según el ejemplo particular de la figura 1, este módulo de estado ME controla los segundos medios de comunicaciones COM1, los segundos medios de encriptación/desencriptación ENC1 así como la memoria MEM1. Según el estado de esta memoria, señales se transmiten independientemente del procesador para activar o desactivar los módulos.

[0027] Esta activación se ilustra en la figura 2 en la cual el módulo de estado ME transmite un comando al módulo de comunicación COM1 y este comando actúa igualmente sobre las señales emitidas o recibidas gracias a un elemento de bloqueo tal como un circuito aislante TSB como por ejemplo Tri-State, "High Voltage bidirectional MOSFETs" o cualquier otro elemento que aísle galvánicamente la conexión física del módulo de seguridad. Este elemento permite aislar una vía de comunicación colocándola en modo alta impedancia. El módulo de estado va por lo tanto a controlar el acoplamiento/desacoplamiento eléctrico de la comunicación COM1.

[0028] Cuando el módulo de seguridad ha desactivado el módulo de comunicación COM1, el módulo de estado ME continua vigilando la actividad sobre el puerto de comunicación COM1. El módulo de estado ME podrá emitir un mensaje de alerta si continua constatando la llegada de parásitos.

[0029] Existen varias maneras de influir en el módulo de estado ME. Como se indica en el preámbulo de la solicitud, el módulo de seguridad determina, en función de las informaciones recibidas de la unidad de usuario, cuál de los estados corresponde a esta unidad.

[0030] Según la variante que ejecuta un mensaje de seguridad, en cuanto este mensaje es recibido y verificado por el módulo de seguridad, éste provoca el cambio del estado del módulo de estado.

[0031] Según esta variante, este mensaje es desencriptado y verificado por el procesador y el resultado es almacenado en el módulo de estado ME. Actúa por lo tanto como una memoria con comandos que salen en dirección a diferentes módulos implicados y de un módulo de supervisión con el fin de vigilar la actividad en todas las vías de comunicación.

[0032] Según otra variante, todo o parte del mensaje es tratado directamente por el módulo de estado ME. El mensaje puede ser pretratado por el procesador, por ejemplo por una clave propia del módulo de seguridad contenida en la primera memoria MEM0, luego transmitida al módulo de estado. Este último dispone de una clave propia Ksm que va a permitir verificar el comando contenido en el mensaje. Esta verificación se puede hacer según varias maneras conocidas, tales como el uso de una firma en el mensaje generado con una clave asimétrica, siendo la otra clave asimétrica la clave Ksm del módulo de la memoria de estado. El microprocesador no puede acceder a la memoria de estado sin conocer la clave propia del módulo de estado. Solo un mensaje preparado por el centro de gestión podrá ser aceptado por el módulo de estado.

[0033] Si la verificación es correcta, el nuevo estado se carga en el módulo de estado con las consecuencias esperadas sobre los otros módulos.

[0034] Según una variante de la invención, el módulo de estado ME ejecuta operaciones de vigilancia del estado del módulo de seguridad. Recibe por ejemplo la alimentación positiva Vdd (habitualmente 5V) que va igualmente sobre el módulo de alimentación PS y observa los comportamientos de riesgo tales como los cambios de tensión bruscos, tensión anormalmente baja o alta. Según los criterios definidos, podrá sin recibir un mensaje modificar su estado, por ejemplo generando un mensaje de error o desactivando ciertas funciones de dicho módulo. Las vías de comunicación (COM1, COM0) son vigiladas por el módulo de estado ME. Por vía de comunicación, se entienden todas las vías por las cuales transitan las informaciones que entran o salen del módulo de seguridad, tales como la vía I/O de la norma IS07816 o las vías USB u otros puertos de alta velocidad, incluido el infrarrojo, etc. Las vías de enlace son, en cuanto a ellas, las otras vías que se conectan con el módulo huésped tales como la alimentación (Vdd, Vss), el reloj (CLK) o el *reset* (RST).

[0035] Igualmente, si constata que hay parásitos, ruidos en los medios de comunicaciones tales como los primeros medios de comunicación, podrá igualmente cambiar de estado o iniciar contramedidas. Además, el módulo de estado ME puede comprender un perfil de vigilancia, por una parte específico de la vía de comunicación o de enlace vigilada y por otra parte según el estado del módulo de estado. Así, los parámetros de verificación del buen funcionamiento de una vía de enlace podrán variar según el estado del módulo de estado. Se podrán tolerar variaciones de tensión de +/-10% en un estado mientras que en otro estado solamente se tolerarán +/-5%. Igualmente para el número de parásitos, microcortes u otros. Estos parámetros son programables y se pueden modificar gracias a la recepción de un mensaje de seguridad.

[0036] Esta vigilancia puede hacerse aunque la vía o el medio de comunicación esté desactivado.

[0037] El módulo de estado ME puede igualmente controlar los recursos internos del módulo de seguridad. La segunda memoria MEM1 puede estar desactivada, sea parcialmente, sea completamente. Además, esta desactivación puede hacerse bien por un comando electrónico (bloqueo de la lectura y/o de la escritura) pero puede actuar directamente sobre la alimentación de dicha memoria. Esta memoria podrá ser definida, según el estado, como sólo de lectura, sólo de escritura o de lectura/escritura. Lo mismo ocurre para los otros recursos del módulo de seguridad tales como los módulos de encriptación/desencriptación (ENC0, ENC1). El módulo de estado (ME) puede controlar los módulos y/o las funcionalidades que están autorizados o prohibidos según el estado del módulo de estado. Estas funcionalidades son por ejemplo el uso de un bus interno de alta velocidad o un mecanismo de regulación del reloj. Estos módulos son por ejemplo un generador de reloj, un módulo de encriptación/desencriptación, una memoria, un regulador de tensión por bomba de carga, etcétera.

[0038] El mensaje que llega al módulo de seguridad proviene preferiblemente de un centro de gestión. Este mensaje puede llegar al módulo de seguridad SM por los primeros o los segundos medios de comunicación. En el momento de la inicialización en el sito del módulo de seguridad y de su dispositivo huésped, se transmiten mensajes a través del dispositivo huésped para el módulo de seguridad. El centro de gestión conoce las características del aparato huésped así como los abonos del abonado relacionados y formatea un mensaje para el módulo de seguridad que contiene su estado de funcionamiento. Este mensaje puede ser propio de cada módulo de seguridad, o idéntico para todos los módulos de seguridad, un mensaje que contiene una versión de unidad de usuario y el nivel de seguridad del módulo de seguridad. Así, si existen 8 diferentes unidades de usuario, encontraremos en el flujo de transmisión ocho mensajes, cada comprendiendo una versión de unidad de usuario y la configuración del módulo de seguridad correspondiente.

[0039] Según otra variante, cada dispositivo huésped según sus características, almacena un mensaje que será transmitido posteriormente al módulo de seguridad en cuanto éste esté conectado. El estado del módulo de seguridad estará por lo tanto en armonía con las especificaciones del dispositivo huésped.

[0040] Cuando el módulo de seguridad SM ha determinado su estado, conserva este estado y por lo tanto se bloquea. Para que el módulo de seguridad acepte una nueva inicialización, el centro de gestión puede enviar un mensaje que autorice un nuevo procedimiento de configuración. Este mensaje puede ser condicional, es decir que puede contener una indicación de versión de módulo de seguridad o un estado del módulo de estado como condición de reinicialización.

REIVINDICACIONES

1. Módulo de seguridad que incluye primeros medios de comunicación (COM0) hacia un dispositivo huésped, primeros medios de almacenamiento (MEM0) y primeros medios de desencriptación (ENC0), al igual que un módulo de estado (ME) y segundos medios de comunicación (COM1), **caracterizado por el hecho de que** comprende medios de acoplamiento/desacoplamiento eléctricos (TSB) de dichos segundos medios, estos medios de acoplamiento/desacoplamiento están controlados por el módulo de estado (ME), y **por el hecho de que** comprende medios de recepción de un mensaje protegido que permite modificar el estado de dicho módulo de estado (ME) y controlar la activación y la desactivación de los segundos medios de comunicaciones (COM1).

2. Módulo de seguridad según la reivindicación 1, **caracterizado por el hecho de que** el módulo de estado (ME) comprende medios para detectar la actividad de los medios de comunicación (COM0, COM1) y para determinar, según esta actividad, el estado de dicho módulo de estado (ME).

3. Módulo de seguridad según las reivindicaciones 1 o 2, **caracterizado por el hecho de que** los segundos medios de comunicación (COM1) están conectados al dispositivo huésped por contactos físicamente distintos de los contactos de los primeros medios de comunicación (COM0).

4. Módulo de seguridad según una de las reivindicaciones 1 a 3, **caracterizado por el hecho de que** los medios de acoplamiento/desacoplamiento eléctricos (TSB) comprenden elementos conductores/aislantes del tipo "Tri-State" o "High Voltage bidirectional MOSFETs".

5. Módulo de seguridad según una de las reivindicaciones 1 a 4, **caracterizado por el hecho de que** los medios de acoplamiento/desacoplamiento eléctricos están colocados en serie con dichos primeros medios de comunicación (COM0) permitiendo aislar eléctricamente dichos primeros medios de comunicación (COM0).

6. Módulo de seguridad según una de las reivindicaciones 1 a 5, **caracterizado por el hecho de que** los medios de acoplamiento/desacoplamiento eléctricos están también colocados en serie con al menos una de las vías de enlace (RST, I/O, CLK) permitiendo aislar eléctricamente dichas vías de enlace (RST, I/O, CLK).

7. Módulo de seguridad según una de las reivindicaciones 1 a 6, **caracterizado por el hecho de que** comprende segundos medios de almacenamiento (MEM1), el módulo de estado (ME) comprende medios de activación/desactivación de dichos segundos medios de almacenamiento.

8. Módulo de seguridad según las reivindicaciones 1 a 7, **caracterizado por el hecho de que** el módulo de estado (ME) comprende módulos y/o funcionalidades que se autorizan o prohíben según el estado del módulo de estado (ME).

9. Módulo de seguridad según la reivindicación 8, **caracterizado por el hecho de que** el estado del módulo de estado (ME) comprende medios para limitar el nivel de acceso a los segundos medios de almacenamiento (MEM1) bien sólo en lectura, sólo en escritura, bien en lectura/escritura.

10. Módulo de seguridad según una de las reivindicaciones 1 a 9, **caracterizado por el hecho de que** comprende segundos medios de desencriptación (ENC1), estos segundos medios de desencriptación son activados/desactivados por el módulo de estado (ME).

11. Módulo de seguridad según la reivindicación 10, **caracterizado por el hecho de que** a los segundos medios de desencriptación se les suministra energía bajo el control del módulo de estado (ME).

12. Módulo de seguridad según cualquiera de las reivindicaciones precedentes, **caracterizado por el hecho de que** el módulo de estado (SM) comprende medios de vigilancia de los parámetros de funcionamiento actuales de todas las vías de enlace del módulo de seguridad y medios que permiten cambiar el estado del módulo de estado (ME) según el resultado de la vigilancia.

13. Módulo de seguridad según la reivindicación 12, **caracterizado por el hecho de que** los medios de vigilancia están conectados igualmente a la vía o las vías de enlace (RST, Vdd, Vss, CLK) de dicho módulo.

14. Módulo de seguridad según una de las reivindicaciones 12 o 13, **caracterizado por el hecho de que** los medios de vigilancia comprenden un perfil de vigilancia de las vías de comunicación que puede ser propio de cada estado del módulo de estado.

Fig. 1

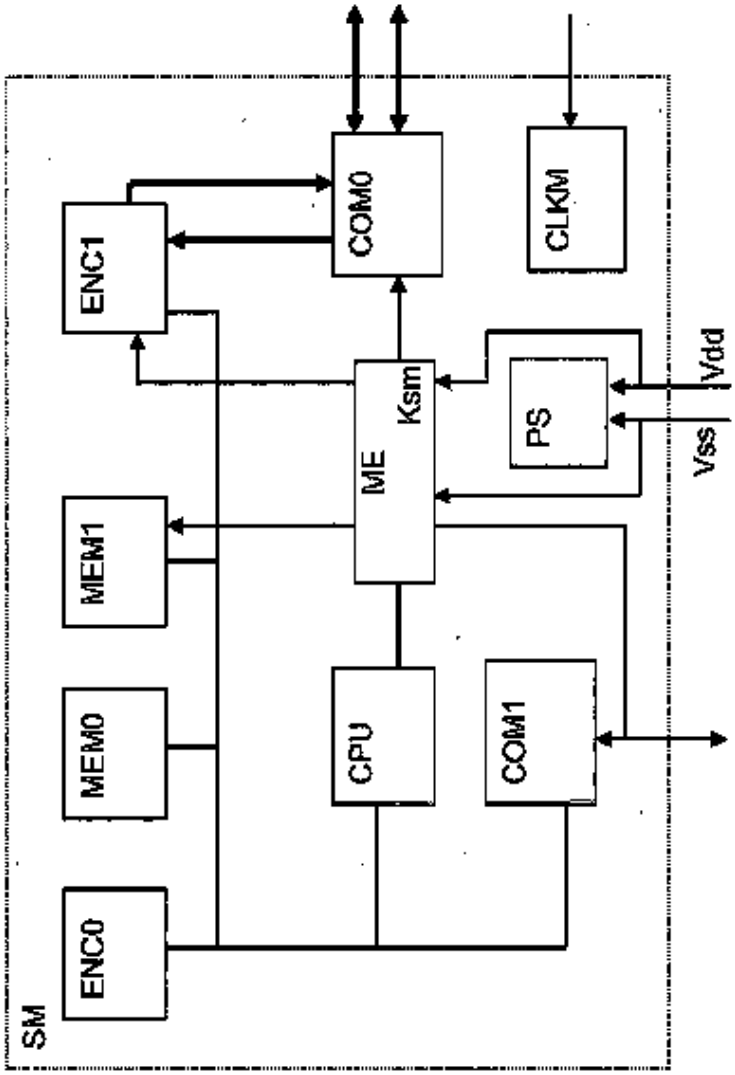
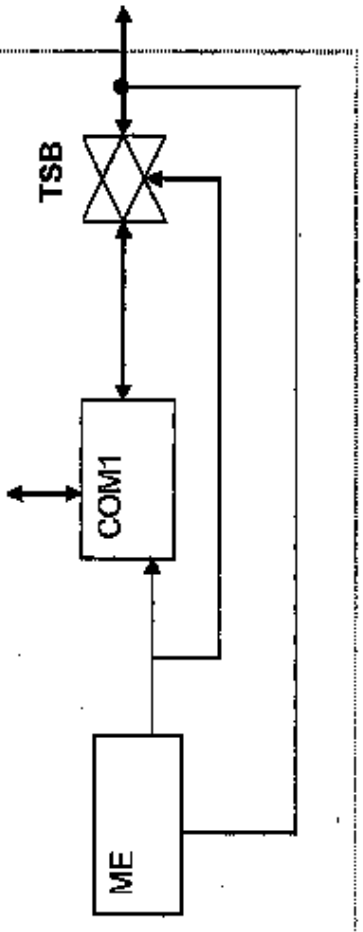

SM
ENC0
MEM0
MEM1
ENC1
CPU
ME
Ksm
COM0
COM1
PS
CLKM
CLK
Vdd
Vss

Fig. 2


TSB
COM1
ME