(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 363 596**

(51) Int. Cl.:
***H04N 7/16*** (2006.01)
***H04N 7/167*** (2006.01)
***G06F 12/14*** (2006.01)
***H04L 12/22*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07823456 .4**
(96) Fecha de presentación : **29.08.2007**
(97) Número de publicación de la solicitud: **2060117**
(97) Fecha de publicación de la solicitud: **20.05.2009**

(54) Título: **Procesador de seguridad, un procedimiento y un soporte de grabación para configurar el comportamiento de este procesador.**

(30) Prioridad: **30.08.2006 FR 06 07631**

(45) Fecha de publicación de la mención BOPI:
**10.08.2011**

(45) Fecha de la publicación del folleto de la patente:
**10.08.2011**

(73) Titular/es: **VIACCESS**
**Les Collines de l'Arche Opera C**
**92057 Paris - La Défense Cedex, FR**

(72) Inventor/es: **Danois, Pascal;**
**Granet, Olivier y**
**Le Henaff, Sébastien**

(74) Agente: **Espiell Volart, Eduardo María**

**DESCRIPCIÓN**

La invención se refiere a un procesador de seguridad, un procedimiento y un soporte de grabación para configurar el comportamiento de este procesador.

Existen procesadores de seguridad para un descodificador adecuado para recibir señales multimedia codificadas con ayuda de una palabra de control. Estos procesadores, tales como una tarjeta de memoria encajable en el descodificador, un módulo material integrado en el descodificador o un módulo de software que se ejecuta en el descodificador, comprende especialmente una memoria no regrabable, conteniendo esta memoria un código de una aplicación que, cuando es ejecutada por un microprocesador permite ejecutar un conjunto de operaciones necesarias para los tratamientos de los mensajes de acceso condicional transmitidos por un emisor de un operador para extraer la palabra de control necesaria para descodificar la señal multimedia codificada.

Existen diversos tipos de mensajes de acceso condicional, tales como los mensajes ECM (Entitlement Control Message) o los mensajes EMM (Entitlement Management Message), pudiendo definirse otros tipos. Son posibles variantes: Existen mensajes EMM cuyo contenido no está encriptado, denominado aquí “mensaje EMM no confidencial” y mensajes EMM confidenciales cuyo contenido está encriptado, denominado aquí mensajes EMMC (Entitlement Management Message Confidential). Más adelante de esta descripción y en las reivindicaciones, a menos que se indique de otro modo, el término “EMM” designa tanto un mensaje EMM no confidencial como un mensaje EMMC.

La patente WO 2004/049141 describe una memoria para el tratamiento de un contenido, comprendiendo dicha memoria al menos un microprocesador.

A veces es deseable modificar el comportamiento del procesador de seguridad. Esto es deseable en particular cuando un pirata encuentra un fallo de seguridad en el código de la aplicación y explota este fallo para obtener fraudulentamente el derecho a descodificar la señal multimedia.

En este sentido, la solicitud de patente publicada con el número WO-03 075233 desvela el reservarse en el código de aplicación unas aberturas para autorizar la conexión de la porción de sustitución de los códigos, denominada “PATCH”. Por ejemplo, el “PATCH” es ejecutado por el microprocesador en vez de una porción del código de aplicación que presenta un fallo de seguridad. Estos “PATCH” permiten entonces modificar el comportamiento del procesador de seguridad.

Estos “PATCH” se graban en una memoria no volátil regrabable. Así, es posible reemplazar un “PATCH” por otro “PATCH”. Esta posibilidad es potencialmente peligrosa pues podría ser explotada por un pirata para instalar en la memoria no volátil regrabable del procesador de seguridad, un PATCH pirata que le permita, por ejemplo, autorizar fraudulentamente el desciframiento de la palabra de control.

La invención busca a resolver este problema.

La invención tiene entonces por objeto un procesador de seguridad en el cual:

- el procesador de seguridad comprende al menos una primera cerradura regrabable cuyo valor es conmutable entre un primer y un segundo valor predeterminado como respuesta a un mensaje EMM,

- el código de aplicación contiene igualmente una función de restricción apta para autorizar y, alternativamente, prohibir, en respuesta a la recepción de un mismo mensaje ECM o EMM y en función del valor de la primera cerradura, solamente una operación particular del procesador de seguridad entre el conjunto de operaciones necesarias para el tratamiento de los mensajes ECM y EMM, aunque permitiendo al procesador de seguridad ejecutar otras operaciones necesarias para el tratamiento de los mensajes EMM y ECM que no hayan sido prohibidas, eligiéndose esta operación particular del grupo formado por:

  - la utilización de una llave criptográfica grabada en una memoria del procesador de seguridad,

  - el tratamiento de un parámetro contenido en un mensaje EMM o ECM recibido, y

  - la ejecución de una función elemental de acceso condicional del código de aplicación, ejecutándose cada función elemental de acceso condicional del código de aplicación independientemente de otras funciones elementales de acceso condicional de manera que la no ejecución de una función elemental de acceso condicional no impide la ejecución, por el microprocesador, de una cualquiera de las otras funciones elementales de acceso condicional.

El comportamiento del procesador de seguridad anteriormente citado, como respuesta al mismo mensaje EMM o ECM, puede ser modificado haciendo conmutar el valor de la primera cerradura entre su primer valor y su segundo valor. Para modificar el comportamiento de este procesador de seguridad, no es necesario entonces instalar porciones de código de la aplicación en una memoria regrabable lo que hace más seguro a este procesador de seguridad. Tampoco es necesario modificar los mensajes ECM o EMM difundidos por la cabeza de red. Todo lo más, es necesario prever enviar un mensaje EMM conteniendo un nuevo parámetro como respuesta al cual la cerradura conmuta entre el

primer y el segundo valor.

Se observará igualmente que este procesador de seguridad presenta al menos una de las siguientes ventajas:

- prohibir la utilización de una llave criptográfica permite impedir la ejecución de una función elemental de acceso condicional cuando ésta utiliza una llave criptográfica particular sin impedir por lo tanto la ejecución de la misma función cuando ésta utiliza otra llave criptográfica lo que aumenta las posibilidades de regulación del comportamiento del procesador de seguridad con respecto a llaves criptográficas,

- prohibir el tratamiento de un parámetro de un mensaje EMM o ECM impide la ejecución de una función elemental de acceso condicional que habrá debido ser provocado como respuesta a la recepción de este parámetro sin impedir por lo tanto la activación de la ejecución de la misma función elemental de acceso condicional para tratar otro parámetro recibido lo que permite aumentar las posibilidades de regulación del comportamiento del procesador de seguridad con respecto a los parámetros contenidos en los mensajes EMM y ECM,

- la prohibición de una función elemental de acceso condicional permite desactivar definitivamente o temporalmente una función elemental de acceso condicional que presenta un fallo de seguridad lo que se puede utilizar para hacer más seguro el comportamiento del procesador de seguridad.

Los modos de realización de este procesador de seguridad pueden comprender una o varias de las siguientes características:

- la memoria comprende al menos un campo FIELDKEY asociado a una de las llaves criptográficas, conteniendo este campo FIELDKEY diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental de acceso condicional respectivo, y la función de restricción es apta para autorizar y, alternativamente, prohibir la utilización de esta llave criptográfica por una función elemental de acceso condicional en función del valor de la cerradura contenido en el campo FIELDKEY y que corresponde a esta función elemental de acceso condicional;

- el procesador de seguridad contiene al menos una lista elegida entre las listas siguientes:

  - una lista FIELDPIEMM asociada a los mensajes EMM no confidenciales, conteniendo esta lista FIELDPIEMM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM no confidencial,

  - una lista FIELDPIEMMC asociada a los mensajes EMM confidenciales (Entitlement Management Message Confidential), conteniendo esta lista FIELDPIEMMC diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM confidencial, y

  - una lista FIELDPIECM asociada a los mensajes ECM, conteniendo esta lista FIELDPIECM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje ECM y

  la función de restricción es apta para autorizar y, alternativamente, prohibir el tratamiento de un parámetro $P_i$ contenido en un mensaje recibido por el procesador de seguridad en función del valor de la cerradura que corresponde a este parámetro en la lista asociada a este mensaje;

- el procesador de seguridad comprende una lista FIELDFCT asociada a las funciones elementales de acceso condicional, conteniendo esta lista FIELDFCT diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental de acceso condicional respectivo y la función de restricción es apta para autorizar y, alternativamente, prohibir la ejecución de una función elemental de acceso condicional en función del valor de la cerradura de la lista FIELDFCT que corresponde a esta función elemental de acceso condicional;

- el procesador de seguridad comprende al menos una segunda cerradura regrabable cuyo valor es conmutable entre un primer y un segundo valor predeterminado como respuesta a un mensaje EMM, siendo apta la función de restricción para autorizar o alternativamente prohibir en función del valor de esta segunda cerradura:

  - la utilización de toda llave criptográfica necesaria para hacer conmutar el valor de la primera o la segunda cerradura,

  - el tratamiento de todo parámetro contenido en un mensaje EMM adecuado para hacer conmutar el valor de la primera o la segunda cerradura, y

  - la ejecución de toda función elemental de acceso condicional adecuada para hacer conmutar el

valor de la primera o la segunda cerradura;

- la función elemental de acceso condicional es diferente de una función de inscripción de nuevos títulos de acceso y una función de inscripción de nuevas llaves criptográficas.

Estos modos de realización presentan además las siguientes ventajas:

- la utilización de un campo FIELDKEY permite hacer más seguro al procesador de seguridad porque permite hacer una llave criptográfica inutilizable por ciertas funciones elementales que presentan un fallo de seguridad aunque conservando la posibilidad de utilizar esta misma llave criptográfica para otras funciones elementales desprovistas de fallo de seguridad,

- la utilización de al menos una lista elegida entre las listas FIELDPIEMM, FIELDPIEMMC y FIELDPIECM permite incrementar las posibilidades e regulación del comportamiento del procesador de seguridad autorizando o prohibiendo el tratamiento de un mismo parámetro en función del mensaje en el que está contenido; otra utilización de al menos las listas FIELDPIEMM y FIELDPIEMMC permite imponer un parámetro, para que sea tratado, en un EMM confidencial, prohibiéndose este parámetro en la lista FIELDPIEMM y autorizado en la lista FIELDPIEMMC,

- la utilización de la lista FIELDFCT permite regular el comportamiento del procesador de seguridad función elemental de acceso condicional por función elemental de acceso condicional,

- impedir la utilización de toda llave o el tratamiento de todo parámetro donde la ejecución de toda función susceptible de modificar el valor de la primera o la segunda cerradura permite paralizar definitivamente el comportamiento del procesador de seguridad en lo que se refiere a las operaciones autorizadas o prohibidas por la primera cerradura.

La invención tiene igualmente por objeto un procedimiento de configuración del procesador de seguridad anterior en el que el procedimiento comprende:

- el suministro de al menos una primera cerradura regrabable cuyo valor es conmutable entre un primer y un segundo valor predeterminado como respuesta a un mensaje EMM,

- la autorización, alternativamente, la prohibición, en función del valor de la primera cerradura, de solamente una operación particular del procesador de seguridad entre el conjunto de operaciones necesarias para el tratamiento de los mensajes ECM y EMM, aunque permitiendo que el procesador de seguridad ejecute las otras operaciones necesarias para el tratamiento de los mensajes EMM y ECM que no hayan sido prohibidos, eligiéndose esta operación particular del grupo formado por:

  - la utilización de una llave criptográfica grabada en una memoria de un procesador de seguridad,

  - el tratamiento de un parámetro contenido en un mensaje EMM o ECM recibido, y

  - la ejecución de una función elemental de acceso condicional por el procesador de seguridad, ejecutándose cada función elemental de acceso condicional independientemente de otras funciones elementales de acceso condicional de manera que la no ejecución de una función elemental de acceso condicional no impide la ejecución, por el procesador de seguridad, de una cualquiera de otras funciones elementales de acceso condicional.

Los modos de realización de este procedimiento de configuración pueden comprender una o varias de las siguientes características:

- el suministro de una memoria que contiene al menos un campo FIELDKEY asociado a una de las llaves criptográficas, conteniendo este campo FIELDKEY diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental de acceso condicional respectivo, y la autorización y, alternativamente, la prohibición de la utilización de esta llave criptográfica asociada al campo FIELDKEY por una función elemental de acceso condicional en función del valor de la cerradura que está contenido en el campo FIELDKEY y que corresponde a esta función elemental de acceso condicional;

- el suministro de una memoria que contiene al menos una lista elegida entre las listas siguientes:

  - una lista FIELDPIEMM asociada a los mensajes EMM no confidenciales, conteniendo esta lista FIELDPIEMM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM no confidencial,

  - una lista FIELDPIEMMC asociada a los mensajes EMM confidenciales (Entitlement Management Message Confidential), conteniendo esta lista FIELDPIEMMC diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM confidencial, y

- una lista FIELDPIECM asociada a los mensajes ECM, conteniendo esta lista FIELDPIECM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje ECM y la autorización y, alternativamente, la prohibición del tratamiento de un parámetro $P_i$ contenido en un mensaje recibido por el procesador de seguridad en función del valor de la cerradura que corresponde a este parámetro en la lista asociada a este mensaje;

- el suministro de una memoria que comprende una lista FIELDFCT asociada a las funciones elementales de acceso condicional, conteniendo esta lista FIELDFCT diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental de acceso condicional respectivo, y la autorización y, alternativamente, la prohibición de la ejecución de una función elemental de acceso condicional en función del valor de la cerradura en la lista FIELDFCT que corresponde a esta función elemental de acceso condicional;

- la configuración inicial por defecto del valor de cada cerradura para que, como respuesta a la recepción del primer mensaje EMM o ECM difundido por la cabeza de red, ninguna operación particular sea prohibida;

- la recepción en un mismo mensaje EMM:

- de un primer parámetro activador de la conmutación del valor de la primera cerradura para autorizar una operación particular del procesador de seguridad,

- de un segundo parámetro activador de la ejecución de esta misma operación particular, y

- de un tercer parámetro activante de la conmutación del valor de la primera cerradura para prohibir esta misma operación particular y el tratamiento por orden por el procesador de seguridad del primer, segundo y tercer parámetro;

- la función elemental de acceso condicional es diferente de una función de inscripción de nuevos títulos de acceso y de una función de inscripción de nuevas llaves criptográficas.

Los modos de realización de este procedimiento de configuración presentan además las siguientes ventajas:

- la configuración inicial del valor de cada cerradura para autorizar el conjunto de las operaciones necesarias para el tratamiento de los mensajes ECM y EMM incrementa la seguridad del procesador de seguridad porque un pirata podrá modificar eventualmente el comportamiento del procesador de seguridad sólo para prohibir las operaciones particulares, y

- autorizar una operación particular por tanto, inmediatamente después, ejecutar esta operación particular, inmediatamente por tanto, después prohibir esta operación particular permite impedir que un pirata se aproveche de un fallo de seguridad en esta operación particular porque la ejecución de esta operación particular no se hace posible más que durante un intervalo de tiempo muy corto.

La invención tiene igualmente por objeto un soporte de grabación de informaciones que comprende las instrucciones para la ejecución del procedimiento de configuración anterior cuando estas instrucciones son ejecutadas por un microprocesador.

La invención se comprenderá mejor con la lectura de la descripción que sigue, dada únicamente a título de ejemplo no limitantivo y referida a los dibujos sobre los cuales :

- la figura 1 es una ilustración esquemática de la arquitectura de un sistema de transmisión de señales multimedia codificadas;

- las figuras 2 y 3 son ilustraciones esquemáticas de porción de trama de mensaje EMM y ECM;

- las figuras 4, 5 y 6 son ejemplos de estructura de datos utilizados en el sistema de la figura 1;

- la figura 7 es un organigrama de un procedimiento de configuración del comportamiento de un procesador de seguridad del sistema de la figura 1, y

- la figura 8 es una ilustración esquemática de una porción de una trama de un mensaje EMM de configuración.

Más adelante de esta descripción, las características y las funciones conocidas por el experto en la materia no se describen con detalle.

La figura 1 representa un sistema 2 de transmisión de señales multimedia codificadas. Las señales multimedia son, por ejemplo, señales audiovisuales que corresponden a unos programas audiovisuales de cadenas de televisión.

El sistema 2 comprende un emisor 4 de señales multimedia codificadas con ayuda de una palabra de control CW con destino a un gran número de receptores mediante una red 6 de transmisión de informaciones. El emisor 4 es

conocido con la expresión “cabeza de red”.

Para simplificar la figura 1, sólo está representado un receptor 8.

La red 6 es, por ejemplo, una red herziana tal como se ilustra aquí o una red cableada de gran distancia.

Aquí, las señales multimedia son generadas por dos operadores distintos 7A y 7B. Más precisamente, cada operador 7A, 7B genera las señales multimedia en claro, es decir no codificadas y las transmite al emisor 4 que se carga de su codificación antes de su difusión mediante la red 6.

Más adelante de esta descripción, los operadores 7A y 7B están asociados, respectivamente, a los identificadores de los operadores $SOID_1$ y $SOID_2$.

El emisor 4 es apto para enviar concomitantemente señales multimedia codificadas de mensajes ECM y mensajes EMM. Por ejemplo, las señales multimedia codificadas y los mensajes ECM y EMM son multiplexados en un mismo paquete de informaciones.

Las figuras 2 y 3 representan los ejemplos de estructura de trama, respectivamente, de un mensaje EMM y un mensaje ECM conforme a la norma UTE C90-007.

La trama del mensaje EMM comienza por un campo ADR que contiene un identificador ADR de un receptor particular o de un grupo de receptores. En el caso de que el mensaje EMM se dirija al conjunto de receptores del sistema 2, el campo ADR puede ser omitido.

A continuación, el mensaje EMM contiene los parámetros $P_i$ destinados a configurar los receptores para que éstos puedan descodificar correctamente las señales multimedia para las que se ha suscrito un abono. Cada uno de estos parámetros está codificado utilizando una estructura TLV (Type Length Value). En estas condiciones, cada parámetro $P_i$ está formado por la yuxtaposición de tres campos $PI_i$, $LI_i$ y $V_i$. El campo $PI_i$ contiene un identificador $PI_i$ del parámetro $P_i$. El campo $L_i$ contiene un valor que indica que es la longitud del campo $V_i$. El campo $V_i$ contiene el valor del parámetro $P_i$.

En la figura 2, se han representado igualmente un parámetro SOID y un parámetro MAC, presente sistemáticamente en los mensajes EMM. El parámetro SOID contiene el identificador SOID del operador que difunde este mensaje EMM.

El parámetro MAC (Message Authentification Code) contiene un código que permite verificar la autenticidad e integridad del mensaje EMM.

Los trazos verticales ondulados indican que sólo una parte de la estructura del mensaje EMM está representada en la figura 2.

Contrariamente al mensaje EMM, la estructura de un mensaje ECM no contiene el campo ADR puesto que el mensaje ECM se dirige a priori al conjunto de los receptores del sistema 2. El mensaje ECM comprende igualmente diversos parámetros codificados según la estructura TLV. Normalmente, el mensaje ECM comprende un parámetro SOID y un parámetro MAC con las mismas funcionalidades que las ya descritas con respecto a la figura 2.

A continuación, el mensaje ECM comprende un parámetro AC y un parámetro CW*. El parámetro AC contiene una condición de acceso a las señales multimedia. Este parámetro AC se identifica aquí en el mensaje ECM por un identificador $PI_{AC}$. Su longitud se define en un campo $L_{AC}$ y su valor está contenido en un campo $V_{AC}$. Cuando el acceso a las señales multimedia depende de diversas condiciones, el mensaje ECM puede contener diversos parámetros AC.

El parámetro CW* está destinado a contener un criptograma CW* de la palabra de control utilizada para descodificar las señales multimedia. Este criptograma CW* es generado por el emisor 4 cifrando la palabra de control CW con ayuda de una llave de explotación $K_e$. Aquí, este parámetro CW* es identificado por un identificador $PI_{cw}$, su longitud está limitada en un campo $L_{cw}$ y su valor está limitado en un campo $V_{cw}$.

Como en la figura 2, en la figura 3, los trazos verticales ondulados indican que el mensaje ECM puede contener otros parámetros.

El receptor 8 es apto para recibir la señales multimedia codificadas así como los mensajes ECM y EMM. A tal efecto, el receptor 8 comprende un decodificador o terminal 40 conectado a un procesador de seguridad 42. El procesador 42 es, por ejemplo, un procesador amovible tal que una tarjeta de memoria que se puede integrar en el descodificador 40. El procesador 42 comunica con el descodificador 40 mediante una interfase procesador/descodificador. Normalmente, la interfase está formada por conectores eléctricos, teniendo cada conector un elemento macho y un elemento hembra cada uno solidario, o descodificador o procesador. La interfase entre el descodificador 40 y el procesador 42 es, por ejemplo, conforme a la norma ISO 7816.

El descodificador 40 está equipado, en la presente memoria, con una antena 44 para recibir las diferentes señales difundidas por el emisor 4. Esta antena 44 empalmada a un bloque 46 de desmultiplexado de las señales y,

eventualmente, filtrado de estas señales. A la salida de este bloque 46, las señales multimedia codificadas son enviadas a un descodificador 48. Los mensajes EMM y ECM son enviados al procesador 42.

El descodificador 48 es apto para descodificar las señales multimedia codificadas con ayuda de una palabra de control CW descifrada por el procesador 42.

El descodificador 40 se ajusta a un dispositivo 50 de descifrado de las señales multimedia descodificadas tales como, por ejemplo, un aparato de televisión.

El procesador 42 está equipado con:

- un microprocesador electrónico 60,
- una memoria 62 no regrabable y no volátil que contiene un código 64 de una aplicación que, cuando es ejecutada por el microprocesador 60, permite tratar los mensajes ECM y EMM para permitir el descifrado de la palabra de control necesaria para la descodificación de las señales multimedia recibidas, y
- una memoria regrabable 66 no volátil tal como por ejemplo una memoria EEPROM (Electrically Erasable Programmable Read Only Memory).

La aplicación representada por el código 64 está constituida por un conjunto de funcionalidades elementales características del tratamiento de los mensajes de acceso condicional. Cada una de estas funcionalidades elementales de acceso condicional puede ser ejecutada independientemente entre sí. Así, la no ejecución de una de dichas funcionalidades elementales no impide la ejecución, por el microprocesador, de una cualquiera de las demás funcionalidades elementales. Por simplicidad, a continuación, se denominará “función elemental” una de dichas funcionalidades elementales de acceso condicional.

Como ilustración la memoria 62 contiene una tabla 70 que permite identificar qué tratamientos del código deben ser ejecutados para realizar esta función elemental. La tabla que sigue a continuación proporciona unos ejemplos de funciones elementales. La primera y segunda columna de esta tabla contienen para cada función elemental, respectivamente, un identificador de la función elemental y una breve descripción de la operación realizada para esta función elemental.

Tabla 1

| | |
|---|---|
| IdF1 | Descifrado de un criptograma CW* con ayuda de una llave $K_e$ |
| IdF2 | Verificación del parámetro MAC de un mensaje ECM |
| IdF3 | Descifrado de un mensaje EMM confidencial |
| IdF4 | Modificación del límite autorizado en compras compulsivas |
| IdF5 | Inscripción de un nuevo título de acceso |
| IdF6 | Inscripción o modificación de una llave criptográfica $K_e$ después de descifrado de su criptograma con ayuda de una llave $K_s$ |
| IdF7 | Configuración del valor de las cerraduras |
| IdF8 | Comparación de las condiciones de acceso recibidas con los títulos de acceso contenidos en el procesador de seguridad |

El código 64 contiene igualmente una función particular elemental, denominada “función de restricción” ilustrada como función Idf7 en la tabla 1, que se describirá con más detalle con respecto a la figura 1.

La memoria 62 contiene igualmente una tabla 72 que comprende las informaciones necesarias para determinar cual o cuáles son las funciones elementales cuya ejecución debe ser activada para tratar los datos identificados por un identificador $P_i$ recibido.

La tabla que sigue a continuación proporciona ejemplos de parámetros $P_i$ susceptibles de estar contenidos en un mensaje EMM o ECM. La primera columna de esta tabla contiene el identificador del parámetro $P_i$ y la segunda columna define sucintamente este parámetro $P_i$.

Tabla 2

| | |
|---|---|
| $PI_{CW}$ | Contiene el criptograma CW* en un mensaje ECM. Este criptograma debe ser descifrado con una llave $K_e$ para obtener la palabra de control CW. |
| $PI_{Ke}$ | Contiene la llave $K_e$ en un mensaje EMM. Este criptograma debe ser descifrado por una llave $K_s$ antes de grabar o modificar la llave $K_e$. |
| $PI_{config}$ | En un mensaje EMM, contiene datos de configuración de las listas FIELDPIEMM, FIELDPIEMMC, FIELDPIECM, FIELDFCT y los campos FIELDKEY. |
| $PI_{SOID}$ | Contiene el identificador SOID de un operador para identificar el contexto criptográfico de lo necesario para el tratamiento del mensaje ECM o EMM. |
| $PI_{MAC}$ | Contiene un código MAC (Message Authentification Code) cuyo control permite verificar la autenticidad e integridad del mensaje ECM o EMM. |
| $PI_{TdA}$ | Contiene datos de inscripción de un nuevo título de acceso. |
| $PI_{AC}$ | Contiene las condiciones de acceso a una señal multimedia para comparar los títulos de acceso presentes en el procesador de seguridad. |

Finalmente, la memoria 62 contiene igualmente una tabla 74 que permite determinar el emplazamiento donde está grabada una llave criptográfica de un operador determinado.

En la presente memoria, para cada operador 7A, 7B, el procesador 42 contiene, por ejemplo, las llaves enumeradas en la tabla siguiente. La primera columna de esta tabla contiene el nombre de la llave, la segunda columna contiene el identificador de esta llave y la tercera columna contiene una breve descripción de la función de esta llave.

Tabla 3

| | | |
|---|---|---|
| $K_e$ | Ke-ID | Llave de descifrado del criptograma CW* de una palabra de control CW |
| $K_u$ | Ku-ID | Llave que permite descifrar un mensaje EMM confidencial |
| $K_s$ | $K_r$-ID | Llave de desciframiento de un criptograma $K_e$* de la llave $K_e$ |

Teniendo en cuenta las notaciones definidas en la tabla 3, la tabla 74 contiene las informaciones enumeradas en la tabla que sigue. La primera columna de esta tabla contiene el identificador de la llave, la segunda columna contiene el identificador del operador que utiliza esta llave y la tercera columna contiene las informaciones por las cuales el procesador puede encontrar el emplazamiento de esta llave en la memoria 66.

Tabla 4

| | | |
|---|---|---|
| Ke-ID | $SOID_1$ | @1-$K_e$ |
| Kc-ID | $SOID_2$ | @2-$K_e$ |
| Ku-ID<br>Ku-ID | $SOID_1$<br>$SOID_2$ | @1-$K_u$<br>@2-$K_u$ |
| Kr-ID | $SOID_1$ | @1-$K_r$ |
| Kr-ID | $SOID_2$ | @2-$K_r$ |

La memoria 66 contiene dos zonas de memoria distintas, denominadas en la presente memoria entidad $E_1$ y entidad $E_2$, en las cuales están almacenadas las llaves criptográficas utilizadas, respectivamente, por los operadores 7A y 7B. Preferentemente, los títulos de acceso a las señales multimedia utilizadas por los operadores 7A y 7B están grabados únicamente en sus entidades $E_1$ y $E_2$ respectivas.

Se observará que en el procesador 42 la misma llave, por ejemplo la llave $K_e$, no está grabada en el mismo lugar según si es controlada y utilizada por el operador 7A o por el operador 7B. Eso permite proporcionar unos valores diferentes a esta llave $K_e$ según que sea utilizada por uno u otro de los operadores.

Por último, la memoria 66 contiene igualmente las listas FIELDKEY, FIELPIEMM, FIELDPIEMMC, FIELDPIECM y FIELDFCT.

La lista FIELDKEY asocia a cada llave criptográfica diversas cerraduras. Más precisamente, como se ilustra en la figura 4, para cada llave, la lista FIELDKEY contiene:

- un campo KEY-ID que contiene el identificador de la llave tal como se define en la tabla 3, y

- un campo FIELDKEY que contiene tantas cerraduras $LO_i$ como identificadores de funciones elementales haciendo intervenir una llave. En la presente memoria, cada cerradura corresponde a un campo destinado a contener únicamente un valor binario tal como “0” o “1”. Teniendo en cuenta que esta cerradura está contenida en la memoria 66, esta es regrabable y su valor se puede conmutar del valor “0” al valor “1” y viceversa.

En la presente memoria, las cerraduras $LO_i$ están dispuestas las unas después de las otras en las zonas de memoria contiguas y sucesivas de manera que la posición de una cerradura permita identificar a que función elemental le corresponda. Por ejemplo, la cerradura $LO_i$ a la iésima posición está asociada únicamente a un solo identificador IdF1 de una función elemental y viceversa.

En la presente memoria, cuando una cerradura $LO_i$ contiene el valor “0” eso significa que la utilización de la llave identificada por KEY-ID por la función elemental correspondiente a esta cerradura $LO_i$ está autorizada. En el caso contrario en que la cerradura $LO_i$ comprende el valor “1”, la función elemental que corresponde a esta cerradura no puede utilizar esta llave criptográfica.

La lista FIELDPIEMM ilustrada en la figura 5 contiene las cerraduras $LP_i$ para indicar, para cada parámetro $P_i$ susceptible de estar contenido en un mensaje EMM no confidencial, si está autorizado o prohibido su tratamiento por el procesador 42. Por ejemplo, la lista FIELDPIEMM contiene tantas cerraduras $LP_i$ como parámetros $P_i$ susceptibles de ser recibidos. Como para la lista FIELDKEY, el valor de cada cerradura es conmutable entre el valor “0” y el valor “1” y viceversa. La lista FIELDPIEMM está realizada por una sucesión de campos que contienen cada uno un valor binario y corresponde a cada uno a una cerradura $LP_i$. La posición de la cerradura $LP_i$ en la lista FIELDPIEMM permite determinar cuál es el único parámetro $P_i$ que corresponde a esta cerradura. Se observará en particular que la lista FIELDPIEMM contiene en la presente memoria una cerradura $LP_{config}$ que corresponde al parámetro $P_{config}$ que contiene las informaciones necesarias para la configuración de cada una de las cerraduras. El valor “0” de la cerradura $LP_i$ significa que el tratamiento del parámetro $P_i$ que corresponde a esta cerradura está autorizado. El valor “1” significa que está prohibido el tratamiento del mismo parámetro $P_i$ .

La lista FIELDPIEMMC contiene las cerraduras $LC_i$ para indicar cuáles son los parámetros, susceptibles de estar contenidos en un mensaje EMMC (Entitlement Management Message Confidential), que deben ser tratados por el procesador 42. Se recuerda que un mensaje EMMC es idéntico a un mensaje EMM salvo por el hecho de que una parte de sus parámetros esté cifrada con ayuda de una llave $K_u$ predefinida. Cada cerradura $LC_i$ Corresponde a un solo parámetro $P_i$. La lista FIELDPIEMMC comprende igualmente una cerradura $LC_{config}$ correspondiendo al parámetro $P_{config}$.

La lista FIELDPIECM contiene las cerraduras $LE_i$ para indicar cuáles son los parámetros de un mensaje ECM cuyo tratamiento está autorizado o prohibido por el procesador 42. Cada cerradura $LE_i$ corresponde a un solo parámetro $P_i$.

Por ejemplo, la estructura de las listas FIELDPIEMMC y FIELDPIECM es idéntica a la descrita con respecto a la figura 5 salvo que las cerraduras son señaladas, respectivamente, $LC_i$ y $LE_i$. El significado de los valores “0” y “1” para estas cerraduras $LC_i$ y $LE_i$ es el mismo que para la cerradura $LP_i$.

La lista FIELDFCT contiene las cerraduras $LF_i$ aptas para indicar cuáles son las funciones elementales cuya ejecución está autorizada o por el contrario prohibida en el interior del procesador 42. Por ejemplo, la estructura de esta lista FIELDFCT representada en la figura 6 contiene tanto la cerradura $LF_i$ como identificadores de las funciones elementales contenidas en la tabla 1 de manera que cada cerradura corresponde a una sola función elemental. Se recuerda que por "función elemental" se entiende en la presente memoria una funcionalidad elemental de acceso condicional. La estructura de la lista FIELDFCT es similar a la estructura descrita con respecto a la figura 5. así, la posición de la cerradura $LF_i$ permite determinar cuál es el único identificador $IdF_i$ que corresponde a esta cerradura. En la presente memoria, cuando la cerradura $LF_i$ toma el valor “0” la ejecución de la función elemental correspondiente está autorizada. Cuando el valor de esta misma cerradura toma el valor “1”, la ejecución de la función elemental correspondiente está prohibida. En este caso, o no es ejecutable ninguna función o se ejecuta automáticamente una función de reemplazo en vez de la función elemental prohibida. El código de esta función de reemplazo está contenido en la memoria 62. En la presente memoria, la función de reemplazo se libra sistemáticamente para estar más seguros de la función elemental que reemplaza eventualmente. Por ejemplo, la función de reemplazo comprende sistemáticamente menos instrucciones que la función elemental que reemplaza.

El funcionamiento del sistema 2 se describe ahora con respecto al procedimiento de la figura 7.

Inicialmente, cuando está configurada una fase 90 de personalización, el procesador 42 mediante una interfase especial tal como por ejemplo una interfase JTAG (Joint Test Action Group) o mediante la misma interfase que la utilizada para el conector al descodificador 40. La fase de personalización se muestra en un medio de seguridad y en particular, las diferentes órdenes de configuración transmitidas al procesador 42 no son nunca transmitidas mediante una red WAN (Wide Avea Network). Durante la fase 90, se utiliza una unidad de configuración independiente del emisor 4 para iniciar el valor de cada una de las cerraduras normalmente al valor “0”.

Una vez acabada la fase de personalización, el procesador 42 se suministra después para insertarse en un descodificador de un abonado. Comienza entonces una fase de utilización 94.

Durante la fase 94, el procesador 42 trata los mensajes EMM y ECM transmitidos por el emisor 4 de manera que se pueda extraer de estos mensajes la palabra de control CW necesaria para descodificar las señales multimedia codificadas recibidas.

Durante la fase de utilización, durante una etapa 96, se transmite un mensaje EMM de configuración al procesador 42 por el emisor 4. Este mensaje de configuración contiene un parámetro $P_{config}$ de configuración. Un ejemplo de estructura de este parámetro $P_{config}$ está representado en la figura 8. Este parámetro $P_{config}$ está codificado según la estructura TLV. Contiene, por tanto, un campo que contiene el identificador $PI_{config}$ que indica que los datos que siguen sean los datos de configuración de las listas FIELDKEY, FIELDPIEMM, FIELDPIEMMC, FIELDPIECM y FIELDFCT. El parámetro $P_{config}$ contiene igualmente un campo $L_{config}$ y un campo $V_{config}$. El campo $L_{config}$ indica la longitud del campo $V_{config}$. El campo $V_{config}$ contiene el conjunto de las informaciones necesarias para poner al día los valores de las cerraduras de las diferentes listas contenidas en la memoria 66. Las diferentes informaciones son por ejemplo en la presente memoria las codificadas utilizando la estructura TLV. Así, el campo $V_{config}$ se divide en cinco porciones respectivamente FIELDKEY, FIELDPIEMM, FIELDPIEMMC, FIELDPIECM y FIELDFCT. Cada una de estas secciones contiene respectivamente las informaciones necesarias para hacer conmutar el valor de cada una de las cerraduras $LO_i$, $LP_i$, $LC_i$, $LE_i$ y $LF_i$.

Durante una etapa 98, como respuesta a la recepción del mensaje EMM de configuración, la ejecución de la función de configuración de los valores de las diferentes cerraduras se activa. Así, durante la etapa 98, el valor de cada una de las cerraduras está regulado en función de las informaciones contenidas en el campo $V_{config}$.

A continuación, si el procesador 42 recibe un mensaje EMM no confidencial o un mensaje EMMC el procesador procede, respectivamente, a las etapas 100 y 102 de gestión de los derechos de acceso y de las llaves criptográficas. Si el procesador 42 recibe un mensaje ECM, procede entonces a una etapa 104 de extracción de la palabra de control.

Al principio de la etapa 100, durante una operación 110 el microprocesador 60 ejecuta la función de restricción para determinar si el tratamiento del primer parámetro $P_i$ recibido está prohibido. Para esto, durante la etapa 110, la función de restricción consulta la lista FIELDPIEMM y verifica si la cerradura que corresponde a este parámetro $P_i$ tiene el valor “1”. En caso negativo, durante una etapa 112, el procesador 42 identifica cual es la función elemental cuya ejecución debe ser activada para tratar el parámetro $P_i$. A tal efecto, se utiliza la tabla 72.

A continuación, durante una operación 114, el microprocesador 60 ejecuta una nueva vez la función de restricción para determinar si la ejecución de la función elemental identificada durante la etapa 112 está prohibida. A tal efecto, durante la etapa 114, se utiliza la lista FIELDFCT. Más precisamente, durante la operación 114, el procesador 42 verifica si el valor de la cerradura que corresponde a la función elemental identificada tiene el valor “1”. En caso negativo, la ejecución de esta función elemental está autorizada y se prosigue el procedimiento por una operación 116 de ejecución de esta función elemental.

Se supone en la presente memoria que durante la ejecución de esta función elemental, esta tiende a acceder a una llave criptográfica en la entidad $E_i$ correspondiente al identificador $SOID_i$ recibido.

En cada intento de acceso a una llave criptográfica, durante una operación 118, el microprocesador ejecuta la función de restricción para verificar si la función elemental ejecutada actualmente está autorizada o no para utilizar la llave a la que tiende a acceder. A tal efecto, durante la operación 118, se utiliza la lista FIELDKEY. Más precisamente, durante la operación 118, el procesador 42 verifica si el valor de la cerradura asociado al identificador ID-KEY de esta llave y que corresponde a esta función elemental es igual a "1". En caso negativo, durante una operación 120, el acceso a esta llave criptográfica está autorizado y el procedimiento vuelve a la operación 116 o la función elemental continúa ejecutándose.

Una vez que se ha ejecutado completamente la operación 116 o si durante una de las operaciones 110, 114 ó 118, el valor de la cerradura testada es igual a “1”, entonces el procedimiento prosigue por una operación 122 de detención inmediata de los tratamientos activados por el parámetro $P_i$ recibido. Además, en el caso en que se proceda a la operación 122, como el valor de una de las cerraduras es igual a “1”, puede ser emitida una indicación de error. En este modo de realización, no se ejecuta ninguna función de reemplazo si el valor de la cerradura es igual a “1”.

Después de la operación 122, el procedimiento vuelve a la operación 110 para tratar el parámetro $P_i$ siguiente

contenido en el mismo mensaje EMM.

Las etapas 110 a 122 son reiteradas para todos los parámetros $P_i$ del mensaje EMM recibido.

Por ejemplo, ajustando el valor de las cerraduras $LO_i$, $LP_i$ y $LF_i$, es posible obtener los siguientes comportamientos del procesador de seguridad:

- el parámetro $P_{Ke}$ que contiene el criptograma de una nueva llave $K_e$ no es tratado si el valor de la cerradura $LP_{Ke}$ es igual a “1”; no es posible por tanto poner al día una llave de desciframiento de palabras de control,

- el parámetro $P_{TdA}$ que contiene los datos para modificar o inscribir un nuevo título de acceso a una señal multimedia no es tratado si el valor de la cerradura $LP_{TdA}$ es igual a “1”; así no es posible grabar o poner al día un abono,

- la utilización de la llave $K_s$ para descifrar el criptograma de la llave $K_e$ no está autorizada para ciertas funciones elementales y puede estarlo para otras funciones elementales,

- la modificación del límite autorizado en compras compulsivas, la inscripción de un nuevo título de acceso o la inscripción o la modificación de una llave criptográfica están prohibidas si el valor de la cerradura $LF_i$ correspondiente es igual a “1”.

Se observará igualmente que la ejecución de la función elemental adecuada para configurar el valor de las cerraduras puede estar prohibida si el valor de la cerradura $LP_{config}$ o $LF_{config}$ es igual a “1”. Así, si el mensaje EMM recibido contiene el parámetro $P_{config}$, y el valor de la cerradura $LP_{config}$ o $LF_{config}$ es igual a ”1”, entonces la modificación del valor de las cerraduras está prohibida de manera que el comportamiento del procesador 42 se detiene definitivamente.

La etapa 102 es idéntica, por ejemplo, a la etapa 100 con excepción de que se procede primero a un desciframiento del mensaje EMMC con ayuda de la llave $K_u$ si se autoriza tal desciframiento y se utiliza la lista FIELDPIEMMC en vez de la lista FIELDPIEMM.

El hecho de utilizar dos listas diferentes FIELDPIEMM y FIELDPIEMMC permite obtener un comportamiento diferente del procesador 42 si trata un mensaje EMM no confidencial o un mensaje EMMC.

Durante la etapa 104, la función de restricción se pone en práctica de una manera similar a lo que se describe con respecto a la etapa 100 con excepción del hecho de que el mensaje tratado sea un mensaje ECM y que por consiguiente se utiliza la lista FIELDPIECM en vez de la lista FIELDPIEMM.

Así, es posible impedir el desciframiento del criptograma CW* jugando con el valor de una o varias de las cerraduras siguientes:

- una cerradura $LO_{cw}$ asociada a la llave $K_e$ y que corresponde a la función elemental de desciframiento del criptograma de la palabra de control,

- una cerradura $LE_{CW}$ de la lista FIELDPIECM que corresponde al parámetro CW*, o

- una cerradura $LF_{CW}$ de la lista FIELDFCT que corresponde a la función elemental de desciframiento del criptograma CW*.

Puede ser útil cuando se ha determinado que el procesador 42 es utilizado de una manera fraudulenta.

Durante la etapa 104, es igualmente posible impedir la comparación de las condiciones de acceso particulares contenidas en un mensaje ECM recibido con los títulos de acceso memorizados en el procesador de seguridad jugando con el valor de una de las cerraduras siguientes:

- una cerradura $LE_{AC}$ de la lista FIELDPIECM que corresponde al parámetro AC de una condición particular, o

- una cerradura $LF_{AC}$ de la lista FIELDFCT que corresponde a la función elemental de comparación de las condiciones de acceso a los títulos de acceso.

Puede ser útil para prohibir la descodificación de ciertas señales multimedia por el receptor 8.

Sin embargo, en el caso normal, después de la fase 104, la palabra de control es descifrada y después proporcionada al descodificador 48 que descodifica las señales multimedia recibidas durante una etapa 130.

Las señales multimedia descodificadas se anuncian a continuación en claro por la pantalla 50, durante una etapa 132.

Una puesta en práctica juiciosa del procedimiento anterior consiste en enviar en un mismo mensaje EMM:

- un primer parámetro $P_{config}$ para hacer conmutar el valor de una cerradura $LO_p$ o $LC_p$ o $LE_p$ o $LF_p$ al valor “0”, seguido inmediatamente,

- un parámetro que activa una operación que no puede sacarse adelante si se ha conmutado el valor de la cerradura modificado por el primer parámetro $P_{config}$ a “ 0 “, e inmediatamente seguido por

- un segundo parámetro $P_{config}$ que permite cambiar el valor de la cerradura modificada por el primer parámetro $P_{config}$ en sentido inverso.

Así, una operación particular del procesador 42 está autorizada únicamente durante un intervalo de tiempo muy corto. Además, el procesador de seguridad tal como el procesador 42 trata en general los parámetros $P_i$ en su orden de llegada y no permite un tratamiento multitarea de diversos parámetros simultáneamente. En estas condiciones, la recepción del mensaje EMM descrita anteriormente impide explotar un fallo de seguridad eventual en esta operación particular. En efecto, antes de la recepción de este mensaje EMM, la operación particular no puede ser ejecutada teniendo en cuenta que el valor de la cerradura es igual a “1”. A continuación, cuando el valor de la cerradura se conmuta a “0” y teniendo en cuenta que el procesador 42 ejecuta esta operación inmediatamente después de la modificación del valor de la cerradura, no es posible intercalar otro tratamiento destinado a explotar el fallo de seguridad de esta operación. A continuación, inmediatamente después de la ejecución de la operación, el valor de la cerradura se conmuta de nuevo a “1” de manera que no sea posible más activar la ejecución de esta operación que presenta un fallo de seguridad. En estas condiciones, es posible ejecutar una operación que presenta un fallo de seguridad sin que este fallo de seguridad pueda ser explotado por un pirata.

Son posibles otros numerosos modos de realización. Por ejemplo, el procesador de seguridad 42 se puede integrar en un módulo recambiable de descodificación conforme a la norma EN 50 221. Como variante, el procesador de seguridad es un módulo material integrado rígidamente en el descodificador o en el módulo recambiable de descodificación. Así este descodificador o este módulo recambiable no forma con el procesador de seguridad más que una misma y sola entidad rígida.

Por último, el procesador de seguridad puede ser igualmente un módulo del software ejecutado por el descodificador o por el módulo recambiable. En este último caso, el microprocesador del procesador de seguridad es el mismo que el utilizado por el descodificador o el módulo recambiable para efectuar otras funciones tales como la descodificación.

Como variante, las cerraduras pueden estar asociadas igualmente a cada título de acceso memorizado en el procesador de seguridad para autorizar y alternativamente, prohibir el acceso a estos títulos de acceso.

En otra variante, una cerradura $LE_i$ posicionada en el valor “0” autoriza (etapa 110) la presencia del parámetro $P_i$ concerniente reservándose el derecho de que el código 64 de aplicación lo autorice natural. Es del mismo modo para una cerradura $LP_i$, $LC_i$, $LO_i$ (etapa 118) o $LF_i$ (etapa 114). Por ejemplo, en el caso en que las listas FIELDPIEMM, FIELDPIEMMC y FIELDPIECM tienen la misma estructura, ciertos parámetros $P_i$ designados en FIELDPIEMM o FIELDEMMC, como los parámetros para descifrar una palabra de control, son prohibidos de manera natural en un mensaje EMM o EMMC por la aplicación misma. En otro ejemplo, una versión funcional de un procesador de seguridad puede soportar la función elemental de inscripción de nuevos títulos de acceso aunque otra versión funcional, concebida como desechable después del acceso a un solo contenido, no lo permita.

**REIVINDICACIONES**

1. Procesador de seguridad para un decodificador adecuado para recibir una señal multimedia codificada con la ayuda de una palabra de control, siendo difundida esta señal por un cabeza de red, comprendiendo este procesador una memoria (62) no regrabable que contiene un código (64) de una aplicación que, cuando se ejecuta por un microprocesador, permite ejecutar un conjunto de operaciones necesarias para el tratamiento de mensajes ECM (Entitlement Control Message) y mensajes EMM (Entitlement Management Message) para extraer la palabra de control necesaria para la descodificación de la señal multimedia codificada, **caracterizado porque**:

- el procesador de seguridad comprende al menos una primera cerradura ($LO_i$, $LP_i$, $LC_i$, $LE_i$, $LF_i$) grabable cuyo valor se puede conmutar entre un primer y un segundo valor predeterminados como respuesta a un mensaje EMM o ECM,

- el código de aplicación contiene igualmente una función de restricción apta para autorizar y, alternativamente, prohibir, en respuesta a la recepción de un mismo mensaje ECM o EMM y en función del valor de la primera cerradura, solamente una operación particular del procesador de seguridad entre el conjunto de operaciones necesarias para el tratamiento de los mensajes ECM y EMM, aunque permitiendo al procesador de seguridad ejecutar otras operaciones necesarias para el tratamiento de los mensajes EMM y ECM que no hayan sido prohibidos, eligiéndose esta operación particular del grupo formado por:

  - la utilización de una llave criptográfica grabada en la memoria de un procesador de seguridad,

  - el tratamiento de un parámetro contenido en un mensaje EMM o ECM recibido, y

  - la ejecución de una función elemental de acceso condicional del código de aplicación, ejecutándose cada función elemental de acceso condicional del código de aplicación independientemente de otras funciones elementales de acceso condicional de manera que la no ejecución de una función elemental de acceso condicional no impide la ejecución, por el microprocesador, de una cualquiera de otras funciones elementales de acceso condicional.

2. Procedimiento de acuerdo con la reivindicación 1, en el que:

- la memoria comprende al menos un campo FIELDKEY asociado a una de las llaves criptográficas, conteniendo este campo FIELDKEY diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental de acceso condicional respectivo y

- la función de restricción es apta para autorizar y, alternativamente, prohibir la utilización de esta llave criptográfica por una función elemental de acceso condicional en función del valor de la cerradura contenida en el campo FIELDKEY y correspondiendo a esta función elemental de acceso condicional.

3. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que:

- el procesador de seguridad contiene al menos una lista escogida entre las listas siguientes:

  - una lista FIELDPIEMM asociada a los mensajes EMM no confidenciales, conteniendo esta lista FIELDPIEMM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM no confidencial,

  - una lista FIELDPIEMMC asociada a los mensajes EMM confidenciales (Entitlement Management Message Confidential), conteniendo esta lista FIELDPIEMMC diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM confidencial, y

  - una lista FIELDPIECM asociada a los mensajes ECM, conteniendo esta lista FIELDPIECM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje ECM,

- la función de restricción es apta para autorizar y, alternativamente, prohibir el tratamiento de un parámetro $P_i$ contenido en un mensaje recibido por el procesador de seguridad en función del valor de la cerradura que corresponde a este parámetro en la lista asociada a este mensaje.

4. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que:

- el procesador de seguridad comprende una lista FIELDFCT asociada a las funciones elementales de acceso condicional, conteniendo esta lista FIELDFCT diversas cerraduras, correspondiendo estas cerraduras cada una a una función elemental de acceso condicional respectivo, y

- la función de restricción es apta para autorizar y, alternativamente, prohibir la ejecución de una función elemental de acceso condicional en función del valor de la cerradura de la lista FIELDFCT que corresponde a

esta función elemental de acceso condicional.

5. Procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que:

- el procesador de seguridad comprende al menos una segunda cerradura regrabable cuyo valor se puede conmutar entre un primer y un segundo valor predeterminados como respuesta a un mensaje EMM o ECM,

- la función de restricción es apta para prohibir en función del valor de esta segunda cerradura:

  - la utilización de cualquier llave criptográfica necesaria para hacer conmutar el valor de la primera o la segunda cerradura,

  - el tratamiento de todo parámetro contenido en un mensaje EMM adecuado para hacer conmutar el valor de la primera o la segunda cerradura, y

  - la ejecución de toda función elemental de acceso condicional adecuada para hacer conmutar el valor de la primera o la segunda cerradura.

6. Procesador de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la función elemental de acceso condicional es diferente de una función de inscripción de nuevos títulos de acceso y de una función de inscripción de nuevas llaves criptográficas.

7. Procedimiento de configuración del comportamiento de un procesador de seguridad para un decodificador adecuado para recibir una señal multimedia codificada con la ayuda de una palabra de control, siendo difundida esta señal por un cabeza de red, comprendiendo este procedimiento:

- el suministro de al menos una primera cerradura regrabable cuyo valor es conmutable entre un primer y un segundo valor predeterminados como respuesta a un mensaje EMM,

- la autorización y, alternativamente, la prohibición (110, 114, 118), como respuesta al mismo mensaje EMM o ECM y en función del valor de la primera cerradura, de solamente una operación particular del procesador de seguridad entre el conjunto de las operaciones necesarias para el tratamiento de los mensajes ECM y EMM, aunque permitiendo que el procesador de seguridad ejecute las otras operaciones necesarias para el tratamiento de los mensajes EMM y ECM que no hayan sido prohibidos, eligiéndose esta operación particular del grupo compuesto por:

  - la utilización (120) de una llave criptográfica grabada en una memoria del procesador de seguridad,

  - el tratamiento (112) de un parámetro contenido en un mensaje EMM o ECM recibido, y

  - la ejecución (116) de una función elemental de acceso condicional por el procesador de seguridad, ejecutándose cada función elemental de acceso condicional independientemente de otras funciones elementales de acceso condicional de manera que la no ejecución de una función elemental de acceso condicional no impide la ejecución, por el procesador de seguridad, de una cualquiera de las otras funciones elementales de acceso condicional.

8. Procedimiento de acuerdo con la reivindicación 7, en el que el procedimiento comprende:

- el suministro de una memoria que contiene al menos un campo FIELDKEY asociado a una de las llaves criptográficas, conteniendo este campo FIELDKEY diversas cerraduras, correspondiendo cada una de estas cerraduras a una función elemental respectiva, y

- la autorización y, alternativamente, la prohibición de la utilización de esta llave criptográfica asociada al campo FIELDKEY por una función elemental de acceso condicional en función del valor de la cerradura que está contenida en el campo FIELDKEY y que corresponde a esta función elemental de acceso condicional.

9. Procedimiento de acuerdo con la reivindicación 7 u 8, en el que el procedimiento comprende:

- el suministro de una memoria que contiene al menos una lista escogida entre las listas siguientes:

  - una lista FIELDPIEMM asociada a los mensajes EMM no confidenciales, conteniendo esta lista FIELDPIEMM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM no confidencial,

  - una lista FIELDPIEMMC asociada a los mensajes EMM confidenciales (Entitlement Management Message Confidential), conteniendo esta lista FIELDPIEMMC diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje EMM confidencial, y

- una lista FIELDPIECM asociada a los mensajes ECM, conteniendo esta lista FIELDPIECM diversas cerraduras, correspondiendo cada una de estas cerraduras a un parámetro respectivo $P_i$ susceptible de estar contenido en un mensaje ECM, y

- la autorización y, alternativamente, la prohibición del tratamiento de un parámetro $P_i$ contenido en un mensaje recibido por el procesador de seguridad en función del valor de la cerradura que corresponde a este parámetro en la lista asociada a este mensaje.

10. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 7 a 9, en el que el procedimiento comprende :

- el suministro de una memoria que comprende una lista FIELDFCT

asociada a las funciones elementales de acceso condicional, conteniendo

esta lista FIELDFCT diversas cerraduras, correspondiendo cada una de

estas cerraduras a una función elemental de acceso condicional respectivo,y

- la autorización y, alternativamente, la prohibición de la ejecución de una función elemental de acceso condicional en función del valor de la cerradura en la lista FIELDFCT que corresponde a esta función elemental de acceso condicional.

11. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 7 a 10, en el que el procedimiento comprende la configuración inicial por defecto del valor de cada cerradura para que, como respuesta a la recepción del primer mensaje EMM o ECM difundido por la cabeza de red, ninguna operación particular sea prohibida.

12. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 7 a 11, en el que el procedimiento comprende:

- la recepción en un mismo mensaje EMM:

  - de un primer parámetro activante de la conmutación del valor de la primera cerradura para autorizar una operación particular del procesador de seguridad,

  - de un segundo parámetro activador de la ejecución de esta misma operación particular, y

  - de un tercer parámetro activante de la conmutación del valor de la primera cerradura para prohibir esta misma operación particular, y

- en tratamiento por orden para el procesador de seguridad del primer, segundo y tercer parámetro.

13. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 7 a 12, en el que la función elemental de acceso condicional es diferente de una función de inscripción de nuevos títulos de acceso y de una función de inscripción de nuevas llaves criptográficas.

14. Suporte de grabación de informaciones que contiene instrucciones para la ejecución de un procedimiento de configuración conforme a una cualquiera de las reivindicaciones 7 a 13, cuando estas instrucciones son ejecutadas por un microprocesador de un procesador de seguridad.

**DOCUMENTOS INDICADOS EN LA DESCRIPCIÓN**

En la lista de documentos indicados por el solicitante se ha recogido exclusivamente para información del lector, y no es parte constituyente del documento de patente europeo. Ha sido recopilada con el mayor cuidado; sin embargo, la EPA no asume ninguna responsabilidad por posibles errores u omisiones.

**Documentos de patente indicados en la descripción**


- WO 2004049141 A **[0004]**
- WO 03075233 A **[0006]**

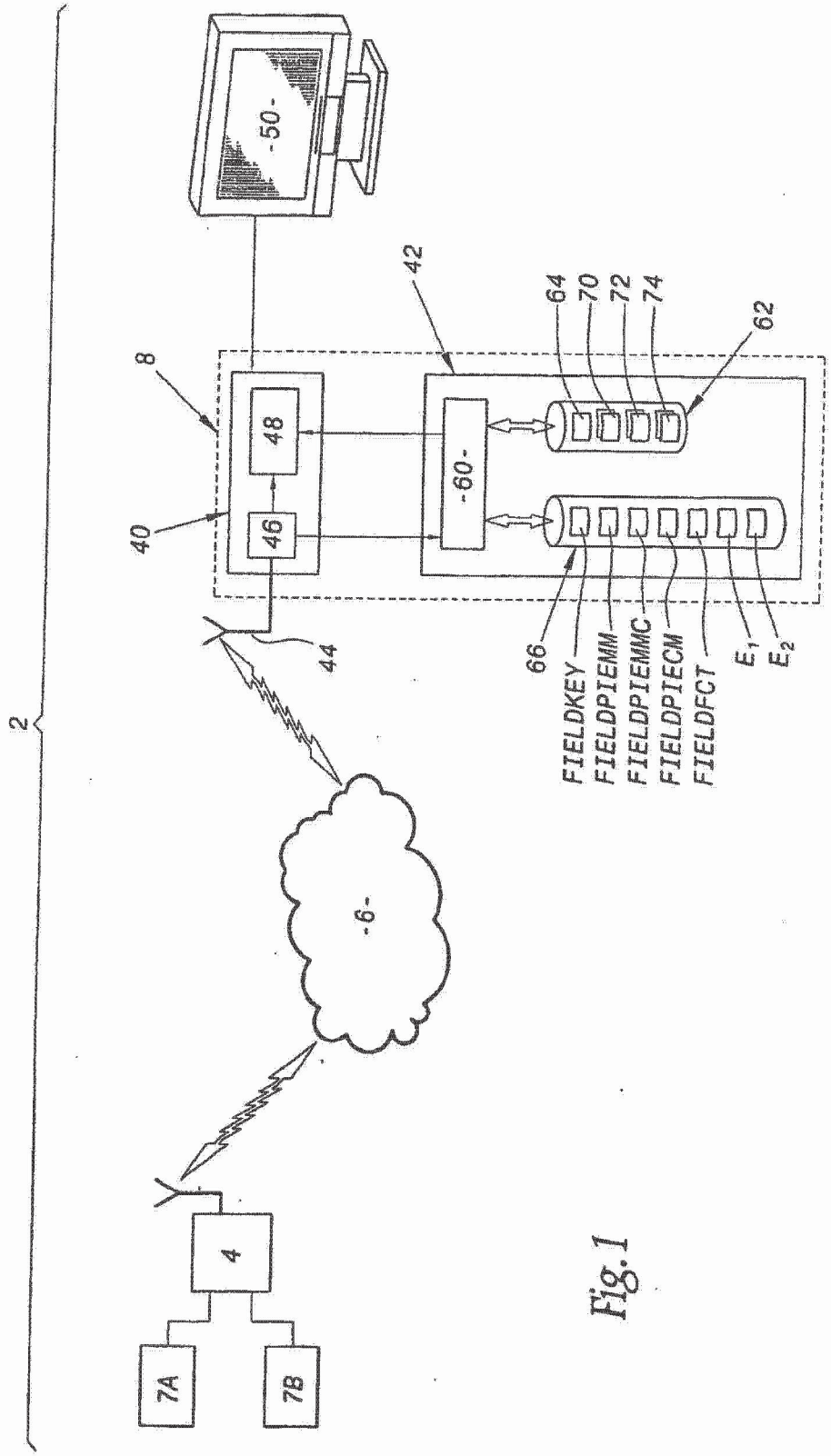

2
-50-
42
64
70
72
74
62
8
48
-60-
40
46
44
66
FIELDKEY
FIELDPIEMM
FIELDPIEMMC
FIELDPIECM
FIELDFCT
E1
E2
-6-
4
7A
7B

Fig. 1

Fig.2

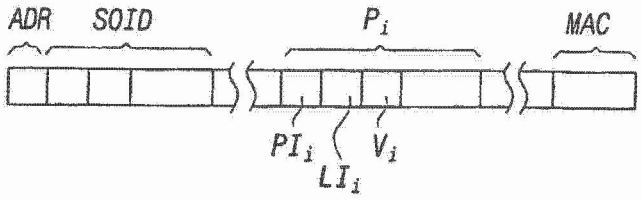



Fig.3

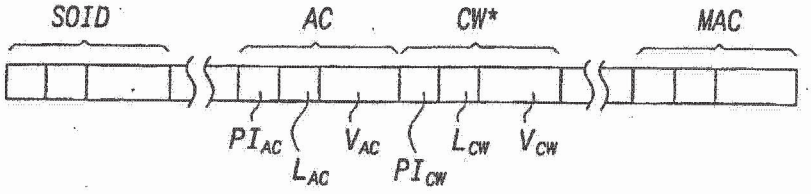



Fig.4

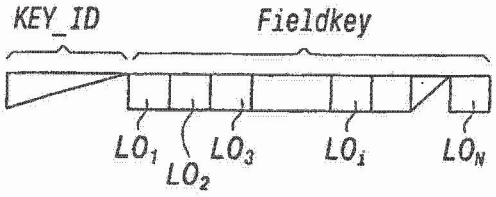



Fig.5

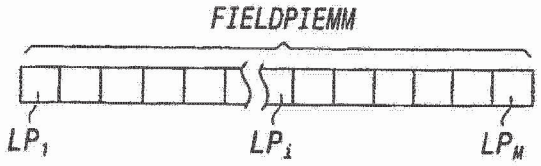



Fig.6

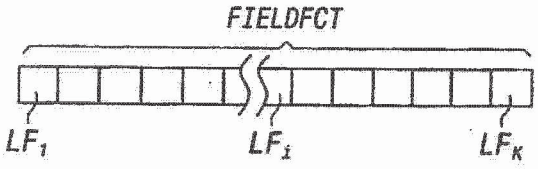
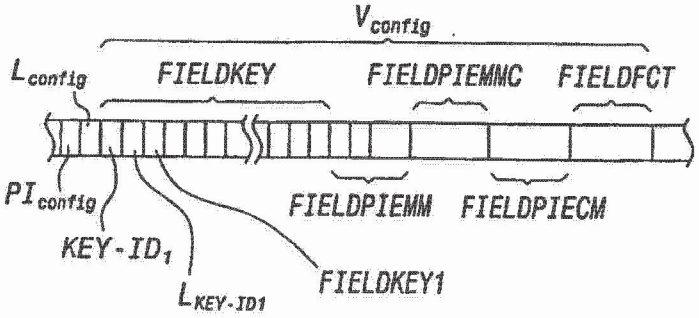



Fig.8



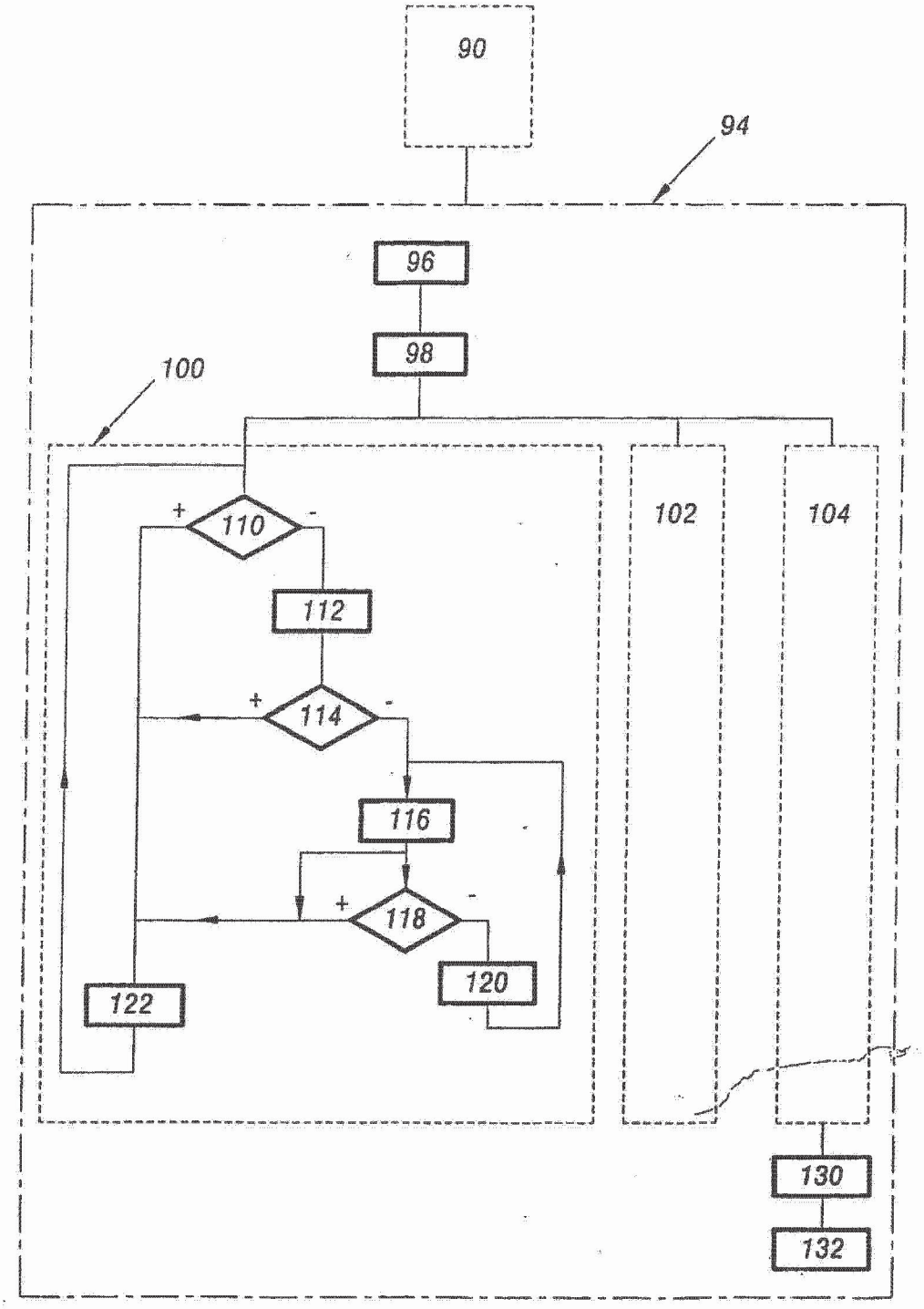



*Fig.7*