(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 500 061**

(51) Int. CI.:

G06F 21/10 (2013.01)
G06F 21/77 (2013.01)
H04N 21/258 (2011.01)
H04N 21/418 (2011.01)
H04N 21/61 (2011.01)
H04N 21/6334 (2011.01)
H04N 7/16 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.02.2003 E 03004320 (2)**

(97) Fecha y número de publicación de la concesión europea: **09.07.2014 EP 1345437**

(54) Título: **Configuración asíncrona**

(30) Prioridad:

28.02.2002 US 85860

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.09.2014

(73) Titular/es:

THE DIRECTV GROUP, INC. (100.0%)
2230 E. Imperial Highway
El Segundo, CA 90245, US

(72) Inventor/es:

COCCHI, RONALD P. y
CURREN, CHRISTOPHER P.

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

CONFIGURACIÓN ASÍNCRONA

Referencia cruzada a solicitudes relacionadas

Esta solicitud está relacionada con las siguientes solicitudes de patente pendientes de resolución y de titularidad compartida, siendo referidas dichas solicitudes en el presente documento:

Solicitud de Patente de Estados Unidos Nº de Serie xx/xxx.xxx, titulada "*MULTIPLE NONVOLATILE MEMORIES*", por Ronald Cocchi, y otros, Expediente Nº PD-200335, presentada en la misma fecha que la presente;

Solicitud de Patente de Estados Unidos Nº de Serie xx/xxx.xxx, titulada "*HIDDEN IDENTIFICATION*", por Ronald Cocchi, y otros, Expediente Nº PD-200336, presentada en la misma fecha que la presente; y

Solicitud de Patente de Estados Unidos Nº de Serie xx/xxx.xxx, titulada "*DEDICATED NONVOLATILE MEMORY*", por Ronald Cocchi, y otros, Expediente Nº PD-200337, presentada en la misma fecha que la presente.

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere a sistemas y procedimientos para limitar el acceso no autorizado a servicios digitales y, en particular, a un procedimiento y un sistema para la incorporación de un hardware basado en un mecanismo de configuración asíncrona en una tarjeta inteligente capaz de reconfigurar dinámicamente una máquina de estados de hardware utilizando un proceso de entrega segura.

2. Descripción de la técnica relacionada

Los servicios digitales, tales como programas de televisión e información relativa a estos programas (por ejemplo, una guía de programas) se distribuyen a los usuarios por medio de una variedad de procedimientos de difusión. Estos servicios pueden ser propietarios y estar disponibles en base a una suscripción. Para impedir el acceso no autorizado a los servicios, se utilizan una gran cantidad de mecanismos de seguridad. Tales mecanismos pueden almacenar información en la memoria, en los que la información se utiliza para validar a un usuario o proporcionar acceso. Sin embargo, las personas a menudo intentan obtener acceso ilegal/no autorizado a los servicios alterando los contenidos de la memoria. Lo que se necesita es la capacidad de impedir o aumentar la dificultad de obtener acceso ilegal a la información y los servicios digitales. Estos problemas se pueden entender mejor mediante una descripción de los actuales procedimientos de difusión, mecanismos de seguridad, y procedimientos para obtener acceso no autorizado a dichos servicios.

Como se describió anteriormente, los programas de televisión y servicios digitales se distribuyen a los televidentes mediante una variedad de procedimientos de difusión. Estos procedimientos incluyen la televisión de difusión analógica tradicional (*National Television Standards Committee* o norma "*NTSC*"), la televisión de difusión digital (*Advanced Television Systems Committee* o norma "*ATSC*") que pronto será necesaria, la televisión por cable (tanto analógica como digital), la difusión por satélite (tanto analógica como digital), así como otros procedimientos. Estos procedimientos permiten que los canales de contenido de televisión sean multiplexados y transmitidos a través de un medio de transmisión común.

Para ver la programación de televisión y tener acceso a los servicios digitales, los usuarios suelen tener un *set top box* (también conocido como un receptor/decodificador integrado [*IRD – Integrated Receiver Decoder*]). Dentro del sistema o *set top box*, se puede utilizar un componente/microcircuito de seguridad conocido como una tarjeta inteligente para evitar el acceso no autorizado a los programas de televisión y servicios digitales. El microcircuito de la tarjeta inteligente puede contener un micro-procesador, componentes de memoria volátil, un componente de memoria no volátil, y un módulo de E/S del sistema. El sistema de seguridad puede verse comprometido si los componentes son atacados o utilizados de maneras imprevistas.

La memoria no volátil se ha utilizado ampliamente en toda la industria de la electrónica. Por ejemplo, en el receptor/decodificador integrado, el micro-procesador utiliza memoria no volátil para contener información de estado (por ejemplo, información de estatus) que se utiliza para proporcionar la funcionalidad deseada y hacer cumplir las políticas de seguridad previstas por los diseñadores. El micro-procesador y/o una unidad de control de acceso a la memoria utilizada por el micro-procesador restringen el acceso a los componentes de la memoria.

En la técnica anterior, prácticamente todos los compromisos de la seguridad eficaces para alterar el software del sistema contenido en la memoria no volátil han sido por medio de ataques externos, no invasivos utilizando el módulo de E/S del sistema. Tales compromisos pueden requerir simplemente un ordenador y un lector de tarjetas barato (de por ejemplo 10 dólares). Por lo tanto, la mayoría de los ataques se producen por la manipulación inadecuada del micro-procesador o de la unidad de control de acceso a la memoria.

Por ejemplo, han habido numerosos intentos por parte de personas o empresas (es decir, hackers o atacantes) de atacar, usar incorrectamente o modificar la memoria no volátil a través de medios externos de reprogramación o, de otro modo, alteración de los contenidos de la memoria cuando el componente de memoria ha estado a disposición del procesador central o, de otro modo, en el bus del sistema. Por ejemplo, se pueden usar ataques que utilizan procedimientos imprevistos o subvierten defensas mal implementadas para obtener acceso no autorizado a los contenidos de la memoria y/o llegar a reprogramar los contenidos de la memoria. La reprogramación o el acceso no autorizado a los contenidos de la memoria pueden llegar a comprometer por completo las características de seguridad previstas en el dispositivo.

La forma más simple y más común de ataque contra los componentes de memoria utiliza medios externos no invasivos que utilizan un módulo de E/S del sistema, debido al bajo coste de los equipos necesarios para implementar esta forma de ataque. La mayoría de los ataques se producen por la manipulación inadecuada de un micro-procesador o una unidad de control de acceso a la memoria. Por ejemplo, se han subvertido contenidos de la memoria cuando se ha comprometido una unidad de control de acceso a memoria (que controla el acceso a un componente de memoria). Una vez que se ha violado el único componente de memoria, el atacante puede entonces tener la capacidad de acceder a todas las ubicaciones de dirección de memoria que se encuentran en otros componentes de memoria.

Con el fin de no comprometer la seguridad a través del software del sistema y la memoria no volátil, algunas técnicas anteriores también emplean hardware personalizado dentro de la tarjeta inteligente. El hardware personalizado proporciona una máquina de estados de hardware que implementa una política de seguridad. Sin embargo, dicha máquina de estados de hardware es fija. En consecuencia, si el hardware se ve comprometido, la tarjeta inteligente debe ser reemplazada físicamente para acomodar a una máquina de estados de hardware diferente. Dicha sustitución puede ser muy cara si la base de clientes desplegada es grande.

Resumen de la invención

Los sistemas de servicios digitales a menudo contienen un componente de seguridad conocido como una tarjeta inteligente para evitar el acceso no autorizado a los servicios. El microcircuito de la tarjeta inteligente contiene un micro-procesador, componentes de memoria volátil, componentes de memoria no volátil, un bloque de lógica personalizada, y un módulo de E/S del sistema. El sistema de seguridad se puede ver comprometido si se utilizan o se atacan componentes de memoria de maneras desatendidas normalmente a través del módulo de E/S del sistema.

Una o más formas de realización de la invención proporcionan un procedimiento, aparato, y artículo de fabricación para la incorporación de un mecanismo basado en hardware, de configuración asíncrona a una tarjeta inteligente capaz de reconfigurar dinámicamente una máquina de estados de hardware mediante un proceso de entrega segura desde el sistema de cabecera (*head-end*). Un sistema de cabecera cifra una clave de configuración y entrega la clave a la tarjeta inteligente a través del flujo de difusión (*broadcast stream*), Internet, devolución de llamada (*callback*) u otro canal de distribución adecuado. La implementación es ocultada con respecto al micro-procesador colocando el motor de descifrado y el mecanismo de configuración en una máquina de estados de hardware. Dado que la implementación se basa en hardware, está protegida de su alteración por parte del micro-procesador o de

medios externos. El motor de descifrado y mecanismos de configuración son seguros porque no son accesibles directamente por el módulo de E/S del sistema o bus del sistema.

WO 02/093332 A1 describe un procedimiento para proteger un circuito lógico contenido en una unidad lógica contra ataques externos. Dicho procedimiento comprende las siguientes operaciones: generar en la unidad una instrucción de programación de un circuito lógico programable comprendido en el circuito lógico; cargar en el circuito lógico programable, en respuesta a la instrucción de programación, una configuración concreta de programación seleccionada de entre una pluralidad de configuraciones diferentes entre sí; programar el circuito lógico programable de acuerdo con la configuración concreta. Sin embargo, esta configuración podría verse comprometida por un ataque externo.

EP 1 085 516 A1, WO 00/77717 A1, EP 1 074 906 A1, EP 1 176 826 A2, EP 0 984 403 A1 y EP 0 851 358 A2 describen diversas técnicas para proteger datos sensibles almacenados en varios dispositivos semiconductores. Éstas no permiten la selección de una configuración particular de entre una pluralidad de tales configuraciones. Estas técnicas no son aplicables para proporcionar una mayor seguridad a servicios digitales juntamente con funciones de mantenimiento fácil y reconfiguración rápida.

Breve descripción de los dibujos

Haciendo referencia ahora a los dibujos en los que números de referencia similares representan partes correspondientes a lo largo de:

La figura 1 es un diagrama que muestra una visión general de un sistema de distribución de vídeo;

La figura 2 es un diagrama de bloques que muestra una configuración típica de enlace de subida (*uplink*) que muestra cómo se sube material de programa de vídeo a un satélite para su transmisión a los abonados usando un solo transpondedor;

La figura 3 es un diagrama de bloques de una forma de realización del subsistema de guía de programas;

La figura 4A es un diagrama de un flujo (*stream*) de datos representativos recibidos procedentes de un satélite;

La figura 4B es un diagrama que ilustra la estructura de un paquete de datos;

La figura 5 es un diagrama de bloques de una forma de realización de un receptor/decodificador integrado;

La figura 6 ilustra la arquitectura de un módulo de acceso condicional de acuerdo con una o más formas de realización de la invención;

La figura 7 ilustra la arquitectura de un bloque de lógica personalizada de acuerdo con una o más formas de realización de la invención; y

La figura 8 es un diagrama de flujo que ilustra el uso del bloque de lógica personalizada para proporcionar acceso a los servicios digitales de acuerdo con una o más formas de realización de la invención.

Descripción detallada de formas de realización preferidas

En la siguiente descripción se hace referencia a los dibujos adjuntos que forman parte de la misma y que muestran, a modo de ilustración, varias formas de realización de la presente invención. Se entiende que se pueden utilizar otras formas de realización y se pueden realizar cambios estructurales sin apartarse del alcance de la presente invención.

Visión general

Un propósito de esta invención es proteger la tarjeta inteligente de permitir la visualización no autorizada. En consecuencia, se han diseñado específicamente unas formas de realización para prevenir ataques externos no invasivos. La protección se consigue mediante la implementación de la invención en un hardware reconfigurable dinámicamente de forma personalizada contenido en la tarjeta inteligente.

Sistema de distribución de vídeo

La figura 1 es un diagrama que ilustra una visión general de un único sistema de distribución de vídeo vía satélite 100. El sistema de distribución de vídeo 100 comprende un centro de control 102 en comunicación con un centro de enlace de subida 104 a través de un enlace terrestre (*ground link*) u otro enlace 114 y con una estación receptora de abonado 110 a través de una red pública de telefonía conmutada (*PSTN – public switched telephone network*) u otro enlace 120. El centro de control 102 proporciona material de programas (por ejemplo, servicios digitales, programas de vídeo, programas de audio y datos) al centro de enlace de subida 104 y se coordina con las estaciones receptoras de abonado 110 para ofrecer, por ejemplo, servicios de programas de pago por visión (*PPV – pay per view*), incluyendo la facturación y el descifrado asociado de los programas de vídeo.

El centro de enlace de subida 104 recibe material de programas e información de control de programas procedente del centro de control 102, y usando una antena de enlace de subida 106 y un transmisor 105, transmite el material de programas y la información de control de programas al satélite 108 a través del enlace de subida 116. El satélite recibe y procesa esta información, y transmite los programas de vídeo y la información de control a la estación receptora de abonado 110 a través del enlace de bajada 118 utilizando el transmisor 107. La estación receptora de abonado 110 recibe esta información a través de la unidad exterior (*ODU – outdoor unit*) 112, que incluye una antena de abonado y un convertidor de bloque de poco ruido (LNB – *low noise block*).

La estación receptora de abonado 110 permite el uso/visualización de la información por parte de un abonado 122. Por ejemplo, la información puede ser utilizada/visualizada en un televisor 124 u otro dispositivo de visualización. Para controlar el acceso a la información, la estación receptora de abonado 110 incluye un receptor/decodificador integrado (IRD) 126. En formas de realización de la invención, el receptor/decodificador integrado 126 está acoplado comunicativamente a un componente de seguridad conocido como un módulo de acceso condicional o tarjeta inteligente que controla el acceso a los servicios de información/digitales.

En una forma de realización, la antena de la estación receptora de abonado es una antena de banda *Ku* de forma ligeramente ovalada de 18 pulgadas. La forma ligeramente ovalada se debe a la alimentación excéntrica de 22,5 grados (*22.5 degree offset feed*) del convertidor de bloque de poco ruido (*LNB – low noise block*) que se utiliza para recibir señales reflejadas desde la antena de abonado. La alimentación excéntrica posiciona el convertidor de bloque de poco ruido de manera que no bloquea cualquier área de la superficie de la antena minimizando la atenuación de la señal de microondas entrante.

El sistema de distribución de vídeo 100 puede comprender una pluralidad de satélites 108 con el fin de proporcionar una cobertura terrestre más amplia, para proporcionar canales adicionales, o para proporcionar un ancho de banda adicional por canal. En una forma de realización de la invención, cada satélite comprende 16 transpondedores para recibir y transmitir material de programa y otros datos de control procedentes del centro de enlace de subida 104 y proporcionarlo a las estaciones receptoras de abonado 110. Con el uso de la compresión de datos y técnicas de multiplexado las capacidades de canal, dos satélites 108 trabajando en conjunto pueden recibir y transmitir más de 150 canales convencionales (no HDTV) de audio y vídeo a través de 32 transpondedores.

Aunque la invención descrita en el presente documento se describirá con referencia a un sistema de distribución de vídeo basado en satélite 100, la presente invención también puede ponerse en práctica con la transmisión terrestre de información de programa, ya sea por medios de difusión, cable, u otros medios. Además, las diferentes funciones asignadas colectivamente entre el centro de control 102 y el centro de enlace de subida 104 como se han descrito anteriormente, se pueden reasignar según se desee sin apartarse del alcance pretendido de la presente invención.

Aunque lo anterior se ha descrito con respecto a una forma de realización en la que el material de programa entregado al abonado 122 es material de programa de vídeo (y audio), tal como una película, el procedimiento anterior puede ser usado para entregar material de programa que comprende simplemente información de audio o también otros datos.

Configuración de enlace de subida

La figura 2 es un diagrama de bloques que muestra una configuración típica de enlace de subida para un solo transpondedor de satélite 108, que muestra cómo se sube material de programas de vídeo al satélite 108 por parte del centro de control 102 y del centro de enlace de subida 104. La figura 2 muestra tres canales de vídeo (que podrían ser aumentados respectivamente con uno o más canales de audio para música de alta fidelidad, información de banda sonora, o un programa de audio secundario para la transmisión de idiomas extranjeros), un canal de datos procedente de un subsistema de guía de programas 206 e información de datos informáticos procedentes de una fuente de datos informáticos 208.

Los canales de vídeo son proporcionados por una fuente de programas de material de vídeo 200A - 200C (denominados colectivamente en lo sucesivo como fuente(s) de vídeo 200). Los datos procedentes de cada fuente de programas de vídeo 200 son proporcionados a un codificador 202A - 202C (denominado colectivamente en lo sucesivo como codificador(es) 202). Cada uno de los codificadores acepta un sello de tiempo de programa (*PTS – program time stamp*) procedente del controlador 216. El sello de tiempo de programa es un sello de tiempo binario envolvente (*wrap-around*) que se utiliza para asegurar que la información de vídeo se sincroniza adecuadamente con la información de audio después de la codificación y la decodificación. Se envía un sello de tiempo *PTS* con cada trama *I-frame* de los datos codificados MPEG.

En una forma de realización de la presente invención, cada codificador 202 es un codificador de segunda generación del grupo de expertos en imágenes en movimiento (*MPEG-2 - Motion Picture Experts Group*), pero también se pueden usar otros decodificadores que implementan otras técnicas de codificación. El canal de datos puede ser sometido a un esquema de compresión similar por parte de un codificador (no mostrado), pero dicha compresión es normalmente innecesaria o realizada por programas informáticos en la fuente de datos informáticos (por ejemplo, los datos fotográficos típicamente se comprimen en archivos *.TIF o archivos *.JPG antes de la transmisión). Después de la codificación por parte de los codificadores 202, las señales son convertidas en paquetes de datos por parte de un empaquetador 204A - 204F (denominado colectivamente en lo sucesivo como empaquetador(es) 204) asociado con cada fuente 200.

Los paquetes de datos se ensamblan usando una referencia procedente del reloj del sistema 214 (*SCR – system clock reference*) y procedente del gestor de acceso condicional 210, el cual proporciona el identificador de canal de servicio (*SCID – service cannel identifier*) a los empaquetadores 204 para su uso en la generación de los paquetes de datos. Estos paquetes de datos a continuación son multiplexados en datos en serie y transmitidos.

Subsistema de Guía de programas

La figura 3 es un diagrama de bloques de una forma de realización del subsistema de guía de programas 206. El sistema de transmisión de datos de guía de programas 206 incluye una base de datos de guías de programas 302, un compilador 304, sub-bases de datos 306A - 306C (denominadas colectivamente como sub-bases de datos 306) y temporizadores (*cyclers*) 308A - 308C (denominados colectivamente como temporizadores 308).

Los suministros de programaciones 310 proporcionan información electrónica de programaciones en cuanto a las horas y el contenido de diversos canales de televisión, tal como la que se encuentra en las programaciones de televisión contenidas en los periódicos y las guías de televisión. Los suministros de programaciones 310 incluyen preferentemente información de una o más empresas especializadas en el suministro de información de programación, tales como *TRIBUNE MEDIA SERVICES*^{TM} y *T.V. DATA*^{TM}. Los datos proporcionados por empresas tales como *TRIBUNE MEDIA SERVICES*^{TM} y *T.V. DATA*^{TM} se transmiten normalmente a través de líneas telefónicas para programar la base de datos de guías 302. Estas empresas ofrecen datos de programación de televisión para todas las estaciones de televisión de todo el país además de los canales a nivel nacional tales como *SHOWTIME*^{TM}, *HBO*^{TM} y *DISNEY CHANNEL*^{TM}. El formato específico de los datos que son proporcionados por estas empresas cambia de una empresa a otra. La base de datos de guías de programas 302 incluye preferiblemente datos de programación para los canales de televisión de toda la nación, incluyendo todos los canales nacionales y los canales locales, independientemente de si los canales son transmitidos por la estación de transmisión.

La base de datos de guías de programas 302 es un sistema informático que recibe datos procedentes de los suministros de programaciones 310 y organiza los datos en un formato estándar. El compilador 304 lee los datos en formato estándar fuera de la base de datos de guías de programas 302, identifica porciones de programación comunes, convierte los datos de guía de programas en el formato adecuado para su transmisión a los usuarios (en concreto, los datos de guía de programas se convierten en unos objetos según se discute más abajo) y genera la datos de guía de programas para una o más de las sub-bases de datos 306.

Los datos de las guías de programas también se pueden introducir manualmente en la base de datos de guías de programas 302 a través de la estación de entrada de datos 312. La estación de entrada de datos 312 permite a un operador introducir información adicional de programación, así como combinar y organizar datos suministrados por las empresas de programaciones. Al igual que con los datos organizados informáticamente, los datos introducidos manualmente son convertidos por el compilador en objetos separados y son enviados a una o más de las sub-bases de datos 306.

Los objetos de guía de programas se almacenan temporalmente en las sub-bases de datos 306 hasta que los temporizadores 308 solicitan la información. Cada uno de los temporizadores 308 puede transmitir objetos a una velocidad diferente que los otros temporizadores 308. Por ejemplo, el temporizador 308A puede transmitir objetos cada segundo, mientras que los temporizadores 308B y 308C pueden transmitir objetos cada 5 segundos y cada 10 segundos, respectivamente.

Dado que los receptores de los abonados pueden no estar siempre encendidos y recibiendo y guardando los objetos, la información de guía de programas se retransmite continuamente. Los objetos de guía de programas para los programas que se visualizarán en el próximo par de horas se envían con mayor frecuencia que los objetos de guía de programas para los programas que se visualizarán más tarde. Por lo tanto, los objetos de guía de programas para los programas más actuales son enviados a un temporizador 308 con una alta velocidad de transmisión, mientras que los objetos de guía de programas para programas posteriores son enviados a temporizadores 308 con una menor velocidad de transmisión. Una o más de las salidas de datos 314 de los temporizadores 308 se envían al empaquetador de un transpondedor en particular, como se muestra en La figura 2.

Se observa que la configuración de enlace de subida representada en la figura 2 y el subsistema de guía de programas representado en la figura 3 pueden ser implementados por uno o más módulos de hardware, uno o más módulos de software que definen instrucciones realizadas por un procesador, o una combinación de ambos.

Formato y Protocolo de Flujo de Datos de Difusión (*Broadcast Data Stream Format and Protocol*)

La figura 4A es un diagrama de un flujo de datos representativo. El primer segmento de paquete 402 comprende información procedente del canal de vídeo 1 (datos procedentes de, por ejemplo, la primera fuente de programas de video 200A). El siguiente segmento de paquete 404 comprende información de datos informáticos que fue obtenida, por ejemplo, de la fuente de datos informáticos 208. El siguiente segmento de paquete 406 comprende información procedente del canal de vídeo 5 (procedente de una de las fuentes de programas de vídeo 200). El siguiente segmento de paquete 408 comprende información de guía de programas tal como la información proporcionada por el subsistema de guía de programas 206. Según se muestra en la figura 4A, se pueden insertar paquetes nulos 410 creados por el módulo de paquetes nulos 212 en el flujo de datos según se desee.

El flujo de datos comprende, por lo tanto, una serie de paquetes procedentes de cualquiera de las fuentes de datos en un orden determinado por el controlador 216. El flujo de datos es cifrado por el módulo de cifrado 218, modulado por el modulador 220 (usando normalmente un esquema de modulación *QPSK*), y proporcionado al transmisor 222, el cual difunde el flujo de datos modulado en un ancho de banda de frecuencia al satélite a través de la antena 106. El receptor 126 recibe estas señales y re-ensambla los paquetes usando el identificador de canal de servicio (*SCID*) para re-generar el material de programas para cada uno de los canales.

La figura 4B es un diagrama de un paquete de datos. Cada paquete de datos (por ejemplo, de 402 a 416) tiene una longitud de 147 bytes, y comprende un número de segmentos de paquete. El primer segmento de paquete 420 comprende dos bytes de información que contienen el identificador de canal de servicio e indicadores (*flags*). El identificador de canal de servicio es un número único de 12 bits que identifica de forma única el canal de datos del paquete de datos. Los indicadores (*flags*) incluyen 4 bits que se utilizan para controlar otras características. El

segundo segmento de paquete 422 está formado por un indicador de 4 bits del tipo de paquete y un contador de continuidad de 4 bits. El tipo de paquete identifica el paquete como uno de los cuatro tipos de datos (vídeo, audio, datos o nulo). Cuando se combina con el identificador de canal de servicio, el tipo de paquete determina cómo se usará el paquete de datos. El contador de continuidad se incrementa una vez para cada tipo de paquete e identificador de canal de servicio. El siguiente segmento de paquete 424 comprende 127 bytes de datos de carga útil (*payload*), que en los casos de los paquetes 402 o 406 es una parte del programa de vídeo proporcionada por la fuente de programas de video 200. El segmento de paquete final 426 son datos requeridos para realizar la corrección de errores hacia adelante (*forward error correction*).

Receptor/decodificador integrado

La figura 5 es un diagrama de bloques de un receptor/decodificador integrado (*IRD – Integrated receiver/decoder*) 126 (en lo sucesivo denominado también alternativamente como receptor 126 o *set top box*). El receptor 126 comprende un sintonizador/demodulador (*tuner/demodulator*) 504 acoplado comunicativamente a una unidad exterior (*ODU*) 112 que tiene uno o más convertidores de bloque de poco ruido (*LNB*) 502. El convertidor de bloque de poco ruido 502 convierte la señal del enlace de bajada 118 de 12,2 hasta 12,7 GHz procedente de los satélites 108 en, por ejemplo, una señal de 950-1450 MHz requerida por el sintonizador/demodulador 504 del receptor/decodificador integrado 126. El convertidor de bloque de poco ruido 502 puede proporcionar una salida doble o una salida única. El convertidor de bloque de poco ruido de salida única 502 sólo tiene un conector RF, mientras que el convertidor de bloque de poco ruido de salida doble 502 tiene dos conectores RF de salida y se pueden utilizar para alimentar un segundo sintonizador 504, un segundo receptor 126, o alguna otra forma de sistema de distribución.

El sintonizador/demodulador 504 aísla un transpondedor de 24 MHz único y modulado digitalmente, y convierte los datos modulados en un flujo de datos digitales. El flujo de datos digitales es suministrado a continuación a un decodificador de corrección de errores hacia adelante (*FEC - forward error correction*) 506. Esto permite que el receptor/decodificador integrado 126 re-ensamble los datos transmitidos por el centro de enlace de subida 104 (el cual ha aplicado la corrección de errores hacia delante a la señal deseada antes de su transmisión a la estación receptora de abonado 110) verificando que se ha recibido la señal de datos correcta, y corrigiendo errores, si los hay. Los datos corregidos sin errores pueden ser suministrados desde el módulo decodificador de corrección de errores hacia adelante 506 al módulo de transporte 508 a través de una interfaz paralela de 8 bits.

El módulo de transporte 508 lleva a cabo muchas de las funciones de procesamiento de datos realizadas por el receptor/decodificador integrado 126. El módulo de transporte 508 procesa los datos recibidos procedentes del módulo decodificador de corrección de errores hacia adelante 506, y proporciona los datos procesados al decodificador MPEG de vídeo 514 y al decodificador MPEG de audio 517. En una forma de realización de la presente invención, el módulo de transporte, el decodificador MPEG de vídeo y el decodificador MPEG de audio están implementados en circuitos integrados. Este diseño promueve tanto el espacio como la eficiencia energética, y aumenta la seguridad de las funciones realizadas en el módulo de transporte 508. El módulo de transporte 508 también proporciona un paso (*passage*) para las comunicaciones entre el micro-controlador 510 y los decodificadores MPEG de vídeo y de audio 514, 517. Según se expone más detalladamente en lo sucesivo, el módulo de transporte también opera con el módulo de acceso condicional (*CAM – conditional access module*) 512 para determinar si se le permite a la estación receptora de abonado 110 acceder a cierto material de programas. Los datos del módulo de transporte se pueden suministrar también a un módulo de comunicación externo 526.

El módulo de acceso condicional 512 funciona en asociación con otros elementos para decodificar una señal cifrada procedente del módulo de transporte 508. El módulo de acceso condicional 512 también se puede utilizar para el seguimiento y la facturación de estos servicios. En una forma de realización de la presente invención, el módulo de acceso condicional 512 es una tarjeta inteligente que tiene contactos que interaccionan en cooperación con contactos del receptor/decodificador integrado 126 para pasar información. Con el fin de implementar el procesamiento realizado en el módulo de acceso condicional 512, el receptor/decodificador integrado 126, y específicamente el módulo de transporte 508 proporciona una señal de reloj al módulo de acceso condicional 512. A continuación se describen detalles de la arquitectura del módulo de acceso condicional 512.

Los datos de vídeo son procesados por el decodificador MPEG de vídeo 514. Usando la memoria de acceso aleatorio (RAM) de vídeo 536, el decodificador MPEG de vídeo 514 decodifica los datos de vídeo comprimidos y los

envía a un codificador o procesador de vídeo 516, el cual convierte la información de vídeo digital recibida procedente del módulo MPEG de vídeo 514 en una señal de salida utilizable por una pantalla u otro dispositivo de salida. A modo de ejemplo, el procesador 516 puede comprender un codificador *NTSC* (*National Television System Committee* - Comisión Nacional de Sistema de Televisión) o *ATSC* (*Advanced Television Systems Committee* - Comité de Sistemas de Televisión Avanzada). En una forma de realización de la invención, se proporcionan tanto señales de S-Video como señales de vídeo convencional (*NTSC* o *ATSC*). También se pueden utilizar otras salidas, y son ventajosas si se procesa programación de alta definición.

Los datos de audio son decodificados igualmente por el decodificador MPEG de audio 517. Los datos de audio decodificados pueden entonces ser enviados a un convertidor digital a analógico (D/A) 518. En una forma de realización de la presente invención, el convertidor D/A 518 es un doble convertidor D/A, uno para los canales derecho e izquierdo. Si se desea, se pueden agregar canales adicionales para su uso en el procesamiento de sonido envolvente o programas de audio secundarios (*SAPs – secondary audio programs*). En una forma de realización de la invención, el propio doble convertidor D/A 518 separa la información de canal izquierdo y derecho, así como cualquier información de canal adicional. Se pueden soportar otros formatos de audio de manera similar. Por ejemplo, se pueden soportar otros formatos de audio tal como el *DOLBY DIGITAL AC-3* multi-canal.

Se puede encontrar una descripción de los procesos realizados en la codificación y decodificación de flujos de vídeo, particularmente con respecto a codificación/decodificación *MPEG* y *JPEG*, en el Capítulo 8 de "*Digital Televisión Fundamentals,*" de *Michael Robin* y *Michel Poulin*, *McGraw-Hill*, 1998, el cual se incorpora por referencia en el presente documento.

El micro-controlador 510 recibe y procesa señales de comando procedentes del control remoto 524, de una interfaz de teclado de un receptor/decodificador integrado 126 y/o de otro dispositivo de entrada. El micro-controlador recibe comandos para realizar sus operaciones procedentes de una memoria de programación del procesador, que almacena de forma permanente dichas instrucciones para la realización de dichos comandos. La memoria de programación del procesador puede comprender una memoria de sólo lectura (*ROM – read only memory*) 538, una memoria de sólo lectura borrable y programable eléctricamente (*EEPROM - Electrically Erasable Programmable Read-Only Memory*) 522 o, un dispositivo de memoria similar. El micro-controlador 510 controla también los otros dispositivos digitales del receptor/decodificador integrado 126 a través de líneas de direcciones y de datos (denotadas "A" y "D", respectivamente, en la Figura 5).

El módem 540 se conecta a la línea telefónica del cliente a través del puerto *PSTN* (*Public Switched Telephone Network* - Red Telefónica Pública Conmutada) 120. Llama, por ejemplo, al proveedor de programas y transmite la información de compra del cliente para fines de facturación, y/u otra información. El módem 540 es controlado por el micro-procesador 510. El módem 540 puede emitir datos a otros tipos de puertos de E/S, incluyendo puertos estándar de E/S paralelos y en serie de un ordenador.

La presente invención también comprende una unidad de almacenamiento local tal como el dispositivo de almacenamiento de vídeo 532 para almacenar datos de vídeo y/o audio obtenidos del módulo de transporte 508. El dispositivo de almacenamiento de vídeo 532 puede ser una unidad de disco duro, un disco compacto de DVD leíble/escribible, una RAM de estado sólido, o cualquier otro medio de almacenamiento. En una forma de realización de la presente invención, el dispositivo de almacenamiento de vídeo 532 es una unidad de disco duro con capacidad de lectura/escritura paralela especializada de tal manera que se pueden leer datos del dispositivo de almacenamiento de vídeo 532 y escribir datos en el dispositivo 532 al mismo tiempo. Para lograr este objetivo, se puede utilizar memoria intermedia (*buffer memory*) adicional accesible por el almacenamiento de vídeo 532 o su controlador. Opcionalmente, se puede usar un procesador de almacenamiento de vídeo 530 para gestionar el almacenamiento y la recuperación de los datos de vídeo del dispositivo de almacenamiento de vídeo 532. El procesador de almacenamiento de vídeo 530 puede comprender también memoria para el almacenamiento intermedio (*buffering*) de datos que entran y salen del dispositivo de almacenamiento de vídeo 532. Alternativamente o en combinación con lo anterior, se puede utilizar una pluralidad de dispositivos de almacenamiento de vídeo 532. También alternativamente o en combinación con lo anterior, el micro-controlador 510 puede realizar también las operaciones requeridas para almacenar y/o recuperar datos de vídeo y otros datos del dispositivo de almacenamiento de vídeo 532.

La entrada del módulo de procesamiento de vídeo 516 se puede suministrar directamente como una salida de vídeo a un dispositivo de visualización tal como un monitor de vídeo o de ordenador. Además, las salidas de vídeo y/o audio se pueden suministrar a un modulador de RF 534 para producir una salida de RF y/o de banda lateral vestigial 8 (*8-VSB: 8-Vestigal Side Band*) adecuada como una señal de entrada a un sintonizador de televisión convencional. Esto permite que el receptor 126 opere con televisiones sin una salida de video.

Cada uno de los satélites 108 comprende un transpondedor, que acepta información de programa procedente del centro de enlace de subida 104, y transmite esta información a la estación receptora de abonado 110. Se utilizan técnicas de multiplexación conocidas de manera que se pueden proporcionar múltiples canales al usuario. Estas técnicas de multiplexación incluyen, a modo de ejemplo, diversas técnicas de multiplexación estadísticas u otro dominio del tiempo y multiplexación de polarización. En una forma de realización de la invención, un único transpondedor que opera en una banda única de frecuencia transporta una pluralidad de canales identificados por la respectiva identificación de canal de servicio (*SCID – service cannel identification*).

Preferiblemente, el receptor/decodificador integrado 126 también recibe y almacena una guía de programas en una memoria disponible para el micro-controlador 510. Típicamente, la guía de programas es recibida en uno o más paquetes de datos en el flujo de datos procedente del satélite 108. La guía de programas puede ser accedida y buscada mediante la ejecución de etapas de operación adecuadas implementadas por el micro-controlador 510 y almacenadas en la ROM del procesador 538. La guía de programas puede incluir datos para mapear números de canal del espectador con los transpondedores del satélite e identificaciones de canal de servicio (*SCIDs*), y también proporcionar información de listado de programas de televisión al abonado 122 que identifica eventos de programa.

La funcionalidad implementada en el receptor/decodificador integrado 126 representado en la Figura 5 puede ser implementada por uno o más módulos de hardware, uno o más módulos de software que definen instrucciones realizadas por un procesador, o una combinación de ambos.

Tarjeta de Acceso

Un módulo de acceso condicional 512 a menudo contiene un micro-procesador, componentes de memoria (un componente volátil y un componente no volátil) y un módulo de E/S del sistema para comunicarse con el transporte 508. Los microprocesadores tradicionales dentro de un módulo de acceso condicional 512 tienen memoria no volátil para contener el estado que se utiliza para proporcionar la funcionalidad deseada y hacer cumplir las políticas de seguridad previstas por los diseñadores. El micro-procesador y/o una unidad de control de acceso a la memoria restringen el acceso a los componentes de memoria.

Como se describió anteriormente, los ataques pueden utilizar procedimientos no previstos o pueden subvertir defensas mal implementadas para obtener acceso no autorizado a los contenidos de la memoria y/o conseguir reprogramar los contenidos de la memoria. Por ejemplo, la mayoría de los ataques se producen por la manipulación inadecuada del micro-procesador o la unidad de control de acceso a la memoria. La reprogramación o el acceso no autorizado a los contenidos de la memoria pueden llevar a comprometer por completo las características de seguridad previstas en el módulo de acceso condicional 512. La forma más simple y más común de ataque contra el componente de memoria utiliza medios externos que usan el módulo de E/S del sistema, debido al bajo coste de los equipos necesarios para implementar esta forma de ataque.

Para evitar este procedimiento de ataque, no se confía en la seguridad proporcionada por la memoria volátil o no volátil. En su lugar, una o más formas de realización de la invención utilizan un bloque de lógica personalizada que no está sujeto a la manipulación por ataques externos no invasivos. El bloque de lógica personalizada está implementado en hardware de estado sólido que implementa una máquina de estados dinámica y/o asíncrona simple y bien definida.

La figura 6 ilustra la arquitectura de un módulo de acceso condicional 512 de acuerdo con una o más formas de realización de la invención. El módulo de acceso condicional 512 contiene un micro-procesador 602, componentes de memoria volátil 604 (por ejemplo, memoria de acceso aleatorio [RAM]), uno o más componentes de memoria no volátil 606 (por ejemplo, memoria de sólo lectura programable y borrable eléctricamente [EEPROM], memoria de sólo lectura programable y borrable [EPROM], o "*batter packed RAM*"), un módulo de E/S del sistema 608, y el bloque de lógica personalizada 610, estando todos ellos comunicativamente acoplados a un bus del sistema 612.

Tal como se utilizan en este documento, los términos lógica personalizada y máquina de estados de hardware se refieren al bloque de lógica personalizada 610 en general y a componentes específicos del bloque de lógica personalizada 610. Por lo tanto, un único componente de bloque de lógica personalizada 610 puede definir de forma individual y/o en combinación con otros componentes la lógica personalizada.

La máquina de estados conectada por cable con el bloque de lógica personalizada 610 define unas funciones permisibles (para la utilización de los servicios digitales). Además, la máquina de estados de hardware puede ser reconfigurada. La reconfiguración se puede producir de forma asíncrona y dinámicamente a través de una población de tarjetas inteligentes (módulos de acceso condicional 512). La implementación en hardware aísla el mecanismo de configuración del módulo de E/S del sistema 608, del bus del sistema 612, del micro-procesador 602, o del entorno externo. En consecuencia, la máquina de estados es aislada de otros componentes 602-608 y 612 en el módulo de acceso condicional 512. Al evitar que el módulo de E/S del sistema 608, el bus del sistema 612, el micro-procesador 602, o la unidad de control de acceso a la memoria tengan acceso directo a la máquina de estados de hardware (dentro del bloque de lógica personalizada 610), los ataques que antes tenían éxito ya no son posibles. Por lo tanto, cualquier modificación o intento de obtener acceso no autorizado deberán hacerse a través de ataques invasivos extremadamente caros para modificar el hardware embebido.

Asegurar que los mecanismos de descifrado y configuración estén protegidos frente a posibles modificaciones preserva la integridad del módulo de acceso condicional 512, lo cual es importante para la defensa del modelo de seguridad. Por lo tanto, la seguridad del módulo de acceso condicional 512 está implementada en un hardware que es fijo pero que, sin embargo, se puede reconfigurar mediante una permutación dinámica en el caso de que una configuración específica se vea comprometida. En consecuencia, la solución hardware proporciona un nuevo modo de operación sin tener que reemplazar físicamente el módulo de acceso condicional 512, que puede ser muy caro si la base de clientes desplegados es grande.

La figura 7 ilustra la arquitectura para el bloque de lógica personalizada 610 de acuerdo con una o más formas de realización de la invención. Como se ilustra, un módulo dedicado de E/S y de control de la configuración hardware 714 que se conecta al bus del sistema 612 controla el acceso a los componentes 716-720 del bloque de lógica personalizada 612. Por consiguiente, el único acceso posible a los componentes 716-720 es a través del módulo de E/S y de control de la configuración hardware 714.

La máquina de estados de hardware 718 puede contener la misma lógica que se utiliza en la técnica anterior y no puede ser modificada. Adicionalmente a la máquina de estados 718, la aplicación consiste en una permutación que emplea una serie de multiplexores configurables al inicio 716 y al final 720 de la máquina de estados de hardware fijo 718. La lógica personalizada (es decir, la lógica de control dentro del módulo de E/S y de control de la configuración hardware 714) interconecta los multiplexores (dentro de las permutaciones 716 y 720) al bus del sistema 612 del módulo de acceso condicional 512. En consecuencia, el módulo de E/S y de control de la configuración hardware 714 que se conecta al bus del sistema 612 controla el acceso a la lógica de la permutación 716 y 720 y de la máquina de estados 718.

La lógica personalizada dentro del módulo de E/S y de control de la configuración hardware 714 implementa un protocolo de intercambio de claves aceptando (o rechazando) una serie de claves pre-autorizadas (por ejemplo, claves encapsuladas (*wrapped*) secuencialmente con $n=10^6$ veces u otro valor grande) u otro protocolo de seguridad. La clave define una configuración para las permutaciones 716 y 720. Las claves válidas sólo son dadas a conocer al sistema de cabecera (*headend*) (por ejemplo, el centro de enlace de subida 104) mediante el uso de cualquier algoritmo de clave pública tal como *Rabin* o *RSA* (*Rivest - Shamir - Adelman*). Según un algoritmo de clave pública, las claves no pueden ser recreadas o generadas por desconocidos. Las claves son entregadas a la tarjeta inteligente ya sea a través del flujo de difusión, Internet, u otro canal de distribución apropiado. Las claves se pueden entregar a la población de tarjetas inteligentes (es decir, módulos de acceso condicional 512) de forma asíncrona (por ejemplo, durante un período de varias horas, días o meses). Las claves pueden ser entregadas usando paquetes cifrados de forma única, cifrados en grupo. Estos paquetes son ininteligibles para los miembros (es decir, los módulos de acceso condicional 512) para los que no estaban cifrados. En otras palabras, los paquetes son sólo inteligibles para esos módulos/miembros de E/S y de control 714 que tienen la clave privada apropiada.

El módulo de E/S y de control de la configuración hardware 714 verifica/autentica la clave. Dicha verificación y/o autenticación puede garantizar que la clave procede de una fuente conocida (por ejemplo, un centro de enlace de

subida 104 conocido, una fuente de programas 200A-200C, etc.), que la clave no es un duplicado de una clave ya recibida, o que la clave no cumple con una medida de seguridad adicional. Como parte del proceso de autenticación, el módulo de E/S y de control 714 descifra las claves. La clave descifrada es entonces verificada/autenticada por la lógica personalizada dentro del módulo 714. Si la clave es válida, la clave es retenida por el módulo de E/S y de control 714 (por ejemplo, almacenando las claves en registros protegidos con ningún mecanismo de salida físico o lógico fuera de la lógica personalizada en el módulo 714). Si la clave no es válida, la clave es rechazada y no puede ser almacenada por el módulo de E/S y de control 714.

Como se ha descrito anteriormente, la clave define una configuración para las permutaciones 716 y 720. Por consiguiente, cuando es el caso, la clave se utiliza para reconfigurar las permutaciones 716 y 720 de forma dinámica (es decir, sobre la marcha). El momento de la reconfiguración puede producirse inmediatamente después de recibir la clave. Alternativamente, la clave puede ser almacenada por el módulo de E/S y de control 714 y ser utilizada para reconfigurar las permutaciones 716 y 720 (por ejemplo, cambiar la configuración por la configuración representada por la clave almacenada) al recibir un comando inalámbrico (*over the air command*). En tal circunstancia, el módulo de E/S y de control 714 puede almacenar una clave actualmente activa (que define una permutación 716 y 720 que se está utilizando actualmente) y una clave futura. En consecuencia, las claves pueden ser entregadas de forma asíncrona en un período muy largo de tiempo a múltiples módulos de acceso condicional 512 en los cuales son validadas y almacenadas de forma asíncrona. A partir de entonces (por ejemplo, una vez que ha pasado un período de tiempo para asegurar que los módulos de acceso condicional 512 apropiados/suficientes tienen la nueva clave), se puede entregar un comando inalámbrico (*over the air command*) de forma sincrónica a todos los módulos de acceso condicional 512 para activar una operación de reconfiguración de una clave. Así, la operación real de reconfiguración puede producirse simultáneamente en todos los módulos de acceso condicional 512, mientras que el mecanismo de entrega y validación de la clave es asíncrono dentro de un período de tiempo.

Para reconfigurar las permutaciones, 716 y 720, el módulo de E/S y de control 714 se comunica bidireccionalmente 722 con las pre-permutaciones 716 y post-permutaciones 720 para configurar dinámicamente la serie de multiplexores de cada permutación respectiva 716 y 720. Una vez configurados, las pre-permutaciones 716 ponen en la forma adecuada la información de servicios digitales recibida a través del enlace de comunicaciones 724 procedente del módulo de E/S y de control 714 para su uso por parte de la máquina de estados de hardware 718. La máquina de estados de hardware 718 puede modificar la información de servicios digitales en base a la lógica personalizada dentro de la máquina de estados 718. A partir de entonces, las post-permutaciones 720 pueden modificar la información de servicios digitales de salida para limitar el uso y la visualización de la información frente a atacantes no autorizados.

La información de salida se transmite después a través del enlace de comunicaciones 724 al módulo de E/S y de control 714 para su uso por parte del bus del sistema 612, el micro-procesador 602 u otros componentes. Cabe señalar que, si bien se pueden utilizar tanto las pre-permutaciones 716 como las post-permutaciones 720, el bloque de lógica personalizada 610 sólo puede utilizar una pre-permutación 716 o una post-permutación 720. Sin embargo, independientemente de la implementación no se permiten accesos externos directos a las permutaciones 716 y 720 o a la máquina de estados de hardware 718.

La figura 8 es un diagrama de flujo que ilustra el uso del bloque de lógica personalizada para proporcionar acceso a los servicios digitales de acuerdo con una o más formas de realización de la invención. En la etapa 800, un componente de seguridad (por ejemplo, una tarjeta inteligente) recibe información de configuración (por ejemplo, una clave de configuración) que ha sido transmitida de forma asíncrona. Como se describió anteriormente, dicha información de configuración puede ser recibida a través de un flujo de difusión, Internet, devolución de llamada (*callback*), u otro canal de distribución. Además, la información de configuración puede estar cifrada (por ejemplo, a través de un protocolo de intercambio de claves tal como un algoritmo de clave pública). Además, la información de configuración puede ser recibida en paquetes cifrados de forma única, cifrados en grupo.

Cuando la configuración está cifrada, la etapa 800 también puede incluir el descifrado, la verificación/autenticación, y el almacenamiento de la información de configuración (por ejemplo, en uno o más registros protegidos) si la información es auténtica.

En la etapa 802, una máquina de estados de hardware (por ejemplo, uno o más componentes de la máquina de estados de hardware o uno o más aspectos configurables de la máquina de estados de hardware) es reconfigurada

dinámicamente (por ejemplo, al recibir un comando síncrono) en base a la información de configuración. Tal como se utiliza en la presente memoria y en referencia a la Figura 7, la máquina de estados de hardware incluye las permutaciones 716 y 720. Por consiguiente, la máquina de estados de hardware 716-720 no puede acceder directamente a un módulo de E/S del sistema 608 o un bus del sistema 612 de un módulo de acceso condicional 512. En cambio, el módulo de E/S y de control de la configuración hardware 714 conecta la máquina de estados de hardware 716-720 al bus del sistema 612 y controla el acceso a la lógica de la máquina de estados de hardware 716-720. La reconfiguración dinámica puede comprender la reconfiguración dinámica de una permutación que emplea una serie de uno o más multiplexores configurables al inicio y/o al final de la máquina de estados de hardware 718.

En la etapa 804, el bloque de lógica personalizada 610 controla el acceso a los servicios digitales a través de la máquina de estados de hardware configurable 716-720. En otras palabras, los servicios digitales son recibidos, procesados a través de las pre-permutaciones 716, procesados por la máquina de estados de hardware 718, procesados a través de las post-permutaciones 720, y puestos a disposición en el bus del sistema 612 para su uso posterior.

Conclusión

La forma más simple y más común de ataque contra un componente de memoria de una tarjeta inteligente utiliza medios externos que usan el módulo de E/S del sistema debido al bajo coste de los equipos necesarios para implementar esta forma de ataque. Para evitar este procedimiento de ataque, el acceso a un motor de descifrado reconfigurable dinámicamente es a través de un hardware personalizado y no conectado directamente al módulo de E/S del sistema, al bus del sistema, o al micro-procesador. El bloque de lógica personalizada está implementado en un hardware que implementa una máquina de estados simple y bien definida que no se puede modificar a través de medios no invasivos.

Como se describió anteriormente, el hardware personalizado se ha utilizado ampliamente en las tarjetas inteligentes/módulos de acceso condicional 512 en toda la industria de la electrónica. Sin embargo, las tarjetas inteligentes basadas en implementaciones hardware personalizadas no han intentado la reconfiguración asíncrona y/o dinámica de la máquina de estados de hardware para que la máquina de estados soporte un motor de cifrado/descifrado basado en hardware significativamente diferente. Unas formas de realización de esta invención intentan que la tarjeta inteligente sea segura implementando una máquina de estados de hardware dinámica y asíncrona que está aislada del entorno exterior y que es no modificable a través de ataques externos no invasivos. Además, aunque los mecanismos de descifrado y de configuración de la invención pueden ser todavía potencialmente modificados a través de ataques invasivos sofisticados, costosos y que consumen mucho tiempo en los cuales se modifica el hardware real, la utilización de la presente invención tiene muchas ventajas.

Por ejemplo, la protección de una máquina de estados de hardware a través de un hardware personalizado reconfigurable dinámicamente es importante porque evita los ataques de bajo coste. Se evitan los ataques de bajo coste porque el estado del hardware sólo se puede reconfigurar por medio de un bloque de lógica personalizada y no puede ser reprogramado por el micro-procesador. La evitación de ataques de bajo coste obliga a los atacantes a utilizar ataques invasivos costosos que no están disponibles para la gran mayoría de los piratas. La inhibición de esta forma simple de ataque evita que los intrusos utilicen ataques que requieren sólo un ordenador y un lector de tarjetas barato (de, por ejemplo, 10 dólares). Además, el compromiso adicional de un dispositivo por medio de un ataque interno e invasivo no conduce a un ataque con éxito a través de un ataque externo de bajo coste. Por lo tanto, evitando que el módulo de E/S del sistema 608, el bus del sistema 612, el micro-procesador 602, o la unidad de control de acceso a la memoria tengan acceso directo a la lógica personalizada de los servicios digitales (por ejemplo, un motor de descifrado y/o mecanismos de configuración) contenida en una máquina de estados de hardware 716-720, los ataques anteriores que tenían éxito ya no son posibles.

Además, la implementación personalizada del hardware puede resistir ataques externos sustanciales sin modificar de forma inconveniente la seguridad proporcionada en la tarjeta inteligente. Además, la reconfiguración extiende la vida de la implementación personalizada del hardware y la de la seguridad proporcionada por la tarjeta inteligente. La extensión de la vida de la tarjeta inteligente pospone la sustitución de la tarjeta, de modo que los costes operativos se mantienen bajos.

Esto concluye la descripción de una o más formas de realización de la presente invención. La descripción anterior de la invención se ha presentado para fines de ilustración y descripción. No se pretende que sea exhaustiva o limite la invención a la forma precisa que se ha descrito. Son posibles muchas modificaciones y variaciones a la luz de las enseñanzas anteriores. En consecuencia, aunque la invención puede proteger la recepción de servicios de vídeo, de audio, de banda ancha y de datos usando un microcircuito que reside en una tarjeta inteligente y *set top box*, la invención no se limita a aplicaciones de tarjetas inteligentes o a un sistema de servicios digitales en particular.

REIVINDICACIONES

1. Un procedimiento para proporcionar acceso a un usuario a servicios digitales de difusión distribuidos entre una población de usuarios que usan respectivamente una población de módulos de acceso condicional, siendo cada módulo de acceso condicional para uso con un respectivo receptor/decodificador integrado de los servicios digitales de difusión, que comprende:

(a) recibir y almacenar en un módulo de acceso condicional (512) información de configuración, en el que:

(1) la información de configuración ha sido transmitida de forma asíncrona durante un período de tiempo a la población de módulos de acceso condicional; y

(2) el módulo de acceso condicional (512) está configurado para controlar el acceso a los servicios digitales e incluye un micro-procesador, una memoria no volátil y un bloque de lógica personalizada (610) que comprende una máquina de estados de hardware (718), incluyendo la máquina de estados de hardware una permutación que utiliza uno o más multiplexores configurables y un motor de descifrado; y

(b) tras un comando suministrado de forma síncrona a la población de módulos de acceso condicional, reconfigurar en el bloque de lógica personalizada (610) el uno o más multiplexores configurables de acuerdo con la información de configuración recibida de modo que la máquina de estados de hardware soporta (*takes on*) un motor de descifrado basado en hardware diferente;

en el que la máquina de estados de hardware (718) comprende una lógica personalizada que está adaptada para controlar el acceso a los servicios digitales de difusión, y en el que la máquina de estados de hardware (718) no es accesible directamente desde un módulo de E/S del sistema (608) ni desde un bus del sistema (612) del módulo de acceso condicional; y

en el que el bloque de lógica personalizada (610) comprende además un módulo dedicado de reconfiguración del hardware y de E/S (714) que conecta la máquina de estados de hardware (718) al bus del sistema (612) del módulo de acceso condicional y controla el acceso a la lógica de la máquina de estados de hardware (718).

2. El procedimiento de la reivindicación 1, en el que la información de configuración está cifrada a través de un protocolo de intercambio de claves que comprende un algoritmo de clave pública.

3. El procedimiento de la reivindicación 1 que comprende además:
descifrar la información de configuración; y
almacenar la información de configuración en uno o más registros protegidos.

4. El procedimiento de la reivindicación 1 que comprende además verificar que la información de configuración es auténtica.

5. El procedimiento de la reivindicación 1, en el que la permutación (716, 720) utiliza una serie de uno o más multiplexores configurables al inicio y/o al final de la máquina de estados de hardware (716, 718, 720); y la reconfiguración de la permutación comprende reconfigurar el uno o más multiplexores incluidos en la permutación (716, 720) según una configuración definida por la información de configuración.

6. Un sistema para proporcionar acceso a un usuario a servicios digitales de difusión distribuidos entre una población de usuarios que usan respectivamente una población de módulos de acceso condicional, siendo cada módulo de acceso condicional para uso con un respectivo receptor/decodificador integrado de los servicios digitales de difusión, comprendiendo el sistema:

un módulo de acceso condicional (512) configurado para recibir y almacenar información de configuración, en el que la información de configuración ha sido transmitida de forma asíncrona durante un período de tiempo a la población de módulos de acceso condicional; en el que

el módulo de acceso condicional comprende un micro-procesador, una memoria no volátil y un bloque de lógica personalizada (610) que comprende una máquina de estados de hardware (718), incluyendo la máquina de estados de hardware una permutación que utiliza uno o más multiplexores configurables y un motor de descifrado; y

el bloque de lógica personalizada (610) está configurado para reconfigurar, tras un comando suministrado de forma síncrona a la población de módulos de acceso condicional, el uno o más multiplexores configurables de acuerdo con la información de configuración recibida, de modo que la máquina de estados de hardware soporta (*takes on*) un motor de descifrado basado en hardware diferente;

en el que la máquina de estados de hardware (718) comprende una lógica personalizada que es utilizada para controlar el acceso a los servicios digitales, en el que la máquina de estados de hardware (718) no es accesible directamente a un módulo de E/S del sistema (608) o bus del sistema (612) del módulo de acceso condicional; y

en el que el bloque de lógica personalizada (610) comprende además un módulo dedicado de reconfiguración del hardware y de E/S (714) que conecta la máquina de estados de hardware (716, 718, 720) al bus del sistema (612) del módulo de acceso condicional y controla el acceso a la lógica de la máquina de estados de hardware (718).

7. El sistema para proporcionar acceso a servicios digitales según la reivindicación 6, que comprende además:

un centro de control (102) configurado para coordinar y proporcionar servicios digitales;

un centro de enlace de subida (104) configurado para recibir los servicios digitales procedentes del centro de control (102) y transmitir los servicios digitales a un satélite (108);

el satélite (108) configurado para:
(i) recibir los servicios digitales procedentes del centro de enlace de subida (104);
(ii) procesar los servicios digitales; y
(iii) transmitir los servicios digitales y la información de configuración para acceder a los servicios digitales a una estación receptora de abonado (110);

la estación receptora de abonado (110) configurada para:
(i) recibir los servicios digitales y la información de configuración procedentes del satélite (108);
(ii) controlar el acceso a los servicios digitales a través de un receptor/decodificador integrado (126);

el módulo de acceso condicional (512) está acoplado comunicativamente al receptor/decodificador integrado (126).

8. El sistema de la reivindicación 6 ó 7, en el que la información de configuración está cifrada a través de un protocolo de intercambio de claves que comprende un algoritmo de clave pública.

9. El sistema de la reivindicación 6 ó 7, en el que el bloque de lógica personalizada (610) está configurado además para:
descifrar la información de configuración; y
almacenar la información de configuración en uno o más registros protegidos.

10. El sistema de la reivindicación 6 ó 7, en el que el bloque de lógica personalizada (610) está configurado además para verificar que la información de configuración es auténtica.

11. El sistema de la reivindicación 6 ó 7, en el que la permutación (716, 720) utiliza una serie de uno o más multiplexores configurables al inicio y/o al final de la máquina de estados de hardware (718), estando adaptada dicha permutación para ser reconfigurada reconfigurando el uno o más multiplexores incluidos en la permutación (716, 720) según la información de configuración.

12. El sistema de la reivindicación 6 ó 7, en el que el bloque de lógica personalizada (610) comprende un módulo dedicado de reconfiguración del hardware y de E/S (714) que conecta la máquina de estados de hardware (718) a un bus del sistema (612) del módulo de acceso condicional y controla el acceso a la lógica de la máquina de estados de hardware (718).

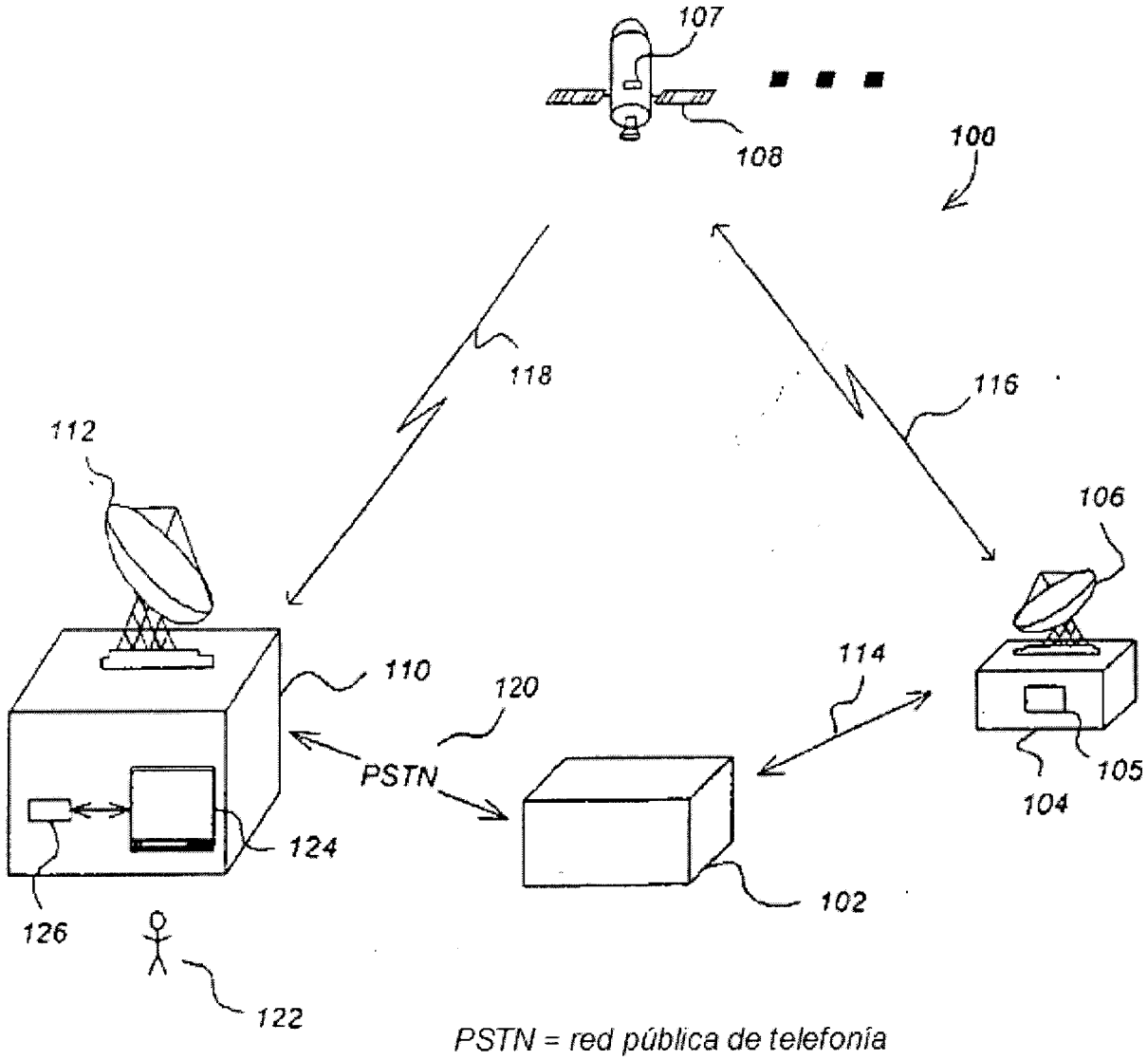

107
108
100
118
116
112
106
110
120
114
PSTN
124
105
104
126
102
122
PSTN = red pública de telefonía conmutada

FIG. 1

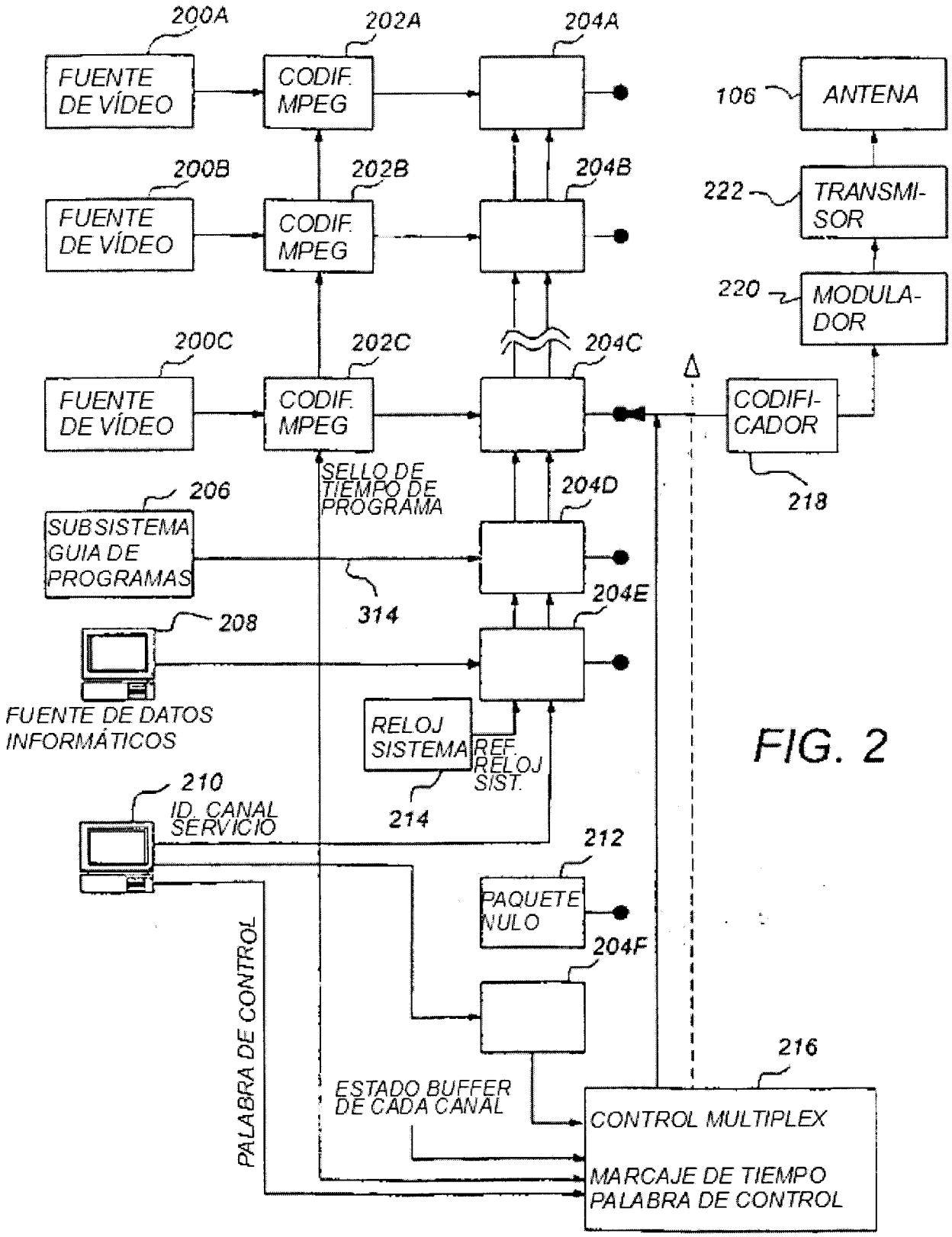

200A
FUENTE DE VÍDEO
202A
CODIF. MPEG
204A
106
ANTENA
200B
FUENTE DE VÍDEO
202B
CODIF. MPEG
204B
222
TRANSMI-SOR
220
MODULA-DOR
200C
FUENTE DE VÍDEO
202C
CODIF. MPEG
204C
CODIFI-CADOR
218
SELLO DE TIEMPO DE PROGRAMA
206
SUBSISTEMA GUIA DE PROGRAMAS
204D
314
204E
208
FUENTE DE DATOS INFORMÁTICOS
RELOJ SISTEMA
REF. RELOJ SIST.
214
210
ID. CANAL SERVICIO
212
PAQUETE NULO
204F
PALABRA DE CONTROL
ESTADO BUFFER DE CADA CANAL
216
CONTROL MULTIPLEX
MARCAJE DE TIEMPO
PALABRA DE CONTROL

FIG. 2

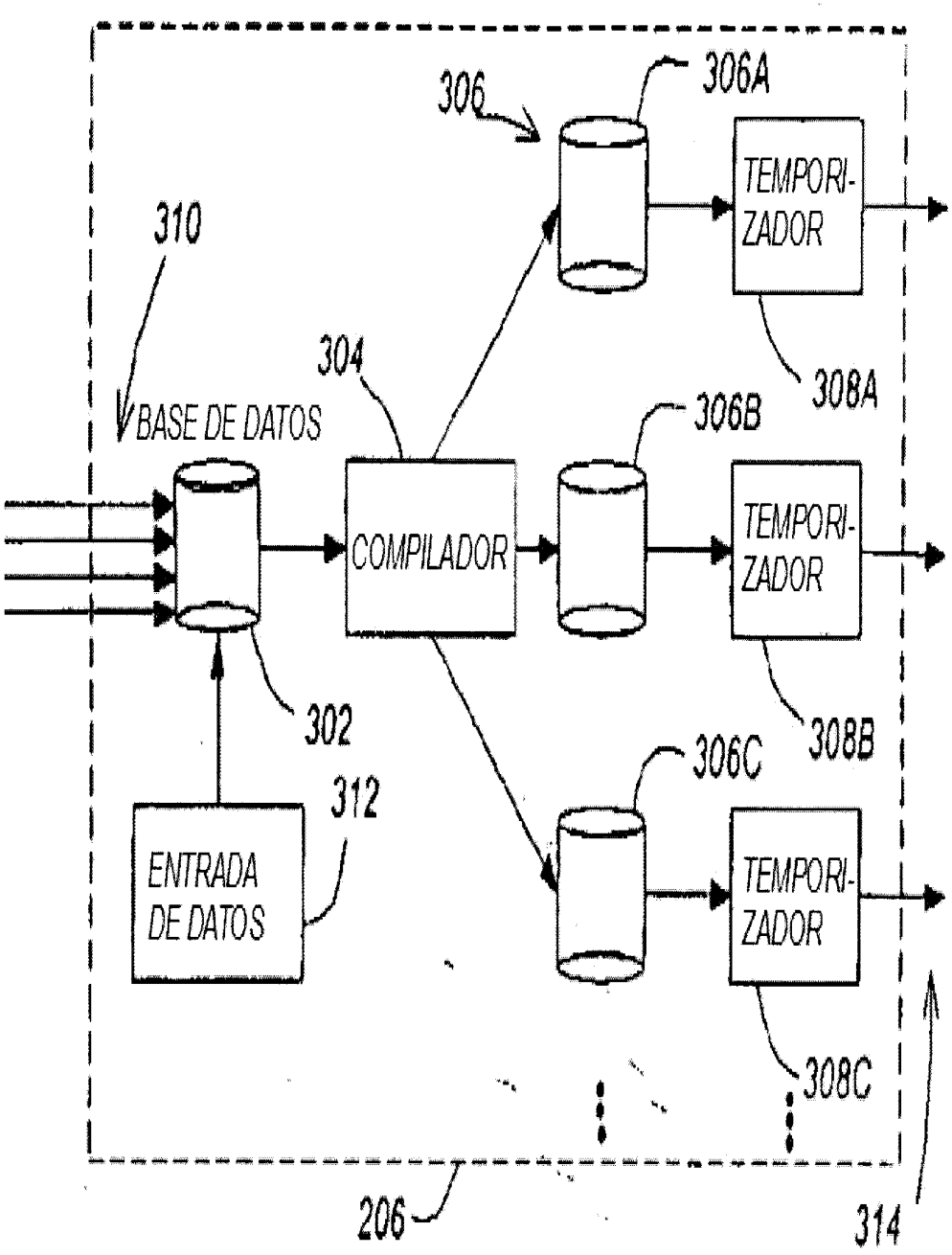

306
306A
TEMPORI-
ZADOR
310
304
308A
BASE DE DATOS
306B
COMPILADOR
TEMPORI-
ZADOR
302
308B
306C
312
ENTRADA
DE DATOS
TEMPORI-
ZADOR
308C
206
314

FIG. 3

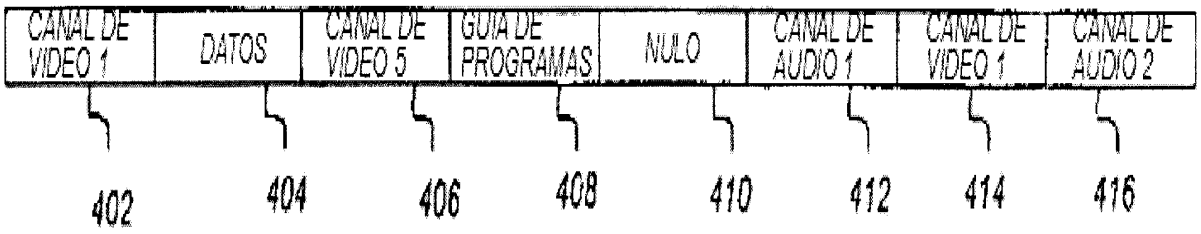

CANAL DE VIDEO 1
DATOS
CANAL DE VIDEO 5
GUÍA DE PROGRAMAS
NULO
CANAL DE AUDIO 1
CANAL DE VIDEO 1
CANAL DE AUDIO 2
402
404
406
408
410
412
414
416

FIG. 4A

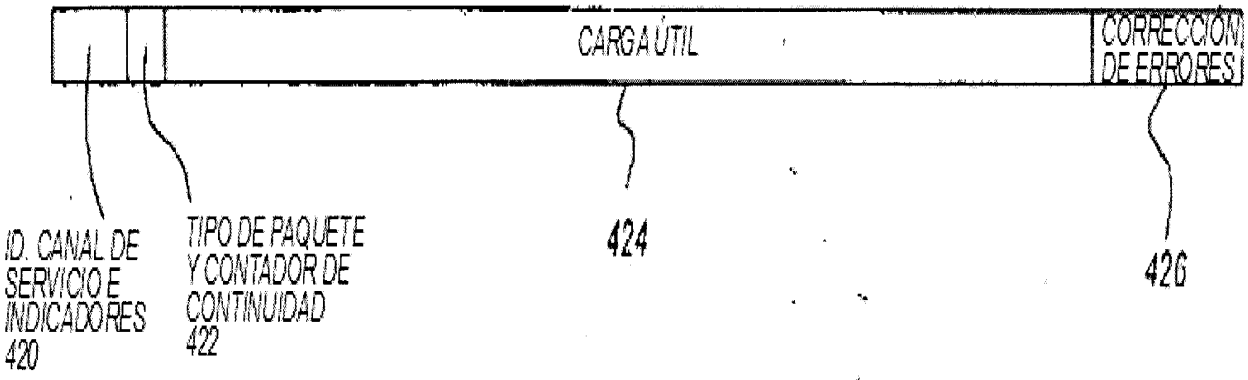

CARGA ÚTIL
CORRECCIÓN DE ERRORES
ID. CANAL DE SERVICIO E INDICADORES
420
TIPO DE PAQUETE Y CONTADOR DE CONTINUIDAD
422
424
426

FIG. 4B

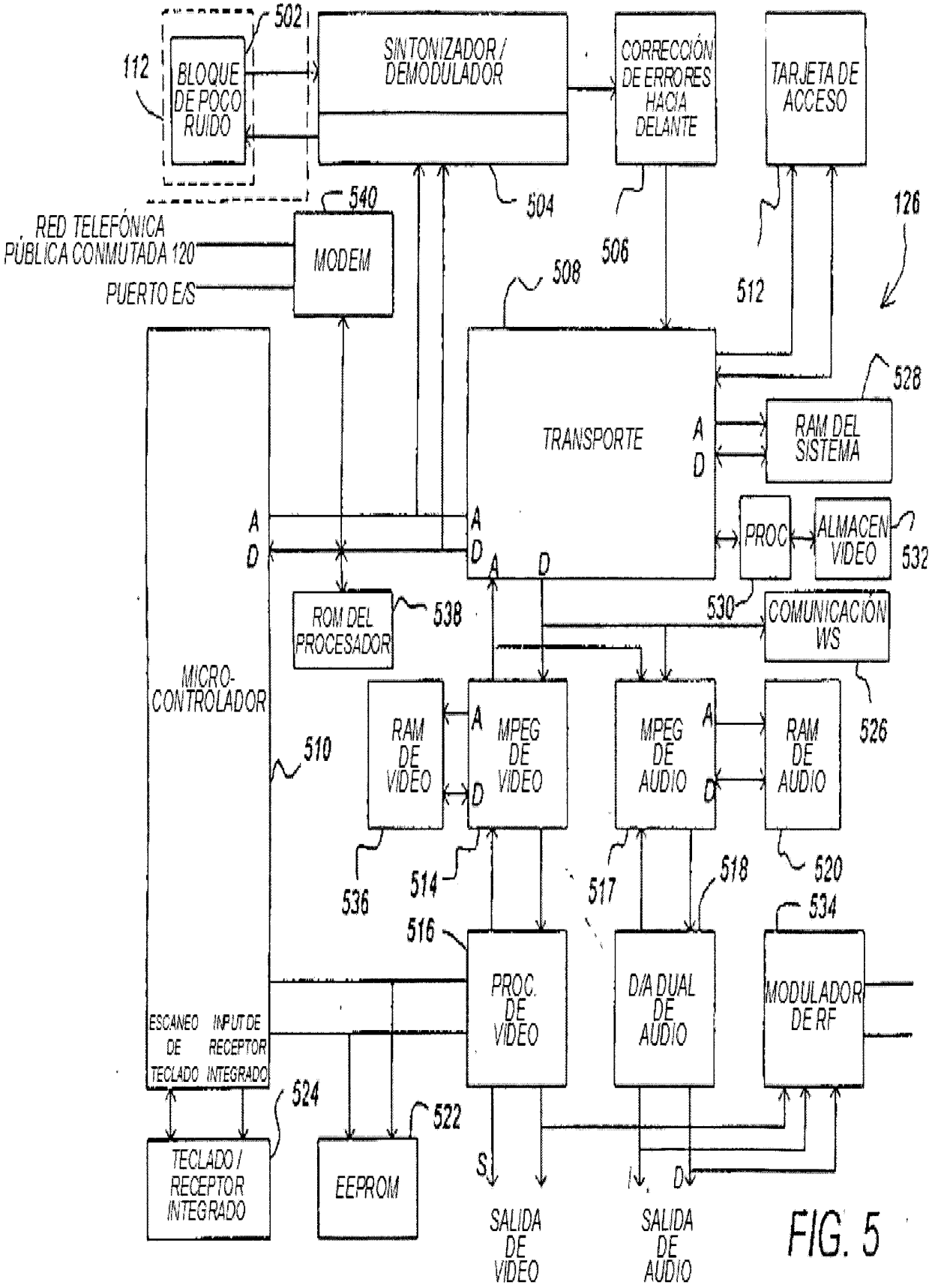

502
112
BLOQUE DE POCO RUIDO
SINTONIZADOR / DEMODULADOR
CORRECCIÓN DE ERRORES HACIA DELANTE
TARJETA DE ACCESO
504
506
512
126
540
RED TELEFÓNICA PÚBLICA CONMUTADA 120
PUERTO E/S
MODEM
508
528
TRANSPORTE
A
D
RAM DEL SISTEMA
PROC
ALMACEN VIDEO
532
530
ROM DEL PROCESADOR
538
COMUNICACIÓN WS
526
MICRO-CONTROLADOR
510
RAM DE VIDEO
MPEG DE VIDEO
MPEG DE AUDIO
RAM DE AUDIO
536
514
517
518
520
516
534
PROC. DE VIDEO
D/A DUAL DE AUDIO
MODULADOR DE RF
ESCANEO DE TECLADO
INPUT DE RECEPTOR INTEGRADO
524
522
TECLADO / RECEPTOR INTEGRADO
EEPROM
S
D
SALIDA DE VIDEO
SALIDA DE AUDIO

FIG. 5

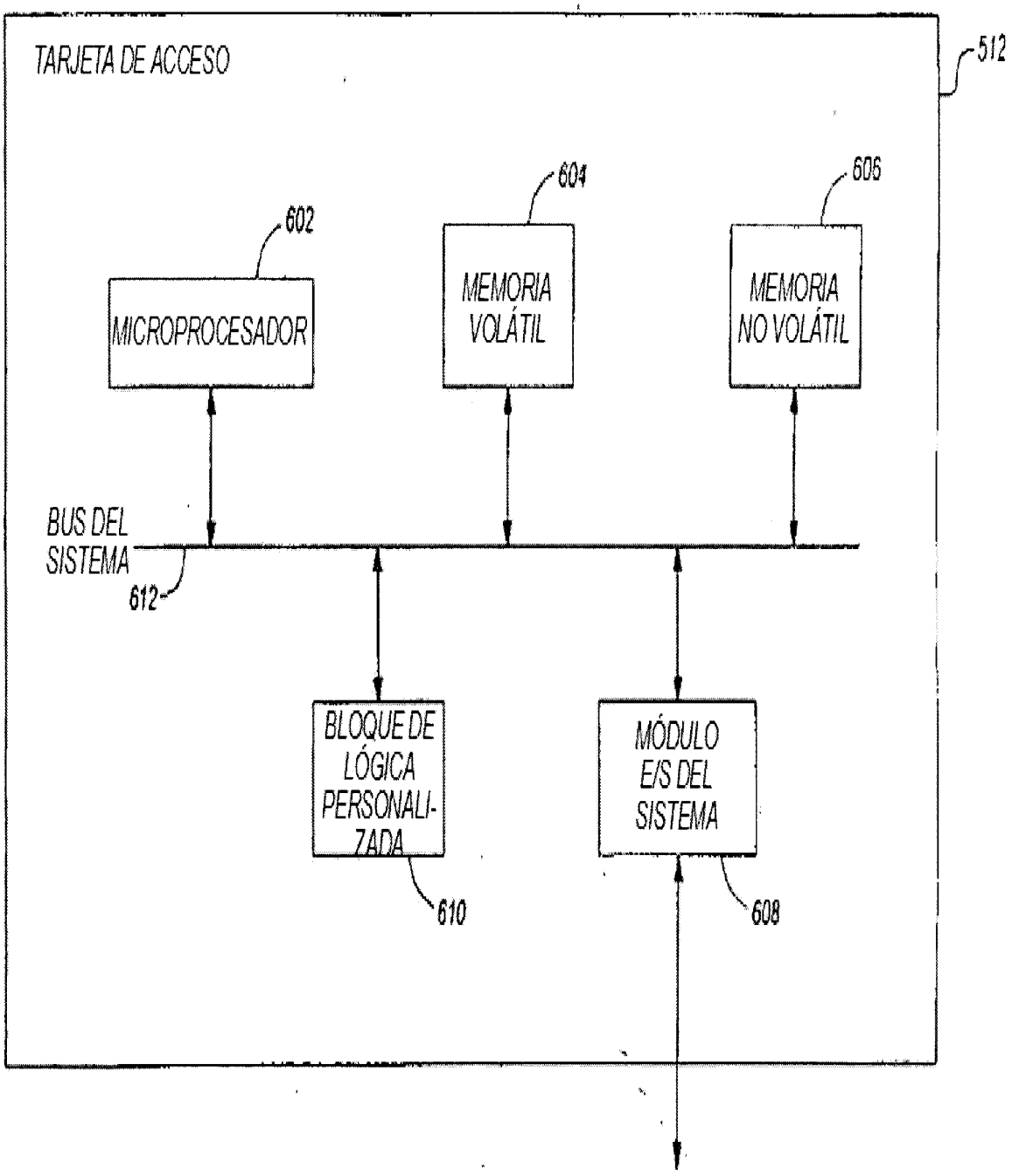

TARJETA DE ACCESO
512
602
MICROPROCESADOR
604
MEMORIA VOLÁTIL
606
MEMORIA NO VOLÁTIL
BUS DEL SISTEMA
612
BLOQUE DE LÓGICA PERSONALI-ZADA
610
MÓDULO E/S DEL SISTEMA
608

FIG. 6

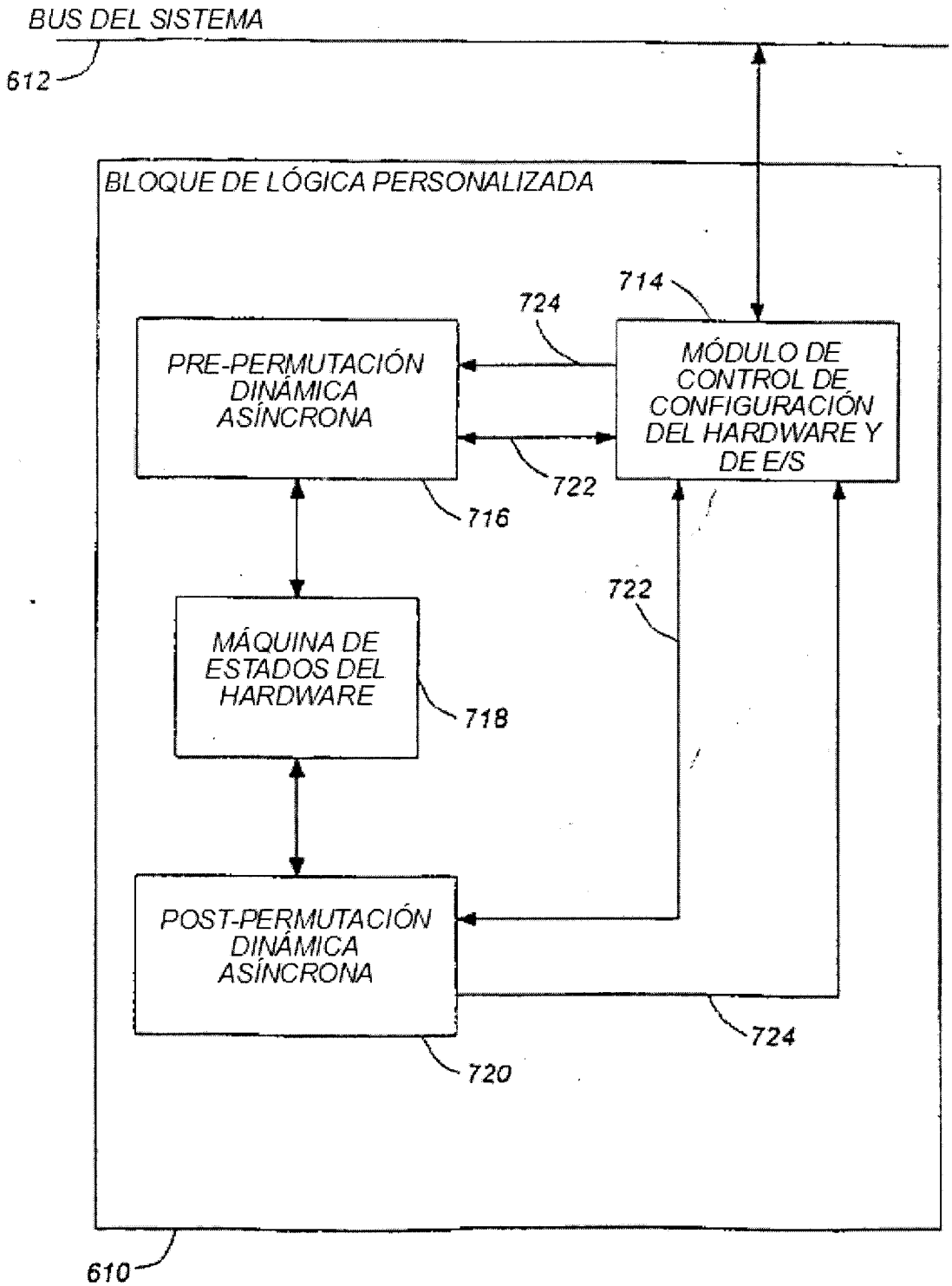
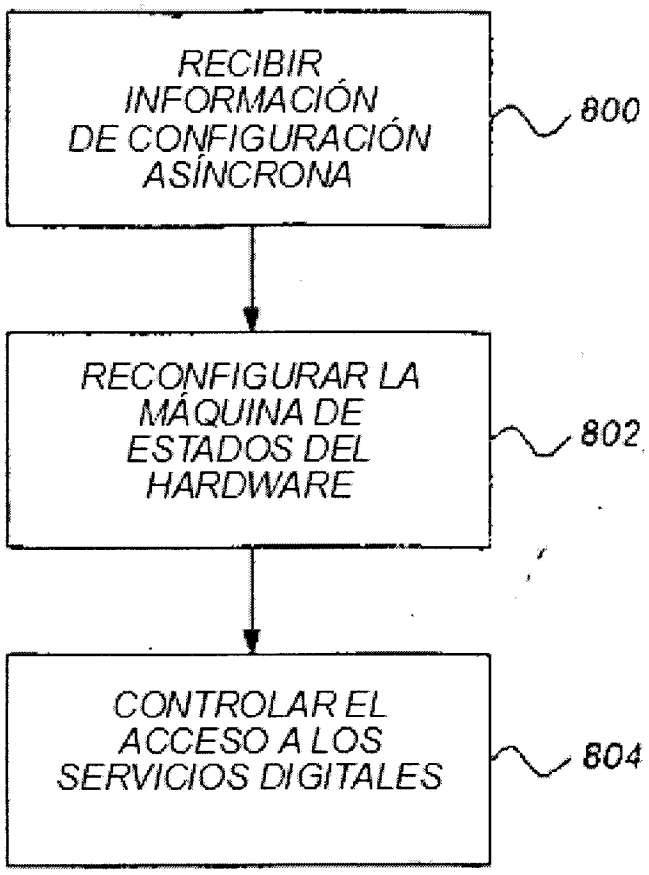

BUS DEL SISTEMA
612
BLOQUE DE LÓGICA PERSONALIZADA
714
724
PRE-PERMUTACIÓN DINÁMICA ASÍNCRONA
MÓDULO DE CONTROL DE CONFIGURACIÓN DEL HARDWARE Y DE E/S
722
716
722
MÁQUINA DE ESTADOS DEL HARDWARE
718
POST-PERMUTACIÓN DINÁMICA ASÍNCRONA
724
720
610

FIG. 7

FIG. 8


RECIBIR INFORMACIÓN DE CONFIGURACIÓN ASÍNCRONA
800
RECONFIGURAR LA MÁQUINA DE ESTADOS DEL HARDWARE
802
CONTROLAR EL ACCESO A LOS SERVICIOS DIGITALES
804