(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 775 923**

(51) Int. CI.:

G06F 21/60 (2013.01)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.03.2017 PCT/US2017/022309**

(87) Fecha y número de publicación internacional: **21.09.2017 WO17160843**

(96) Fecha de presentación y número de la solicitud europea: **14.03.2017 E 17714090 (2)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2019 EP 3412019**

(54) Título: **Anticlonación de cablemódem**

(30) Prioridad:

14.03.2016 US 201662307922 P
06.10.2016 US 201662404804 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2020

(73) Titular/es:

ARRIS ENTERPRISES LLC (100.0%)
3871 Lakefield Drive
Suwanee, GA 30024, US

(72) Inventor/es:

NEGAHDAR, ALI y
CARTER, WADE E.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Anticlonación de cablemódem

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

Esta solicitud es una solcitud no provisional que reivindica el beneficio de la Solicitud Provisional de los EE. UU. Nº 62/307,922, titulada «Mating Device Address with System-on-a-Chip», que se presentó el 14 de marzo de 2016, y además reivindica el beneficio de la Solicitud Provisional de los Estados Unidos. Nº 62/404,804, titulada «Cable Modem AntiCloning», que se presentó el 6 de octubre de 2016.

CAMPO TÉCNICO

Esta descripción se refiere a la prevención de la clonación de cablemódem.

ANTECEDENTES

La memoria descriptiva de la interfaz de servicio de datos por cable (DOCSIS) no aborda completamente la anticlonación del cablemódem. El estándar DOCSIS requiere que el nombre común del sujeto del certificado del dispositivo de cablemódem contenga la dirección de control de acceso a medios (MAC) del cablemódem. La autenticación de la interfaz de privacidad de la línea base plus (BPI+) falla si un sistema de terminación de cablemódem (CMTS) detecta que el nombre común en el certificado del dispositivo de cablemódem no coincide con la dirección MAC del cablemódem de dispositivo. DOCSIS recomienda que la política para CMTS aplique BPI+ en todos los cablemódems. Sin embargo, si un cablemódem está completamente clonado, es decir, clonada toda la memoria de acceso aleatorio no volátil (NVRAM) que contiene tanto el certificado del dispositivo como la dirección MAC del cablemódem, entonces la recomendación de DOCSIS contra la clonación no será suficiente. El número de clones reportados ha aumentado drásticamente y los proveedores de servicios de Internet (ISP) tienen dificultades para mantenerse al día y encargarse de los dispositivos clonados. Por lo tanto, existe la necesidad de mejorar los procedimientos y sistemas para prevenir la clonación de cablemódem.

El documento US 9081963 B1 se refiere a medidas de seguridad para prevenir el uso no autorizado de dispositivos de hardware. El documento US 7006446 B1 se refiere a la detección de participantes duplicados en un entorno de módem bidireccional.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIGURA 1 es un diagrama de bloques que ilustra un entorno de red de ejemplo que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC.

La FIGURA 2 es un diagrama de bloques que ilustra un cablemódem de ejemplo que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC.

La FIGURA 3 es un diagrama de bloques que ilustra un cablemódem de ejemplo que puede funcionar para facilitar el cifrado de un
identificador de dispositivo usando una clave de ofuscación generada a partir de una propiedad de identificación de un SoC.

La FIGURA 4 es un diagrama de flujo que ilustra un procedimiento de ejemplo que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC.

La FIGURA 5 es un diagrama de flujo que ilustra un procedimiento de ejemplo que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una clave de ofuscación generada a partir de una propiedad de identificación de un SoC.

La FIGURA 6 es un diagrama de bloques de una configuración de hardware que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC.

Los números de referencia y las designaciones similares en los diversos dibujos indican elementos similares.

DESCRIPCIÓN DETALLADA

Dado que el problema de la clonación de cablemódem no puede abordarse simplemente aplicando la política CMTS BPI+, debe existir algún grado de protección a nivel de dispositivo de cablemódem para evitar la clonación de direcciones MAC. En esta solicitud se describe un procedimiento y un sistema para emparejar la dirección MAC del cablemódem al sistema en un chip (SOC) en ese dispositivo de manera que la dirección MAC del cablemódem no se pueda clonar en ningún otro dispositivo. Además, los procedimientos y sistemas descritos en esta solicitud no requieren que la dirección MAC se fusione con el programable por única vez (OTP) del SOC. No todos los SOC admiten la personalización de datos OEM (fabricante de equipos originales) en el OTP. Además, la fusión de la dirección MAC en el OTP requiere la personalización del SOC y complica el procedimiento de fabricación y los procedimientos de devolución/reparación del dispositivo.

Los procedimientos, sistemas y medios legibles por computadora pueden funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. Un identificador único de un cablemódem puede cifrarse usando una clave única u otra propiedad única de un SoC asociado con el cablemódem. Cuando se inicia un procedimiento de autenticación en el cablemódem, el identificador único cifrado del cablemódem puede descifrarse usando la clave única u otra propiedad única del SoC, produciendo así el identificador único del

cablemódem. El identificador único descifrado del cablemódem puede enviarse desde el cablemódem a un controlador aguas arriba durante el procedimiento de autenticación. En realizaciones, se puede usar una clave de ofuscación para cifrar y descifrar el identificador único del cablemódem, y la clave de ofuscación se puede generar usando un identificador único del SoC.

La FIGURA 1 es un diagrama de bloques que ilustra un entorno de red 100 de ejemplo que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. En realizaciones, un cablemódem 105 puede recibir y/o entregar uno o más servicios (por ejemplo, video, datos, voz, seguridad y/u otros servicios) a un suscriptor. El cablemódem 105 puede ser un cablemódem independiente o puede estar integrado en un decodificador (STB), dispositivo de puerta de enlace multimedia, enrutador, extensor inalámbrico y/u otros dispositivos.

En realizaciones, el cablemódem 105 puede recibir uno o más servicios y puede transmitir y recibir otras comunicaciones hacia y desde uno o más componentes de la red aguas arriba a través de una red de acceso 110 y una red de área amplia (WAN) 115. La red de acceso 110 puede incluir cualquiera de una variedad de enlaces de comunicación entre el cablemódem 105 y una WAN 115, tal como una red coaxial de fibra híbrida (HFC) y otras.

En realizaciones, un cablemódem 105 puede comunicarse con un CMTS (sistema de terminación de cablemódem) 120 u otro dispositivo central ubicado aguas arriba del cablemódem 105. Por ejemplo, durante el tiempo de ejecución, el cablemódem 105 puede pasar por un procedimiento de autenticación con un CMTS 120 para verificar que se haya otorgado permiso al cablemódem 105 para proporcionar uno o más servicios a un suscriptor. Una vez que el procedimiento de autenticación se ha completado con éxito, el CMTS 120 puede entregar uno o más servicios al cablemódem 105 en función de una suscripción asociada con el cablemódem 105. El procedimiento de autenticación entre el cablemódem 105 y el CMTS 120 puede incluir una transmisión de un identificador único del cablemódem 105 al CMTS 120 y una verificación por parte del CMTS 120 de que el cablemódem 105, identificado por el identificador único, tiene permiso para proporcionar uno o más servicios a una premisa de suscriptor. Por ejemplo, el identificador único del cablemódem 105 puede ser una dirección MAC (control de acceso al medio) asociada con el cablemódem 105 u otro identificador asociado con el cablemódem 105. El procedimiento de autenticación entre el cablemódem 105 y el CMTS 120 puede ser un procedimiento de autenticación de interfaz de privacidad de la línea base plus (BPI+) en el que el cablemódem 105 llena una solicitud de autorización BPI+ con la dirección MAC del cablemódem 105 y transmite la solicitud de autorización BPI+ al CMTS 120. Debe entenderse que el procedimiento de autenticación puede incluir varios otros procedimientos.

En realizaciones, un identificador único de un cablemódem 105 (por ejemplo, la dirección MAC del cablemódem 105) se puede emparejar a un SoC del cablemódem 105 de modo que el SoC se vuelva necesario para el almacenamiento y la recuperación de la dirección MAC para fines de autenticar el cablemódem 105 con un CMTS 120. Sin acceso al SoC del cablemódem 105, un dispositivo que intente clonar el cablemódem 105 no puede entregar una dirección MAC válida al CMTS 120. Por ejemplo, la dirección MAC del cablemódem 105 puede cifrarse usando una o más propiedades exclusivas del SoC del cablemódem 105.

Una solución basada en hardware para emparejar una dirección MAC de un cablemódem 105 a un SoC del cablemódem 105 puede implementarse dentro del cablemódem 105. La solución basada en hardware se puede usar cuando el SoC del cablemódem 105 admite la raíz de confianza de hardware y la escalera de claves basada en hardware. En realizaciones, la dirección MAC del cablemódem 105 puede protegerse con una clave de dispositivo basada en hardware única asociada con el SoC del cablemódem 105. Por ejemplo, durante la fabricación del cablemódem 105, la dirección MAC del cablemódem 105 puede pasarse a un motor de seguridad del cablemódem 105 SoC para cifrarse y firmarse usando la clave de dispositivo basada en hardware asociada con el SoC. Por ejemplo, la clave de dispositivo basada en hardware asociada con el SoC puede usarse como clave de cifrado/descifrado para cifrar/descifrar la dirección MAC del cablemódem 105. El motor de seguridad puede generar una o más claves de cifrado/descifrado a partir de la clave de dispositivo basada en hardware asociada con el SoC. La clave de dispositivo basada en hardware asociada con el SoC puede protegerse en hardware y protegerse del acceso fuera del motor de seguridad. La salida del motor de seguridad es una dirección MAC cifrada que solo puede ser descifrada y autenticada por el mismo SoC que cifró/firmó la dirección MAC. La dirección MAC encriptada puede almacenarse en el cablemódem 105 (por ejemplo, en NVRAM (memoria de acceso aleatorio no volátil)). En tiempo de ejecución, el cablemódem 105 recupera la dirección MAC cifrada, descifra y valida la dirección MAC cifrada usando la clave de dispositivo basada en hardware asociada con el SoC y utiliza la dirección MAC validada en el procedimiento de autenticación BPI+. Si se clona un cablemódem 105, el clon no puede descifrar/verificar la dirección MAC cifrada, ya que el clon no tendría acceso a la clave de dispositivo basada en hardware asociada con el SoC que se utilizó para cifrar la dirección MAC. Por lo tanto, el clon no podría completar el mensaje de solicitud de autorización BPI+ con la dirección MAC adecuada.

En realizaciones, si el SoC de un cablemódem 105 no soporta una escalera de claves basada en hardware, se puede implementar una ofuscación basada en software. La solución basada en software proporciona un mecanismo para emparejar una dirección MAC de un cablemódem 105 a un SoC del cablemódem 105 al generar una clave de ofuscación que se basa en una o más propiedades únicas del SoC. La semilla (o parte de la semilla) para generar la clave de ofuscación puede ser un identificador único del SoC del cablemódem 105, y la semilla no se almacenaría en

la memoria no volátil del cablemódem 105. Durante la fabricación, la dirección MAC del cablemódem 105 se puede pasar a un motor de ofuscación del cablemódem 105. El motor de ofuscación puede obtener el identificador único del SoC a partir del SoC y puede usar el identificador único como parte de la semilla para generar la clave de ofuscación. Como el identificador único del SoC es único para cada SOC y cablemódem 105, la clave de ofuscación será única para ese cablemódem 105. El motor de ofuscación puede cifrar y firmar la dirección MAC del cablemódem 105 usando la clave de ofuscación. Por ejemplo, la clave de ofuscación puede usarse como clave de cifrado para cifrar la dirección MAC del cablemódem. La dirección MAC cifrada puede almacenarse en la NVRAM del cablemódem 105. En tiempo de ejecución, el cablemódem 105 puede recuperar la dirección MAC cifrada y descifrar y validar la dirección MAC usando un motor de desofuscación. El motor de desofuscación puede usar el identificador único del SoC para generar una clave de desofuscación. Por ejemplo, la clave de desofuscación puede usarse como clave de descifrado para descifrar la dirección MAC cifrada. El cablemódem 105 puede usar la dirección MAC validada en el procedimiento de autenticación BPI+. Sin acceso al identificador único del SoC y la clave de desofuscación, una solicitud de autorización BPI+ fallará en un clon, ya que el clon no tendría acceso a la ID de SOC que se usó para crear la clave de ofuscación. En cambio, el clon usaría un identificador único de un SoC asociado con el clon como la entrada al motor de desofuscación para descifrar/verificar la dirección MAC segura, produciendo así una dirección MAC no válida.

La FIGURA 2 es un diagrama de bloques que ilustra un ejemplo de cablemódem 105 que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. En realizaciones, el cablemódem 105 puede incluir un SoC (sistema en un chip) 205, un almacén de datos de identificador seguro 210 y un módulo de autorización 215. El SoC 205 puede incluir un motor de seguridad 220.

En realizaciones, el motor de seguridad 220 del SoC 205 puede recuperar la dirección MAC del cablemódem 105. El motor de seguridad 220 puede recuperar una clave de dispositivo basada en hardware asociada con el SoC 205, y el motor de seguridad 220 puede cifrar y firmar la dirección MAC recuperada usando la clave de dispositivo basada en hardware asociada con el SoC 205. Por ejemplo, el motor de seguridad 220 puede usar la clave de dispositivo asociada con el SoC 205 como clave de cifrado para cifrar la dirección MAC del cablemódem 105. El motor de seguridad 220 puede enviar la dirección MAC cifrada al almacén de datos de identificador seguro 210. En realizaciones, el almacén de datos de identificador seguro 210 puede incluir NVRAM.

En tiempo de ejecución, el motor de seguridad 220 puede recuperar la dirección MAC cifrada del almacén de datos de identificador seguro 210. En realizaciones, el motor de seguridad 220 puede descifrar y validar la dirección MAC cifrada usando la clave de dispositivo basada en hardware asociada con el SoC 205. Por ejemplo, el motor de seguridad 220 puede usar la clave del dispositivo como clave de descifrado para descifrar la dirección MAC cifrada del cablemódem 105. Después del descifrado y la validación de la dirección MAC encriptada, el motor de seguridad 220 puede pasar la dirección MAC validada al módulo de autorización 215, y el módulo de autorización 215 puede enviar la dirección MAC a un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1) como parte de un procedimiento de autenticación entre el cablemódem 105 y el controlador aguas arriba. Por ejemplo, el módulo de autorización 215 puede llenar un mensaje de solicitud de autorización BPI+ con la dirección MAC y puede enviar el mensaje de solicitud de autorización BPI+ a un CMTS 120.

La FIGURA 3 es un diagrama de bloques que ilustra un ejemplo de cablemódem 105 que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una clave de ofuscación generada a partir de una propiedad de identificación de un SoC. En realizaciones, el cablemódem 105 puede incluir un SoC (sistema en un chip) 305, un almacén de datos de identificación segura 310, un motor de ofuscación 315, un motor de desofuscación 320 y un módulo de autorización 325.

En realizaciones, el motor de ofuscación 315 puede generar una clave de ofuscación que se basa en una o más propiedades únicas del SoC 305. La semilla (o parte de la semilla) para generar la clave de ofuscación puede ser un identificador único del SoC 305. Por ejemplo, el motor de ofuscación 315 puede obtener el identificador único del SoC 305 a partir del SoC 305 y puede usar el identificador único como parte de la semilla para generar la clave de ofuscación. La dirección MAC del cablemódem 105 puede ser recuperada por el motor de ofuscación 315, y el motor de ofuscación 315 puede cifrar y firmar la dirección MAC del cablemódem 105 usando la clave de ofuscación. Por ejemplo, el motor de ofuscación 315 puede usar la clave de ofuscación como clave de encriptación para cifrar la dirección MAC del cablemódem 105. La dirección MAC cifrada puede almacenarse en la NVRAM del cablemódem 105 (por ejemplo, en el almacén de datos de identificación segura 310).

En el tiempo de ejecución, el motor de desofuscación 320 puede recuperar la dirección MAC cifrada del almacén de datos de identificador seguro 310, y el motor de desofuscación 320 puede descifrar y validar la dirección MAC usando una clave de desofuscación. La clave de desofuscación puede ser una clave generada por el motor de desofuscación a partir del identificador único del SoC 305. El motor de desofuscación 320 puede usar la clave de desofuscación como clave de descifrado para descifrar la dirección MAC cifrada del cablemódem 105. El cablemódem 105 puede usar la dirección MAC validada en el procedimiento de autenticación BPI+. Después del descifrado y la validación de la dirección MAC encriptada, el motor de desofuscación 320 puede pasar la dirección MAC validada al módulo de autorización 325, y el módulo de autorización 325 puede enviar la dirección MAC a un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1) como parte de un procedimiento de autenticación entre el cablemódem 105 y el controlador aguas arriba. Por ejemplo, el módulo de autorización 325 puede llenar un mensaje de solicitud de

autorización BPI+ con la dirección MAC y puede enviar el mensaje de solicitud de autorización BPI+ a un CMTS 120.

La FIGURA 4 es un diagrama de flujo que ilustra un procedimiento de ejemplo 400 que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. El procedimiento 400 puede comenzar en 405 donde se recibe un identificador único de un cablemódem en un SoC (por ejemplo, SoC 205 de la FIGURA 2) asociado con el cablemódem. Por ejemplo, el identificador único del cablemódem (por ejemplo, cablemódem 105 de la FIGURA 1) puede ser recibido por un motor de seguridad (por ejemplo, el motor de seguridad 220 de la FIGURA 2) del SoC (por ejemplo, SoC 205 de la FIGURA 2) asociado con el cablemódem 105. En realizaciones, el identificador único del cablemódem 105 puede ser una dirección MAC asociada con el cablemódem 105.

En 410, se puede usar una clave única del SoC para cifrar el identificador único del cablemódem, creando así un identificador único cifrado asociado con el cablemódem. El identificador único del cablemódem puede estar cifrado, por ejemplo, por el motor de seguridad (por ejemplo, el motor de seguridad 220) del SoC asociado con el cablemódem 105. En realizaciones, el motor de seguridad 220 puede recuperar el identificador único (por ejemplo, dirección MAC) del cablemódem 105 y la clave única del SoC (por ejemplo, clave de dispositivo basada en hardware asociada con el SoC 205). El motor de seguridad 220 puede cifrar y firmar el identificador único recuperado usando la clave de dispositivo basada en hardware asociada con el SoC 205. Por ejemplo, el motor de seguridad 220 puede usar la clave de dispositivo basada en hardware como clave de cifrado para cifrar el identificador único del cablemódem 105.

En 415, se puede almacenar el identificador único cifrado del cablemódem. El identificador único cifrado del cablemódem puede almacenarse, por ejemplo, en un almacenamiento asociado con el cablemódem (por ejemplo, en el almacén de datos de identificador seguro 210 de la FIGURA 2). En realizaciones, el identificador único cifrado del cablemódem puede almacenarse dentro de la NVRAM del cablemódem 105.

En 420, se puede iniciar un procedimiento de autenticación por cablemódem. Por ejemplo, el procedimiento de autenticación por cablemódem puede ser un procedimiento para autenticar el cablemódem con un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1). El procedimiento de autenticación puede ser un procedimiento de autenticación BPI+ u otro procedimiento para autenticar un cablemódem en un controlador aguas arriba. En realizaciones, el procedimiento de autenticación puede iniciarse cuando el cablemódem solicita uno o más servicios o permiso para acceder al controlador aguas arriba.

En 425, se puede recuperar el identificador único cifrado del cablemódem. El identificador único cifrado puede ser recuperado, por ejemplo, por el motor de seguridad del cablemódem SoC (por ejemplo, el motor de seguridad 220). En realizaciones, el motor de seguridad 220 puede recuperar el identificador único cifrado (por ejemplo, dirección MAC encriptada) del almacenamiento en el cablemódem (por ejemplo, del almacén de datos del identificador seguro 210).

En 430, el identificador único cifrado del cablemódem puede descifrarse usando la clave única del SoC, produciendo así el identificador único del cablemódem. El identificador único cifrado puede ser descifrado, por ejemplo, por el motor de seguridad (por ejemplo, el motor de seguridad 220 de la FIGURA 2) del SoC asociado con el cablemódem. En realizaciones, el motor de seguridad 220 puede descifrar y validar el identificador único cifrado (por ejemplo, dirección MAC) usando la clave de dispositivo basada en hardware asociada con el SoC 205 para producir el identificador único asociado con el cablemódem. Por ejemplo, el motor de seguridad 220 puede usar la clave de dispositivo basada en hardware como clave de descifrado para descifrar el identificador único cifrado del cablemódem 105.

En 435, se puede completar un mensaje de solicitud de autorización con el identificador único del cablemódem. El mensaje de solicitud de autorización puede rellenarse con el identificador único del cablemódem, por ejemplo, mediante un módulo de autorización (por ejemplo, el módulo de autorización 215 de la FIGURA 2) del cablemódem. En realizaciones, el mensaje de solicitud de autorización puede ser un mensaje de solicitud de autorización BPI+. El mensaje de solicitud de autorización puede enviarse desde el cablemódem a un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1) en 440.

La FIGURA 5 es un diagrama de flujo que ilustra un procedimiento de ejemplo 500 que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una clave de ofuscación generada a partir de una propiedad de identificación de un SoC. El procedimiento 500 puede comenzar en 505 donde se recibe un identificador único de un cablemódem en un SoC (por ejemplo, SoC 305 de la FIGURA 3) asociado con el cablemódem. Por ejemplo, el identificador único del cablemódem (por ejemplo, cablemódem 105 de la FIGURA 1) puede ser recibido por un motor de ofuscación (por ejemplo, el motor de ofuscación 315 de la FIGURA 3). En realizaciones, el identificador único del cablemódem 105 puede ser una dirección MAC asociada con el cablemódem 105.

En 510, se puede recuperar un identificador único de un SoC asociado con el cablemódem. El identificador único del SoC puede ser recuperado, por ejemplo, por un motor de ofuscación (por ejemplo, el motor de ofuscación 315 de la FIGURA 3). En realizaciones, el motor de ofuscación 315 puede recuperar el identificador único del SoC a partir del SoC del cablemódem 105 (por ejemplo, del SoC 305 de la FIGURA 3). El identificador único del SoC puede ser un identificador u otra propiedad única del SoC 305.

En 515, el identificador único del SoC puede usarse para generar una clave de ofuscación. La clave de ofuscación puede ser generada, por ejemplo, por un motor de ofuscación (por ejemplo, el motor de ofuscación 315 de la FIGURA 3). En realizaciones, el motor de ofuscación 315 puede generar una clave de ofuscación que se basa en el identificador único del SoC 305. Una semilla (o parte de una semilla) para generar la clave de ofuscación puede ser el identificador único recuperado del SoC 305.

En 520, la clave de ofuscación puede usarse para cifrar el identificador único del cablemódem, creando así un identificador único cifrado asociado con el cablemódem. El identificador único del cablemódem puede cifrarse, por ejemplo, por el motor de ofuscación (por ejemplo, el motor de ofuscación 315). En realizaciones, el motor de ofuscación 315 puede cifrar y firmar el identificador único (por ejemplo, dirección MAC) del cablemódem 105 usando la clave de ofuscación. Por ejemplo, el motor de ofuscación 315 puede usar la clave de ofuscación como clave de cifrado para cifrar el identificador único asociado con el cablemódem 105.

En 525, se puede almacenar el identificador único cifrado del cablemódem. El identificador único cifrado del cablemódem puede almacenarse, por ejemplo, en un almacenamiento asociado con el cablemódem (por ejemplo, en el almacén de datos de identificador seguro 310 de la FIGURA 3). En realizaciones, el identificador único cifrado del cablemódem puede almacenarse dentro de la NVRAM del cablemódem 105.

En 530, se puede iniciar un procedimiento de autenticación por cablemódem. Por ejemplo, el procedimiento de autenticación por cablemódem puede ser un procedimiento para autenticar el cablemódem con un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1). El procedimiento de autenticación puede ser un procedimiento de autenticación BPI+ u otro procedimiento para autenticar un cablemódem en un controlador aguas arriba. En realizaciones, el procedimiento de autenticación puede iniciarse cuando el cablemódem solicita uno o más servicios o permiso para acceder al controlador aguas arriba.

En 535, se puede recuperar el identificador único cifrado del cablemódem. El identificador único cifrado puede ser recuperado, por ejemplo, por un motor de desofuscación del cablemódem 105 (por ejemplo, el motor de desofuscación 320 de la FIGURA 3). En realizaciones, el motor de desofuscación 320 puede recuperar el identificador único cifrado (por ejemplo, dirección MAC encriptada) del almacenamiento en el cablemódem 105 (por ejemplo, del almacén de datos de identificación segura 310).

En 540, el identificador único cifrado del cablemódem se puede descifrar usando una clave de desofuscación, produciendo así el identificador único del cablemódem. El identificador único cifrado puede ser descifrado, por ejemplo, por el motor de desofuscación (por ejemplo, el motor de desofuscación 320 de la FIGURA 3). En realizaciones, el motor de desofuscación 320 puede descifrar y validar el identificador único (por ejemplo, la dirección MAC) del cablemódem 105 usando una clave de desofuscación para producir el identificador único asociado con el cablemódem 105. La clave de desofuscación puede ser una clave generada por el motor de desofuscación 320 a partir del identificador único del SoC 305 (por ejemplo, el identificador único del SoC recuperado en 510). El motor de desofuscación 320 puede usar la clave de desofuscación como clave de descifrado para descifrar el identificador único cifrado asociado con el cablemódem 105.

En 545, se puede completar un mensaje de solicitud de autorización con el identificador único del cablemódem. El mensaje de solicitud de autorización puede rellenarse con el identificador único del cablemódem, por ejemplo, mediante un módulo de autorización (por ejemplo, el módulo de autorización 325 de la FIGURA 3) del cablemódem 105. En realizaciones, el mensaje de solicitud de autorización puede ser un mensaje de solicitud de autorización BPI+. El mensaje de solicitud de autorización puede enviarse desde el cablemódem a un controlador aguas arriba (por ejemplo, CMTS 120 de la FIGURA 1) en 550.

La FIGURA 6 es un diagrama de bloques de una configuración de hardware 600 que puede funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. La configuración de hardware 600 puede incluir un procesador 610, una memoria 620, un dispositivo de almacenamiento 630 y un dispositivo de entrada/salida 640. Cada uno de los componentes 610, 620, 630 y 640 puede, por ejemplo, interconectarse usando un bus de sistema 650. El procesador 610 puede ser capaz de procesar instrucciones para su ejecución dentro de la configuración de hardware 600. En una implementación, el procesador 610 puede ser un procesador de subproceso único. En otra implementación, el procesador 610 puede ser un procesador multiproceso. El procesador 610 puede ser capaz de procesar instrucciones almacenadas en la memoria 620 o en el dispositivo de almacenamiento 630.

La memoria 620 puede almacenar información dentro de la configuración de hardware 600. En una implementación, la memoria 620 puede ser un medio legible por computadora. En una implementación, la memoria 620 puede ser una unidad de memoria volátil. En otra implementación, la memoria 620 puede ser una unidad de memoria no volátil.

En algunas implementaciones, el dispositivo de almacenamiento 630 puede ser capaz de proporcionar almacenamiento masivo para la configuración de hardware 600. En una implementación, el dispositivo de almacenamiento 630 puede ser un medio legible por computadora. En diversas implementaciones diferentes, el dispositivo de almacenamiento 630 puede, por ejemplo, incluir un dispositivo de disco duro, un dispositivo de disco

óptico, memoria flash o algún otro dispositivo de almacenamiento de gran capacidad. En otras implementaciones, el dispositivo de almacenamiento 630 puede ser un dispositivo externo a la configuración de hardware 600.

El dispositivo de entrada/salida 640 proporciona operaciones de entrada/salida para la configuración de hardware 600. En realizaciones, el dispositivo de entrada/salida 640 puede incluir uno o más de un dispositivo de interfaz de red (por ejemplo, una tarjeta Ethernet), un dispositivo de comunicación en serie (por ejemplo, un puerto RS-232), una o más interfaces de bus serie universal (USB) (por ejemplo, un puerto USB 2.0), uno o más dispositivos de interfaz inalámbricos (por ejemplo, una tarjeta 802.11), y/o una o más interfaces para enviar video, voz, datos y/u otros servicios a un dispositivo (por ejemplo, cablemódem 105 de la FIGURA 1, dispositivo del equipo del establecimiento del cliente (CPE), dispositivo del cliente, etc.). En realizaciones, el dispositivo de entrada/salida puede incluir dispositivos de controlador configurados para enviar comunicaciones y recibir comunicaciones de una o más redes (por ejemplo, la red de acceso 110 de la FIGURA 1, WAN 115 de la FIGURA 1, etc.).

Los expertos en la técnica apreciarán que la invención mejora los procedimientos y sistemas para prevenir la clonación de cablemódem. Los procedimientos, sistemas y medios legibles por computadora pueden funcionar para facilitar el cifrado de un identificador de dispositivo usando una propiedad de identificación de un SoC. Un identificador único de un cablemódem puede cifrarse usando una clave única u otra propiedad única de un SoC asociado con el cablemódem. Cuando se inicia un procedimiento de autenticación en el cablemódem, el identificador único cifrado del cablemódem puede descifrarse utilizando la clave única u otra propiedad única del SoC, produciendo así el identificador único del cablemódem. El identificador único descifrado del cablemódem puede enviarse desde el cablemódem a un controlador aguas arriba durante el procedimiento de autenticación. En realizaciones, se puede usar una clave de ofuscación para cifrar y descifrar el identificador único del cablemódem, y la clave de ofuscación se puede generar usando un identificador único del SoC.

La materia objeto de esta descripción, y sus componentes, se puede realizar mediante instrucciones que, al ejecutarse, hacen que uno o más dispositivos de procesamiento lleven a cabo los procedimientos y funciones descritos anteriormente. Dichas instrucciones pueden, por ejemplo, comprender instrucciones interpretadas, como instrucciones de script, por ejemplo, instrucciones JavaScript o ECMAScript, o código ejecutable, u otras instrucciones almacenadas en un medio legible por computadora.

Las implementaciones de la materia y las operaciones funcionales descritas en esta memoria descriptiva se pueden proporcionar en circuitos electrónicos digitales, o en software, firmware o hardware de computadora, incluidas las estructuras divulgadas en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de uno o más de ellos. Las realizaciones de la materia descrita en esta memoria descriptiva pueden implementarse como uno o más productos de programas de computadora, es decir, uno o más módulos de instrucciones de programas de computadora codificados en un soporte de programa tangible para ejecución o para controlar la operación de un aparato de procesamiento de datos.

Un programa de computadora (también conocido como programa, software, aplicación de software, script o código) se puede escribir en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, o los lenguajes declarativos o de procedimiento, y se puede implementar en cualquier forma, incluso como un programa independiente o como un módulo, componente, subrutina u otra unidad adecuada para su uso en un entorno informático. Un programa de computadora no necesariamente corresponde a un archivo en un sistema de archivos. Un programa puede almacenarse en una parte de un archivo que contiene otros programas o datos (por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcado), en un único archivo dedicado al programa en cuestión o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o partes de código). Un programa de computadora puede implementarse para ejecutarse en una computadora o en varias computadoras que están ubicadas en un sitio o distribuidas en múltiples sitios e interconectadas por una red de comunicación.

Los procedimientos y flujos lógicos descritos en esta memoria descriptiva son realizados por uno o más procesadores programables que ejecutan uno o más programas de computadora para realizar funciones operando con datos de entrada y generando salida, vinculando el procedimiento a una máquina en particular (por ejemplo, una máquina programada para realizar los procedimientos descritos en esta invención). Los procedimientos y los flujos lógicos también pueden realizarse y el aparato también puede implementarse como un circuito lógico de propósito especial, por ejemplo, un FPGA (matriz de compuerta programable en campo) o un ASIC (circuito integrado específico de la aplicación).

Los medios legibles por computadora adecuados para almacenar instrucciones y datos de programas de computadora incluyen todas las formas de memoria no volátil, medios y dispositivos de memoria, incluidos, por ejemplo, dispositivos de memoria semiconductores (por ejemplo, EPROM, EEPROM y dispositivos de memoria flash); discos magnéticos (p. ej., discos duros internos o discos extraíbles); discos magnetoópticos; y discos CD ROM y DVD ROM. El procesador y la memoria pueden complementarse o incorporarse en circuitos lógicos de propósito especial.

Si bien esta memoria descriptiva contiene muchos detalles de implementación específicos, estos no deben interpretarse como limitaciones en el alcance de ninguna invención o de lo que puede reivindicarse, sino más bien

como descripciones de características que pueden ser específicas para realizaciones particulares de invenciones particulares. Ciertas características que se describen en esta memoria descriptiva en el contexto de realizaciones separadas también se pueden implementar en combinación en una sola realización. Por el contrario, varias características que se describen en el contexto de una sola realización también pueden implementarse en múltiples realizaciones por separado o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como que actúan en ciertas combinaciones e incluso reivindicarse inicialmente como tales, una o más características de una combinación reivindicada pueden en algunos casos eliminarse de la combinación, y la combinación reivindicada puede dirigirse a una subcombinación o variación de una subcombinación.

De manera similar, aunque las operaciones se representan en los dibujos en un orden particular, esto no debe entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que todas las operaciones ilustradas se realicen, para lograr resultados deseables. En ciertas circunstancias, la multitarea y el procesamiento paralelo pueden ser ventajosos. Además, la separación de varios componentes del sistema en las realizaciones descritas anteriormente no debe entenderse que requiere tal separación en todas las realizaciones, y debe entenderse que los componentes y sistemas del programa descritos en general pueden integrarse juntos en un solo producto de software o empaquetarse en múltiples productos de software.

Se han descrito realizaciones particulares del tema descrito en esta memoria descriptiva. Otras realizaciones están dentro del alcance de las siguientes reivindicaciones. Por ejemplo, las acciones enumeradas en las reivindicaciones se pueden realizar en un orden diferente y aún lograr resultados deseables, a menos que se indique expresamente lo contrario. Como un ejemplo, los procedimientos representados en las figuras adjuntas no requieren necesariamente el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. En algunas implementaciones, el procesamiento multitarea y paralelo puede ser ventajoso.

REIVINDICACIONES

1. Un procedimiento que comprende:

recuperar un identificador único asociado con un cablemódem (105);
recuperar una clave única asociada con un sistema en un chip (205; 305) asociado con el cablemódem;
usar la clave única como clave de cifrado para cifrar el identificador único asociado con el cablemódem, produciendo así un identificador único cifrado;
usando la clave única como clave de descifrado para descifrar el identificador único cifrado, por lo tanto producir el identificador único asociado con el cablemódem; y
enviar el identificador único asociado con el cablemódem a un controlador aguas arriba, en el que el identificador único asociado con el cablemódem se emite como un mensaje de solicitud de autorización.

2. El procedimiento de la reivindicación 1, en el que la clave única asociada con el sistema en un chip (205; 305) comprende una clave de dispositivo basada en hardware asociada con el sistema en un chip.

3. El procedimiento de la reivindicación 1, en el que recuperar la clave única asociada con el sistema en un chip (205; 305) comprende:

recuperar un identificador único asociado con el sistema en un chip; y
usar el identificador único asociado con el sistema en un chip como semilla para generar la clave única asociada con el sistema en un chip.

4. El procedimiento de la reivindicación 1, que comprende además: almacenar el identificador único cifrado dentro de la memoria de acceso aleatorio no volátil del cablemódem (105).

5. El procedimiento de la reivindicación 1, en el que el identificador único asociado con el cablemódem (105) comprende

una dirección de control de acceso a medios asociada con el cablemódem.

6. El procedimiento de la reivindicación 1, en el que el controlador aguas arriba comprende un sistema de terminación de cablemódem (120).

7. El procedimiento de la reivindicación 1, en el que el mensaje de solicitud de autorización comprende un mensaje de solicitud de autorización de interfaz de privacidad de la línea base plus.

8. Un cablemódem (105) que comprende uno o más módulos configurados para:

recuperar un identificador único asociado con el cablemódem;
recuperar una clave única asociada con un sistema en un chip (205; 305) asociado con el cablemódem;
usar la clave única como clave de cifrado para cifrar el identificador único asociado con el cablemódem, produciendo así un identificador único cifrado;
usar la clave única como clave de descifrado para descifrar el identificador único cifrado, produciendo así el identificador único asociado con el cablemódem; y
enviar el identificador único asociado con el cablemódem a un controlador aguas arriba, en el que el identificador único asociado con el cablemódem se emite como un mensaje de solicitud de autorización.

9. El cablemódem (105) de la reivindicación 8, en el que recuperar la clave única asociada con el sistema en un chip (205; 305) comprende:

recuperar un identificador único asociado con el sistema en un chip; y
usar el identificador único asociado con el sistema en un chip como semilla para generar la clave única asociada con el sistema en un chip.

10. El cablemódem (105) de la reivindicación 8, en el que el mensaje de solicitud de autorización comprende un mensaje de solicitud de autorización de interfaz de privacidad de la línea base plus.

11. Uno o más medios legibles por computadora no transitorios que tienen instrucciones operativas para hacer que uno o más procesadores realicen las operaciones que comprenden:

recuperar un identificador único asociado con un cablemódem (105);
recuperar una clave única asociada con un sistema en un chip (205; 305) asociado con el cablemódem;
usar la clave única como clave de cifrado para cifrar el identificador único asociado con el cablemódem, produciendo así un identificador único cifrado;
usar la clave única como clave de descifrado para descifrar el identificador único cifrado, produciendo así el

identificador único asociado con el cablemódem; y
enviar el identificador único asociado con el cablemódem a un controlador aguas arriba, en el que el identificador único asociado con el cablemódem se emite como un mensaje de solicitud de autorización.

12. El uno o más medios legibles por computadora no transitorios de la reivindicación 11, en el que la clave única asociada con el sistema en un chip (205; 305) comprende una clave de dispositivo basada en hardware asociada con el sistema en un chip.

13. El uno o más medios legibles por computadora no transitorios de la reivindicación 11, en el que recuperar la clave única asociada con el sistema en un chip (205; 305) comprende:

recuperar un identificador único asociado con el sistema en un chip; y
usar el identificador único asociado con el sistema en un chip como semilla para generar la clave única asociada con el sistema en un chip.

14. El uno o más medios legibles por computadora no transitorios de la reivindicación 11, en el que el controlador aguas arriba comprende un sistema de terminación de cablemódem (120).

15. El uno o más medios legibles por computadora no transitorios de la reivindicación 11, en el que el mensaje de solicitud de autorización comprende un mensaje de solicitud de autorización de interfaz de privacidad de la línea base plus.

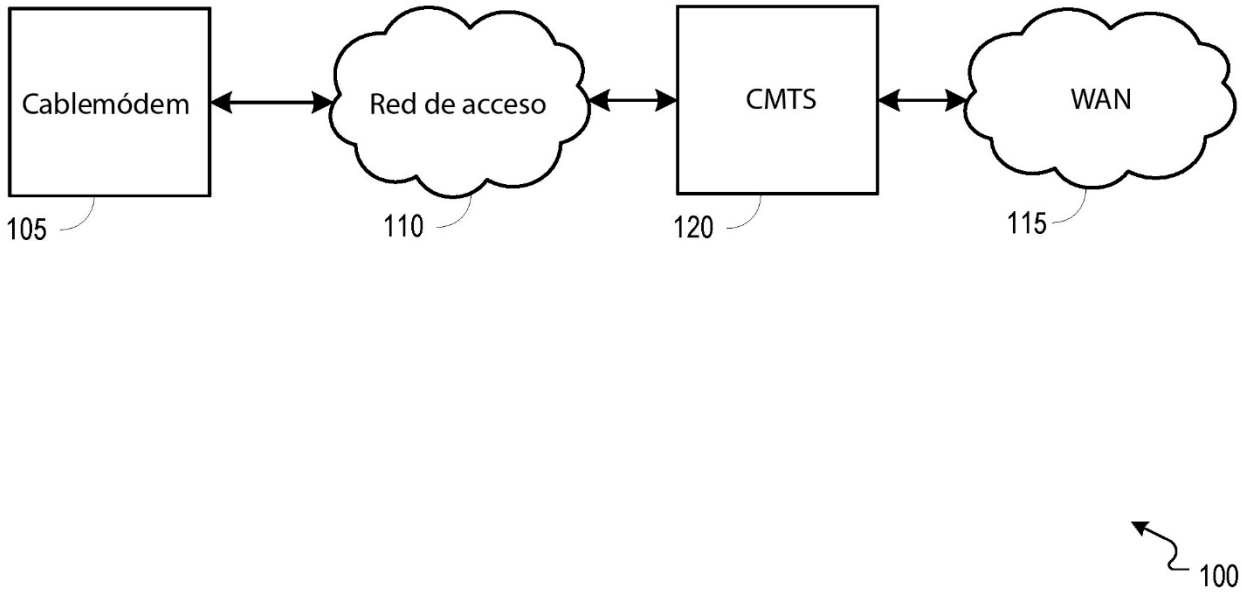

FIG. 1

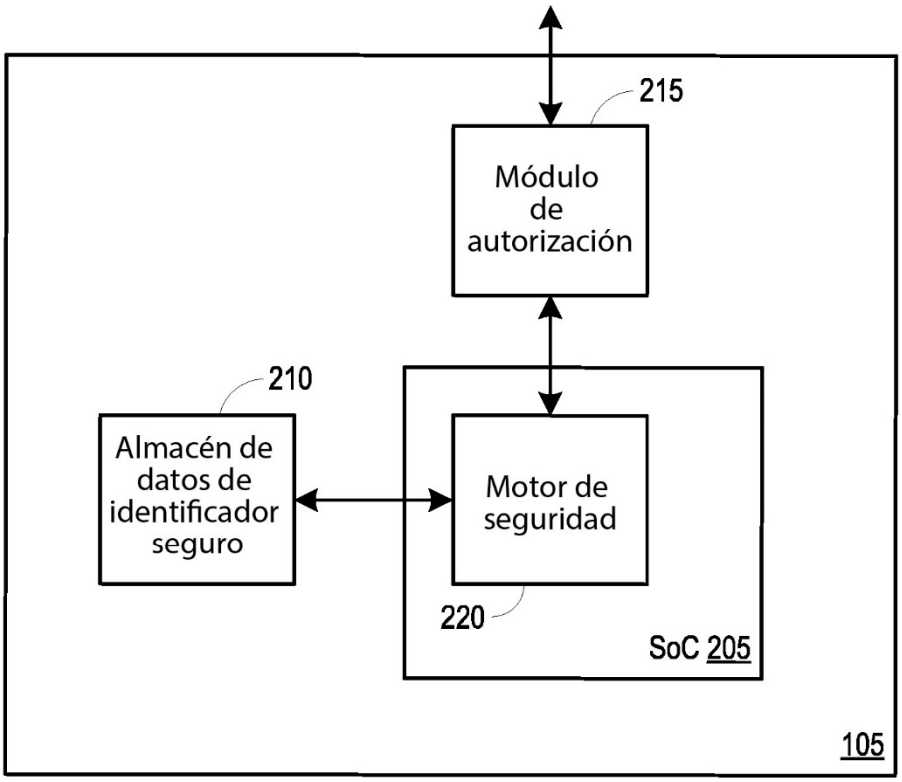
215
Módulo de autorización
210
Almacén de datos de identificador seguro
Motor de seguridad
220
SoC 205
105

FIG. 2

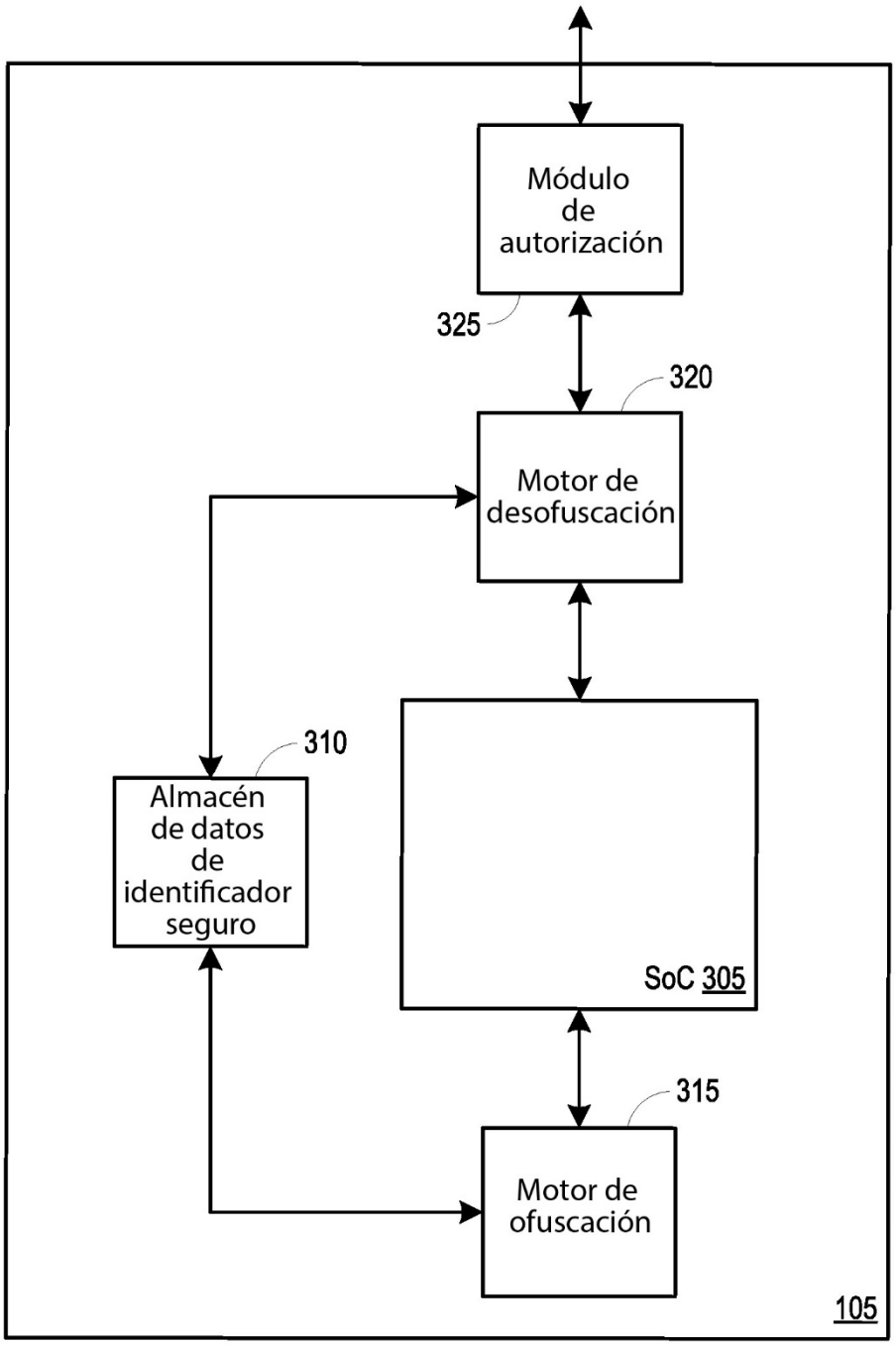
Módulo de autorización
325
320
Motor de desofuscación
310
Almacén de datos de identificador seguro
SoC 305
315
Motor de ofuscación
105

FIG. 3

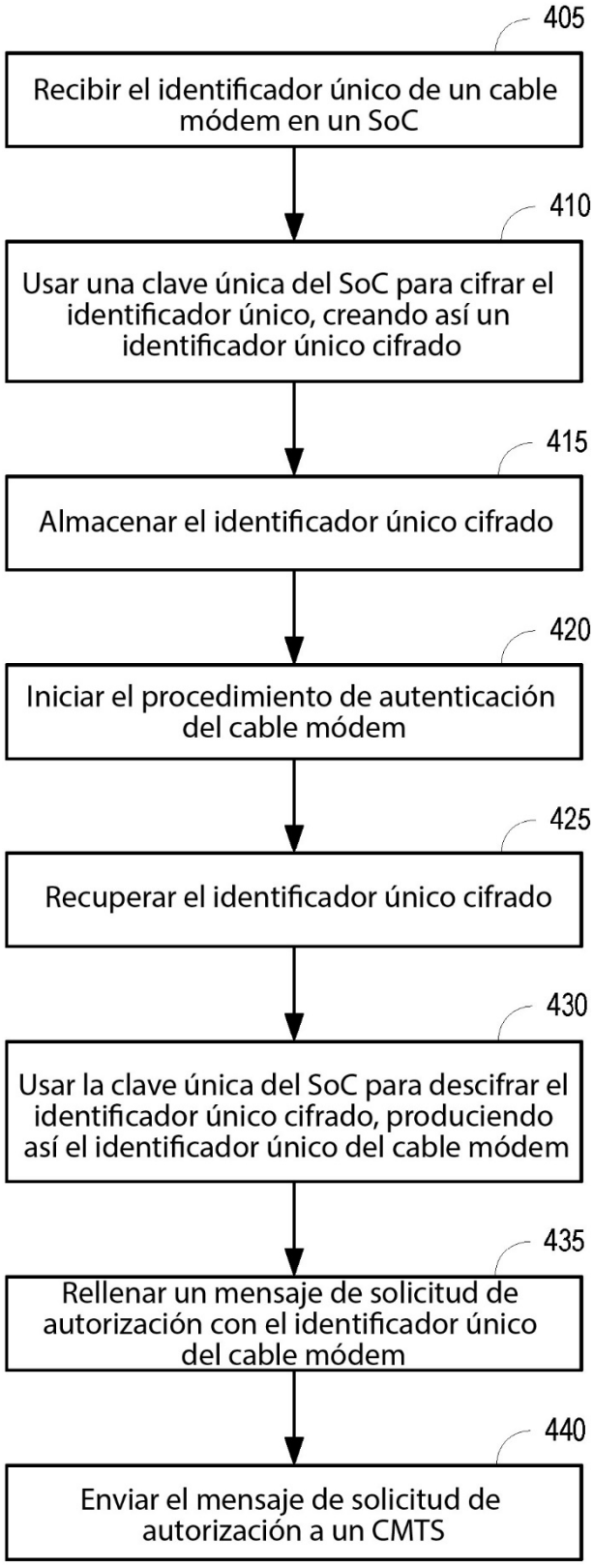
405
Recibir el identificador único de un cable módem en un SoC
410
Usar una clave única del SoC para cifrar el identificador único, creando así un identificador único cifrado
415
Almacenar el identificador único cifrado
420
Iniciar el procedimiento de autenticación del cable módem
425
Recuperar el identificador único cifrado
430
Usar la clave única del SoC para descifrar el identificador único cifrado, produciendo así el identificador único del cable módem
435
Rellenar un mensaje de solicitud de autorización con el identificador único del cable módem
440
Enviar el mensaje de solicitud de autorización a un CMTS
400

FIG. 4

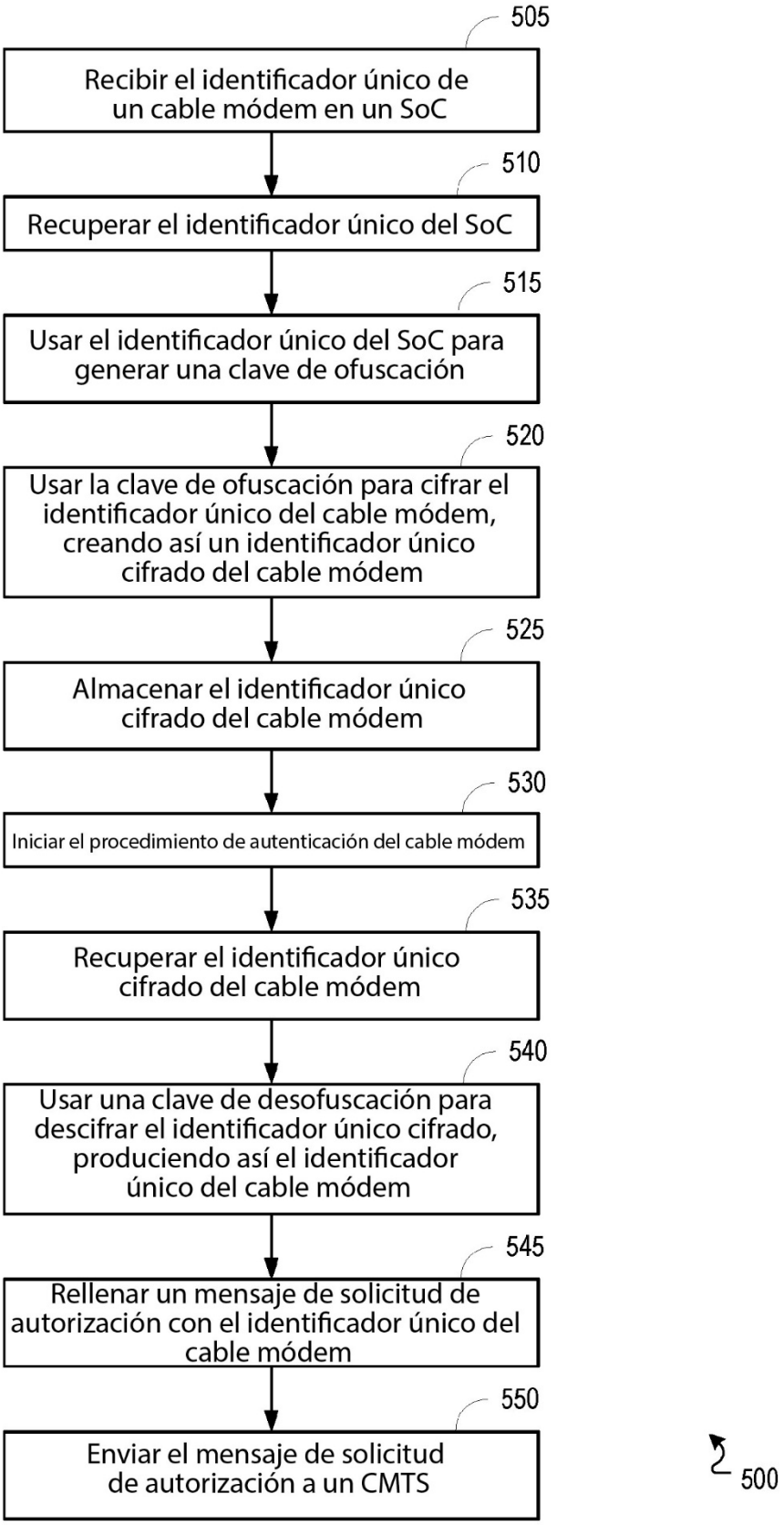
505
Recibir el identificador único de un cable módem en un SoC
510
Recuperar el identificador único del SoC
515
Usar el identificador único del SoC para generar una clave de ofuscación
520
Usar la clave de ofuscación para cifrar el identificador único del cable módem, creando así un identificador único cifrado del cable módem
525
Almacenar el identificador único cifrado del cable módem
530
Iniciar el procedimiento de autenticación del cable módem
535
Recuperar el identificador único cifrado del cable módem
540
Usar una clave de desofuscación para descifrar el identificador único cifrado, produciendo así el identificador único del cable módem
545
Rellenar un mensaje de solicitud de autorización con el identificador único del cable módem
550
Enviar el mensaje de solicitud de autorización a un CMTS
500

FIG. 5

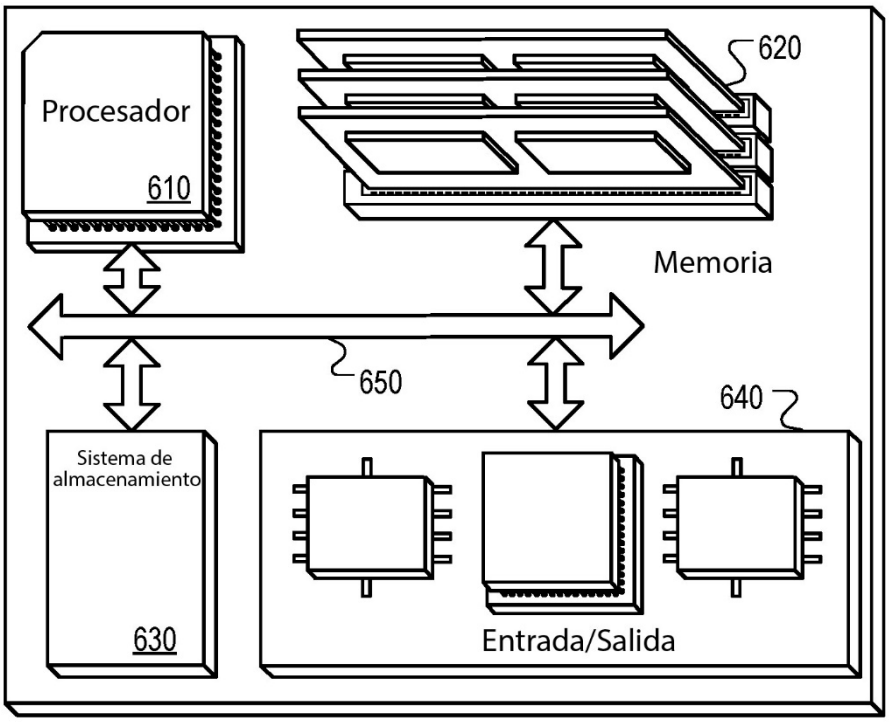
Procesador
610
620
Memoria
650
640
Sistema de almacenamiento
630
Entrada/Salida
600

FIG. 6