(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 959**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04Q 11/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.07.2010 E 14200355 (7)**

(97) Fecha y número de publicación de la concesión europea: **21.09.2016 EP 2882134**

(54) Título: **Mejora de seguridad de una red óptica pasiva sobre la base de una interfaz de control de gestión de terminal de red óptica**

(30) Prioridad:

31.07.2009 US 230520 P
27.07.2010 US 844173

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.03.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
B1-3A Intellectual Property Department, Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

EFFENBERGER, FRANK J.

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Mejora de seguridad de una red óptica pasiva sobre la base de una interfaz de control de gestión de terminal de red óptica

ANTECEDENTES DE LA INVENCIÓN

Una red óptica pasiva (PON) es un sistema para proporcionar acceso de red a través de la denominada "última milla". La red PON es una red de punto a multipunto constituida por un terminal de línea óptica (OLT) en la oficina central, una red de distribución óptica (ODN) y una pluralidad de unidades de redes ópticas (ONUs) en las instalaciones del cliente. Las transmisiones de datos de flujo descendente son objeto de difusión a todas las unidades ONUs, mientras que las transmisiones de datos de flujo ascendente son transmitidas al terminal OLT utilizando un sistema de acceso múltiple por división temporal (TDMA) o de acceso múltiple por división de onda (WMDA). Los sistemas PON, tal como Gigabit PONS (GPONs), pueden soportar algunas funciones de seguridad para proteger los datos de usuarios, p.e., para la difusión de flujo descendente. A modo de ejemplo, las transmisiones de difusión desde el terminal OLT a la unidad ONU pueden ser encriptadas.

El documento US 2009/049532 A1 se refiere a un método, un dispositivo y un sistema para la autenticación del usuario en una PON. El método incluye las siguientes etapas: un terminal OLT recibe una demanda de autenticación del usuario iniciada por una unidad ONU, que lleva una contraseña ID; el terminal OLT autentica de acuerdo con la contraseña de usuario ID comunicada por la unidad ONU, y abre o cierra un canal de la unidad ONU al lado de la red de acuerdo con el resultado de la autenticación.

El documento US 2006/129814 A1 se refiere a un método de autenticación para la protección del enlace entre un terminal OLT y una unidad ONU recién conectado a esta en una EPON, que se implementa en una capa de enlace de datos a la cual se aplica criptografía.

El documento CN 101 064 719 A se refiere a un método para programar una aritmética de encriptación en un sistema PON, donde el método incluye las siguientes etapas: la obtención del modo de la aritmética soportado por la unidad de red óptica; la selección del modo de la aritmética de acuerdo con el modo de la aritmética permitido por la estrategia preestablecida; el establecimiento de la red óptica que utiliza dicho modo de la aritmética seleccionado. La invención puede proporcionar el método de disposición de la aritmética de múltiples modos de la aritmética de encriptación durante el curso de distribución del sistema, al mejorar el protocolo existente, se pueden realizar la demanda de aplicaciones con múltiples aritméticas de encriptación, se mejora la compatibilidad del producto.

SUMARIO DE LA INVENCIÓN

En una forma de realización, la invención incluye un aparato que comprende un terminal de línea óptica, OLT (110), configurado para leer y/o escribir en una interfaz de control de gestión de unidad ONU, OMCI, una entidad de gestión, ME en una unidad de red óptica, ONU (120, 200), en donde la OMCI ME comprende una pluralidad de atributos que soportan una pluralidad de funciones de seguridad para transmisiones de flujo ascendente entre la unidad ONU y el terminal OLT, en donde los atributos que comprenden un atributo de tabla de respuesta de autenticación de terminal OLT para especificar una respuesta a utilizarse en una función de autenticación de terminal OLT, un atributo de estado de respuesta de autenticación de terminal OLT para controlar y comunicar el estado del atributo de tabla de respuesta de autenticación de terminal OLT durante la función de autenticación de OLT; en donde el valor falso del atributo de estado de respuesta de autenticación de terminal OLT indica que el atributo de tabla de respuesta de autenticación de terminal OLT no está completo, el valor verdadero del atributo de estado de respuesta de autenticación de terminal OLT indica que el atributo de tabla de respuesta de autenticación de terminal OLT está completo y en donde los atributos se comunican por intermedio de un canal OMCI entre la unidad ONU y el terminal OLT y se proporcionan las funciones de seguridad para la unidad ONU y el terminal OLT.

En otra forma de realización, la idea inventiva incluye un método que comprende el intercambio de una pluralidad de atributos de seguridad con una unidad ONU que utiliza un canal OMCI, proporcionando, de este modo, una pluralidad de funciones de seguridad para la comunicación de flujo ascendente desde la unidad ONU, en donde los atributos comprenden un atributo de tabla de respuesta de autenticación de terminal OLT para especificar una respuesta a utilizarse en una función de autenticación de terminal OLT, un atributo de estado de respuesta de autenticación de terminal OLT para controlar y comunicar el estado del atributo de tabla de respuesta de autenticación de terminal OLT; en donde el valor falso del atributo de estado de respuesta de autenticación del terminal OLT indica que el atributo de tabla de respuesta de autenticación del terminal OLT no está completo, el valor verdadero del atributo de estado de respuesta de autenticación de terminal OLT indica que el atributo de tabla de respuesta de autenticación del terminal OLT está completo.

Estas y otras características serán más claramente entendidas a partir de la siguiente descripción detallada en la que se hace referencia a los dibujos adjuntos y a las reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para un entendimiento más completo de esta idea inventiva, se hace ahora referencia a la siguiente breve descripción, tomada en relación con los dibujos adjuntos y una descripción detallada, en donde las referencias numéricas similares representan partes similares.

La Figura 1 es un diagrama esquemático de una forma de realización de una PON.

La Figura 2 es un diagrama esquemático de una forma de realización de una unidad ONU.

La Figura 3 es un diagrama de protocolo de una forma de realización de una secuencia de intercambio de mensajes de autenticación.

La Figura 4 es un diagrama esquemático de una forma de realización de una pluralidad de estados de unidad ONU.

La Figura 5 ilustra un diagrama esquemático de una forma de realización de un sistema informático de uso general.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Debe entenderse, desde el principio, que aunque se proporciona a continuación una puesta en práctica ilustrativa de una o más formas de realización, los sistemas y/o métodos de la invención pueden ponerse en práctica utilizando cualquier número de técnicas, actualmente conocidas o en existencia. La idea inventiva no debe estar en ninguna forma limitada a las puestas en práctica ilustrativas, dibujos y técnicas ilustradas a continuación, incluyendo los diseños y puestas en práctica, a modo de ejemplo, que se ilustran y se describen en esta memoria, pero pueden modificarse dentro del alcance de protección de las reivindicaciones adjuntas junto con su alcance completo de las equivalentes.

En los sistemas PON, las transmisiones de difusión de flujo descendente desde el terminal OLT a la unidad ONU pueden ser susceptibles de amenazas de la seguridad, tales como una 'amenaza de escucha clandestina denominada *eavesdropping* que puede intentarse por un usuario con intención maliciosa. A modo de ejemplo, un usuario no suscrito puede intentar recibir canales no autorizados y/o intervalos temporales desde el terminal OLT. Para superar dichas amenazas de seguridad, se suelen encriptar las difusiones de flujo descendente. Las transmisiones de flujo ascendente pueden también ser objeto de encriptación. Sin embargo, las transmisiones de flujo ascendente pueden ser más seguras que las transmisiones de difusión de flujo descendente puesto que las unidades ONUs legítimas o autorizadas no pueden recibir transmisiones de flujo ascendente desde otras unidades ONUs debido a la arquitectura física del sistema PON y la naturaleza direccional de las señales ópticas. Por lo tanto, la información privilegiada se suele transmitir en flujo ascendente desde las unidades ONUs en un formato de texto simple, p.e., sin encriptación. Sin embargo, métodos de ataque perfeccionados, tales como la derivación con cables de transmisión óptica, pueden todavía presentar amenazas de seguridad en los sistemas PON. Por consiguiente, pueden desearse mejoras de seguridad para las transmisiones de flujo descendente y/o de flujo ascendente en sistemas PON, a modo de ejemplo, para proteger las claves de encriptación y/o otra información de contraseñas.

Medios para proporcionar algunas mejoras de la seguridad han sido propuestos con anterioridad, pero suelen requerir la modificación del canal de PLOAM. Puesto que el procesamiento de PLOAM suele tener lugar en la capa física, la modificación del canal de PLOAM puede implicar la degradación del hardware en una pluralidad de componentes de la red, p.e., en la unidad ONU y/o los terminales OLTs. El canal de PLOAM no puede modificarse con facilidad mediante software y puede requerir instalaciones distantes para actualizar el hardware en los componentes del sistema. En consecuencia, las mejoras de seguridad anteriormente propuestas, basadas en la modificación del canal de PLOAM, pueden no ser prácticas o resultar costosas.

Lo que aquí se da a conocer es un método y sistema para proporcionar una seguridad mejorada en los sistemas PON. La seguridad puede mejorarse intercambiando parámetros de seguridad y datos utilizando un canal OMCI, que puede utilizarse para proporcionar una pluralidad de funciones de seguridad. Las funciones de seguridad proporcionadas pueden comprender el descubrimiento de capacidad de seguridad, autenticación de unidad ONU, autenticación de terminal OLT, privacidad de las claves o algunas de sus combinaciones. Las funciones de seguridad pueden soportarse comunicando una pluralidad de atributos correspondientes en el canal OMCI. Los atributos pueden añadirse al canal OMCI utilizando una entidad OMCI ME. Las funciones de seguridad pueden proporcionarse por la OMCI por intermedio de las puestas en práctica de software y de este modo, puede ser extensible o mejorarse sin una dificultad importante para admitir los cambios del sistema. En consecuencia, las funciones de seguridad pueden proporcionarse sin cambios importantes ni modificaciones al canal de PLOAM.

La Figura 1 ilustra una forma de realización de un sistema PON 100. El PON 100 puede comprender un terminal OLT 110, una pluralidad de unidades ONU 120 y una ODN 130, que pueden acoplarse al terminal OLT 110 y a las unidades ONU 120. El sistema PON 100 puede ser una red de comunicación que no requiera componentes activos para distribuir datos entre el terminal OLT 110 y las unidades ONU 120. En cambio, el sistema PON 100 puede utilizar los componentes ópticos pasivos en la red ODN 130 para distribuir datos entre el terminal OLT 110 y las unidades ONU 120. La red PON 100 puede ser un sistema de acceso de la siguiente generación (NGA), tal como un

sistema de diez Gigabits por segundo (Gbps), GPON (o XGPON), que puede tener un ancho de banda de flujo descendente de aproximadamente diez Gbps y un ancho de banda de flujo ascendente de al menos aproximadamente 2.5 Gbps. Otras realizaciones, a modo de ejemplo, de PONS adecuados 100 incluyen el modo de transferencia asíncrona de red PON (APON) y el PON de difusión (BPON) definido por la norma G.983 del Sector de Normalización de las Telecomunicaciones de la Unidad Internacional de Telecomunicaciones (ITU-T), la red GPON definida por la norma G.984 de ITU-T, la red PON de Ethernet (EPON), definida por la norma 802.3ah del Institute of Electrical and Electronics Engineers (IEEE), la red 10G-EPON definida por la norma IEEE 802.3av y la red PON Multiplexada por División de Longitud de Onda (WDM) denominada (WPON).

En una forma de realización, el terminal OLT 110 puede ser cualquier dispositivo que esté configurado para comunicarse con las unidades ONU 120 y otra red (no ilustrada). Más concretamente, el terminal OLT 110 puede actuar como un intermediario entre la otra red y las unidades ONU 120. A modo de ejemplo, el terminal OLT 110 puede reenviar los datos recibidos desde la red a las unidades ONU 120 y reenviar los datos recibidos desde las unidades ONU 120 a la otra red. Aunque la configuración específica del terminal OLT 110 puede variar dependiendo del tipo de PON 100, en una forma de realización, el terminal OLT 110 puede comprender un transmisor y un receptor. Cuando la otra red esté utilizando un protocolo de red, tal como Gestión de Red Óptica Síncrona o por Ethernet (SONET)/Jerarquía Digital Síncrona (SDH), que es diferente del protocolo de PON utilizado en el sistema PON 100, el terminal OLT 110 puede comprender un convertidor que convierta el protocolo de red en el protocolo de PON. El convertidor del terminal OLT 110 puede convertir también el protocolo de PON en el protocolo de red. El terminal OLT 110 puede estar normalmente situado en una localización central, tal como una oficina central, pero puede ubicarse también en otras posiciones.

En una forma de realización, las unidades ONU 120 pueden ser cualesquiera dispositivos que estén configurados para comunicarse con el terminal OLT 110 y un cliente o usuario (no ilustrado). Más concretamente, las unidades ONU pueden actuar como un intermediario entre el terminal OLT 110 y el cliente. A modo de ejemplo, las unidades ONU 120 pueden reenviar datos recibidos desde el terminal OLT 110 al cliente y reenviar los datos recibidos desde el cliente en el terminal OLT 110. Aunque la configuración específica de las unidades ONU 120 pueden variar dependiendo del tipo de PON 100, en una forma de realización, las unidades ONU 120 pueden comprender un transmisor óptico configurado para enviar señales ópticas al terminal OLT 110 y un receptor óptico configurado para recibir señales ópticas desde el terminal OLT 110. Además, las unidades ONU 120 pueden comprender un convertidor que convierta la señal óptica en señales eléctricas para el cliente, tales como señales en el protocolo de Ethernet y un segundo transmisor y/o receptor que pueda enviar y/o recibir las señales eléctricas para un dispositivo de cliente. En algunas formas de realización, las unidades ONU 120 y los terminales de redes ópticas (ONTs) son similares y por ello, los términos se utilizan aquí de forma intercambiable. Normalmente, las unidades ONU pueden estar situadas en posiciones distribuidas, tales como las instalaciones del cliente, pero pueden ubicarse también en otras posiciones.

En una forma de realización, la red ODN 130 puesta en estado de espera ser un sistema de distribución de datos, que puede comprender cables de fibras ópticas, acopladores, divisores, distribuidores y/o otros equipos. En una forma de realización, los cables de fibras ópticas, los acopladores, los divisores, los distribuidores y/o otros equipos pueden ser componentes ópticos pasivos. Más concretamente, los cables de fibras ópticas, los acopladores, los divisores, los distribuidores y/o otros equipos pueden ser componentes que no requieran ninguna alimentación de energía para distribuir señales de datos entre el terminal OLT 110 y las unidades ONU 120. Como alternativa, la red ODN 130 puede comprender uno o una pluralidad de equipos de procesamiento, tales como amplificadores ópticos. La red ODN 130 puede normalmente extenderse desde el terminal OLT 110 a las unidades ONU 120 en una configuración de derivación según se ilustra en la Figura 1, pero puede configurarse, como alternativa, en cualquier otra configuración del tipo punto a multipunto.

En una forma de realización, las unidades ONU 120 y/o el terminal OLT 110 pueden comunicarse utilizando una interfaz OMCI, a modo de ejemplo, para intercambiar información de control en la red PON 100. En consecuencia, el terminal OLT puede establecer un canal de OMCI para controlar algunas de las actividades y/o operaciones de las unidades ONU 120. La interfaz OMCI puede utilizarse para gestionar una o más capas de definición de servicios. Más concretamente, la interfaz OMCI puede modelar el flujo de datos entre el terminal OLT 110 y las unidades ONU 120 utilizando una base de información de gestión independiente del protocolo (MIB) que comprende una pluralidad de entidades MEs. Dicha configuración se describe en la interfaz OMCI para GPON, la norma G.984.4 de ITU-T y sus modificaciones. En la interfaz OMCI, los paquetes del cliente pueden ser objeto de mapeado de correspondencia con los puertos del Método de Encapsulación de GPON (GEM) utilizando una operación de Filtrado de Gestión de Redes de Área Local Virtual (VLAN), según se describe en la norma IEEE 802.1p.

La OMCI en la unidad ONU puede ponerse en práctica utilizando software, hardware o ambos a la vez, en donde nuevas entidades ME pueden añadirse para soportar capacidades adicionales o nuevas, p.e., capacidades que satisfacen diferentes necesidades de clientes. Cada entidad ME en la OMCI puede comprender una arquitectura de datos que representa un recurso y/o servicio soportado por la OMCI. A modo de ejemplo, la entidad ME puede describir la finalidad de la ME, la relación entre la ME y otras ME, los atributos de la ME o algunas de sus combinaciones. La entidad ME puede comprender una pluralidad de atributos, propiedades, propiedades de atributos o algunas de sus combinaciones. La OMCI puede describirse en la recomendación G.983.2 de la ITU-T,

titulada “Especificación de interfaz de control y de gestión de ONU para B-PON”, recomendación G.984.4 de ITU-T, titulada “Redes ópticas pasivas capaces de Gigabits (G-PON): especificación de interfaz de control de gestión de ONU”, o la recomendación G.988 de la ITU-T titulada “Especificación de interfaz de control y de gestión de ONU (OMCI)”.

En una forma de realización, la OMCI puede comprender una entidad ME de Control de Seguridad Mejorada que mejora la seguridad en los sistemas PON. La entidad ME de control de seguridad mejorada puede proporcionar características y/o funciones de seguridad, que pueden comprender una función de descubrimiento de capacidad de seguridad, una función de autenticación de ONU, una función de autenticación del terminal OLT y una función de privacidad de claves. La entidad OMCI ME puede comprender una pluralidad de atributos, p.e., tablas y/o parámetros, que soportan las funciones de seguridad, tales como las descritas en conjunción con la Figura 2 siguiente. Los atributos y las funciones de seguridad pueden utilizarse para proporcionar funciones de seguridad para transmisiones de flujo ascendente desde las unidades ONUs y de forma opcional, para añadir seguridad a las transmisiones de flujo descendente desde el terminal OLT.

La función de descubrimiento de la capacidad de seguridad puede permitir a uno de los terminales OLT o de las unidades ONU descubrir la existencia y/o disponibilidad de una o más capacidades de seguridad del otro componente. La función de descubrimiento de la capacidad de seguridad puede permitir también al componente de red descubrir uno o más algoritmos de seguridad que soportan una capacidad de seguridad del otro componente. Además, la función de capacidad de seguridad puede permitir al componente seleccionar cuál de los algoritmos de seguridad activar. En una forma de realización, el terminal OLT puede utilizar la función de descubrimiento de capacidad de seguridad para informar a la unidad ONU, por intermedio del canal OMCI de las capacidades de seguridad y/o algoritmos que puedan proporcionarse por el terminal OLT. Las capacidades de seguridad y/o algoritmos pueden proporcionarse a la unidad ONU en uno o más atributos susceptibles de lectura y/o escritura en la unidad ONU, p.e., en la entidad ME de control de seguridad mejorada en la unidad ONU. El terminal OLT puede utilizar también la función de descubrimiento de capacidad de seguridad para recibir desde la unidad ONU, por intermedio del canal OMCI, las capacidades de seguridad y/o algoritmos soportados por la unidad ONU. Las capacidades de seguridad y/o los algoritmos pueden estar situados en uno o más atributos legibles p.e., en la entidad ME de control de seguridad mejorada en la unidad ONU y pueden indicar la existencia de una capacidad de seguridad y/o definir el nivel de soporte de la unidad ONU para una capacidad particular y/o algoritmo.

Además, la función de descubrimiento de capacidad de seguridad puede permitir al terminal OLT especificar uno o más algoritmos de seguridad que pueden utilizarse para proporcionar la función de autenticación de ONU, la función de autenticación de OLT, la función de privacidad de claves o una de sus combinaciones. En algunas formas de realización, una o más de estas capacidades de funciones de seguridad/algoritmos pueden especificarse por administrador en lugar del terminal OLT o de la unidad ONU. Las capacidades de seguridad/algoritmos pueden especificarse como parte de la función de descubrimiento de la capacidad de seguridad, p.e., antes de iniciar la función de autenticación de ONU, la función de autenticación de OLT y/o la función de privacidad de claves. Como alternativa, las capacidades/algoritmos pueden especificarse como parte del establecimiento de funciones de seguridad diferentes.

La función de autenticación de la unidad ONU puede permitir al terminal OLT verificar que la unidad ONU es un usuario autorizado y/o satisface uno o más criterios de calificación de seguridad. En una forma de realización, el terminal OLT puede intercambiar información para la autenticación de ONU con la unidad ONU por intermedio del canal OMCI. A modo de ejemplo, el procedimiento de autenticación de ONU puede comprender un procedimiento de autenticación de respuesta a reto operativo, que puede establecerse entre el terminal OLT y la unidad ONU utilizando el canal OMCI. El procedimiento de autenticación de respuesta a reto operativo puede ser similar al procedimiento de autenticación descrito en la publicación nº 180-3 de las Normas Federales de Procesamiento de Información (FIPS), tituladas “Especificaciones para la Norma de Protección Segura contra Intrusiones”. Durante un procedimiento de autenticación de respuesta a reto operativo, el terminal OLT puede enviar un reto operativo en la forma de un número aleatorio usado una sola vez, denominado *nonce*, p.e., un número generado de forma aleatoria, a la unidad ONU por intermedio del canal OMCI. Posteriormente, la ONU puede enviar una respuesta que comprende una combinación de huella digital denominada *hash* del número *nonce* y un secreto mutuamente compartido al terminal OLT por intermedio del canal OMCI. A modo de ejemplo, el terminal OLT puede realizar la escritura del número *nonce* en la entidad OMCI ME de la unidad ONU y luego, efectuar la lectura de la combinación de huella digital *hash* de la entidad OMCI ME. El terminal OLT puede realizar la autenticación de la unidad ONU verificando que la combinación de *hash* es prácticamente igual a un valor de autenticación de la unidad ONU que puede calcularse por el terminal OLT con independencia de la combinación de *hash*. En algunas formas de realización, el terminal OLT puede enviar un mensaje de confirmación de autenticación de ONU a la unidad ONU, por intermedio del canal OMCI, después de determinar que la combinación de huella digital *hash* es prácticamente igual al valor de autenticación de ONU. El mensaje de confirmación de autenticación de ONU puede indicar que la unidad ONU ha sido objeto de autenticación por el terminal OLT.

La función de autenticación del terminal OLT puede permitir a la unidad ONU verificar que el terminal OLT es un terminal OLT legítimo, p.e., asignado a la unidad ONU y/o satisface uno o más criterios de calificación de seguridad. En una forma de realización, la unidad ONU puede intercambiar información necesaria para la autenticación del

terminal OLT con el OLT por intermedio del canal OMCI. A modo de ejemplo, la autenticación de OLT puede comprender un procedimiento de autenticación de respuesta a reto operativo, que puede establecerse entre el terminal OLT y la unidad ONU utilizando el canal OMCI. Durante un procedimiento de autenticación de respuesta a reto operativo, la unidad ONU puede enviar un reto operativo, en la forma de un número *nonce*, al terminal OLT por intermedio del canal OMCI. En respuesta, el terminal OLT puede enviar un mensaje que contenga una combinación de *hash* del número *nonce* y un secreto mutuamente compartido a la unidad ONU por intermedio del canal OMCI. A modo de ejemplo, el terminal OLT puede efectuar la lectura de un número *nonce* desde la entidad OMCI ME en la unidad ONU y luego, efectuar la escritura de la combinación de *hash* en la entidad OMCI ME. La unidad ONU puede comparar la combinación de *hash* con un valor de autenticación del terminal OLT que se calcula por la unidad ONU para realizar la autenticación del terminal OLT. En algunas formas de realización, la unidad ONU puede enviar un mensaje de confirmación de autenticación de terminal OLT al terminal OLT por intermedio del canal OMCI después de confirmar que la combinación de *hash* es prácticamente igual al valor de autenticación del terminal OLT. La combinación de *hash* y el valor de autenticación del terminal OLT pueden calcularse de forma independiente por el terminal OLT y la unidad ONU, respectivamente. Además, el número *nonce* y la combinación en *hash* que se utilizan en el procedimiento de autenticación del terminal OLT pueden ser diferentes respecto al número *nonce* y la combinación de huella digital *hash* que utilizan en el procedimiento de autenticación de la unidad ONU.

La función de privacidad de claves puede permitir al terminal OLT y a la unidad ONU intercambiar, por intermedio del canal OMCI, claves de encriptación y/o otros parámetros de seguridad o información para establecer un protocolo de encriptación para posteriores transmisiones de flujo ascendente y/o de flujo descendente. A modo de ejemplo, la función de privacidad de claves puede permitir al terminal OLT enviar información de claves a la unidad ONU por intermedio del canal OMCI. La función de privacidad de claves puede permitir también a la unidad ONU enviar información de claves al terminal OLT por intermedio del canal OMCI. La información de claves puede comprender cualquier información que se utilice para establecer un protocolo de encriptación. La información de claves puede asociarse con un protocolo de claves públicas que utiliza un algoritmo de claves asimétrico. Algunas técnicas comunes que pueden utilizarse en la criptografía de claves públicas pueden describirse en la norma IEEE 1363 titulada “Especificaciones estándar para criptografía de claves públicas. La criptografía de claves públicas puede comprender un método para la encriptación de datos utilizando una clave pública y una función de desencriptación de datos utilizando una clave privada, en donde la clave pública puede ser ampliamente distribuida y la clave privada puede mantenerse secreta. En tales casos, la clave privada puede no ser derivada matemáticamente a partir de la clave pública y en consecuencia, un intruso que no tenga posesión de la clave pública puede enviarse que decodifique un mensaje encriptado. A modo de ejemplo, la función de privacidad de claves puede permitir al terminal OLT efectuar la escritura de una clave pública a la OMCI en la unidad ONU. La unidad ONU puede encriptar luego una clave de Norma de Encriptación Avanzada (AES) con la clave pública y enviar la clave encriptada a través del canal de PLOAM. Posteriormente, el terminal OLT puede obtener la clave encriptada y obtener también la clave AES a partir de la clave encriptada.

En formas de realización diferentes, la función de descubrimiento de la capacidad de seguridad, la función de autenticación de la unidad ONU, la función de autenticación del terminal OLT y la función de privacidad de claves pueden consolidarse en una función de autenticación única o realizarse simultáneamente. En algunas formas de realización, el terminal OLT puede intercambiar con la unidad ONU, por intermedio del canal OMCI, capacidades criptográficas, información de autenticación y/o información de claves que pertenecen al terminal OLT y/o la unidad ONU, p.e., mediante la lectura y/o escritura de una pluralidad de atributos de la entidad ME de control de seguridad mejorada. Los atributos pueden intercambiarse en una secuencia de intercambio de mensajes de autenticación según se describe en detalle más adelante.

La Figura 2 ilustra una forma de realización de una unidad ONU 200, que puede comprender una entidad ME de control de seguridad mejorada 210. La entidad ME de control de seguridad mejorada 210 puede comprender una pluralidad de atributos de ME 220 (p.e., A1-AN). Estos atributos de ME 220 pueden representar estructuras de datos, p.e., tablas, parámetros y/o variables de sistemas, que pueden comprender datos que describen diferentes características de la unidad ONU y/o en una secuencia de intercambio de mensajes de autenticación. Los atributos de ME 220 pueden comprender un atributo de ME ID, un atributo de capacidades criptográficas del terminal OLT, un atributo de tabla de reto operativo aleatorio del terminal OLT, un atributo de estado de reto operativo de OLT, un atributo de capacidades criptográficas seleccionadas de la unidad ONU, un atributo de tabla de reto operativo aleatorio de ONU, un atributo de tabla de resultado de autenticación de ONU, un atributo de tabla de resultado de autenticación del terminal OLT, un atributo de estado de resultado de OLT, un atributo de estado de autenticación de ONU, un atributo de nombre de clave de sesión maestra, un atributo de tabla de claves de difusión, un atributo de longitud de clave efectiva o una de sus combinaciones. Estos atributos pueden utilizarse para soportar o proporcionar características y/o funciones de seguridad, tales como en la función de descubrimiento de capacidad de seguridad, la función de autenticación de ONU, la función de autenticación de OLT, la función de privacidad de claves o una de sus combinaciones. En consecuencia, algunos de los atributos de ME 220 pueden utilizarse, por separado, en diferentes funciones de seguridad o conjuntamente en una función de seguridad combinada que consolida al menos algunas de las funciones de seguridad. A modo de ejemplo, los atributos de ME 220 pueden utilizarse para poner en práctica un proceso de autenticación de tres etapas sobre la base de claves simétricas.

El atributo de ME ID puede utilizarse para identificar cada instancia operativa de la entidad ME de control de

seguridad mejorada 210. En una forma de realización, puede ser una instancia única de la entidad ME de control de seguridad mejorada 210 asociada con la unidad ONU, en donde la instancia operativa puede tener un valor de ME ID igual a aproximadamente 'cero'. En otras formas de realización, pueden ser instancias múltiples de la entidad ME de control de seguridad mejorada 210 en asociación con la unidad ONU, en donde cada instancia operativa puede tener un valor de ME ID diferente. El atributo de ME ID puede ser legible y tener una longitud aproxima de 2 bytes.

El atributo de capacidades criptográficas del terminal OLT puede especificar uno o más de los mecanismos criptográficos disponibles o soportados por el terminal OLT. En una forma de realización, el atributo de capacidades criptográficas del terminal OLT puede formatearse como un mapa de bits, en donde cada uno de los bits en el mapa de bits puede corresponder a un algoritmo, p.e., según se ilustra en la tabla 1. En consecuencia, un bit puede establecerse a aproximadamente '1' para indicar que se soporta un algoritmo de autenticación o criptográfico correspondiente por el terminal OLT o a aproximadamente 'cero' para indicar que el algoritmo correspondiente no está soportado por el terminal OLT. El atributo de capacidades criptográficas del terminal OLT puede ser susceptible de escritura y tiene una longitud aproximada de 16 bytes. En algunos casos, cada bit en el atributo de capacidades criptográficas del terminal OLT puede establecerse a aproximadamente 'cero' para indicar que el terminal OLT no soporta ningún algoritmo.

La tabla 1 describe una forma de realización del mapa de bits del atributo de capacidades criptográficas del terminal OLT. Más concretamente, diferentes posiciones de bits en el mapa de bits pueden corresponder a diferentes algoritmos criptográficos. A modo de ejemplo, la posición de bit 'uno' (el bit menos significativo (LSB)) puede corresponder a un algoritmo AES-CMAC-128, la posición de bit 'dos' puede corresponder a un algoritmo HMAC-SHA-256, la posición de bit 'tres' puede corresponder a un algoritmo HMAC-SHA-512 y las posiciones de bits de cuatro a aproximadamente 128 pueden estar reservadas.

Tabla 1

Posición de bit	Algoritmo
1 (LSB)	AES-CMAC-128
2	HMAC-SHA-256
3	HMAC-SHA-512
4-128	Reservado

El atributo de tabla de reto operativo aleatorio del terminal OLT puede especificar un reto operativo aleatorio emitido por el terminal OLT durante una secuencia de autenticación. En una forma de realización, el atributo de tabla de reto operativo aleatorio del terminal OLT puede ser una tabla que comprende N entradas (siendo N un número entero), que pueden determinarse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 17 bits, en donde el primer byte de cada entrada puede comprender un índice de entrada o un identificador de entrada y los bytes restantes de cada entrada pueden comprender contenidos. El terminal OLT puede efectuar la escritura de las entradas en la tabla y luego, iniciar operativamente la ONU para procesar las entradas de la tabla, p.e., utilizando el atributo de estado de reto operativo del terminal OLT. Puesto que el atributo de tabla de reto operativo aleatorio del terminal OLT puede tener un número variable de entradas (p.e., N), la longitud y por lo tanto, la complejidad del reto operativo aleatorio puede aumentarse para mejorar la seguridad de la función de autenticación si fuere necesario. El atributo de tabla de reto operativo aleatorio del terminal OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de 17xN bytes.

El atributo de estado de reto operativo del terminal OLT puede utilizarse para controlar y comunicar el estado del atributo de capacidades criptográficas de OLT y/o el atributo de tabla de reto operativo aleatorio de OLT. En una forma de realización, el atributo de estado de reto operativo del terminal OLT puede ser un atributo booleano que puede establecerse para un primer o valor verdadero booleano (p.e., aproximadamente 'uno') cuando el atributo de capacidades criptográficas del terminal OLT y/o el atributo de tabla de reto operativo aleatorio de OLT están completos o a un segundo o falso valor booleano (p.e., aproximadamente 'cero') cuando el atributo de capacidades criptográficas del terminal OLT y/o el atributo de tabla de reto operativo aleatorio de OLT no están completos. A modo de ejemplo, el terminal OLT puede establecer el atributo de estado de reto operativo de OLT al valor falso (p.e., aproximadamente 'cero') antes o mientras se realiza la escritura para el atributo de capacidades criptográficas de OLT y/o el atributo de tabla de reto operativo aleatorio de OLT. Posteriormente, el terminal OLT puede establecer al Tribunal de estado de reto operativo de OLT a un valor verdadero (p.e., aproximadamente 'uno') al completar el proceso de escritura para el atributo de capacidades criptográficas de OLT y/o el atributo de tabla de reto operativo aleatorio de OLT. El terminal OLT puede establecer el atributo de estado de reto operativo de OLT al valor falso, efectuar la escritura de una pluralidad de entradas en el atributo de capacidades criptográficas de OLT y/o el atributo de tabla de reto operativo aleatorio de OLT, establecer el atributo de estado de reto operativo de OLT al valor verdadero y de este modo, iniciar operativamente la unidad ONU para procesar los contenidos del atributo de capacidades criptográficas de OLT y/o el atributo de la tabla de reto operativo aleatorio de OLT. El atributo de estado de reto operativo de OLT puede ser legible, susceptible de lectura y tener una longitud aproximada de un byte.

El atributo de capacidades criptográficas seleccionadas de la unidad ONU puede especificar una capacidad criptográfica que se selecciona por la unidad ONU, p.e., en una secuencia de autenticación. El atributo de capacidades criptográficas seleccionadas de la unidad ONU puede establecerse a un valor que índice un algoritmo soportado por el terminal OLT, p.e., en el atributo de capacidades criptográficas de OLT. El valor puede especificar una de las posiciones de bits que fue establecida a aproximadamente 'uno' en el atributo de capacidades criptográficas del terminal OLT.

El atributo de tabla de reto operativo aleatorio de ONU puede especificar un reto operativo aleatorio emitido por la unidad ONU durante la secuencia de autenticación. En una forma de realización, el atributo de tabla de reto operativo aleatorio de la unidad ONU puede ser una tabla que comprenda P entradas (siendo P un número entero), que pueden establecerse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 16 bytes, en donde el primer byte de cada entrada puede comprender un índice de entradas o identificador de entrada y los bytes restantes de cada entrada pueden comprender contenidos. La unidad ONU puede efectuar la escritura del atributo de tabla de reto operativo aleatorio de ONU en respuesta al terminal OLT que genera el atributo de estado de reto operativo de OLT. Después de generar el atributo de tabla de reto operativo aleatorio de ONU, la unidad ONU puede notificar al terminal OLT, p.e., utilizando una acción de cambio de valor de atributo (AVC), que la tabla de reto operativo está establecida para inicializar operativamente el terminal OLT para comenzar una secuencia de 'obtener/obtener siguiente' para conseguir el contenido de la tabla. Puesto que el atributo de la tabla de reto operativo aleatorio de la unidad ONU puede tener un número variable de entradas, la longitud y por lo tanto, la complejidad del reto operativo aleatorio puede aumentarse para mejorar la seguridad de la función de autenticación. El atributo de tabla de reto operativo aleatorio de ONU puede ser legible y tener una longitud aproximada de 16xP bytes.

El atributo de tabla de resultado de autenticación de ONU puede especificar un resultado del reto operativo de autenticación desde la unidad ONU en función del atributo de capacidades criptográficas seleccionadas de ONU. El valor del atributo de tabla de resultado de autenticación de ONU puede generarse utilizando una función de huella digital denominada *hash* seleccionada por la unidad ONU, tal como:

SelectedHashFunction (PSK, (ONU_selected_crypto_capabilites | OLT_random_challenge_table | ONU_random_challenge_table | 0x0000 0000 0000 0000)),

en donde "|" indica la concatenación y el término ONU_selected_crypto_capabilities representa las capacidades criptográficas seleccionadas por la unidad ONU.

En una forma de realización, el atributo de tabla de resultado de autenticación de ONU puede ser una tabla de datos que comprenda Q entradas (siendo Q un número entero), que pueden determinarse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 16 bytes. La unidad ONU puede efectuar la escritura del atributo de tabla de resultado de autenticación de ONU en respuesta al terminal OLT que genera el atributo de estado de reto operativo de OLT. Después de generar el atributo de tabla de resultado de autenticación de ONU, la unidad ONU puede notificar al terminal OLT, p.e., utilizando una notificación o mensaje AVC, que la tabla está establecida para inicializar operativamente el terminal OLT para comenzar una secuencia de 'obtener/obtener siguiente' para conseguir el contenido de la tabla. Puesto que el atributo de tabla de respuesta de autenticación de ONU puede tener un número variable de entradas, la longitud y por lo tanto, la complejidad de la combinación de huella digital (*hash*) puede aumentarse para mejorar la seguridad de la función de autenticación de la unidad ONU, si fuere necesario. El atributo de tabla de resultado de autenticación de ONU puede ser legible y tener una longitud aproximada de 16xQ bytes.

El atributo de tabla de resultado de autenticación de OLT puede especificar un resultado del cálculo de la autenticación desde el terminal OLT. El valor del atributo de tabla de resultado de autenticación de OLT puede generarse utilizando una función hash seleccionada por el terminal OLT, tal como

SelectedHashFunction (PSK, (ONU_selected_crypto_capabilites | OLT_random_challenge_table | OLT_random_challenge_table | ONU_serial_number)),

en donde ONU_serial_number es el número de serie de la entidad ONU ME que puede especificarse por un atributo del número de serie de la unidad ONU.

En una forma de realización, el atributo de tabla de resultado de autenticación del terminal OLT puede ser una tabla de datos que comprenda R entradas (siendo R un número entero) que puede establecerse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 17 bytes, en donde el primer byte de cada entrada puede comprender un índice de entrada o un identificador de entrada y en donde los bytes restantes de cada entrada pueden comprender contenidos. El terminal OLT puede efectuar la escritura de las entradas en el atributo de tabla de resultado de autenticación de OLT y luego, iniciar operativamente la unidad ONU para procesar la tabla con el atributo de estado de resultado de OLT. Puesto que la tabla de resultado de autenticación de OLT puede tener un número variable de entradas, la longitud y por lo tanto, la complejidad, del

resultado puede aumentarse para mejorar la seguridad de la función de autenticación de OLT si fuere necesario. La tabla de respuesta de autenticación del terminal OLT puede ser susceptible de escritura y tener una longitud aproximada de 17xR bytes.

El atributo de estado de resultado de OLT puede utilizarse para controlar y/o comunicar el estado del atributo de tabla de resultado de autenticación de OLT. En una forma de realización, el atributo de estado de resultado del terminal OLT puede ser un atributo booleano que puede establecerse a un valor verdadero de aproximadamente 'uno' cuando el atributo de tabla de resultado de autenticación de ONU está completo o a un valor booleano falso de aproximadamente 'cero' cuando el atributo de tabla de resultado de autenticación de ONU no está completo. A modo de ejemplo, el terminal OLT puede establecer el atributo de estado de resultado de OLT a falso (p.e., aproximadamente 'cero') antes o mientras se realiza la escritura para el atributo de tabla de resultado de autenticación de OLT y posteriormente, a un valor verdadero (p.e., aproximadamente 'uno') al completar el proceso de escritura del resultado al atributo de tabla de resultado de autenticación de OLT. El terminal OLT puede establecer el atributo de estado de resultado de autenticación de OLT a un valor falso con la escritura de una pluralidad de entradas al atributo de tabla de resultado de autenticación de OLT, establecer el atributo de estado de resultado de OLT a verdadero y de este modo, iniciar operativamente la unidad ONU para procesar el atributo de tabla de resultado de OLT. El atributo de estado de resultado de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte.

El atributo de estado de autenticación de ONU puede indicar el estado de la relación de autenticación desde la perspectiva de la unidad ONU. El atributo de estado de autenticación de la unidad ONU puede tener un valor aproximado de cero para indicar que la unidad ONU está en un estado inactivo S0, p.e., en donde el procedimiento de autenticación no está activo. El atributo de estado de autenticación de la unidad ONU puede tener un valor de aproximadamente 'uno' para indicar que la unidad ONU está en un estado S1 pendiente del reto operativo del terminal OLT, p.e., cuando el procedimiento de autenticación está en proceso. El atributo de estado de autenticación de ONU puede tener un valor de aproximadamente 'dos' para indicar que la unidad ONU está en un estado S2 pendiente de reto operativo de ONU. El atributo de estado de autenticación de ONU puede tener un valor de aproximadamente 'tres' para indicar que la unidad ONU está en un estado de éxito operativo de autenticación S3, p.e., cuando el procedimiento de autenticación está completado y la unidad ONU ha realizado la autenticación del terminal OLT. El atributo de estado de autenticación de ONU puede tener un valor de aproximadamente 'cuatro' para indicar que la unidad ONU está en un estado de fallo de autenticación S4, p.e., cuando el procedimiento de autenticación está completado y la unidad ONU no ha realizado la autenticación del terminal OLT. Como alternativa, el atributo de estado de autenticación de ONU puede tener un valor de aproximadamente 'cinco' para indicar que la unidad ONU está en un estado de error de autenticación S5, p.e., cuando el procedimiento de autenticación se ha iniciado pero no pudo completarse. Cuando el atributo de autenticación de ONU tiene un valor de aproximadamente 'tres', p.e., en el éxito operativo de la autenticación S2, una pluralidad de claves de encriptación puede intercambiarse en una capa de contenedor de transmisión (TC), p.e., utilizando una clave de sesión maestra según se describe en la norma G.984 o una clave de encriptación de claves según se describe en la norma G.987. El terminal OLT puede comprobar el valor del atributo de estado de autenticación de ONU antes de iniciar una conmutación de claves. Además, el terminal OLT puede ser avisado de un cambio en el estado del atributo de estado de autenticación de ONU, p.e., un cambio desde el estado S1 al estado S2, recibiendo un mensaje AVC o una notificación desde la unidad ONU por intermedio del canal OMCI. El atributo de estado de autenticación de ONU puede ser legible y tener una longitud de un byte.

El atributo de nombre de clave de sesión maestra puede comprender el nombre de la clave de sesión actual, p.e., después de una autenticación operativamente satisfactoria. Una clave de sesión maestra puede definirse mediante una función hash seleccionada por la unidad ONU, tal como

SelectedHashFunction (PSK, (OLT_random_challenge | ONU_random_challenge)).

El atributo de nombre de clave de sesión maestra puede definirse como:

SelectedHashFunction (PSK, (ONU_random_challenge | OLT_random_challenge | 0x 3141 5926 5358 9793 3141 5926 5358 9793)),

en donde el número 0x 3141 5926 5358 9793 3141 5926 5358 9793 es una realización, a modo de ejemplo, de un número de serie de unidad ONU. Si la función de huella digital *hash* seleccionada genera más de aproximadamente 128 bits, el resultado puede ser truncado a la parte más a la izquierda, p.e., la parte más significativa, en aproximadamente 128 bits. A la terminación de una clave de sesión maestro, p.e., debido a una reposición de ONU o a una decisión local de unidad ONU de que ha caducado la clave maestra, la ONU puede establecer el atributo de nombre de clave de sesión maestra a una secuencia de aproximadamente 'cero'. El atributo de nombre de clave de sesión maestra puede ser legible y tener una longitud aproximada de 16 bytes.

El atributo de tabla de claves de difusión puede comprender una clave de difusión generada por el terminal OLT. El atributo de tabla de clave de difusión puede comprender una tabla que incluya una o más filas. Cada fila puede comprender una parte de control de fila, una parte de identificador de fila y una parte de fragmento de claves. El control de filas puede comprender aproximadamente un byte, el identificador de fila puede comprender también

aproximadamente un byte y el fragmento de clave puede comprender aproximadamente 16 bytes. En consecuencia, el atributo de tabla de claves de difusión puede legible y susceptible de escritura, opcional y tener una longitud aproximada de 18*N bytes.

El control de fila puede describir la acción a tomarse sobre una fila especificada, p.e., la fila especificada por el identificador de fila. Aproximadamente dos bits menos significativos LSBs en el control de fila pueden determinar el comportamiento del atributo bajo una acción establecida, p.e., según se ilustra en la tabla 2. En la tabla 2, los dos bytes menos significativos LSBs pueden establecerse a aproximadamente 00 para la fila especificada, a aproximadamente 01 para eliminar la fila especificada, a aproximadamente 10 para eliminar la tabla completa o a aproximadamente 11 para indicar una entrada reservada. Además, aproximadamente cuatro bits más significativos (MSBs) en el control de fila pueden especificar la longitud del fragmento de clave correspondiente. Los dos bits restantes, en el control de fila, pueden estar reservados. Los dos bits menos LSBs del control de fila pueden leerse como aproximadamente 'cero' bajo la acción de 'obtener-obtener siguiente' y pueden comportarse de una manera coherente con la tabla 2 bajo la acción establecida.

Tabla 2

LSBs	Comportamiento bajo al acción establecida
0	Establecer la fila especificada
1	Eliminar la fila especificada
0	Eliminar la tabla completa
11	Reservados

El identificador de fila puede identificar la fila especificada. Aproximadamente dos bits MSBs, en el identificador de fila, puede representar el índice de claves, que puede aparecer en la cabecera de una trama del Método de Encapsulación GPON difundido encriptado (GEM). Un índice de claves de aproximadamente 'cero' puede indicar un texto simple y por ello no puede aparecer en el identificador de fila. Aproximadamente cuatro bits LSBs en el identificador de fila pueden identificar el número de fragmentos de claves y puede iniciarse desde aproximadamente 'cero'. Los restantes dos bits en el identificador de fila pueden estar reservados. El fragmento de claves puede comprender una parte de clave especificada, p.e., especificada por la unidad ONU. A modo de ejemplo la parte de claves puede encriptarse con el libro de códigos de AES-Electronic (ECB) utilizando la clave de encriptación de claves (KEK).

El atributo de longitud de clave efectiva puede especificar una longitud efectiva máxima (p.e., en bits) de las claves generadas en la unidad ONU. El atributo de longitud de clave efectiva puede ser legible, opcional y tener una longitud aproximada de dos bytes.

De forma adicional o alternativa, el atributo de la entidad ME 220 puede comprender una atributo de capacidad de autenticación, un atributo de selección de autenticación de ONU, un atributo de tabla de *nonce* (nombre arbitrario usado una sola vez) de autenticación de ONU, un atributo de estado de nonce de autenticación de ONU, un atributo de tabla de respuesta de autenticación de ONU o una de sus combinaciones. Los atributos de la entidad ME 220 pueden comprender un atributo de selección de autenticación de OLT, un atributo de tabla de números *nonce* de autenticación de OLT, un atributo de tabla de respuesta de autenticación de OLT, un atributo de estado de respuesta de autenticación de OLT, un atributo de capacidad de claves públicas de OLT, un atributo de selección de claves públicas de OLT, un atributo de tabla de claves públicas de OLT, un tabla de claves públicas de OLT o una de sus combinaciones.

El atributo de capacidad de autenticación puede especificar los mecanismos de autenticación disponibles en la unidad ONU y/o los algoritmos de autenticación soportados por la unidad ONU. En una forma de realización, el atributo de capacidad de autenticación puede formatearse como un mapa de bits, en donde algunos o la totalidad de los bits, en el mapa de bits, puede corresponder a un algoritmo de autenticación, a modo de ejemplo, en conformidad con lo indicado en la tabla 3. En consecuencia, un bit puede establecerse a aproximadamente 'uno' para indicar que un algoritmo de autenticación correspondiente es soportado por la unidad ONU o a aproximadamente 'cero' para indicar que el algoritmo de autenticación correspondiente no está soportado por la unidad ONU. El atributo de capacidad de autenticación puede ser legible y tener una longitud aproximada de 16 bytes. En algunos casos, cada bit, en el atributo de capacidad de autenticación, puede establecerse a aproximadamente 'cero' para indicar que ningún algoritmo de autenticación es soportado por la unidad ONU.

Tabla 3

Posición de bits (LSB = 1, MSB = 64)	Algoritmo soportado

0	HA3
1	MD5

El atributo de selección de autenticación de la unidad ONU puede especificar el algoritmo de autenticación a utilizarse durante la función de autenticación de la unidad ONU. A modo de ejemplo, el atributo de selección de autenticación de ONU puede establecerse a un valor que indique un algoritmo de autenticación soportado por la unidad ONU. El valor puede indicar un algoritmo de autenticación que puede ser objeto de listado en el atributo de capacidad de autenticación. El atributo de selección de autenticación de la unidad ONU puede utilizarse para dar instrucciones a la unidad ONU para utilizar el correspondiente algoritmo de autenticación para generar una combinación de huella digital *hash*, p.e., durante la puesta en práctica de la función de autenticación de ONU. El atributo de selección de autenticación de ONU puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte. El atributo de selección de autenticación de ONU puede establecerse también a aproximadamente 'cero' para indicar que ningún algoritmo de autenticación se utiliza en la función de autenticación de la unidad ONU.

El atributo de tabla de números *nonce* de autenticación de ONU puede especificar un número arbitrario usado una sola vez, denominado *nonce*, que se utiliza para la función de autenticación de ONU. El *nonce* puede ser un número aleatorio o pseudo-aleatorio generado para la finalidad de aumentar la seguridad de la función de autenticación de ONU. En una forma de realización, la tabla de números *nonce* de autenticación de ONU puede ser una tabla de datos que comprende N entradas (siendo N un número entero) que pueden determinarse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 25 bytes, en donde el primer byte de cada entrada puede comprender un índice de entradas o un identificador de entrada y los bytes restantes de cada entrada pueden comprender contenidos. Puesto que la tabla de números nonce de autenticación de ONU puede tener un número variable de entradas (p.e., N), la longitud y por lo tanto, la complejidad del nonce puede aumentarse para mejorar la seguridad de la función de autenticación de ONU, si fuere necesario. La tabla de números *nonce* de autenticación de ONU puede ser legible y tener una longitud aproximada de 25xN bytes.

El atributo de estado de *nonce* de autenticación de ONU puede utilizarse para controlar y comunicar el estado del atributo de tabla de *nonce* de autenticación de ONU durante la función de autenticación de ONU. En una forma de realización, el atributo de estado de *nonce* de autenticación de ONU puede establecerse a un primer valor o valor booleano verdadero (p.e., aproximadamente 'uno') cuando la tabla de autenticación de ONU está completa o a un segundo valor o valor booleano falso (p.e., aproximadamente 'cero') cuando la tabla de autenticación de ONU está incompleta. A modo de ejemplo, el terminal OLT puede establecer el estado de *nonce* de autenticación de ONU al valor falso de aproximadamente 'cero' al iniciar el proceso de escritura del número *nonce* para el atributo de tabla de *nonce* de autenticación de ONU y posteriormente, a un valor verdadero de aproximadamente 'uno' al terminar el proceso de escritura del número *nonce* para el atributo de tabla de *nonces* de autenticación de ONU. En una forma de realización, el terminal OLT puede establecer el atributo de estado de *nonce* de autenticación de ONU al valor falso, escribir una pluralidad de entradas en el atributo de tabla de números *nonce* de autenticación de ONU, establecer el atributo de estado de *nonce* de autenticación de ONU al valor verdadero y de este modo, iniciar operativamente la unidad ONU para procesar el atributo de tabla de números *nonce* de autenticación de ONU. El atributo de estado de *nonce* de autenticación de ONU puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte.

El atributo de tabla de respuesta de autenticación de ONU puede especificar una respuesta, p.e., la combinación de la huella digital *hash*, que puede utilizarse en la función de autenticación de ONU. El atributo de tabla de respuesta de autenticación de ONU puede comprender una combinación de huella digital *hash* que se calcula por la unidad ONU. La combinación *hash* puede calcularse procesando el número *nonce*, p.e., los contenidos del atributo de tabla de números *nonce* de autenticación de ONU, utilizando un algoritmo de autenticación que se especifica por el atributo de selección de autenticación de ONU. El terminal OLT puede obtener la combinación de huella digital *hash* mediante la lectura del atributo de tabla de respuesta de autenticación de ONU. El terminal OLT puede autenticar luego la unidad ONU confirmando que la combinación de huella digital *hash* es prácticamente igual al valor de autenticación de ONU. En otra forma de realización, el atributo de tabla de respuesta de autenticación de ONU puede ser una tabla de datos que comprenda M entradas (siendo M un número entero) que puede determinarse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 25 bytes, en donde el primer byte de cada entrada puede comprender un índice de entradas o un identificador de entrada y los bytes restantes de cada entrada pueden comprender contenidos. Puesto que el atributo de tabla de respuesta de autenticación de ONU puede tener un número variable de entradas, la longitud y por lo tanto la complejidad de la combinación de *hash* puede aumentarse para mejorar la seguridad de la función de autenticación de ONU, si fuere necesario. El atributo de tabla de respuesta de autenticación de ONU puede ser legible y tener una longitud aproximada de 25xM bytes.

El atributo de selección de autenticación del terminal OLT puede especificar un mecanismo de autenticación a utilizarse durante la función de autenticación del terminal OLT. En una forma de realización, el atributo de selección de autenticación del terminal OLT puede establecerse a un valor que indique un algoritmo de autenticación soportado por la unidad ONU. El valor puede corresponder a un algoritmo de autenticación listado en el atributo de

capacidad de autenticación. El atributo de selección de autenticación del terminal OLT puede dar instrucciones a la unidad ONU para utilizar un algoritmo de autenticación especificado para generar una combinación de huella digital *hash* durante la función de autenticación del terminal OLT. El atributo de selección de autenticación de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte. El atributo de selección de autenticación del terminal OLT puede establecerse también a aproximadamente 'cero' para indicar que no se utiliza ningún algoritmo de autenticación durante la función de autenticación de OLT.

El atributo de tabla de números *nonce* de autenticación de OLT puede especificar un número *nonce* a utilizase en la función de autenticación del terminal OLT. El número *nonce* puede generarse para mejorar la seguridad de la función de autenticación de OLT. En una forma de realización, la tabla de números *nonce* de autenticación del terminal OLT puede ser una tabla de datos que comprenda P entradas (siendo P un número entero) que puede establecerse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 25 bytes, en donde el primer byte de cada entrada puede comprender un índice de entrada o un identificador de entrada y los bytes restantes de cada entrada pueden comprender contenidos. Puesto que el atributo de tabla de números *nonce* de autenticación de OLT puede tener un número variable de entradas, la longitud y por lo tanto, la complejidad del número *nonce*, puede aumentarse para mejorar la seguridad de la función de autenticación del terminal OLT. El atributo de tabla de números *nonce* de autenticación de ONU puede ser legible y tener una longitud aproximada de 25xP bytes.

El atributo de tabla de respuesta de autenticación del terminal OLT puede especificar la respuesta, p.e., la combinación de huella digital *hash*, a utilizarse en la función de autenticación de OLT. El atributo de tabla de respuesta de autenticación de OLT puede comprender la combinación de *hash* que puede calcularse por el terminal OLT. El terminal OLT puede calcular la combinación de huella digital *hash* procesando el número *nonce* en el atributo de tabla de números *nonce* de autenticación de OLT utilizando el algoritmo de autenticación especificado en el atributo de selección de autenticación de OLT. En consecuencia, la unidad ONU puede leer el atributo de tabla de respuesta de autenticación de OLT para obtener el valor de la combinación de huella digital *hash*. La unidad ONU puede autenticar luego el terminal OLT confirmando que el valor de la combinación de *hash* es prácticamente similar a un valor de autenticación de OLT. En una forma de realización, la tabla de respuesta de autenticación de OLT puede ser una tabla de datos que comprenda Q entradas (siendo Q un número entero) que puede establecerse por un administrador. Cada entrada en la tabla de datos puede tener una longitud fija, p.e., aproximadamente 25 bytes, en donde el primer byte de cada entrada puede comprender un índice de entradas o un identificador de entrada y en donde los bytes restantes de cada entrada pueden comprender contenidos. Puesto que la tabla de respuesta de autenticación de ONU puede tener un número variable de entradas, la longitud y por lo tanto, la complejidad de la combinación de huella digital *hash* puede aumentarse para mejorar la seguridad de la función de autenticación del terminal OLT, si fuere necesario. La tabla de respuesta de autenticación de OLT puede ser legible y tener una longitud aproximada de 25xQ bytes.

El atributo de estado de respuesta de autenticación de OLT puede utilizarse para controlar y/o comunicar el estado del atributo de tabla de respuesta de autenticación de OLT durante la función de autenticación de OLT. En una forma de realización, el atributo de estado de respuesta de autenticación del terminal OLT puede establecerse a un valor booleano verdadero de aproximadamente 'uno' cuando la tabla de autenticación de ONU está completa o a un valor booleano falso de aproximadamente 'cero' cuando la tabla de autenticación ONU no está completa. A modo de ejemplo, el terminal OLT puede establecer a falso el estado de respuesta de autenticación de OLT, p.e., aproximadamente 'cero', a la iniciación del proceso de escritura del número *nonce* para el atributo de tabla de respuesta de autenticación de OLT y posteriormente, a un valor verdadero, p.e., aproximadamente 'uno', al terminar el proceso de escritura del número *nonce* para el atributo de tabla de respuesta de autenticación de OLT. En una forma de realización, el terminal OLT puede establecer el atributo de estado de respuesta de autenticación de OLT a falso, p.e., aproximadamente 'cero', escribir una pluralidad de entradas para el atributo de tabla de respuesta de autenticación de OLT, establecer el atributo de estado de respuesta de autenticación de OLT a un valor verdadero (p.e., aproximadamente 'uno') y de este modo, iniciar operativamente la unidad ONU para procesar el atributo de tabla de respuesta de autenticación de OLT en consecuencia. El atributo de estado de respuesta de autenticación de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte.

El atributo de capacidad de clave pública de OLT puede especificar los mecanismos de claves públicas disponibles en la unidad ONU 200. En una forma de realización, el atributo de capacidad claves públicas de OLT puede formatearse como un mapa de bits, en donde algunos o la totalidad de los bits, en el mapa de bits, pueden corresponder a un algoritmo de claves públicas específico, a modo de ejemplo según se ilustra en la tabla 4. A modo de ejemplo, un bit establecido a aproximadamente 'uno', puede indicar que el algoritmo de claves públicas correspondiente está soportado por la unidad ONU y un bit establecido a aproximadamente 'cero' puede indicar que el algoritmo de claves públicas correspondiente no está soportado por la unidad ONU 200. El atributo de capacidad de claves públicas del terminal OLT puede ser legible y tener una longitud aproximada de 16 bytes. En algunas formas de realización, cada bit en el atributo de capacidad de claves públicas de OLT puede establecerse a aproximadamente 'cero' para indicar que ningún algoritmo de claves públicas se soporta por el terminal OLT 200.

Tabla 3

Posición del bit (LSB = 1, MSB = 64)	Algoritmo soportado
0	Rivest Shamir-Adleman (RSA)
1	Curva elíptica

El atributo de selección de claves públicas de OLT puede especificar el mecanismo de claves públicas a utilizar durante la función de privacidad de claves. En una forma de realización, el atributo de selección de claves públicas de OLT puede establecerse a un valor que indique la presencia de un algoritmo de autenticación soportado por la unidad ONU 200, según se especifica por el atributo de capacidad de claves públicas de OLT. En una forma de realización, el atributo de selección de claves públicas de OLT puede utilizarse para dar instrucciones a la unidad ONU para utilizar el algoritmo de claves públicas especificado para la encriptación de la clave AES durante la función de privacidad de claves. El atributo de selección de claves públicas de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte. En algunas formas de realización, el atributo de selección de claves públicas de OLT puede establecerse a aproximadamente 'cero' para indicar que no se utiliza ningún algoritmo de claves públicas.

El atributo de tabla de claves públicas de OLT puede especificar las claves públicas a utilizarse durante la función de privacidad de claves. En una forma de realización, el terminal OLT puede realizar la escritura de la clave pública para el atributo de tabla de claves públicas de OLT. El atributo de tabla de claves públicas de OLT puede ser una tabla que comprenda R entradas (siendo R un número entero) que puede ser establecida por un administrador. Cada entrada en la tabla puede tener una longitud fija, p.e., aproximadamente 25 bytes, en donde el primer byte de cada entrada puede comprender un índice de entradas o un identificador de entrada y en donde los bytes restantes de cada entrada pueden comprender contenidos. Puesto que el atributo de tabla de claves públicas de OLT puede tener un número variable de entradas, la longitud, y por lo tanto, la complejidad de la clave pública puede aumentarse para mejorar la seguridad de la función de privacidad de claves, cuando fuere necesario. El atributo de tabla de claves públicas de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de 25xR bytes.

El atributo de estado de claves públicas de OLT puede utilizarse para controlar y/o comunicar el estado del atributo de tabla de claves públicas de OLT durante la función de privacidad de claves. En una forma de realización, el atributo de estado de claves públicas de OLT puede establecerse a un valor booleano verdadero, p.e., aproximadamente 'uno', cuando la tabla de claves públicas está completa o a un valor booleano falso, p.e., aproximadamente 'cero', cuando la tabla de claves públicas está incompleta. A modo de ejemplo, el terminal OLT puede establecer a falso el estado de las claves públicas de OLT, p.e., aproximadamente 'cero', al iniciar el proceso de escritura de la clave pública para el atributo de tabla de claves públicas de OLT y posteriormente, establecer a verdadero el estado de claves públicas de OLT, p.e., aproximadamente 'uno', al completar el proceso de escritura de la clave pública para el atributo de tabla de claves públicas de OLT. En otra forma de realización, el terminal OLT puede establecer el atributo de estado de claves públicas de OLT a falso, p.e., aproximadamente 'cero', escribir una pluralidad de entradas para el atributo de tabla de claves públicas de OLT, establecer el atributo de estado de claves públicas de OLT a verdadero, p.e., aproximadamente 'uno' y de este modo, iniciar operativamente la unidad ONU para procesar el atributo de tabla de claves públicas de OLT en consecuencia. El atributo de estado respuesta de autenticación de OLT puede ser legible, susceptible de escritura y tener una longitud aproximada de un byte.

El terminal OLT puede utilizar varias acciones, p.e., tipos de instrucciones, cuando se comunica con la unidad ONU por intermedio del canal OMCI tal como una acción de 'conseguir', una acción de 'conseguir siguiente' y una acción establecida. La acción de 'obtener' puede permitir al terminal OLT efectuar la lectura de uno o más atributos de la entidad OMCI ME en la unidad ONU, la acción de 'conseguir siguiente' puede permitir al terminal OLT la lectura de una cadena o conjunto de atributos de la entidad OMCI ME y la acción establecida puede permitir a la unidad ONU la escritura de uno o más atributos de la entidad OMCI ME.

El terminal OLT puede recibir también una o más notificaciones de OMCI durante las funciones de seguridad. Las notificaciones de OMCI pueden recibirse en la forma de mensajes AVC, que pueden comunicarse por intermedio del canal OMCI. Cada mensaje AVC puede tener un valor numérico, que puede corresponder a un tipo de mensaje diferente, p.e., según se ilustra en la tabla 5A o 5B. A modo de ejemplo, según se ilustra en la tabla 3, un mensaje AVC asociado con el atributo de tabla de reto operativo aleatorio de ONU se le puede asignar un valor de aproximadamente cinco. Un mensaje AVC asociado con el atributo de tabla de resultado de autenticación de ONU se le puede asignar un valor de aproximadamente seis. Un mensaje AVC asociado con el atributo de estado de autenticación de ONU se le puede asignar un valor de aproximadamente 10. Los valores restantes, p.e., desde aproximadamente 'uno' a aproximadamente cuatro, desde aproximadamente siete a aproximadamente nueve y desde aproximadamente once a aproximadamente dieciséis pueden estar reservados.

Tabla 5A

Número	Cambio del valor del atributo	Descripción
1..4	Reservado	
5	Tabla de reto operativo aleatorio de ONU	Un nuevo reto operativo de ONU ha sido cargado en la tabla para el OLT objeto de recuperación
6	Tabla de resultado de autenticación de ONU	Una nueva respuesta de ONU ha sido cargada en la tabla para el terminal OLT a recuperar
7..9	Reservado	
10	Estado de autenticación de ONU	Ha cambiado el estado de autenticación de ONU
11..16	Reservado	

Tabla 5B

Número	Cambio del valor del atributo	Descripción
1..7	No aplicable	
8	Cambio de respuesta de autenticación de ONU	Una nueva respuesta de la unidad ONU se ha cargado en la tabla para el terminal OLT a recuperar
9	Cambio de número *nonce* de autenticación de OLT	Un nuevo número *nonce* de la unidad ONU se ha cargado en la tabla para el terminal OLT a recuperar
10-13	No aplicable	
14..16	Reservado	

En una forma de realización, la entidad ME de control de seguridad mejorada puede comprender una pluralidad de medios para realizar una secuencia de autenticación basada en una huella digital *hash* de tres etapas convencional, p.e., según se describe en la publicación 9798-4 de la Organización de Normalización Internacional (ISO)/Comisión Electrotécnica Internacional (IEC) titulada “Tecnología de la información – técnica de seguridad – autenticación de la entidad – Parte 4: mecanismos que utilizan una función de comprobación criptográfica”. La secuencia de autenticación de tres etapas convencional puede utilizarse en los sistemas DSL que emplean un protocolo MS-CHAPv2 u otros sistemas que puedan utilizar mensajes de obtención y establecidos. La estructura lógica de la secuencia de tres etapas convencional puede comprender mensajes, p.e., mensaje 1, mensaje 2 y mensaje 3, tal como:

Mensaje 1: (Peer 1 → peer 2) my_cryptographic_capabilities | random_challenge_1,

Mensaje 2: (Peer 2 → peer 1): selected_cryptographic_capabilities | random_challenge_2 | MsgHash (PSK, (selected_cryptographic_capabilities | random_challenge_1 | random_challenge_2, peer_1_identity)), y

Mensaje 3: (Peer 1 → peer 2): MsgHash (PSK, (selected_cryptographic_capabilities | random_challenge_2 | random: challenge_1 | peer_2_identity)),

en donde MsgHash () es un función de huella digital *hash* de claves del mensaje, PSK es la clave previamente compartida conocida solamente para los usuarios del mismo nivel de la sesión, Peer_1_identity se establece a aproximadamente 0x0000 0000 0000 0000 y Peer_2_identity es el número de serie de la unidad ONU.

Un requisito previo para utilizar la secuencia de autenticación basada en hash de tres etapas puede ser la disponibilidad de un secreto previamente compartido (PSK). Un PSK de aproximadamente 128 bits puede simplificar la aplicación de algoritmos de seguridad sobre la base de un AES-128 (p.e., AES-CMAC-128). Un PSK puede asociarse con una unidad ONU y puede memorizarse en esa unidad ONU y en la infraestructura del operador. En el lado del operador, el PSK para la unidad ONU puede memorizarse en el terminal OLT que está acoplado a la unidad ONU o en un servidor central al que el terminal OLT puede acceder durante la autenticación. La configuración del PSK en la unidad ONU y en la infraestructura del operador puede realizarse en cualquier manera que satisfaga estos requisitos.

La Figura 3 ilustra una forma de realización de una secuencia de intercambio de mensajes de autenticación 300, que puede establecerse en el terminal OLT y la unidad ONU en el canal OMCI. La secuencia de intercambio de mensajes de autenticación 300 puede proporcionar una seguridad mejorada en sistemas PON, p.e., para transmisiones de flujo ascendente. La secuencia de intercambio de mensajes de autenticación 300 puede comprender varias acciones, que pueden poner en práctica por el terminal OLT para comunicarse con la unidad ONU por intermedio del canal OMCI y para acceder a la entidad ME de control de seguridad mejorada. A modo de

ejemplo, el terminal OLT puede efectuar la escritura de varios atributos de ME de control de seguridad mejorada (p.e., atributos de ME 220) utilizando la acción establecida. El terminal OLT puede realizar múltiples operaciones establecidas, cuando sea necesario, para la escritura de múltiples entradas para uno o más atributos utilizando la acción establecida. El terminal OLT puede efectuar la lectura de varios atributos de ME de control de seguridad mejorada utilizando la función de 'obtener', que puede iniciar operativamente un mensaje de obtener respuesta *get_response* que obtiene los contenidos o parte de los contenidos de uno o más atributos de ME de control de seguridad mejorada. Además, el terminal OLT puede recibir una o más notificaciones de OMCI en la forma de mensajes AVC.

La secuencia de intercambio de mensajes de autenticación 300 puede comenzar en la etapa 302, en donde el terminal OLT puede efectuar la escritura para el atributo de capacidades criptográficas de OLT y/o el atributo de tabla de reto operativo aleatorio de OLT utilizando una acción establecida. En la etapa 304, el terminal OLT puede efectuar la escritura de un valor verdadero, p.e., aproximadamente 'uno', para el atributo de estado de reto operativo de OLT utilizando una acción establecida para indicar la unidad ONU que el atributo de capacidades criptográficas de OLT y/o los atributos de tabla de reto operativo aleatorio de OLT están establecidos. En la etapa 306, el terminal OLT puede recibir de la unidad ONU un mensaje AVC que notifique al terminal OLT que está establecido el atributo de tabla de reto operativo aleatorio de ONU. En la etapa 308, el terminal OLT puede recibir desde la unidad ONU un mensaje AVC que notifica al terminal OLT que está establecido el atributo de tabla de resultado de autenticación de ONU.

En la etapa 310, el terminal OLT puede demandar el atributo de capacidades criptográficas seleccionadas de ONU, el atributo de tabla de reto operativo aleatorio de ONU, el atributo de tabla de resultado de autenticación de ONU o una de sus combinaciones desde la unidad ONU que utiliza una acción de 'obtener'. En la etapa 312, la unidad ONU puede responder al terminal OLT enviando la información demandada utilizando una acción de obtener respuesta get_response. En la etapa 314, el terminal OLT puede efectuar la escritura para el atributo de tabla de resultado de autenticación de OLT utilizando una acción establecida. En la etapa 316, el terminal OLT puede efectuar la escritura de un valor verdadero para el atributo de estado de resultado de OLT utilizando una acción establecida. En la etapa 318, el terminal OLT puede recibir desde la unidad ONU un mensaje AVC que notifique al terminal OLT que está establecido el atributo de estado de autenticación de ONU. En la etapa 320, el terminal OLT puede demandar el atributo de nombre de clave de sesión maestra desde la unidad ONU utilizando una acción de 'obtener'. En la etapa 322, la unidad ONU puede responder al terminal OLT enviando la información demandada utilizando una acción de obtener respuesta get_response. Entonces puede finalizar el intercambio de mensajes de autenticación.

La Figura 4 ilustra una forma de realización de una pluralidad de estados de ONU 400. Los estados de ONU 400 pueden especificarse por una máquina de estados, que puede operar el estado O5 según se define en las normas G.784.3 y G.987.3 de la ITU-T. Inicialmente, en el bloque 410 la unidad ONU puede estar en un estado inactivo (S0), p.e., después del registro de la unidad ONU. El estado S0 puede indicarse por el atributo de autenticación de ONU utilizando un valor de aproximadamente 'cero'. El terminal OLT puede iniciar entonces un proceso de autenticación mediante la escritura de un reto operativo para el atributo de tabla de reto operativo aleatorio de OLT en la entidad OMCI ME en la unidad ONU.

En el bloque 420, el terminal OLT puede introducir un estado pendiente de reto operativo (S1), p.e., después de que el terminal OLT realice la escritura de su reto operativo para el atributo de tabla de reto operativo aleatorio de OLT. El estado pendiente de reto operativo de OLT (S1) puede indicarse por el atributo de estado de autenticación de ONU utilizando un valor de aproximadamente 'uno'. Durante el estado S1, la unidad ONU puede seleccionar el atributo de reto operativo aleatorio de ONU y/o calcular el atributo de tabla de resultado de autenticación de ONU y el terminal OLT puede no efectuar la escritura de un nuevo valor en el atributo de tabla de reto operativo aleatorio de OLT. A continuación, la unidad ONU puede efectuar la transición a un estado pendiente de reto operativo de ONU (S2) después de seleccionar el atributo de reto operativo aleatorio de ONU y/o calcular el atributo de tabla de resultado de autenticación de ONU. Si la unidad ONU es incapaz de realizar las operaciones necesarias para la transición al estado S2, entonces, la unidad ONU puede efectuar la transición a un estado de error de autenticación (S5) en lugar del estado S2.

En el bloque 430, la unidad ONU puede introducir el estado S2 p.e., después de seleccionar el atributo de reto operativo aleatorio de ONU y/o calcular el atributo de tabla de resultado de autenticación de ONU. El estado S2 puede indicarse por el atributo de estado de autenticación de ONU utilizando valor de aproximadamente dos. Durante el estado S2, la unidad ONU puede esperar a que el terminal OLT efectúe la lectura de los atributos/tablas pertinentes, p.e., el atributo de capacidades criptográficas seleccionadas de la ONU, el atributo de tabla de reto operativo aleatorio de ONU, el atributo de tabla de resultado de autenticación de ONU, o una de sus combinaciones, y proceder a la escritura del resultado del reto operativo de autenticación de ONU para el atributo de tabla de resultado de autenticación de OLT. La respuesta del terminal OLT puede estar limitada en el tiempo. A modo de ejemplo, el terminal OLT puede necesitar responder al reto operativo de autenticación de ONU antes de que termine un periodo del temporizador (T1). A modo de ejemplo, T1 puede establecerse para terminar en aproximadamente 3 segundos. Si el terminal OLT deja de responder durante el estado S2 antes de que termine el periodo de T1, la unidad ONU puede efectuar la transición al estado S5. Si el terminal OLT responde antes de que termine el periodo T1, p.e., mediante la escritura del resultado del reto operativo de autenticación de ONU en el atributo de tabla de

resultado de autenticación de ONU, entonces, la unidad ONU puede efectuar la transición a un estado de éxito operativo de autenticación (S3) o a un estado de fallo de la autenticación (S4), dependiendo de si el terminal OLT fue autenticado, de forma satisfactoria o no, por la unidad ONU. Si el resultado es prácticamente el mismo que un valor de autenticación de OLT, entonces, el terminal OLT puede haber sido autenticado satisfactoriamente por la unidad ONU y la unidad ONU puede efectuar la transición al estado S3. Si el resultado no es el mismo que el valor de autenticación de OLT, entonces, el terminal OLT puede no haber sido autenticado de forma satisfactoria y la unidad ONU puede efectuar la transición al estado S4. Mientras la unidad ONU está en el estado S2, el terminal OLT puede no efectuar la escritura de un nuevo valor en el atributo de tabla de reto operativo aleatorio de OLT.

Antes de introducir el estado S3 en el bloque 440, la unidad ONU puede establecer un valor válido para el atributo del nombre de clave de sesión maestra. En el estado S3, el terminal OLT puede efectuar la lectura del atributo de nombre de clave de sesión maestra al recibir un mensaje AVC desde la unidad ONU que indique al terminal OLT que el valor de atributo de estado de autenticación de ONU se ha cambiado al valor de estado S3, p.e., utilizando un valor de aproximadamente tres. La espera para la notificación AVC antes de efectuar la lectura del atributo de nombre de clave de sesión maestra puede permitir al terminal OLT garantizar que la unidad ONU esté sincronizada y la nueva clave está preparada para utilizarse dentro de la función PLOAM de la aparato TC.

El estado de fallo de autenticación S4 en el bloque 450 puede indicarse por el atributo de estado de autenticación de ONU utilizando un valor de aproximadamente cuatro. Durante el estado S4, la unidad ONU y/o el terminal OLT pueden abandonar el presente intento de autenticación. El estado de fallo de autenticación S4 puede significar que el procedimiento de autenticación haya fallado por algún motivo, p.e., debido a una falta de correspondencia de PSK. La unidad ONU puede efectuar la transición desde el estado S4 al estado S0 después de que haya transcurrido un periodo de tiempo predeterminado (T2), p.e., después de aproximadamente un segundo.

El estado S5 puede indicarse por el atributo de estado de autenticación de ONU utilizando un valor de aproximadamente cinco. Durante el estado S5 (bloque 460), la unidad ONU y/o el terminal OLT pueden abandonar el presente intento de autenticación. El estado S5 puede significar que se inició el procedimiento de autenticación pero que no pudo completarse, p.e., debido a un error de comunicación, tal como una pérdida de conexión. La unidad ONU puede efectuar la transición del estado S5 al estado S0 después de que haya transcurrido un periodo de tiempo predeterminado (T3) p.e., después de aproximadamente un segundo.

En una forma de realización, el terminal OLT puede configurarse para la sincronización con una capa TC p.e., en un PLOAM y conseguir otras consideraciones de seguridad, p.e., como en los sistemas G.984. Cuando la unidad ONU está en un estado autenticado, la unidad ONU puede utilizar su clave de sesión maestra para la encriptación de la clave transmitida en un mensaje encryption_key de PLOAM. La clave de sesión maestra puede definirse como:

MasterSessionKey = SelectedHashFunction (PSK, (OLT_random_challenge | ONU random challenge)),

en donde SelectedHashFunction () es la función *hash* seleccionada por la unidad ONU en el atributo de capacidades criptográficas seleccionadas de ONU a partir de una lista suministrada por el terminal OLT.

En algunos casos, la encriptación de la clave de encriptación puede realizarse utilizando una clave AES -128 en el modo ECB. Puesto que la clave de encriptación incluida en el mensaje PLOAM de la clave de encriptación puede no estar protegida contra la intrusión, puede existir una posibilidad de que la clave pueda ser falsificada y reproducida por un intruso. Las claves falsificadas y reproducidas pueden detectarse utilizando mecanismos de sincronización de claves. Sin embargo un ataque de reproducción no autorizada puede forzar al terminal OLT a utilizar una clave de encriptación antigua, que puede violar los requisitos de seguridad de la encriptación de datos de flujo descendente. En consecuencia, un terminal OLT designado para soportar un ataque de reproducción no autorizada puede garantizar que la unidad ONU no envíe una clave de encriptación anteriormente citada entre ciclos de autenticación.

Los componentes de red anteriormente descritos pueden realizarse en cualquier componente de red de uso general, tal como un componente de ordenador o de red con poder de procesamiento suficiente, recursos de memoria y capacidad de rendimiento de la red suficiente para gestionar la carga de trabajo colocada sobre dicho componente. La Figura 5 ilustra un componente de red de uso general típico 500 adecuado para poner en práctica una o más formas de realización de los componentes aquí dados a conocer. El componente de red 500 incluye un procesador 502 (que puede referirse como una unidad de procesador central o CPU) que está en comunicación con los dispositivos de memoria que incluyen una memoria secundaria 504, una memoria de solamente lectura (ROM) 506, una memoria de acceso aleatorio (RAM) 508, dispositivos de entrada/salida (I/O) 510 y dispositivos de conectividad de red 512. El procesador 502 puede ponerse en práctica como uno o más circuitos integrados de la unidad CPU o puede ser parte de uno o más circuitos integrados específicos de la aplicación (ASICs).

La memoria secundaria 504 suele estar constituida por una o más unidades de disco o unidades de cinta y se utiliza para la memorización no volátil de datos y como un dispositivo de memorización de datos de sobreflujo si la memoria RAM 508 no tiene suficiente capacidad para mantener todos los datos de servicio. La memoria secundaria 504 puede utilizarse para memorizar programas que se cargan en la memoria RAM 508 cuando dichos programas se seleccionan para su ejecución. La memoria ROM 506 se utiliza para memorizar instrucciones y quizás datos que

son objeto de lectura durante la ejecución del programa. La memoria ROM 506 es un dispositivo de memoria no volátil que suele tener una pequeña capacidad de memoria relativa a la capacidad de memoria mayor de la memoria secundaria 504. La memoria RAM 508 se utiliza para memorizar datos volátiles y quizás para memorizar instrucciones. El acceso a ambas memorias ROM 506 y RAM 508 suele ser más rápido que para la memoria secundaria 504.

Al menos una forma de realización se da a conocer y las variaciones, combinaciones y/o modificaciones de las formas de realización y/o características de las formas de realización realizadas por un experto en esta técnica están dentro del alcance de protección de la invención. Formas de realización alternativas que resultan de la combinación, integración y/o omisión de características de las formas de realización están también dentro del alcance de protección de la invención. En donde márgenes numéricos o limitaciones están expresamente establecidos, dichos márgenes expresos o limitaciones deben entenderse para incluir márgenes iterativos o limitaciones de magnitud semejante que caigan dentro de los márgenes expresamente establecidos o sus limitaciones (p.e., desde aproximadamente 1 a aproximadamente 10 incluye 2, 3, 4, etc.; mayor que 0.10 incluye 0.11, 0.12, 0.13, etc.). A modo de ejemplo, cuando se da a conocer un margen numérico con un límite inferior R_1 y un límite superior R_u cualquier número que caiga dentro del margen se da a conocer concretamente. En particular, los siguientes números dentro del margen son dados a conocer concretamente: $R = R_1 + k * (R_u – R_1)$, en donde k es una variable que varía desde 1 por ciento a 100 por ciento dentro de un incremento porcentual, esto es, k es 1 por ciento, 2 por ciento, 3 por ciento, 4 por ciento, 5 por ciento,… 50 por ciento, 51 por ciento, 52 por ciento, …, 95 por ciento, 96 por ciento, 97 por ciento, 98 por ciento, 99 por ciento o 100 por ciento. Además, cualquier margen numérico definido por dos números R según se define con anterioridad se da a conocer también concretamente. El uso del término “opcionalmente” con respecto a cualquier elemento de una reivindicación significa que el elemento es requerido o de forma alternativa, el elemento no es requerido, estando ambas alternativas dentro del alcance de protección de la reivindicación. El uso de términos más amplios tales como ‘comprende’, ‘incluye’ y ‘que tiene’ deben entenderse que proporcionan soporte para términos más restringidos tales como ‘consiste’, ‘consiste esencialmente’ y ‘consiste esencialmente de’. En consecuencia, el alcance de protección no está limitado por la descripción anteriormente establecida, sino que se define por las reivindicaciones siguientes, cuyo alcance incluye todos los equivalentes del contenido de las reivindicaciones. Todas y cada una de las reivindicaciones está incorporada como una idea inventiva adicional en la especificación y las reivindicaciones son formas de realización de la presente invención. La discusión de una referencia en la idea inventiva no es una admisión de que es una técnica anterior, en particular cualquier referencia que tenga una fecha de publicación posterior a la fecha de prioridad de esta solicitud de patente.

Aunque varias formas de realización han sido dadas a conocer en la presente invención, debe entenderse que los sistemas y métodos dados a conocer podrían materializarse en muchas otras formas específicas sin desviarse por ello del alcance de protección de la presente invención. Las presentes realizaciones, a modo de ejemplo, han de considerarse como ilustrativas y no restrictivas y la intención no ha de ser limitarse a los detalles aquí proporcionados. A modo de ejemplo, los diversos elementos o componentes pueden combinarse o integrarse en otro sistema o se pueden omitir algunas características o no ponerse en práctica.

Además, técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diversas formas de realización, como discretos o separados, pueden combinarse o integrarse con otros sistemas, módulos, técnicas o métodos sin desviarse por ello del alcance de protección de la presente invención. Otros elementos ilustrados o examinados como acoplados o evidentemente acoplados o en comunicación entre sí pueden acoplarse indirectamente o comunicarse a través de alguna interfaz, dispositivo o componente inmediato, bien sea de tipo eléctrico, mecánico o de cualquier otro. Otras realizaciones, a modo de ejemplo, de cambios, sustituciones y alteraciones son discernibles por un experto en esta técnica y podrían realizarse sin desviarse por ello del alcance de protección aquí dado a conocer.

REIVINDICACIONES

1. Un aparato que comprende:

un terminal de línea óptica, OLT (110), configurado para leer y/o escribir una interfaz de control de gestión de unidad ONU, OMCI, una entidad de gestión, ME en una unidad de red óptica, ONU (120, 200);

en donde la entidad OMCI ME comprende una pluralidad de atributos que soportan una pluralidad de características de seguridad para transmisiones en sentido ascendente entre la unidad ONU y el terminal OLT, en donde los atributos comprenden un atributo de tabla de respuesta de autenticación de terminal OLT para especificar una respuesta a utilizarse en una función de autenticación de terminal OLT, un atributo de estado de respuesta de autenticación de terminal OLT que permite controlar y comunicar el estado del atributo de tabla de respuesta de autenticación de terminal OLT durante la función de autenticación de terminal OLT; en donde el valor falso del atributo de estado de respuesta de autenticación del terminal OLT indica que el atributo de tabla de respuesta de autenticación de terminal OLT no está completo, el valor verdadero del atributo de estado de respuesta de autenticación de terminal OLT indica que el atributo de tabla de respuesta de autenticación de terminal OLT está completo; y

en donde los atributos se comunican por intermedio de un canal de interfaz OMCI entre la unidad ONU (120, 200) y el terminal OLT (110) y proporciona las características de seguridad para la unidad ONU (120, 200) y para el terminal OLT (110).

2. El aparato según la reivindicación 1, en donde los atributos comprenden un atributo de identificador ID, de entidad ME, de aproximadamente dos bytes que identifican una instancia operativa de la entidad ME.

3. Un método que comprende:

intercambiar, mediante una unidad de red óptica, ONU (120, 200) una pluralidad de atributos de seguridad con un terminal de línea óptica, OLT (110), utilizando un canal OMCI de interfaz de control de gestión de unidad ONU, lo que proporciona una pluralidad de características de seguridad para comunicaciones en sentido ascendente a partir de la unidad ONU (120, 200), en donde los atributos comprenden un atributo de tabla de respuesta de autenticación de terminal OLT para especificar una respuesta a utilizarse en una función de autenticación de terminal OLT, un atributo de estado de respuesta de autenticación de terminal OLT para controlar y comunicar el estado del atributo de tabla de respuesta de autenticación de terminal OLT, en donde el valor falso del atributo de estado de respuesta de autenticación de terminal OLT indica que el atributo de tabla de respuesta de autenticación del terminal OLT no está completo, indicando el valor verdadero del atributo de estado de respuesta de autenticación del terminal OLT que el atributo de tabla de respuesta de autenticación de terminal OLT está completo.

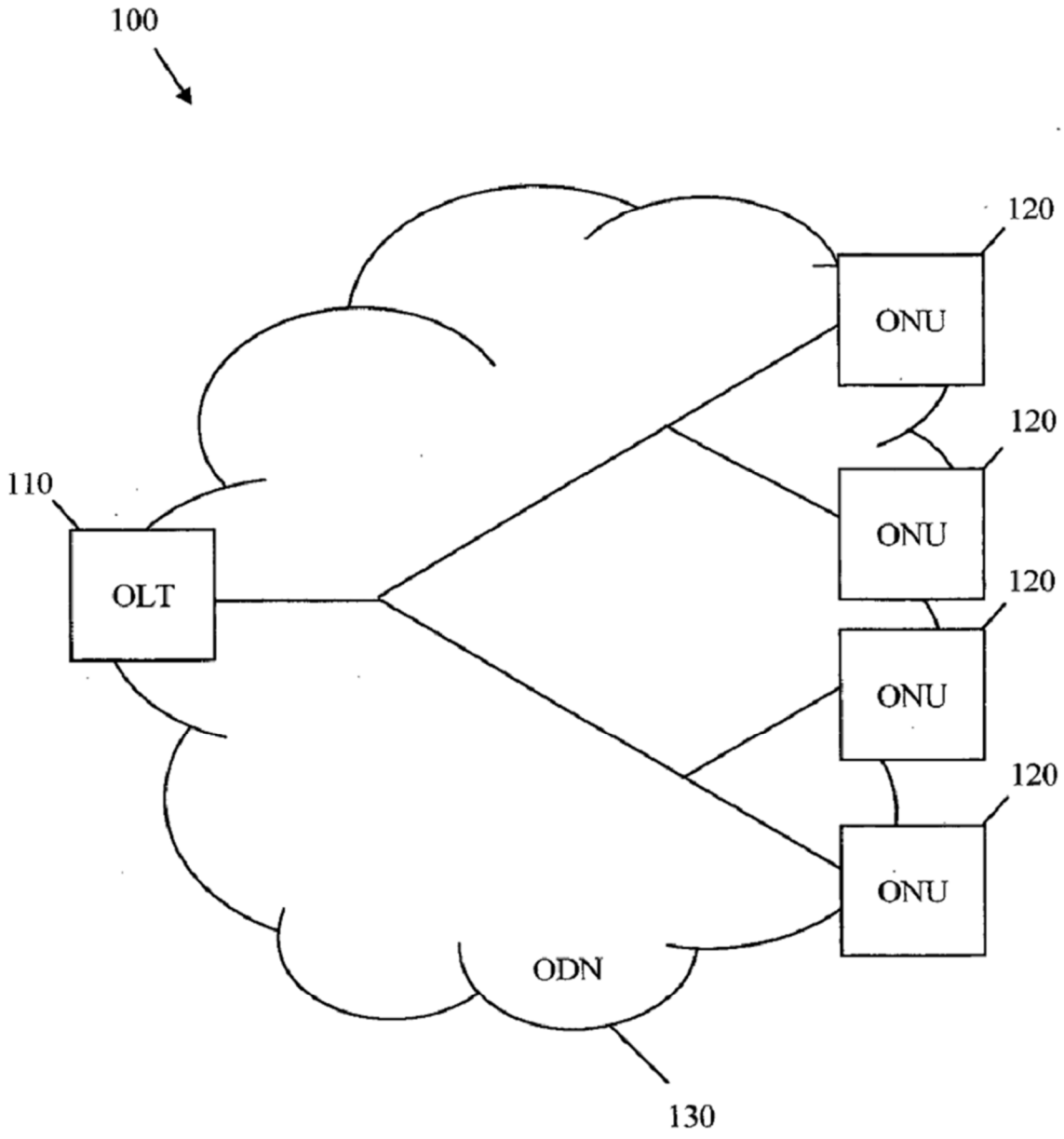

FIG. 1

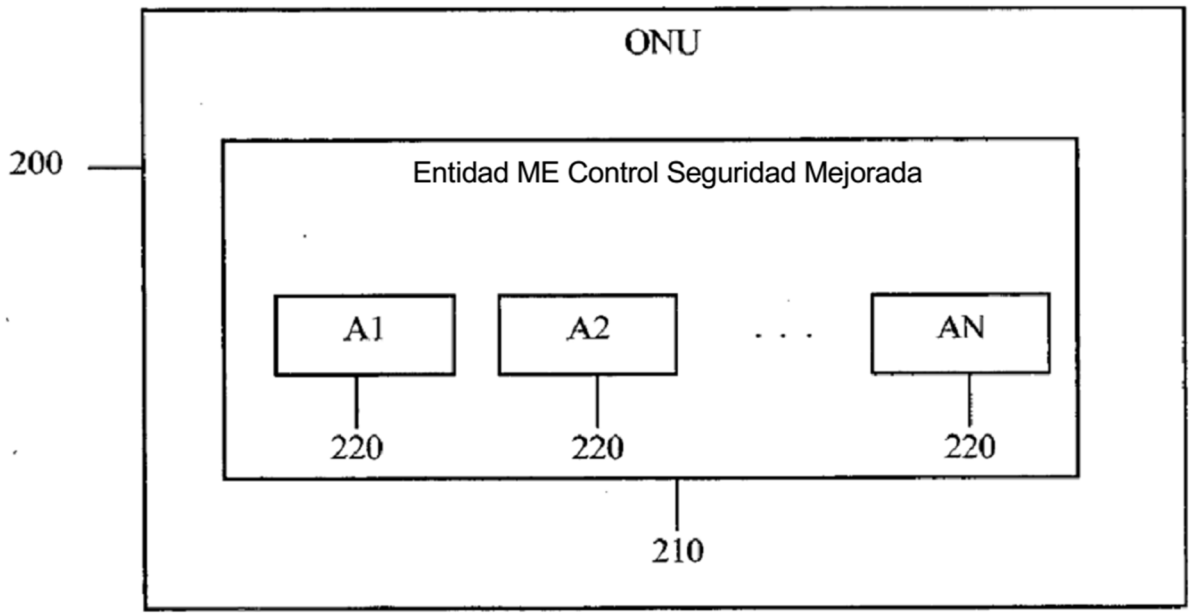
ONU
200
Entidad ME Control Seguridad Mejorada
A1
A2
. . .
AN
220
220
220
210

FIG. 2

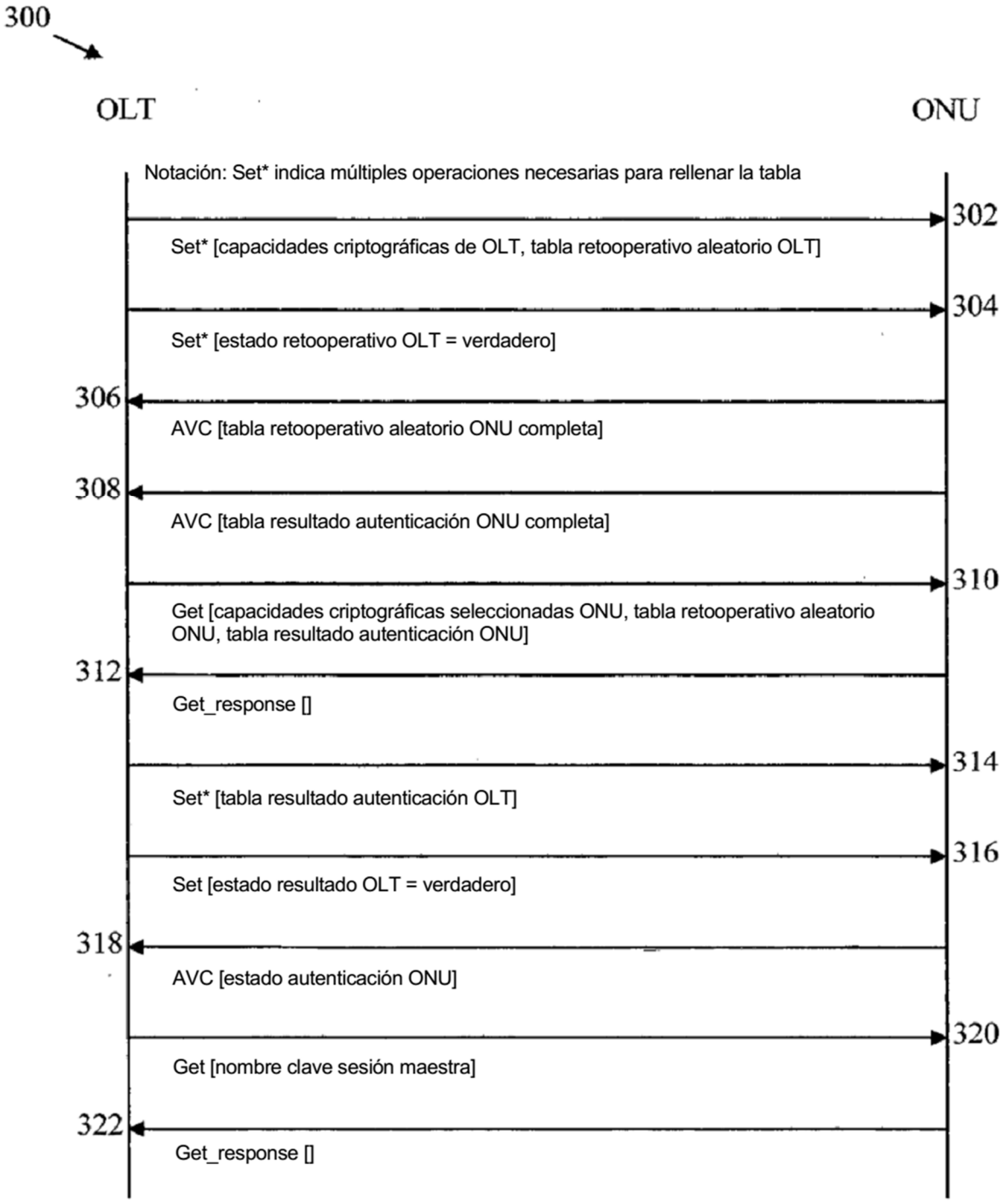
300
OLT
ONU
Notación: Set* indica múltiples operaciones necesarias para rellenar la tabla
302
Set* [capacidades criptográficas de OLT, tabla retooperativo aleatorio OLT]
304
Set* [estado retooperativo OLT = verdadero]
306
AVC [tabla retooperativo aleatorio ONU completa]
308
AVC [tabla resultado autenticación ONU completa]
310
Get [capacidades criptográficas seleccionadas ONU, tabla retooperativo aleatorio ONU, tabla resultado autenticación ONU]
312
Get_response []
314
Set* [tabla resultado autenticación OLT]
316
Set [estado resultado OLT = verdadero]
318
AVC [estado autenticación ONU]
320
Get [nombre clave sesión maestra]
322
Get_response []

FIG. 3

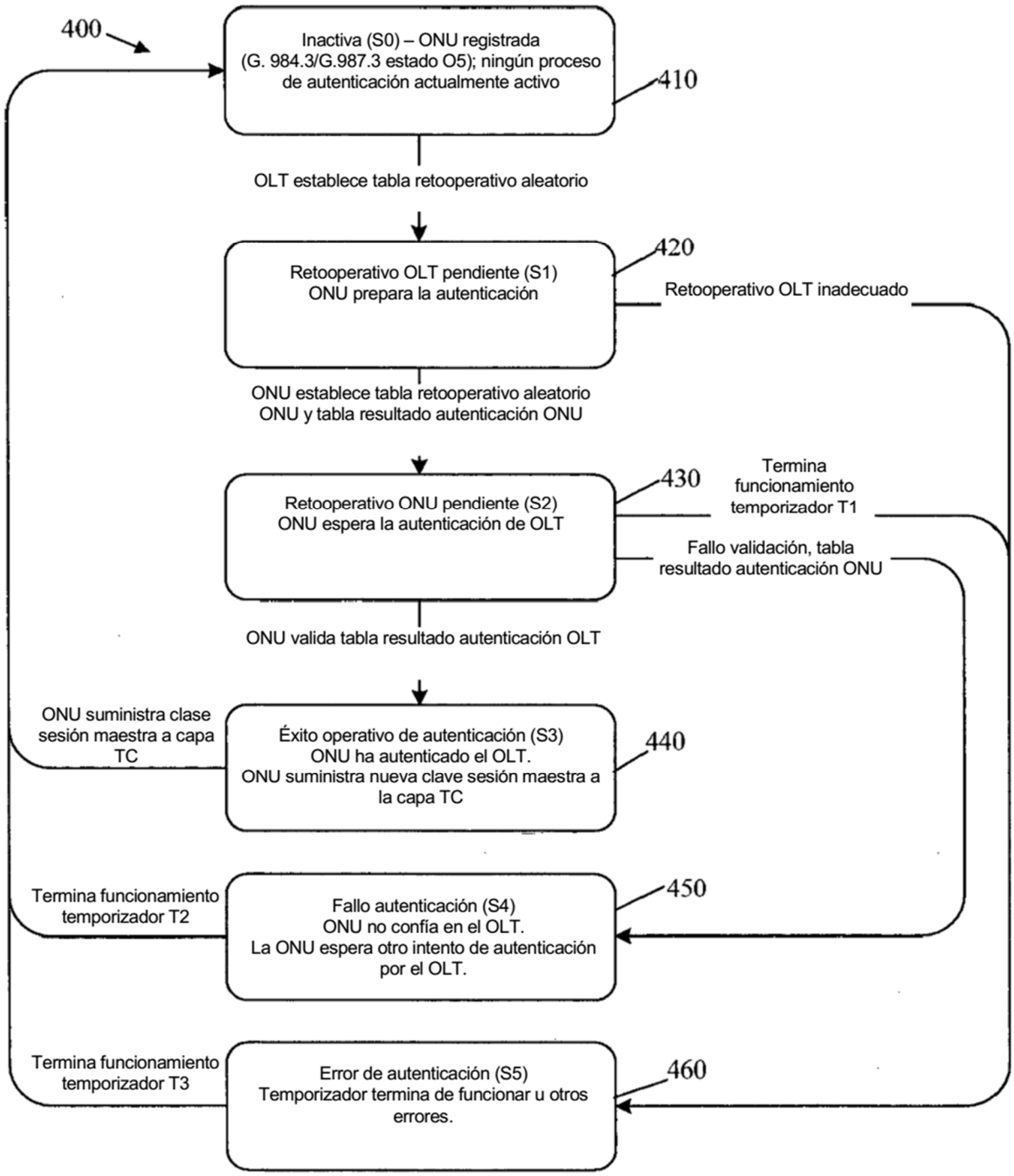
400
Inactiva (S0) – ONU registrada (G. 984.3/G.987.3 estado O5); ningún proceso de autenticación actualmente activo
410
OLT establece tabla retooperativo aleatorio
Retooperativo OLT pendiente (S1) ONU prepara la autenticación
420
Retooperativo OLT inadecuado
ONU establece tabla retooperativo aleatorio ONU y tabla resultado autenticación ONU
Retooperativo ONU pendiente (S2) ONU espera la autenticación de OLT
430
Termina funcionamiento temporizador T1
Fallo validación, tabla resultado autenticación ONU
ONU valida tabla resultado autenticación OLT
ONU suministra clase sesión maestra a capa TC
Éxito operativo de autenticación (S3) ONU ha autenticado el OLT. ONU suministra nueva clave sesión maestra a la capa TC
440
Termina funcionamiento temporizador T2
Fallo autenticación (S4) ONU no confía en el OLT. La ONU espera otro intento de autenticación por el OLT.
450
Termina funcionamiento temporizador T3
Error de autenticación (S5) Temporizador termina de funcionar u otros errores.
460

FIG. 4

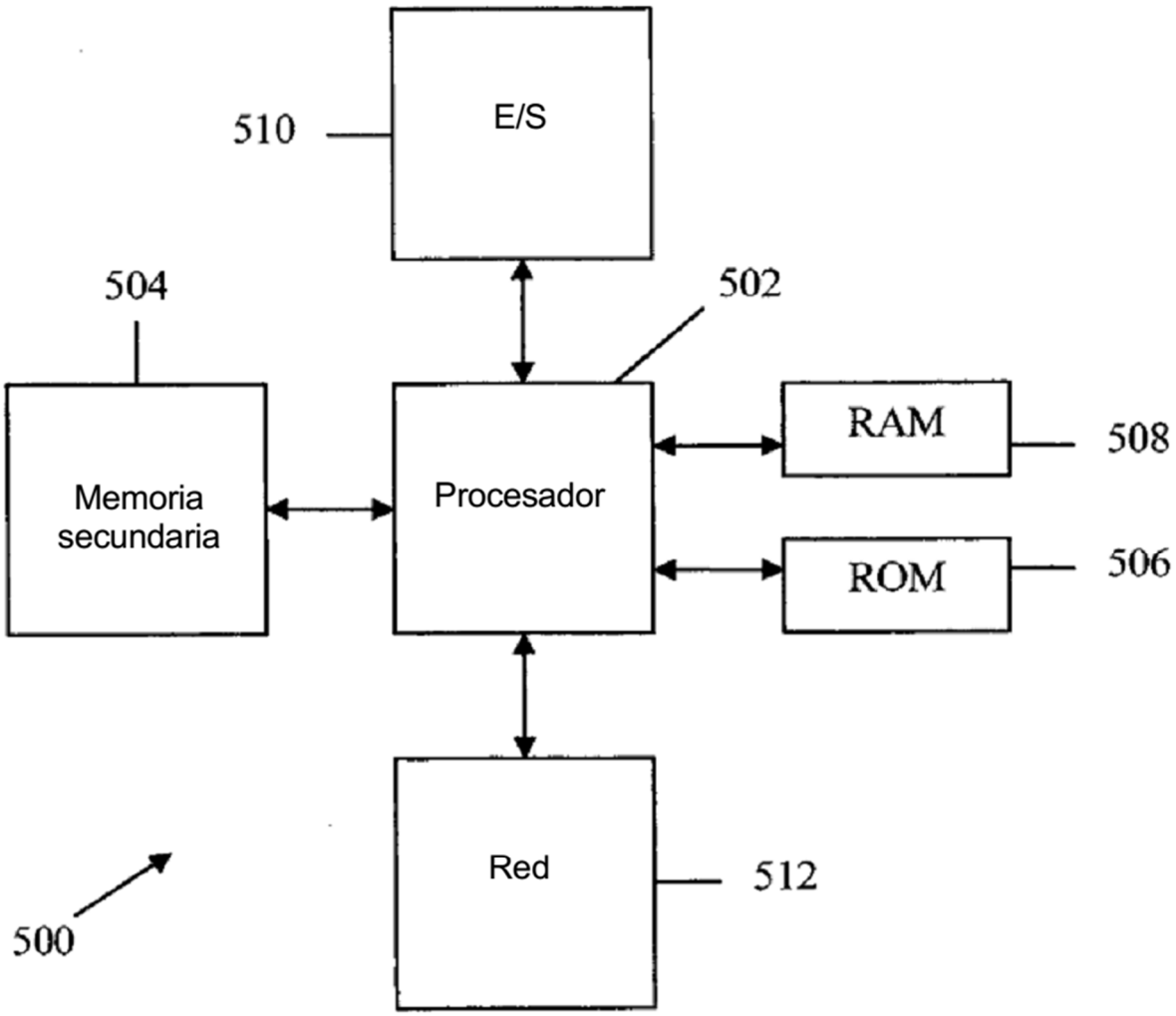
510
E/S
504
502
Memoria secundaria
Procesador
RAM
508
ROM
506
Red
512
500

FIG. 5