Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1362

(03/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad – Seguridad en la Internet de las cosas (IoT)

Procedimiento de encriptación simple para la Internet de las cosas (IoT)

Recomendación UIT-T X.1362

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	**X.1360–X.1369**
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1379
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1362

Procedimiento de encriptación simple para la Internet de las cosas (IoT)

Resumen

La Internet de las cosas (IoT) se considera unas de las esferas más significativas en materia de normalización futura. Desde el punto de vista del UIT-T, la IoT se define como una infraestructura mundial para la sociedad de la información que permite prestar servicios avanzados mediante la interconexión de objetos (tanto físicos como virtuales).

En determinados casos, en particular en lo concerniente a los dispositivos IoT, es necesario llevar a cabo el procesamiento de tareas en tiempo real en un periodo de tiempo determinado. Con objeto de velar por la confidencialidad y protección integral de los datos, una de las contramedidas fundamentales es la aplicación de algoritmos de encriptación o autentificación de datos. Las aplicaciones normales de los algoritmos de encriptación o autenticación de datos presentan la dificultad de no satisfacer ese requisito.

La Recomendación UIT-T X.1362 tiene como objetivo especificar la encriptación con datos de máscara asociados (EAMD) para los dispositivos de la Internet de las cosas. Además, describe la EAMD y el modo en que ésta proporciona una serie de servicios de seguridad a los efectos de tráfico de datos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1362	2017-03-30	17	11.1002/1000/13196

Palabras clave

Aplicación de algoritmos de encriptación/autenticación de datos, dispositivos IoT, encriptación con datos de máscara asociados (EAMD), entornos IoT, requisito de procesamiento en tiempo real.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

La Internet de las cosas (IoT) se considera unas de las esferas más significativas en materia de normalización futura. Desde el punto de vista del UIT-T, la IoT se define en [b-UIT-T Y.2060] como una infraestructura mundial para la sociedad de la información que permite prestar servicios avanzados mediante la interconexión de objetos (tanto físicos como virtuales) sobre la base de tecnologías de la información y comunicación compatibles existentes o en fase de desarrollo.

Las redes de sensores ubicuos (USN) constituyen uno de los aspectos más importantes de la IoT. Las USN son redes de nodos de sensores inteligentes que pueden desplegarse "en cualquier lugar y en cualquier momento por cualquier persona o cosa". Las técnicas de seguridad para redes de sensores ubicuos se consideran eficaces en la IoT, habida cuenta de las numerosas afinidades de dichas redes con la IoT con respecto a la utilización de dispositivos de detección y accionamiento. En lo concerniente a la seguridad de las USN, se han publicado varias Recomendaciones, en particular las siguientes: Marco de seguridad para red de sensores ubicuos [b-UIT-T X.1311], Directrices de programa intermedio de seguridad para redes de sensores ubicuos [b-UIT-T X.1312] y Requisitos de seguridad para el encaminamiento en la red de sensores inalámbrica [b-UIT-T X.1313]. No obstante, no se han estudiado Recomendaciones sobre confidencialidad y técnicas de protección de la integralidad de los datos para proporcionar seguridad en las USN a nivel de capa de dispositivos. En consecuencia, la seguridad de la capa de dispositivos constituye una esfera no tenida en cuenta en las USN o en la IoT, por lo que se debería estudiar y debatir dicha esfera a los efectos de normalización futura.

Por otro lado, en determinados casos, en particular en lo concerniente a los dispositivos IoT de detección y accionamiento que pueden utilizarse en sistemas de control industrial, es necesario llevar a cabo el procesamiento de tareas en tiempo real en un periodo de tiempo determinado. Con objeto de velar por la confidencialidad y protección integral de los datos, una de las contramedidas fundamentales es la aplicación de algoritmos de encriptación o autentificación de datos. Las aplicaciones normales de los algoritmos de encriptación o autenticación de datos presentan la dificultad de no satisfacer ese requisito. Otra dificultad añadida es la integración de diversos niveles de seguridad. En particular, en un paquete de comunicación, el correspondiente nivel de seguridad que requieren los datos difiere en función de su posición. De ahí que la encriptación de datos respeto de una posición que denote un bajo nivel de seguridad se considere una tara de procesamiento innecesaria.

Como se ha mencionado anteriormente, a fin de lograr la seguridad necesaria en la IoT, especialmente en dispositivos IoT, se requiere una nueva aplicación para los algoritmos de encriptación/autentificación de datos que satisfaga el requisito de procesamiento en tiempo real e integre distintos niveles de seguridad.

En consecuencia, la encriptación con datos de máscara asociados únicamente encripta los datos de un paquete de comunicación que requiera un nivel de seguridad elevado. Los datos de máscara asociados se utilizan para indicar el nivel de seguridad de los datos en cada posición de un paquete

Recomendación UIT-T X.1362

Procedimiento de encriptación simple para la Internet de las cosas (IoT)

1 Alcance

En la presente Recomendación se proporciona un procedimiento de encriptación relativo a la seguridad de los dispositivos de la Internet de las cosas. Dicho procedimiento es aplicable a la IoT, en particular a dispositivos IoT con capacidad obligatoria de comunicación y capacidad opcional de detección, accionamiento y almacenamiento y procesamiento de datos. En esta Recomendación se especifica la encriptación con datos de máscara asociados (EAMD) para la IoT. También se describe la EAMD y el modo en que ésta proporciona una serie de servicios de seguridad a los efectos de tráfico de datos. En el Anexo A figuran varios ejemplos de aplicación.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[IETF RFC 7296] IETF RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2).*

[IETF RFC 7321] IETF RFC 7321 (2014), *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[ISO/IEC 10116] ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher.*

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

En esta Recomendación se utilizan los siguientes términos definidos en otras Recomendaciones:

3.1.1 accionador [b-UIT-T Y.4109]: Dispositivo que activa una acción física tras recibir el estímulo de una señal de entrada.

NOTA – A título de ejemplo, un accionador puede actuar sobre el flujo de un gas o de un líquido, la distribución de energía eléctrica o una operación mecánica. Los reguladores y los relés son ejemplos de accionadores. La decisión de activar el accionador puede proceder de una aplicación MOC, de un ser humano o de dispositivos y pasarelas MOC.

3.1.2 cabida útil de seguridad de encapsulado (ESP) [IETF RFC 4303]: Protocolo IPsec utilizado para proporcionar confidencialidad, autentificación del origen de los datos, integridad sin conexión, servicio anti-reproducción (un modo de integridad secuencial fraccional) y confidencialidad de flujo de tráfico (de forma limitada). El conjunto de servicios proporcionado depende de las opciones escogidas al establecerse la asociación de seguridad (SA) y de la localización de la implantación en la topología de la red.

3.1.3 índice de parámetros de seguridad (SPI) [b-IETF RFC 4301]: Valor arbitrario de 32 bits utilizado por un receptor para identificar la SA a la que ha de vincularse un paquete entrante.

3.1.4 datos detectados [b-UIT-T F.4104]: Datos detectados por un sensor conectado a un nodo de sensor específico.

3.1.5 sensor [b-UIT-T Y.4105]: Dispositivo electrónico que detecta una condición física o un componente químico y entrega una señal electrónica proporcional a la característica observada.

3.1.6 número de secuencia [IETF RFC 4303]: Campo de 32 bits sin signo que contiene el valor de un contador que aumenta una unidad por cada paquete enviado, es decir, un número de secuencia de paquete por cada SA.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 controlador programable: Dispositivo electrónico para controlar los accionadores sobre la base de los datos detectados por los sensores.

3.2.2 asociación de seguridad con máscara (SAM): Conjunto de parámetros específicos del protocolo de seguridad. La SAM permite definir los servicios y mecanismos necesarios para la protección del tráfico mediante encriptación con datos de máscara asociados (EAMD). La SAM guarda relación con su protocolo asociado, dependiendo de las capas de protocolo tales como la capa de transporte o la capa del protocolo Internet (IP). Dichos parámetros pueden incluir los identificadores y modos de algoritmos y los identificadores de capa a los que se aplica la EAMD, así como las claves criptográficas.

4 Abreviaturas y acrónimos

Esta Recomendación hace uso de las siguientes abreviaturas y acrónimos:

AES	Norma de encriptación avanzada (*advanced encryption standard*)
CBC	Concatenación de bloques cifrados (*cipher block chaining*)
CMAC	Código cifrado de autenticación de mensaje (*cipher-based message authentication code*)
EAMD	Encriptación con datos de máscara asociados (*encryption with associated mask data*)
EAMDSP	Cabida útil de seguridad EAMD (EAMD *security payload*)
ESP	Cabida útil de seguridad de encapsulado (*encapsulating security payload*)
ICS	Sistema de control industrial (*industrial control system*)
IP	Protocolo Internet
IPSec	Seguridad IP
IoT	Internet de las cosas (*Internet of things*)
IV	Vector de inicialización (*initialization vector*)
MAC	Código de autenticación de mensaje (*message authentication code*)
SA	Asociación de seguridad (*security association*)
SAM	Asociación de seguridad con máscara (*security association with mask*)
SAMD	Base de datos de la SAM (SAM *database*)
SPI	Índice de parámetros de seguridad (*security parameters index*)
TCP	Protocolo de control de transmisión (*transmission control protocol*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

USN Redes de sensores ubicuos (*ubiquitous sensor networks*)

XOR O exclusivo (*exclusive* OR)

5 Convenios

Ninguno.

6 Introducción a la encriptación con datos de máscara asociados (EAMD)

6.1 Especificación del procedimiento EAMD

Existe una gran variedad de amenazas para la seguridad de la IoT [b-ZT]. La presente Recomendación hace hincapié en las amenazas enumeradas a continuación:

1) Ataques por suplantación de identidad que interceptan datos legítimos o datos legítimos falsos y tienen como consecuencia la divulgación o alteración indebida de la información.

2) Ataques por escucha indiscreta que capturan paquetes de la red transmitidos por computadores de terceros y que permiten leer el contenido de los datos para obtener información confidencial de índole diversa.

3) Ataques pirata encubiertos en forma de componentes legítimos para alterar indebidamente datos o información.

Con objeto de mitigar esas amenazas en la IoT, en particular para los dispositivos IoT, en la presente Recomendación se especifica la encriptación con datos de máscara asociados (EAMD) que permite llevar a cabo operaciones criptográficas de forma fraccionada en paquetes de comunicaciones ordinarios transmitidos entre varios dispositivos. Las operaciones criptográficas abarcan la encriptación/desencriptación y la generación/verificación del código de autenticación de mensaje (MAC), así como la encriptación autentificada. Los algoritmos criptográficos utilizados en la EAMD quedan fuera del alcance de esta Recomendación, si bien las referencias [b-ISO/CEI 9797], [b-ISO/CEI 18033] y [b-ISO/CEI 19772] son útiles para los algoritmos de encriptación, los algoritmos MAC y los algoritmos de encriptación autentificada, respectivamente.

Cabe señalar que la construcción descrita en esta cláusula puede considerarse un protocolo que utiliza encriptación previa al MAC [b-ASIACRYPT] y [b-EUROCRYPT].

En el paquete de comunicaciones, los bloques de datos en los que se realizan operaciones criptográficas se indican mediante una máscara.

Se realiza la hipótesis de que el emisor conoce el algoritmo de encriptación, la clave, el vector inicial y la máscara relativos a la comunicación segura EAMD, y de que el emisor y el receptor conocen el identificador del algoritmo y la clave de ambos. Habida cuenta de ello, la comunicación segura EAMD se basa en la obtención de información de encriptación con datos de máscara asociados en el extremo del emisor y la compartición de información de encriptación con el receptor. En la Figura 1 se muestra una visión general de la encriptación con datos de máscara asociados.

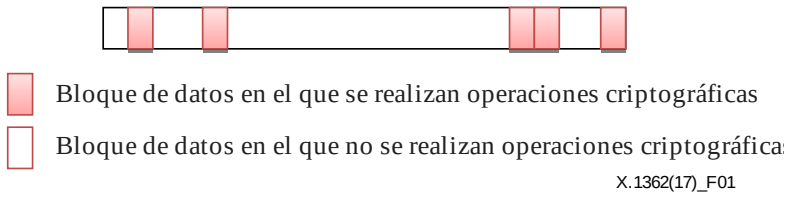

Figura 1 – Paquete transmitido a través de una comunicación mediante encriptación con datos de máscara asociados

En una comunicación segura EAMD, el procesamiento de salida se realiza mediante:

1) La adición de los datos de relleno necesarios para la encriptación.
2) La extracción de los datos de encriptación mediante la máscara de encriptación y su copia en la memoria intermedia, utilizada a los efectos de cómputo temporal.
3) La encriptación del resultado en la memoria intermedia por medio de la clave y el algoritmo de encriptación, entre otros datos necesarios.
4) La sustitución del resultado en el paquete que utiliza la máscara.
5) La encapsulación del resultado en el campo de cabida útil.

Si se ha escogido integridad, el procesamiento tendrá lugar mediante[1]:

6) La extracción de datos para la generación del MAC mediante la máscara prevista a tal efecto y su copia en la memoria intermedia.
7) La incorporación de los datos de relleno necesarios para la generación del MAC.
8) La generación del MAC respecto del resultado en la memoria intermedia.
9) La incorporación del MAC en el paquete.

En la Figura 2 se muestra el procesamiento de salida.

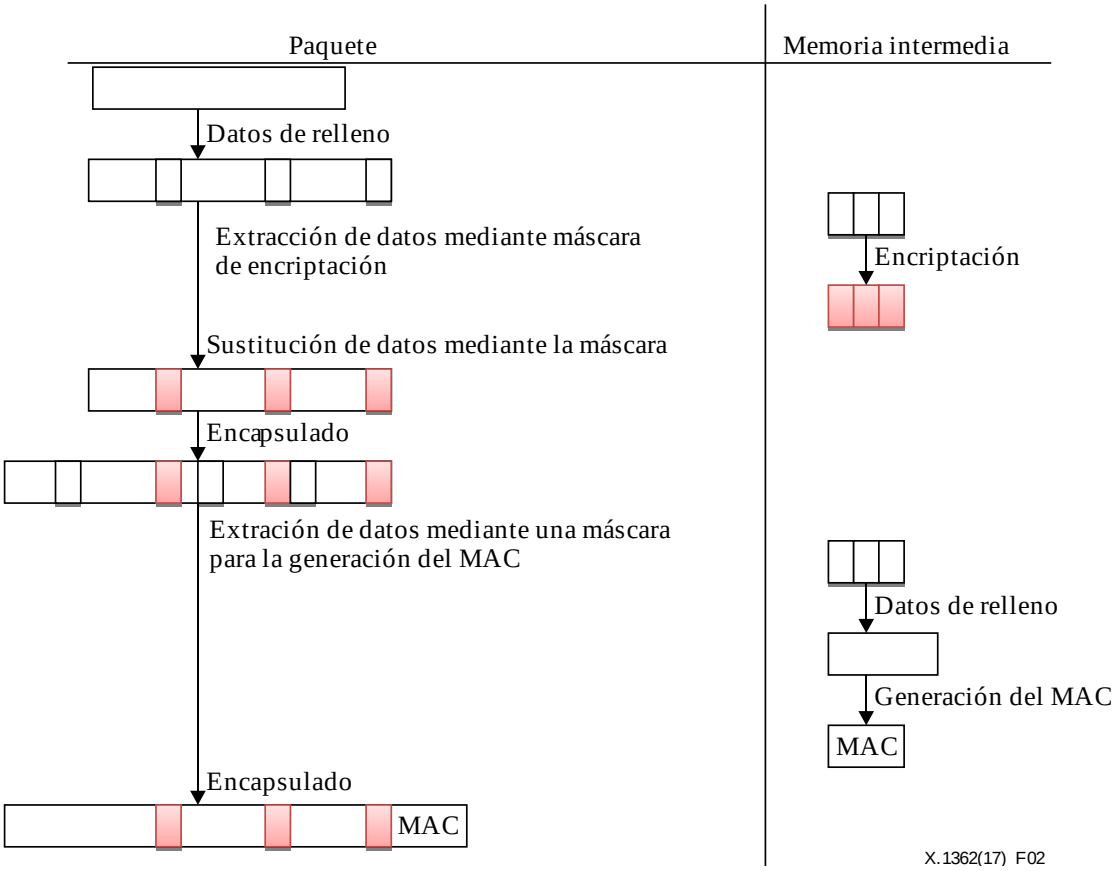

Figura 2 – Generación de un paquete mediante encriptación con datos de máscara asociados durante el procesamiento de salida

[1] A fin de recurrir a la encriptación con vinculación entre los datos de máscara asociados y el protocolo IPsec, cabe garantizar la confidencialidad por medio de la autenticación.

En una comunicación segura EAMD, el procesamiento de entrada se realiza del modo siguiente:

Si se ha escogido integridad, cabe observar las etapas 1 a 3 siguientes[1]:

1) Extracción de los datos del paquete excepto el MAC en la memoria intermedia, con arreglo a la máscara de generación del MAC.
2) Incorporación de los datos de relleno necesarios para la generación del MAC.
3) Cómputo del MAC respecto de los datos de relleno mediante el algoritmo de integridad especificado y comprobación de que se trata del MAC transportado en el paquete. Si el MAC computado y el MAC recibido coinciden el paquete será válido y se aceptará. Si el resultado de la prueba es negativo el receptor descartará el paquete recibido y lo considerará no válido.
4) Supresión del encabezamiento del paquete.
5) Extracción de los datos relativos al resultado para incorporarlos a la memoria intermedia con arreglo a la máscara de desencriptación.
6) Desencriptación de los datos extraídos relativos al resultado para incorporarlo a la memoria intermedia.
7) Sustitución de los datos relativos al resultado en la memoria intermedia para incorporarlos al paquete que utiliza la máscara de desencriptación.
8) Supresión en el paquete de los datos de relleno para la encriptación.

En la Figura 3 se muestra el procesamiento de entrada.

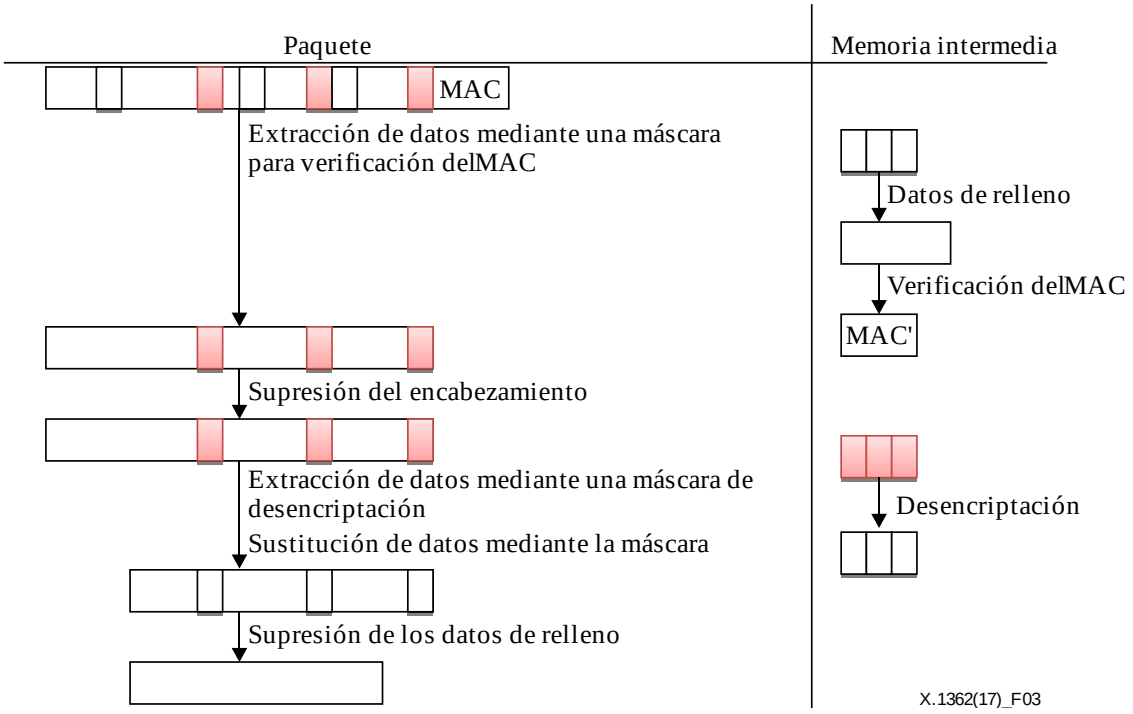

Figura 3 – Generación de un paquete mediante encriptación con datos de máscara asociados durante el procesamiento de entrada

6.2 Máscara de extracción de datos objetivo para la encriptación con datos de máscara asociados

En las operaciones de encriptación con datos de máscara asociados los datos objetivo del bloque de entrada al algoritmo correspondiente se extraen dividiendo el paquete con arreglo al tamaño del bloque que utiliza el algoritmo de encriptación, según el parámetro de la máscara.

7 Encriptación con datos de máscara asociados

Mediante la presente cláusula se describe la forma de proporcionar un conjunto de servicios de seguridad para el tráfico de cada capa. Esta Recomendación permite definir una comunicación segura mediante encriptación con datos de máscara asociados basada en la cabida útil de seguridad EAMD (EAMDSP). En la Figura 4 se muestra una visión general de este tipo de comunicación. El flujo de comunicación segura de la EAMD se describe pormenorizadamente de la forma siguiente:

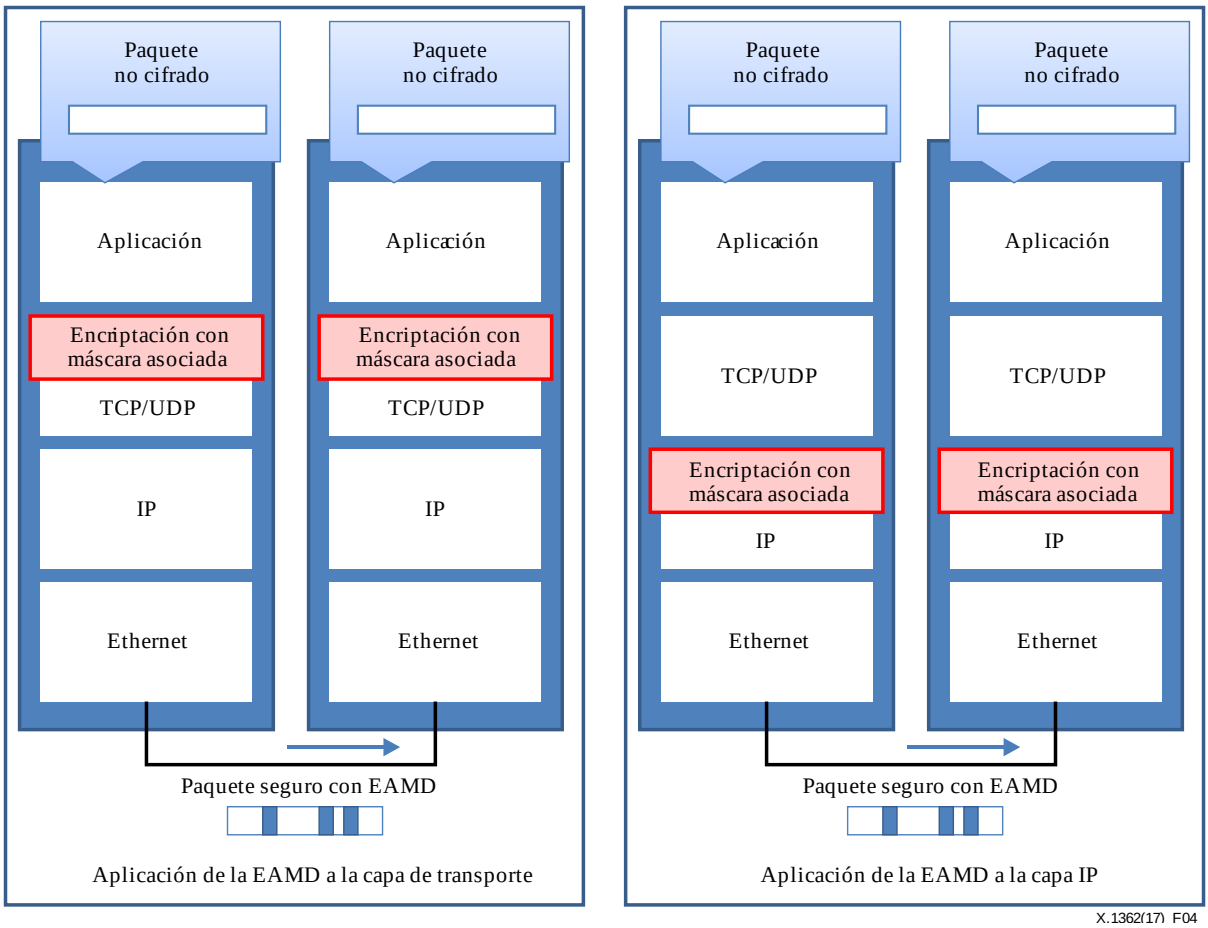

Figura 4 – Visión general de la comunicación mediante encriptación con datos de máscara asociados (EAMD)

7.1 Asociación de seguridad con máscara (SAM)

La asociación de seguridad con máscara (SAM) se define como un conjunto de parámetros específico del protocolo de seguridad. La SAM definir los servicios y mecanismos necesarios para proteger el tráfico mediante la aplicación de la EAMD. La SAM guarda relación con su protocolo asociado, dependiendo de las capas de protocolo tales como la capa de transporte o la capa del protocolo Internet (IP). Dichos parámetros pueden incluir los identificadores y modos de algoritmos y los identificadores de capa a los que se aplica la EAMD, así como parámetros específicos de la capa como la dirección y el puerto IP y las claves criptográficas. La SAM contiene el conjunto de parámetros criptográficos CryptCtx. Los datos de estado asociados a la SAM se representan en la base de datos de la SAM (SAMD).

Con arreglo a este formato, cada parámetro obligatorio se describe en el Cuadro 1.

Cuadro 1 – Parámetros obligatorios en la asociación de seguridad (SA) CryptCtx

N.°	Parámetro	Significado
1	encAlg	Identificador de algoritmo para la encriptación
2	encKey	Clave de encriptación
3	encMask	Zona que se encripta

Todos los parámetros opcionales se describen en el Cuadro 2.

Cuadro 2 – Parámetros opcionales de CryptCtx en la SA

N.°	Parámetro	Significado
1	encRoundKey	Clave sucesiva para la encriptación
2	decRoundKey	Clave sucesiva para la desencriptación
3	encIV	Vector inicial (IV) para la encriptación
4	macRoundKey	Clave sucesiva del MAC
5	macK1	Subclave para el CMAC K1
6	macK2	Subclave para el CMAC K2
7	KeyStream	Números aleatorios generados de antemano
8	KeyStreamHead	Puntero al encabezamiento de números aleatorios no utilizados
9	KeyStreamTail	Puntero a la cola de números aleatorios no utilizados
10	EncIVTail	Vector inicial para la generación de números aleatorios
11	macAlg	Identificador del algoritmo para el MAC
12	macKey	Clave del MAC
13	macMask	Zona que se utiliza para generar el MAC mediante la designación de un algoritmo

7.2 Formato de paquete de cabida útil de seguridad de la EAMD (EAMDSP)

En la Figura 5 se muestra el formato de paquete de cabida útil de seguridad de la EAMD (EAMDSP). El paquete comienza con el encabezamiento de la EAMDSP, de longitud variable. A este campo siguen los datos de cabida útil, cuya estructura depende del algoritmo y del modo de encriptación escogidos. Tras los datos de cabida útil figuran los campos de relleno y de longitud de relleno, así como del encabezamiento siguiente. El campo opcional del código de autenticación de mensaje (MAC) sirve para completar el paquete. El indicador de fin de la EAMDSP está formado por los campos de relleno, longitud de relleno y encabezamiento siguiente.

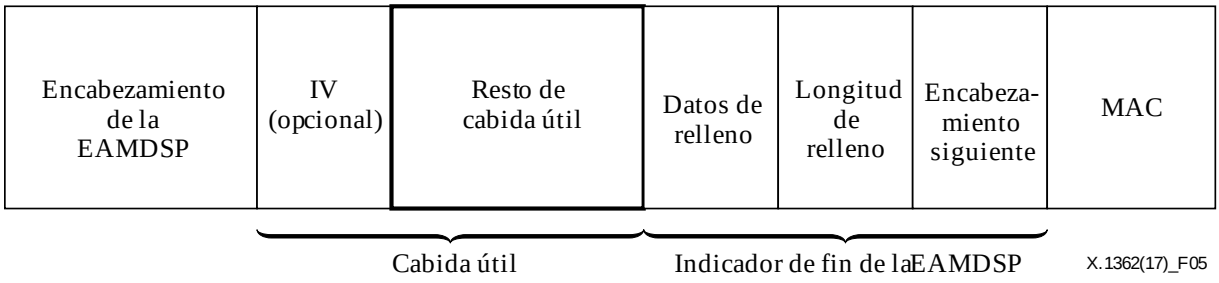

Figura 5 – Formato de paquete de la EAMDSP

El indicador de fin de la EAMDSP (transmitido) está formado por los campos de relleno, longitud de relleno y encabezamiento siguiente. El cómputo de integridad abarca datos implícitos adicionales del indicador de fin de la EAMDSP.

Si se escoge el servicio de integridad, el cómputo de integridad abarcará el encabezamiento de la EAMDSP, los datos de cabida útil y el indicador de fin de la EAMDSP. Si se escoge el servicio de confidencialidad, el texto cifrado estará formado por los datos de cabida útil (salvo los datos de sincronización criptográfica que pudieran incluirse) y el indicador de fin de la EAMDSP.

En las cláusulas siguientes se describen los campos del formato del encabezamiento. "Opcional" conlleva la omisión del campo si no se escoge ninguna opción, es decir, no está presente en el paquete transmitido o formateado respecto del cómputo del MAC. La selección de una opción viene determinada en el marco del establecimiento de la SAM. En consecuencia, el formato de los paquetes de la EAMDSP para una SAM específica se establece para la duración de la SAM. Sin embargo, los campos "obligatorios" siempre están presentes en el formato de paquete de la EAMDSP para todas las SAM.

7.2.1 Datos de cabida útil

Los datos de cabida útil constituyen un campo de longitud variable que incluye datos (del paquete original) definidos por el campo del encabezamiento siguiente. El campo de datos de cabida útil es obligatorio y su longitud viene dada por un número entero de bytes. Si el algoritmo utilizado para encriptar los datos de cabida útil requiere datos de sincronización criptográfica, por ejemplo un vector de inicialización (IV), esos datos se transportarán explícitamente en el campo de cabida útil, si bien no se requerirán en un campo independiente en la EAMDSP, es decir, la transmisión de un IV explícito es invisible para la EAMDSP.

7.2.2 Datos de relleno (para la encriptación)

Si se emplea un algoritmo de encriptación para el que es necesario que el texto en lenguaje claro sea un múltiplo de varios bytes, por ejemplo el tamaño de bloque de un cifrado de bloques, el campo de datos de relleno se utilizará para completar el texto en lenguaje claro (formado por los campos de datos de cabida útil, relleno, longitud de relleno y siguiente encabezamiento) hasta alcanzar el tamaño que requiera el algoritmo.

7.2.3 Longitud de relleno

El campo de longitud de relleno indica el número de bytes de relleno adyacentes anteriores en el campo de relleno. El campo de longitud de relleno es obligatorio.

7.2.4 Encabezamiento siguiente

El campo del encabezamiento siguiente es obligatorio. Dicho campo sirve para identificar el tipo de datos contenidos en el campo de datos de cabida útil, por ejemplo un encabezamiento y datos relativos a la capa siguiente.

7.2.5 Código de autenticación de mensaje (MAC)

El código de autenticación de mensaje es un campo de longitud variable computado con respecto a los datos cuya protección, en términos de integridad, es designada por la máscara. Los campos implícitos de indicador de fin de la EAMDSP, tales como el relleno para la generación del MAC, se abarcan en el cómputo del MAC. El campo del MAC es opcional. Sólo está presente si se ha seleccionado el servicio de integridad, y lo proporciona un algoritmo de integridad independiente o un algoritmo de modo combinado que utiliza el MAC. La longitud del campo se especifica mediante el algoritmo de integridad seleccionado asociado a la SAM. La especificación del algoritmo de integridad deberá determinar la longitud del MAC, así como las reglas de comparación y las etapas de procesamiento a los efectos de validación.

7.3 Procesamiento de paquetes

7.3.1 Procesamiento de paquetes salientes

El procesamiento de salida mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

   Antes de que se aplique la EAMDSP a un paquete de salida, la SAM correspondiente que requiera el procesamiento de la EAMDSP se determinará en función de información tal como el identificador de capa y el parámetro específico de la capa, por ejemplo la dirección o el número de puerto IP del paquete. La SAM designa la clave y las máscaras para la encriptación y la generación del MAC.

2) Transformación de datos mediante la EAMD, según se describe en la cláusula 6.1.

3) Envío de paquetes:

   El encabezamiento original se añade al paquete trasformado mediante la EAMD y se envía el paquete resultante a la red.

7.3.2 Procesamiento de paquetes entrantes

El procesamiento de entrada mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

   Tras la recepción de un paquete que contiene un encabezamiento de la EAMDSP, el receptor determinará la SAM adecuada previo examen de la SAMD. El registro de la SAM en la SAMD indica asimismo la capa de la EAMD aplicable durante el procesamiento de salida, así como el parámetro específico de capa, por ejemplo la dirección o el número de puerto IP del paquete, y si ha de incluirse el campo MAC. El registro en la SAMD especifica asimismo los algoritmos y las claves que han de utilizarse para la desencriptación y la verificación del MAC (de ser necesario).

2) Verificación de los datos del encabezamiento de la EAMDSP:

   La verificación de los datos del encabezamiento de la EAMDSP puede llevarse a cabo mediante determinados valores del encabezamiento de la EAMDSP antes de la comprobación de integridad y la desencriptación. Si el resultado de la verificación es negativo, el paquete se descartará.

La transformación de datos mediante la EAMD se describe en la cláusula 6.1.

8 EAMD mediante un algoritmo de encriptación autentificada

8.1 Asociación de seguridad con máscara (SAM)

En el caso de las EAMD que emplean algoritmos de encriptación autenticada, la SAM también se define en la cláusula 7.1.

Todos los parámetros obligatorios con arreglo a este formato se describen en el Cuadro 3.

Cuadro 3 – Parámetros obligatorios en CryptCtx en la SA

N.°	Parámetro	Significado
1	auencAlg	Identificador de algoritmo para la encriptación autentificada
2	auencKey	Clave para la encriptación autentificada
3	encMask	Zona que va a encriptarse

Todos los parámetros opcionales se describen en el Cuadro 4.

Cuadro 4 – Parámetros opcionales de CryptCtx en la SA

N.°	Parámetro	Significado
1	auencRoundKey	Clave sucesiva para la encriptación autentificada
2	audecRoundKey	Clave sucesiva para la desencriptación
3	IV	Vector inicial para la encriptación autentificada
4	Nonce	Clave sucesiva para la encriptación autentificada

8.2 Formato de paquete de cabida útil de seguridad de la EAMD (EAMDSP)

En Figura 6 se muestra el formato de paquete de la EAMDSP (cabida útil de seguridad de la EAMD). El paquete comienza con el encabezamiento de la EAMDSP, de longitud variable. A este campo siguen los datos de cabida útil, cuya subestructura depende del algoritmo y del modo de encriptación escogidos. Tras los datos de cabida útil figuran los campos de relleno y de longitud de relleno, así como el campo del encabezamiento siguiente. El indicador de fin de la EAMDSP está formado por los campos de relleno, longitud de relleno y encabezamiento siguiente.

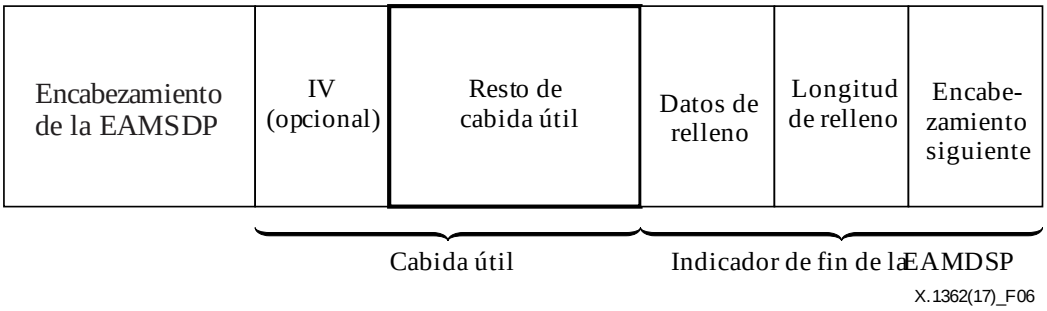

Figura 6 – Formato de paquete de la EAMDSP sin el MAC (para la encriptación autentificada)

El indicador de fin de la EAMDSP (transmitido) está formado por los campos de relleno, longitud de relleno y encabezamiento siguiente. El cómputo de integridad abarca datos implícitos adicionales del indicador de fin de la EAMDSP (que no se transmiten).

Si se escoge el servicio de integridad, el cómputo de integridad abarcará el encabezamiento de la EAMDSP, los datos de cabida útil y el indicador de fin de la EAMDSP. Si se escoge el servicio de confidencialidad, el texto cifrado estará formado por los datos de cabida útil (salvo los datos de sincronización criptográfica que pudieran incluirse) y el indicador de fin de la EAMDSP.

En las cláusulas siguientes se describen los campos del formato del encabezamiento. "Opcional" conlleva la omisión del campo si no se escoge ninguna opción, es decir, no está presente en el paquete transmitido o formateado respecto del cómputo del MAC. La selección de una opción viene determinada en el marco del establecimiento de la SAM. En consecuencia, el formato de los paquetes EAMDSP para una SAM específica se establece para la duración de la SAM. Sin embargo, los campos "obligatorios" siempre están presentes en el formato de paquete de la EAMDSP para todas las SAM.

8.2.1 Datos de cabida útil

Los datos de cabida útil constituyen un campo de longitud variable que incluye datos (del paquete original) definidos por el campo del encabezamiento siguiente. El campo de datos de cabida útil es obligatorio y su longitud corresponde a un número entero de bytes.

El formato de paquete de la cabida útil de seguridad de encapsulado (ESP) puede expresarse como ESP = SPI || Número de secuencia || IV || C, siendo C el texto cifrado que genera el algoritmo de encriptación autentificada. En este caso C incluye la etiqueta de autentificación.

8.2.2 Datos de relleno (para la encriptación autentificada)

Si se emplea un algoritmo de encriptación autentificada para el que es necesario que el texto en lenguaje claro sea un múltiplo de varios bytes, por ejemplo el tamaño de bloque de un cifrado de bloques, el campo de datos de relleno se utilizará para completar el texto en lenguaje claro (formado por los campos de datos de cabida útil, relleno, longitud de relleno y siguiente encabezamiento) hasta alcanzar el tamaño que requiera el algoritmo.

8.2.3 Longitud de relleno

El campo de longitud de relleno indica el número de bytes de relleno adyacentes anteriores en el campo de relleno. El campo de longitud de relleno es obligatorio.

8.2.4 Encabezamiento siguiente

El campo del encabezamiento siguiente es obligatorio. Dicho campo sirve para identificar el tipo de datos contenidos en el campo de datos de cabida útil, por ejemplo un encabezamiento y datos relativos la capa siguiente.

8.3 Procesamiento de paquetes

8.3.1 Procesamiento de paquetes salientes

El procesamiento de salida mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

   Antes de que se aplique la EAMDSP a un paquete de salida, la SAM correspondiente que requiera el procesamiento de la EAMDSP se determinará en función de información tal como el identificador de capa y el parámetro específico de la capa, por ejemplo la dirección o el número de puerto del protocolo Internet (IP) del paquete. La SAM designa la clave y las máscaras para la encriptación autentificada.

2) Transformación de datos mediante el modo de encriptación autentificada de la EAMD:

   1) Incorporación de los datos de relleno necesarios para la encriptación.
   2) Extracción de los datos para la encriptación mediante la máscara de encriptación y copia de los mismos en la memoria intermedia, que se utiliza a los efectos de cómputo temporal.
   3) Encriptación del resultado en la memoria intermedia mediante la clave y el algoritmo de encriptación, entre otros datos necesarios.
   4) Sustitución del texto cifrado en el paquete mediante la máscara.
   5) Incorporación de la etiqueta de autentificación al paquete como MAC.

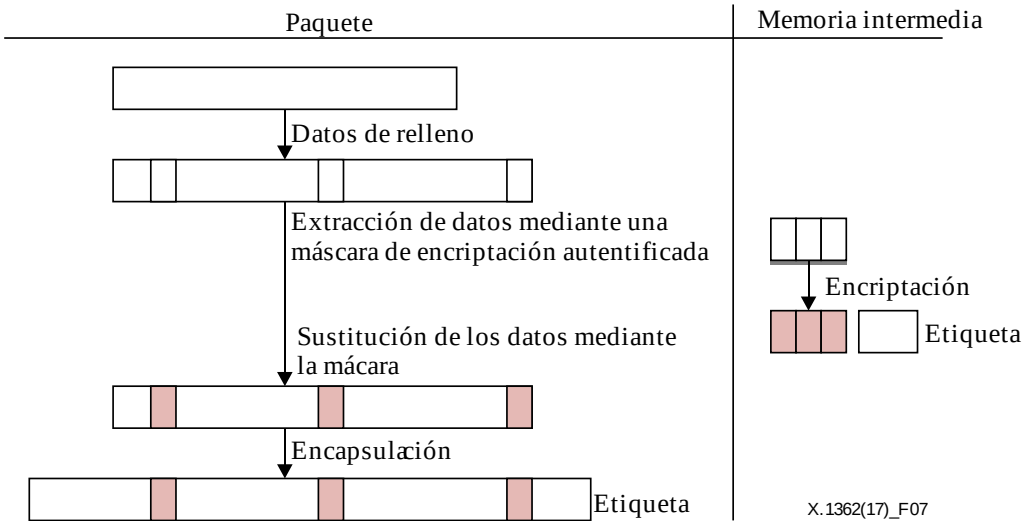

Figura 7 – Procesamiento de paquetes de salida para el modo de encriptación autentificada

3) Envío del paquete:

El encabezamiento original se añade al paquete transformado mediante la EAMD y se envía el paquete resultante a la red.

8.3.2 Procesamiento de paquetes entrantes

El procesamiento de entrada mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

Tras la recepción de un paquete que contiene un encabezamiento de la EAMDSP, el receptor determinará la SAM adecuada previo examen de la SAMD. El registro de la SAM en la SAMD indica asimismo la capa EAMD aplicable durante el procesamiento de salida, así como el parámetro específico de capa, por ejemplo la dirección o el número de puerto IP del paquete. El registro en la SAMD especifica asimismo los algoritmos y las claves que han de utilizarse para la desencriptación y la verificación del etiquetado;

2) Verificación de los datos del encabezamiento de la EAMDSP:

La verificación de los datos del encabezamiento de la EAMDSP puede llevarse a cabo mediante determinados valores del encabezamiento de la EAMDSP antes de la comprobación de integridad y de la desencriptación. Si el resultado de la verificación es negativo, el paquete se descartará;

3) Transformación de datos mediante el modo de desencriptación autentificada de la EAMD:

   1) Supresión del encabezamiento del paquete;
   2) Extracción de los datos para la desencriptación mediante la máscara de desencriptación y copia de los mismos en la memoria intermedia, que se utiliza a los efectos de cómputo temporal;
   3) Separación de la etiqueta de autentificación del paquete y copia de la misma en la memoria intermedia;
   4) Desencriptación del resultado en la memoria intermedia mediante la clave y el algoritmo de desencriptación, entre otros datos necesarios;
   5) Sustitución del resultado de la desencriptación en el paquete mediante la máscara si la desencriptación es satisfactoria.

4) Supresión de los datos de relleno para la encriptación en el paquete.

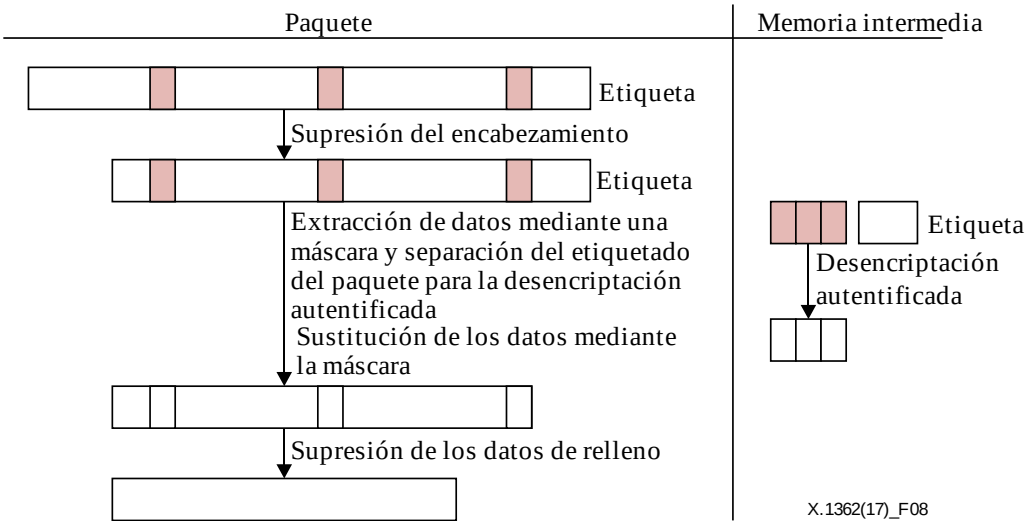

Figura 8 – Procesamiento de paquetes de entrada para el modo de encriptación autentificada

9 Orientaciones y limitaciones

9.1 Orientaciones sobre el establecimiento de la SAM

En lo concerniente al método de enmascaramiento de la encriptación de la EAMD cabe señalar que si una entidad mal intencionada fuera capaz de modificar la máscara, podría alterar el valor de la misma de forma que impidiera la encriptación de los datos. Una vez que la máscara se modifica de este modo todos los datos del dispositivo se transmitirían "sin cifrar" (no encriptados). Ello implicaría una vulnerabilidad significativa en materia de seguridad.

Para subsanar esta deficiencia es necesario abordar las cuestiones siguientes:

1) Seguridad de las comunicaciones con enmascaramiento

   Con objeto de inicializar y actualizar la información sobre claves, por ejemplo las claves criptográficas y los vectores iniciales, entre otros parámetros de seguridad, existen varios protocolos de establecimiento de claves, por ejemplo el Protocolo de intercambio de claves de Internet -Versión 2 (IKEv2) [IETF RFC 7296], Acuerdo de claves, y Transporte de claves.

   Es necesario garantizar que la máscara se inicializa y actualiza a tenor de la inicialización y la actualización de la información sobre claves durante la comunicación entre entidades conexas por medio de estos protocolos. Por ejemplo, durante el proceso de comunicación para el establecimiento de claves, la información sobre claves anteriormente mencionada debería incluir asimismo la máscara, con objeto de garantizar la integridad y confidencialidad de la máscara por medio de los algoritmos de encriptación y los algoritmos MAC utilizados en esos protocolos.

2) Seguridad en el almacenamiento de máscaras

   Es necesario garantizar, una vez que el dispositivo incorpore la máscara, que no exista ningún protocolo que permita al otro dispositivo leer la máscara.

   A tal efecto, cabe proponer los métodos enumerados a continuación.

   El primero de ellos se basa en un diseño de sistema seguro que asigna los componentes del sistema de forma tal que los dispositivos a los que se aplica la EAMD no se comuniquen directamente con una entidad fuera del sistema, aunque un componente de pasarela segura de gran capacidad de cómputo se comunique con dicha entidad.

El segundo método se basa en la protección del dispositivo mediante soportes físicos a prueba de manipulaciones o el método de ocultación de soporte lógico que genera un código oculto cuya comprensión resulta compleja para el ser humano.

9.2 Orientaciones sobre la utilización adecuada de vectores de inicialización y palabras de ocasión

En la presente cláusula se proporcionan orientaciones sobre la utilización adecuada de vectores de inicialización (y modos de cifrado de bloque y datos de relleno). La utilización inadecuada de vectores de inicialización o de datos de relleno constituye una trampa habitual en ataques a protocolos. Es probable que la función que desempeñe un vector de inicialización o una palabra de ocasión resulte fundamental a los efectos de seguridad del protocolo.

Con objeto de utilizar el modo de concatenación de bloques cifrados (CBC) [ISO/IEC 10116] para la encriptación mediante la combinación de bloques de texto no cifrado con los bloques de texto cifrado anteriores, cabe aplicar los principios expuestos a continuación.

Cuando se utilice el modo CBC como modo de operación del cifrado de bloques, ha de considerarse la seguridad frente a los ataques de "oráculo" (por lo general un servidor) mediante datos de relleno en [b-CBCPADD]. El modo CBC requiere un IV para combinarse con el primer bloque de texto no cifrado. No es necesario que el IV sea secreto, pero deberá ser impredecible.

A fin de utilizar un algoritmo de encriptación autentificada de forma segura, cabe aplicar los principios expuestos a continuación.

Si una aplicación no puede reunir los requisitos en materia de exclusividad sobre generación de palabras de ocasión, deberá utilizar una palabra de ocasión de longitud cero. Los algoritmos aleatorios o por estados [b-IETF RFC 5116] son adecuados para dichas aplicaciones. En otros casos, la aplicación ha de utilizar palabras de ocasión de doce octetos de longitud.

Si las palabras de ocasión o los IV se repiten, el O exclusivo (XOR) de dos paquetes podría poner de manifiesto numerosas modalidades de ataques posibles. En consecuencia, se recomienda encarecidamente velar por que el IV o la palabra de ocasión sean únicos.

9.3 Restricción de la utilización de la EAMD

La utilización de la EAMD se restringe con respecto a los requisitos de calidad de funcionamiento del sistema en tiempo real.

El factor de calidad de la EAMD se optimiza para el sistema en el que los emisores y el receptor poseen un cierto grado de capacidad de cómputo, en particular las arquitecturas CPU de 16 ó 32 bits con valores adecuados de frecuencia (cientos de MHz) y memoria.

Cabe señalar que la EAMD quizá no sea una buena solución para los sistemas con requisitos de restricción de potencia, puesto que el consumo de energía para el almacenamiento en la memoria intermedia de la EAMD podría dar lugar a un encabezamiento considerable.

Cabe destacar asimismo el alto grado de sensibilidad del enmascaramiento, al igual que la clave criptográfica mencionada anteriormente, de ahí que la EAMD sea aplicable únicamente si se realiza la hipótesis de que la máscara se gestiona y protege de forma segura.

Anexo A

Vinculación a protocolos existentes

(Este anexo forma parte de la presente Recomendación)

Con objeto de lograr una comunicación segura mediante encriptación con datos de máscara asociados, deberá establecerse la capa en la que se aplica la encriptación. Diversas capas reúnen las condiciones necesarias a tal efecto, por ejemplo la capa de transporte, la capa IP, etc. En el presente anexo se describe la forma de vincular la encriptación con datos de máscara asociados a protocolos existentes. Al proceder a la encriptación con vinculación entre los datos de máscara asociados y el protocolo IPsec, es preciso garantizar la confidencialidad y la autenticación. En ese sentido, conviene asegurar la confidencialidad por medio de la autenticación [IETF RFC 7321].

A.1 Vinculación al protocolo IP ESP de seguridad IP (IPSec) IETF RFC 4303

A.1.1 Formato de la SAM

La SAM define los servicios y mecanismos de protección de tráfico necesarios mediante la aplicación de la EAMD. En la Figura A.1 se describe una asociación de seguridad con máscara (SAM) si la EAMD se aplica a la capa de red.

```
SecurityAssertion ::= SEQUENCE {
  layerIdentifier OCTET STRING (SIZE(1)),
  SPI             OCTET STRING (SIZE (4)),
  ipAddr          OCTET STRING (SIZE (4)),
  cryptCtx        CryptCtx
}
CryptCtx ::= SEQUENCE {
  encAlg    OCTET STRING (SIZE (4))
  encKey    OCTET STRING (SIZE (keySizeMax)),
  encMask   OCTET STRING (SIZE (maskLength))
}
keySizeMax INTEGER ::= 64
maskLength INTEGER ::= 16
```

Figura A.1 – Formato de la SAM para la capa de red

A.1.2 Formato de paquete

En la Figura A.2 se muestra un ejemplo de formato de paquete de cabida útil de seguridad de la EAMD (EAMDSP). El paquete comienza con el encabezamiento de la EAMDSP, de longitud variable. A este campo siguen los datos de cabida útil, cuya subestructura depende del algoritmo y del modo de encriptación escogidos. Tras los datos de cabida útil figuran los campos de relleno y de longitud de relleno, así como el campo del encabezamiento siguiente. El campo opcional del código de autenticación de mensaje (MAC) completa el paquete. El indicador de fin de la EAMDSP está formado por los campos de relleno, longitud de relleno y encabezamiento siguiente. Teniendo en cuenta la cantidad de tráfico asociado al cómputo del MAC de la EAMD y la encriptación de la EAMD, en otros tipos de formato la longitud del número de secuencia puede ser 8B y el campo de encabezamiento siguiente puede incluirse en el encabezamiento de la EAMDSP.

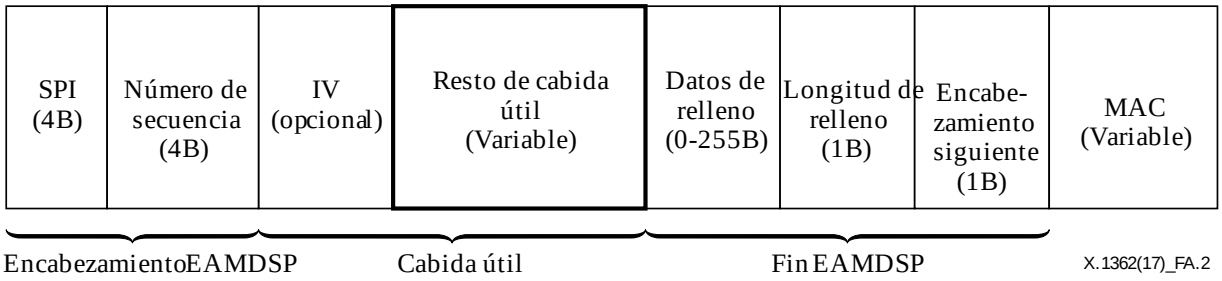

Figura A.2 – Ejemplo de formato de paquete EAMDSP para su asociación a un protocolo ESP IpSec

1) Índice de parámetros de seguridad (SPI):

El SPI es un valor arbitrario de 32 bits utilizado por un receptor para identificar la SAM a la que se vincula un paquete de entrada. El campo del SPI es obligatorio. El SPI se incorpora al protocolo para que el sistema receptor pueda seleccionar la SAM que permitirá procesar los paquetes recibidos.

2) Número de secuencia:

Este campo de 32 ó 64 bits sin signo contiene el valor de un contador que aumenta una unidad por cada paquete enviado, es decir, un número de secuencia de paquete por cada SAM, o un valor generado con respecto a una regla no ambigua.

3) Datos de cabida útil:

Los datos de cabida útil constituyen un campo de longitud variable que incluye datos (del paquete original) definidos por el campo del encabezamiento siguiente. El campo de datos de cabida útil es obligatorio y su longitud viene dada por un número entero de bytes. Si el algoritmo utilizado para encriptar los datos de cabida útil requiere datos de sincronización criptográfica, por ejemplo un vector de inicialización (IV), esos datos se transportarán explícitamente en el campo de cabida útil, si bien no se requerirán en un campo independiente en la EAMDSP, es decir, la transmisión de un IV explícito es invisible para la EAMDSP.

4) Cabida útil (para encriptación):

Los datos de cabida útil también pueden ser necesarios con independencia de los requisitos del algoritmo de encriptación, con objeto de garantizar que el final del texto cifrado resultante se rija por un límite de 4 bytes. En particular, los campos de longitud de relleno y de encabezamiento siguiente deberán alinearse en la parte derecha con arreglo a una palabra de 4 bytes, según se indica en las figuras anteriores en las que se muestra el formato de paquete de la EAMDSP, a fin de velar por la alineación del campo del MAC (de existir) con respecto a un límite de 4 bytes.

5) Longitud de cabida útil:

El campo de longitud de relleno indica el número de bytes de relleno adyacentes anteriores en el campo de relleno. La gama de valores válidos oscila entre 0 y 255, en la que el valor cero corresponde al caso en el que no existen bytes de relleno. El campo de la longitud de relleno es obligatorio.

6) Encabezamiento siguiente:

El campo del encabezamiento siguiente es obligatorio y posee 8 bits; permite identificar el tipo de datos contenidos en el campo de datos de relleno, por ejemplo un encabezamiento y datos de la siguiente capa.

7) Código de autenticación de mensaje (MAC):

El código de autentificación de mensaje constituye un campo de longitud variable que se determina con respecto a los datos que indica la máscara a los efectos de protección de la integridad. Los campos implícitos de indicador de fin de la EAMDSP, por ejemplo los datos de relleno para la generación del MAC, se incluyen en el cómputo del MAC. El campo del MAC es opcional.

A.1.3 Procesamiento de paquetes

El procesamiento de salida mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

La SAM asociada que requiere el procesamiento de la EAMDSP se determina con arreglo a información tal como el identificador de capa y el parámetro específico de la capa, por ejemplo la dirección o el número de puerto IP del paquete.

2) Transformación de datos mediante la EAMD:

La encriptación y la generación del MAC se llevan a cabo mediante la EAMD de conformidad con el proceso que figura en la cláusula 6.1.

3) Envío de paquetes:

El encabezamiento original se incorpora al paquete trasformado mediante la EAMD y se envía el paquete resultante a la red.

El procesamiento de entrada mediante encriptación con datos de máscara asociados se realiza del modo siguiente:

1) Examen de la SAM:

La SAM asociada que requiere el procesamiento de la EAMDSP se determina con arreglo a información tal como el identificador de capa que determina la capa de transporte y la dirección y el número de puerto IP del paquete.

2) Verificación del número de secuencia:

La verificación del número de secuencia se efectúa mediante el valor del número de secuencia del encabezamiento de la EAMDSP, antes de la comprobación de integridad y la desencriptación. Si el resultado de la verificación es negativo, el paquete se descartará.

3) Transformación de datos mediante la EAMD:

La verificación del MAC y la encripción se realizan mediante la EAMD, de conformidad con el proceso que figura en la cláusula 6.1.

A.1.4 Máscara para la extracción de los datos objetivo de la encriptación con datos de máscara asociados

En las operaciones de encriptación con datos de máscara asociados, el bloque de datos objetivo de la encriptación que se proporciona al algoritmo correspondiente se extrae dividiendo el paquete con arreglo al tamaño del bloque del algoritmo de encriptación utilizado, según el parámetro de la máscara. Por ejemplo, en el caso de encriptación con datos de máscara asociados mediante la norma de encriptación avanzada (AES), los datos de cabida útil se dividen en grupos de 128 bits porque la longitud de los bloques AES es de 128 bits. El bloque de datos objetivo de la desencriptación se extrae mediante la identificación del bloque con respecto a la máscara. Tras ello, los datos objetivo de la operación se generan mediante la concatenación del bloque de datos objetivo de la desencriptación. El formato de la máscara se describe en las figuras A.3 y A.4. Este parámetro permite determinar el bloque que debe encriptarse o desencriptarse en caso de dividir los datos de cabida útil con arreglo al tamaño de bloque del algoritmo de encriptación utilizado.

```
MaskFormat ::= SEQUENCE {
  encryptionArea OCTET STRING (SIZE (12))
  reserved OCTET STRING (SIZE (4))
}
```

Figura A.3 – Formato de máscara

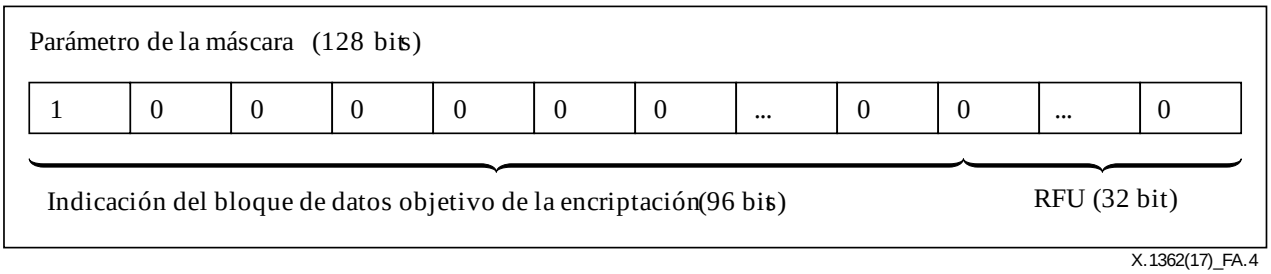

Figura A.4 – Formato pormenorizado del parámetro de máscara

En este caso, el parámetro de máscara significa que únicamente se encripta el primer bloque, puesto que el primer bit del parámetro de la máscara es verdadero. Para encriptar determinadas zonas es necesario que varios bits del parámetro de máscara pasen de ser falsos a verdaderos.

A.1.5 Algoritmo relativo a los datos de relleno

Los algoritmos relativos a los datos de relleno pueden describirse de la forma siguiente:

– Inserción de '0x80' al final de los datos de cabida útil.

– Si la longitud de los datos de cabida útil es múltiplo de la longitud del bloque de datos del algoritmo de encriptación, el proceso de relleno habrá concluido.

Si la longitud de los datos de cabida útil NO es múltiplo de la longitud del bloque de datos del algoritmo de encriptación, se insertará '0x00' al final de los datos de cabida útil hasta que la longitud de los datos de cabida útil sea múltiplo de la longitud del bloque de datos.

Bibliografía

[b-UIT-T F.4104] Recomendación UIT-T F.4104/F.744 (2009), *Requisitos y descripción del servicio para soportes intermedios (middleware) de redes de sensores ubicuas.*

[b-UIT-T X.1311] Recomendación UIT-T X.1311 (2011) | ISO/IEC 29180:2012, *Tecnología de la información – Marco de seguridad para red de sensores ubicuos.*

[b-UIT-T X.1312] Recomendación UIT-T X.1312 (2011), *Directrices de programa intermedio de seguridad para redes de sensores ubicuos.*

[b-UIT-T X.1313] Recomendación UIT-T X.1313 (2012), *Requisitos de seguridad para el encaminamiento en la red de sensores inalámbrica.*

[b-UIT-T Y.4000] Recomendación UIT-T Y.4000/Y.2060 (2012), *Visión general de la Internet de las cosas.*

[b-UIT-T Y.4105] Recomendación UIT-T Y.4105/Y.2221 (2010), *Requisitos para el soporte de los servicios y aplicaciones de redes de sensores ubicuos en el entorno de las redes de próxima generación.*

[b-UIT-T Y.4109] Recomendación ITU-T Y.4109/Y.2061 (2012), *Requisitos de apoyo a las aplicaciones de comunicación orientada a las máquinas en el entorno de las redes de próxima generación.*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 5116] IETF RFC 5116 (2008), *An Interface and Algorithms for Authenticated Encryption.*

[b-ISO/CEI 9797] ISO/CEI 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) — Parte 1: Mechanisms using a block cipher*.

[b-ISO/CEI 18033] ISO/CEI 18033-3:2010, *Information technology – Security techniques – Encryption algorithms – Parte 3: Block ciphers.*

[b-ISO/CEI 19772] ISO/CEI 19772:2009, *Information technology – Security techniques – Authenticated encryption.*

[b-ASIACRYPT] Bellare, M., and Namprempre, C. (2000), *Authenticated encryption:* Relations *among notions and analysis of the generic composition paradigm*, in Tatsuaki Okamoto, editor, ASIACRYPT 2000, Vol. 1976 of LNCS, Springer, Diciembre, p. 531-545.

[b-CBCPADD] Vaudenay, S. (2002), *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS*, EUROCRYPT 2002.

[b-EUROCRYPT] Namprempre, C., Rogaway, P., and Shrimpton, T. (2014), *Reconsidering generic composition*, in Phong Q. Nguyen and Elisabeth Oswald, editors, EUROCRYPT 2014, Vol. 8441 of LNCS, Springer, Mayo, pp. 257-274.

[b-ZT] Li, Zhang, y Xin, Tong (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, *Journal of Convergence Information Technology (JCIT)*, Vol. 8, Nº 5, marzo.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017