UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.274

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(07/94)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

INTERCONEXIÓN DE SISTEMAS ABIERTOS – PROTOCOLOS DE SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCAMBIO DE TELECOMUNICACIONES E INFORMACIÓN ENTRE SISTEMAS – PROTOCOLO DE SEGURIDAD DE LA CAPA DE TRANSPORTE

Recomendación UIT-T X.274

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

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. El texto de la Recomendación UIT-T X.274 se aprobó el 1 de julio de 1994. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10736-4.

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.

RECOMENDACIONES DE LA SERIE UIT-T X

REDES DE DATOS
Y COMUNICACIÓN DE SISTEMAS ABIERTOS

(Febrero 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificación de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-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	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Procesamiento de transacción	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Sumario

Esta Recomendación | Norma Internacional especifica el protocolo que soporta todos los servicios de integridad, confidencialidad, autenticación y control de acceso que, según se identifica en el modelo de seguridad OSI, son aplicables a la capa de transporte. El protocolo soporta estos servicios mediante el empleo de mecanismos criptográficos, etiquetas de seguridad y atributos de seguridad asignados, tales como claves criptográficas.

Introducción

El protocolo especificado en la Rec. UIT X.224 | ISO/CEI 8073 proporciona el servicio de transporte en modo conexión descrito en la Rec. UIT-T X.214 | ISO/CEI 8072. El protocolo de transporte especificado en la Rec. UIT-T X.234 | ISO 8602 proporciona el servicio de transporte en modo sin conexión descrito en ISO 8072/AD1. La presente Recomendación | Norma Internacional especifica funciones facultativas adicionales a las especificadas en la Rec. UIT-T X.224 | ISO/CEI 8073 y a la Rec. UIT-T X.234 | ISO 8602 que permiten la utilización de técnicas criptográficas para dar protección de datos a las conexiones de transporte o a las transmisiones de TPDU en modo sin conexión.

Los Anexos A y B forman parte integrante de esta Recomendación | Norma Internacional. Los Anexos C y D tienen carácter informativo solamente.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCAMBIO DE TELECOMUNICACIONES E INFORMACIÓN ENTRE SISTEMAS – PROTOCOLO DE SEGURIDAD DE LA CAPA DE TRANSPORTE

1 Alcance

Los procedimientos especificados en la presente Recomendación | Norma Internacional constituyen ampliaciones de los definidos por la Rec. UIT-T X.224 | ISO/CEI 8073 y por la Rec. UIT-T X.234 | ISO 8602 y no excluyen la comunicación no protegida entre entidades de transporte que aplican la Rec. UIT-T X.224 | ISO/CEI 8073 o la Rec. UIT-T X.234 | ISO 8602.

La protección conseguida mediante el protocolo de seguridad definido en esta Recomendación | Norma Internacional depende del funcionamiento adecuado de la gestión de seguridad, incluida la gestión de claves. Sin embargo, esta Recomendación | Norma Internacional no especifica las funciones y protocolos de gestión necesarios para soportar el referido protocolo de seguridad.

Este protocolo puede soportar todos los servicios de integridad, confidencialidad, autenticación y control de acceso identificados en la Rec. X.800 del CCITT | ISO 7498-2 como pertinentes a la capa de transporte. El protocolo soporta estos servicios utilizando mecanismos criptográficos, etiquetado y atributos de seguridad, tales como claves e identidades autenticadas, preestablecidos por la gestión de seguridad, o establecidos mediante el empleo del protocolo de asociación de seguridad (SA-P).

La protección sólo puede proporcionarse dentro del contexto de una política de seguridad.

Este protocolo soporta la autenticación de entidades pares en el momento del establecimiento de la conexión. Además, se soporta la reaplicación de clave dentro del protocolo, mediante el uso del SA-P o por medios externos al protocolo.

Las asociaciones de seguridad sólo pueden establecerse en el contexto de una política de seguridad. Incumbe a cada usuario establecer su propia política de seguridad, la cual puede tener que ajustarse a los procedimientos especificados en esta Recomendación | Norma Internacional.

Los siguientes puntos pudieran incluirse en una política de seguridad:

a) el método de establecimiento/liberación de la SA, la duración de SA;

b) los mecanismos de autenticación/control de acceso;

c) el mecanismo de etiquetas;

d) el procedimiento que se sigue cuando se recibe una TPDU no válida durante el procedimiento del establecimiento de la SA o la transmisión de una PDU protegida;

e) la duración de la clave;

f) el intervalo del procedimiento de reaplicación de clave para actualizar la clave, y el procedimiento de intercambio de información de control de seguridad (SCI);

g) la temporización del intercambio de SCI y del procedimiento de reaplicación de clave;

h) el número de nuevos intentos de intercambio de SCI y de procedimiento de reaplicación de clave.

Esta Recomendación | Norma Internacional define un protocolo que puede utilizarse para el establecimiento de la asociación de seguridad. Las entidades que deseen establecer una SA deben emplear mecanismos comunes para la autenticación y distribución de claves. Esta Recomendación | Norma Internacional especifica un algoritmo para la autenticación y distribución de claves basado en sistemas de criptografía de claves públicas. La implementación de éste no es obligatoria; no obstante, si se utiliza un mecanismo alternativo, deberá satisfacer las siguientes condiciones:

a) derivación de todos los atributos SA definidos en 5.2;

b) autenticación de las claves derivadas.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

– Recomendación UIT-T X.214 (1993) | ISO 8072:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de transporte.*

– Recomendación UIT-T X.234 (1993) | ISO 8602:1987, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo para proporcionar el servicio de transporte en modo sin conexión.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

– Recomendación X.200 del CCITT (1988), *Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT.*

ISO 7498:1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*

– Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones del CCITT.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

– Recomendación UIT-T X.224 (1993), *Protocolo para proporcionar el servicio de transporte en modo sin conexión OSI.*

ISO/CEI 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*

– Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno (ASN.1).*

ISO/CEI 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*

– Recomendación X.209 del CCITT (1988), *Especificación de reglas básicas de codificación para la notación de sintaxis abstracta.*

ISO 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

– Recomendación UIT-T X.264 (1993), *Mecanismo de identificación del protocolo de transporte*.

ISO/CEI 11570:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Transport protocol identification mechanism.*

2.3 Referencias adicionales

– ISO/CEI 7498/AD1:1987, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission*.

– ISO 8072/AD1:1986, *Information processing systems – Open Systems Interconnection – Transport service definition – Addendum: Connectionless-mode transmission.*

– ISO/CEI 9834-1:1993, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities – Part 1: General Procedures.*

– ISO/CEI 9834-3:1990, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities – Part 3: Registration of object identifier component values for joint ISO/CCITT use.*

3 Definiciones

La presente Recomendación | Norma Internacional se basa en los conceptos desarrollados en el modelo de referencia de interconexión de sistemas abiertos (Rec. X.200 del CCITT | ISO 7498), incluida la Rec. X.800 del CCITT | ISO 7498-2 sobre arquitectura de seguridad.

3.1 Definiciones del modelo de referencia de seguridad

La presente Recomendación | Norma Internacional utiliza los términos siguientes definidos en la Rec. X.800 del CCITT | ISO 7498-2:

a) control de acceso;

b) asimétrico;

c) criptograma (o texto cifrado);

d) texto claro;

e) confidencialidad;

f) integridad de los datos;

g) autenticación del origen de los datos;

h) denegación de servicio;

i) cifrado de extremo a extremo;

j) clave;

k) gestión de claves;

l) política de seguridad;

m) simétrico.

3.2 Definiciones adicionales

A los efectos de la presente Recomendación | Norma Internacional, son aplicables las definiciones que se indican a continuación.

3.2.1 periodo de criptografía: Periodo durante el cual se permite la utilización de una clave criptográfica. Una vez expirado ese periodo de tiempo, la clave debe ser sustituida.

3.2.2 mecanismo de protocolo dentro de banda: Mecanismo de protocolo definido en esta Recomendación | Norma Internacional.

3.2.3 mecanismo de protocolo fuera de banda: Mecanismo de protocolo no definido en esta Recomendación | Norma Internacional.

3.2.4 clave por pares: Un par de valores de clave relacionados (clave pública) o idénticos (clave secreta) generados para su utilización entre dos participantes determinados.

3.2.5 protección contra la reflexión: Mecanismo de protección para detectar cuándo ha sido devuelta al originador una unidad de datos de protocolo.

3.2.6 asociación de seguridad: Relación entre entidades comunicantes para la que existen los correspondientes atributos de asociación de seguridad.

3.2.7 atributos de la asociación de seguridad: Recopilación de la información requerida para controlar la seguridad de las comunicaciones entre una entidad y su(s) par(es) distante(s).

3.2.8 unidad de datos del protocolo de transporte de encapsulación de seguridad: TPDU encapsulada por seguridad, para enviar la TPDU definida en la Rec. UIT-T X.224 | ISO/CEI 8073 o en la Rec. UIT-T X.234 | ISO 8602, después de asegurarla.

4 Abreviaturas

Esta Recomendación | Norma Internacional utiliza las siguientes abreviaturas de la cláusula 4 de la Rec. UIT-T X.224 | ISO/CEI 8073:

CR TPDU	TPDU de petición de conexión (*connection request TPDU*)
DC TPDU	TPDU de confirmación de desconexión (*disconnect confirm TPDU*)
DR TPDU	TPDU de petición de desconexión (*disconnect request TPDU*)
DST-REF	(Campo de) referencia de destino (*destination reference*)
DT TPDU	TPDU de datos (*data TPDU*)
ED TPDU	TPDU de datos acelerados (*expedited data TPDU*)
ED-TPDU-NR	Número de TPDU de datos acelerados (*expedited data TPDU number*)
ER TPDU	TPDU de error (*error TPDU*)
LI	(Campo de) indicador de longitud (*length indicator*)
NC	Conexión de red (*network connection*)
SN	Número de secuencia (*sequence number*)
SRC-REF	(Campo de) referencia de origen (*source reference*)
TC	Conexión de transporte (*transport connection*)
TPDU	Unidad de datos del protocolo de transporte (*transport protocol data unit*)
TPDU-NR	(Campo de) número de DT TPDU (*DT TPDU number*)

En la presente Recomendación | Norma Internacional se utilizan además las siguientes abreviaturas:

CBTSS	Servicio de seguridad de transporte basado en conexión (*connection based transport security service*)
Conf_no	No se proporciona confidencialidad
Conf_yes	Se proporciona confidencialidad
DEK	Clave de cifrado de datos (*data encipherment key*)
GTSS	Servicio de seguridad de transporte general (*general transport security service*)
ICV	Valor de comprobación de integridad (*integrity check value*)
Integ_no	No se proporciona integridad
Integ_yes	Se proporciona integridad
KEK	Clave de cifrado de clave (*key encipherment key*)
KEY-ID	Identificador de clave (*key identifier*)
Kg_esp	Se utiliza una clave criptográfica distinta para cada par de sistemas de extremo
Kg_esp_sr	Se utiliza una clave criptográfica distinta para cada par de sistemas de extremo y conjunto de niveles de seguridad
Kg_tc	Se utiliza una clave criptográfica distinta para cada conexión de transporte
LABEL	Etiqueta de seguridad (*security label*)
LLSG	Directrices de seguridad de capa inferior (*lower layer security guidelines*)
LME	Entidad de gestión de capa (*layer management entity*)
MAC	Código de autenticación de mensaje (*message authentication code*)
MDC	Código de detección de manipulación (*manipulation detection code*)
NLSP	Protocolo de seguridad de capa de red (*network layer security protocol*)
NSAP	Punto de acceso al servicio de red (*network service access point*)
NSDU	Unidad de datos del servicio de red (*network service data unit*)
PAD	(Campo de) relleno [*padding* (*field*)]
Ppl_abs	Etiqueta de seguridad nunca utilizada en las TPDU
Ppl_pres	Etiqueta de seguridad utilizada en cada TPDU

SA-P	Protocolo de asociación de seguridad (*security association – protocol*)
SE TPDU	TPDU de encapsulación de seguridad (*security encapsulation TPDU*)
TLSP	Protocolo de seguridad de la capa de transporte (*transport layer security protocol*)

5 Visión general del protocolo

5.1 Introducción

La Rec. X.800 del CCITT | ISO 7498-2 identifica los siguientes servicios de seguridad como pertinentes a la capa de transporte:

- autenticación de entidad par;
- autenticación del origen de los datos;
- servicio de control de acceso;
- confidencialidad en modo con conexión;
- confidencialidad en modo sin conexión;
- integridad en modo con conexión con recuperación;
- integridad en modo con conexión sin recuperación;
- integridad en modo sin conexión.

NOTAS

1 La Rec. UIT-T X.214 | ISO 8072 define actualmente cuatro niveles de calidad de protección:

a) sin prestaciones de protección;

b) protección contra supervisión pasiva;

c) protección contra modificación, reproducción, adición o supresión;

d) tanto b) como c),

que equivalen a los siguientes servicios de seguridad.

La Rec. X.800 del CCITT| ISO 7498-2 sobre arquitectura de seguridad de la interconexión de sistemas abiertos utiliza los siguientes términos para estos servicios de seguridad:

a) sin servicios de seguridad;

b) confidencialidad en modo con/sin conexión;

c) integridad en modo con/sin conexión (con o sin recuperación); y

d) confidencialidad e integridad en modo con/sin conexión.

Se ha elaborado un Informe de defectos relativo a la Rec. UIT-T X.214 | ISO 8072, en previsión de estas y posiblemente otras formas de protección.

2 La integridad en modo sin conexión no protege contra la adición o supresión de las SDU y sólo proporciona una protección limitada contra la reproducción.

El TLSP utilizado con la Rec. UIT-T X.224 | ISO/CEI 8073 admite la integridad de conexión con y sin recuperación, la confidencialidad de la conexión, el servicio de control de acceso y la autenticación de entidad par, con protección individual de cada una de las conexiones. No obstante, una clave puede ser compartida entre varias conexiones.

El TLSP utilizado con la Rec. UIT-T X.234 | ISO 8602 admite la integridad en modo sin conexión, la confidencialidad en modo sin conexión, el servicio de control de acceso y la autenticación del origen de los datos.

La presente Recomendación | Norma Internacional especifica ampliaciones de protocolo para proporcionar la confidencialidad y la protección de los datos de integridad, incluidos:

a) los procedimientos que incorporan técnicas criptográficas en el tratamiento de los protocolos;

b) las características mínimas de los algoritmos criptográficos con los que pueden utilizarse estos protocolos;

c) la estructura y la codificación de las unidades de datos necesarias para conseguir el interfuncionamiento.

Las Figuras 1 y 2 muestran la ubicación del TLSP en el modelo ISO de siete capas.

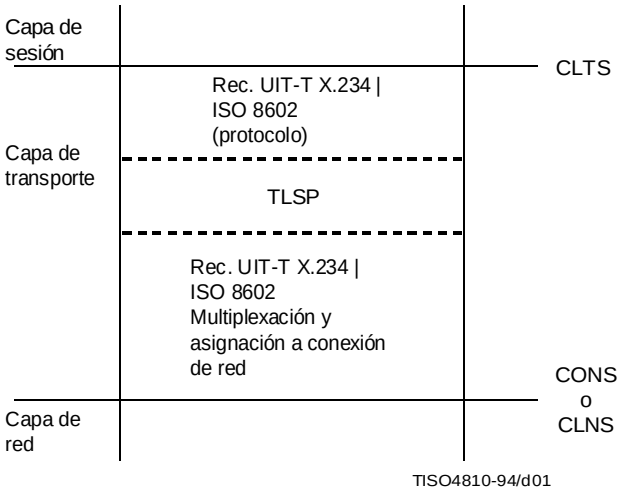


Figura 1 – TLSP con Rec. UIT-T X. 234 | ISO/CEI 8602

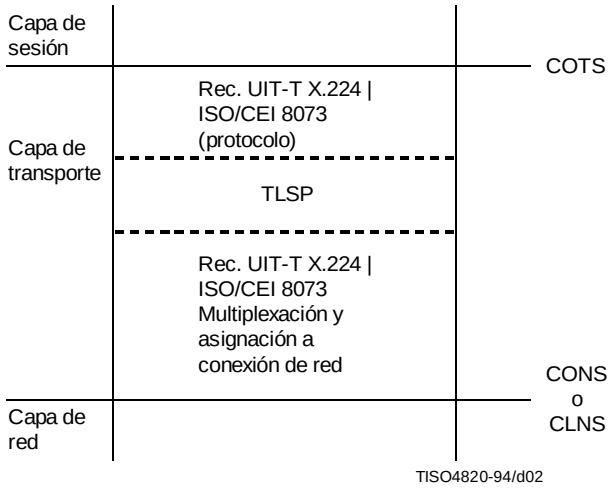


Figura 2 – TLSP con Rec. UIT-T X.224 | ISO/CEI 8073

5.2 Asociaciones y atributos de seguridad

Las opciones específicas de tratamiento del TLSP utilizadas en un caso de comunicaciones están determinadas por el conjunto de atributos de seguridad, incluidas las claves de protección por pares. El TLSP supone que dos entidades de transporte comparten un conjunto de atributos correspondiente. El identificador de asociación de seguridad, SA-ID, identifica un conjunto de atributos que pueden utilizarse para proteger una comunicación.

Cada asociación de seguridad se define por un conjunto de atributos en cada sistema de extremo. El medio para establecer todos los atributos que han de utilizarse en una asociación está actualmente fuera del ámbito de la presente especificación. Algunos atributos podrían establecerse por intercambio manual, y otros mediante un conjunto convenido de reglas de seguridad (ASSR). Un ASSR es un conjunto común de reglas que especifican el mecanismo de seguridad

que debe utilizarse, incluidos todos los parámetros necesarios para definir el funcionamiento del mecanismo para uno o más servicios de protección dados. Las reglas de seguridad y sus identificadores pueden ser registrados por terceros. Véase en el Anexo C un ejemplo ilustrativo de ASSR.

En el marco de la política de seguridad pueden definirse otros atributos, tales como la duración y la temporización del procedimiento de cambio de claves.

El TLSP utiliza estos atributos de asociación de seguridad para determinar las características de procesamiento de los datos de usuario. En lo que sigue se describen los atributos para el TLSP y se hace una relación de las abreviaturas nemotécnicas utilizadas para referirse a estos atributos en la presente especificación. El conjunto de atributos apropiado para dos sistemas de extremo comunicantes depende de los mecanismos utilizados y de la política de seguridad.

a) Identificación de SA

   1) Local_SAID: Cadena de octetos, identificador local de la SA

   2) Peer_SAID: Cadena de octetos, identificador par a distancia de la SA

   3) SAID_Len: Entero, longitud del SAID definido por el ASSR
   Entero de la gama comprendida entre 2 y 126.

   El valor de Local_SAID y Peer_SAID se fija al establecerse la SA. El valor de SAID_Len está definido para un ASSR dado.

   Cuando una entidad de TLSP determina discontinuar una SA particular, pondrá el SA-ID, que ha atribuido, en estado congelado. Mientras está congelado, el SA-ID no será reutilizado. El periodo durante el cual el SA-ID permanece congelado será superior a la duración de las PDU de la red subyacente.

b) Indicador de la entidad de TLSP que asume el cometido de «iniciador» y de la entidad que asume el de «respondedor». Este atributo indica cómo debe fijarse el indicador de sentido para detectar las TPDU reflejadas.

   Iniciador: Booleano (Boolean)

   El valor de este atributo se fija al establecerse la SA.

c) Dirección de entidad(es) de TLSP par(es)

   Peer_Adr: Cadena de octetos.

   El valor de este atributo se fija al establecerse la SA e indica la dirección del NSAP de la entidad de transporte, si la misma clave es compartida por varias conexiones, o el identificador de conexión mediante los números de referencia de transporte local y distante, si la clave es sólo para una conexión.

d) Identificador del conjunto acordado de reglas de seguridad que han de aplicarse para esta asociación.

   ASSR_ID: Identificador de objeto, como se define en la Rec. UIT-T X.208 del CCITT (relativa a la ASN.1) | ISO/CEI 8824

   El valor de este atributo se fija al establecerse la SA o está preestablecido.

e) QOS de protección seleccionada para la SA

   QOS_Label: Formato definido por el ASSR

   AC: (Nivel de control de acceso) Entero de la gama definida por el ASSR.

   Los siguientes parámetros de QOS sólo corresponden al TLSP utilizado junto con la Rec. UIT-T X.234 | ISO 8602:

   – DOAuth: (Nivel de autenticación del origen de los datos), entero de la gama definida por el ASSR

   – CLConf: (Nivel de confidencialidad en modo sin conexión), entero de la gama definida por el ASSR

   – CLInt: (Nivel de integridad en modo sin conexión), entero de la gama definida por el ASSR.

Los siguientes parámetros de QOS sólo corresponden al TLSP utilizado junto con la Rec. UIT-T X.224 | ISO/CEI 8073:

- Auth: (Nivel de autenticación de entidad par), entero de la gama definida por el ASSR
- CO Conf: (Nivel de confidencialidad en modo con conexión), entero de la gama definida por el ASSR
- CO Int: (Integridad en modo con conexión sin recuperación), entero de la gama definida por el ASSR
- CO Intr: (Integridad en modo con conexión con recuperación), entero de la gama definida por el ASSR
- CLConf: (Nivel de confidencialidad en modo sin conexión), entero de la gama definida por el ASSR
- CLInt: (Nivel de integridad en modo sin conexión), entero de la gama definida por el ASSR.

El valor de estos atributos se fijan al establecerse la SA o está preestablecido.

f) Mecanismos seleccionados para la SA

- Etiqueta: Booleano – Etiquetado explícito de las TPDU
- Conf: Booleano – Confidencialidad de una transferencia de datos segura mediante cifrado
- ICV: Booleano – Integridad del contenido de una transferencia de datos segura utilizando un valor de comprobación de integridad
- SN: Booleano – Procedimiento que ha de utilizarse de número de secuencia de integridad de conexión
- PE-Authentication: Booleano – Autenticación de entidad par utilizando el intercambio de PDU encapsuladas de petición de conexión/respuesta de conexión
- UNProt: Booleano – TPDU no protegidas.

g) Atributos de mecanismo de etiqueta

Los valores de estos atributos se fijan al establecerse la SA o están preestablecidos. Este atributo especifica el conjunto de etiquetas de seguridad permitidas para la asociación de seguridad.

```
Label_set: Set of {
        Label_Ref: Integer
        Label_Defining_Auth: Object Identifier
        Label_Content: Format defined by Label_Defining_Auth
}
```

h) Atributos del mecanismo de ICV

- ICV_Alg: Identificador de objeto
- ICV_Len: Entero
- ICV_Blk: Tamaño del bloque de enteros de relleno para el algoritmo de ICV.

Los atributos que se indican a continuación sólo están presentes si el algoritmo es criptográfico.

- ICV_Kg: Entero de valor Kg_tc o Kg_esp o Kg_esp_sr

  La granularidad de la clave es:

  - Kg_tc Se utiliza una clave criptográfica distinta para cada conexión de transporte
  - Kg_esp Se utiliza una clave criptográfica distinta para cada par de sistemas de extremo
  - Kg_esp_sr Se utiliza una clave criptográfica independiente para cada par de sistemas de extremo y conjunto de niveles de seguridad.

Los valores de los atributos anteriores están definidos por el ASSR dada la QOS de protección.

– ICV_Gen_key: Referencia de la clave de generación de ICV, forma definida por el ASSR

– ICV_Check_Key: Referencia de la clave de comprobación de ICV, forma definida por el ASSR.

i) Atributos del mecanismo de SN

Los atributos indicados a continuación sólo corresponden al TLSP utilizado junto con la Rec. UIT-T X.224 | ISO/CEI 8073.

– Data_Local_SN: SN para los últimos datos normales enviados

– Data_Peer_SN: SN para los últimos datos normales recibidos.

Los valores iniciales de estos atributos se fijan como parte de la conexión normal. El SN es el número de secuencia utilizado por la Rec. UIT-T X.224 | ISO/CEI 8073.

j) Atributos del mecanismo de EXSN

Los atributos indicados a continuación sólo corresponden al TLSP utilizado junto con la Rec. UIT-T X.224 | ISO/CEI 8073.

– Data_Local_EXSN: EXSN para los últimos datos acelerados enviados

– Data_Peer_EXSN: EXSN para los últimos datos acelerados recibidos

Los valores iniciales de estos atributos se fijan como parte del procedimiento acelerado. El EXSN es el número de secuencia utilizado por la Rec. UIT-T X.224 | ISO/CEI 8073.

k) Atributos del mecanismo de cifrado

– Enc_Alg: Identificador de objeto atribuido en virtud de la Norma ISO 9979

– Enc_Blk: Tamaño del bloque de enteros de relleno para el algoritmo de cifrado

– Enc_Kg: Entero de valor Kg_tc o Kg_esp o Kg_esp_sr

Los atributos de granularidad de la clave se definen en h)

El valor de este atributo está definido por el ASSR, dada la QOS de protección.

– Enc_Key: Referencia de la clave de cifrado, forma definida por el ASSR

– Dec_Key: Referencia de la clave de descifrado, forma definida por el ASSR

NOTA – Mecanismos y atributos adicionales pueden ser identificados en versiones futuras de la presente Recomendación | Norma Internacional y/o para mecanismos privados.

5.2.1 Servicios de seguridad para el protocolo de transporte en modo con conexión

Cuando se utiliza el TLSP para prestar servicios de seguridad en modo con conexión, la entidad de transporte debe asociar un SA-ID a cada conexión de transporte protegida (Kg_tc), cada par de sistemas de extremo de transporte (Kg_esp) o cada sistema de extremo de transporte y conjunto de niveles de seguridad (Kg_esp_sr). El SA-ID se creará de manera explícita para la conexión o conexiones de transporte protegidas. Los servicios de seguridad que han de prestarse en la conexión son los definidos por la asociación de seguridad. Todas las TPDU enviadas o recibidas por una(s) conexión(es) de transporte protegidas se protegerán de acuerdo con los servicios asociados a la asociación de seguridad. En el caso de Kg_tc, existe una relación de uno a uno entre una conexión de transporte y una asociación de seguridad.

Si se desea integridad en modo con conexión, los servicios de seguridad asociados a la asociación de seguridad deben incluir el procesamiento del valor de comprobación de integridad (ICV = verdadero). Deben descartarse cualesquiera TPDU protegidas inadecuadamente que se reciban. La recepción de TPDU protegidas inadecuadamente es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

5.2.2 Servicio de seguridad para el protocolo de transporte en modo sin conexión

Cuando se utiliza el TLSP para prestar servicios de seguridad en el servicio de transporte en modo sin conexión, la entidad de transporte debe asociar un SA-ID a:

- cada par de entidades de transporte (Kg_esp),
- cada par de entidad de transporte y conjunto de niveles de seguridad (Kg_esp_sr).

La entidad de transporte emisora protegerá cada una de la TPDU de acuerdo con los atributos asociados al SA-ID y situará el identificador par (SA-ID) en el parámetro SA-ID de la SE TPDU. Al recibirse una SE TPDU, la clave especificada por el parámetro SA-ID se utilizará para descifrar la TPDU y/o verificar su ICV. Se descartarán cualesquiera TPDU protegidas inadecuadamente que se reciban. La recepción de TPDU protegidas inadecuadamente es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

5.3 Servicios supuestos de la capa de red

Los servicios de seguridad prestados por el protocolo TLSP son independientes de cualesquiera servicios de seguridad que puedan ser utilizados por la capa de red.

5.4 Requisitos de gestión de seguridad

Este protocolo de seguridad exige que los atributos de una asociación de seguridad se hayan establecido con anterioridad a un caso de comunicación protegida de datos de usuario. Dichos atributos pueden establecerse utilizando funciones de gestión de seguridad que quedan fuera del ámbito de la presente Recomendación | Norma Internacional, o utilizando el protocolo SA-P.

El grado de protección alcanzado dependerá de la gestión adecuada de la seguridad, incluida la gestión de claves. En los procedimientos de la presente Recomendación | Norma Internacional se supone que:

a) se dispone de almacenamiento de claves criptográficas;

b) las entidades de transporte emisoras y receptoras disponen de la misma clave criptográfica, si se utiliza un sistema de asignación de claves simétrica. Si la asignación de claves es asimétrica, las entidades de TLSP emisoras y receptoras no disponen de las mismas claves criptográficas. La presente Recomendación | Norma Internacional permite el sistema de claves simétricas o el de claves asimétricas;

c) las claves criptográficas están emparejadas. Véase 3.2.4.

Esta Recomendación | Norma Internacional no especifica cómo se crean, se actualizan o se gestionan en general las claves criptográficas.

5.5 Características mínimas de los algoritmos

Las entidades de transporte emisoras y receptoras deben utilizar el mismo o los mismos algoritmos criptográficos. En relación con estos algoritmos se establecen las siguientes hipótesis:

a) Para la prestación de los servicios de confidencialidad e integridad deberá utilizarse el mismo algoritmo o un algoritmo diferente.

b) El cifrado y el descifrado se efectúa en múltiplos de octetos.

c) La sincronización o la inicialización criptográfica se realiza para cada TPDU.

Queda fuera del ámbito de la presente Recomendación | Norma Internacional la especificación de un algoritmo particular o la evaluación de la solidez o las deficiencias, con respecto a la seguridad, de determinados algoritmos.

5.6 Función de encapsulación de seguridad

La encapsulación se utiliza junto con la función de cifrado y/o comprobación de integridad para la prestación de servicios de confidencialidad e integridad en modo con conexión o en modo sin conexión. La función de cifrado tiene siempre una base criptográfica mientras que las funciones de comprobación de integridad pueden basarse o no en la criptografía. Esto depende de los requisitos del usuario. Cuando es utilizada por la entidad emisora, la encapsulación se

aplica después de todas las funciones de procesamiento de protocolo descritas en la Rec. UIT-T X.224 | ISO/CEI 8073 y en la Rec. UIT-T X.234 | ISO 8602, excepto antes de la multiplexación y la asignación de conexión de red. La desencapsulación es aplicada por la entidad receptora después de la demultiplexación y antes que cualesquiera otras funciones de procesamiento de protocolos.

5.6.1 Función de cifrado de datos

Un mecanismo de cifrado proporciona la confidencialidad de los datos. Cada SE TPDU contiene información suficiente para el descifrado con independencia de la información en cualquier otra SE TPDU. Esto comprende la identificación de los atributos de asociación de seguridad (SA-ID) que han de utilizarse para el descifrado, así como cualesquiera secuencias de sincronización criptográfica o de inicialización de algoritmos.

5.6.2 Función de integridad

Esta función sustenta la integridad y la autenticación del origen de los datos en modo sin conexión o con conexión. Los elementos de integridad y los mecanismos utilizados para proporcionarlos son:

Protección contra	Mecanismo	CBTSS (CO)	GTSS (CL)
Modificación	ICV calculado en el encabezamiento protegido y la PDU encapsulada	x	x
Inserción	ICV y números de secuencia de transporte	x	
Supresión	ICV y números de secuencia de transporte	x	
Reproducción de conexión	Clave independiente por cada conexión de transporte (Kg_tc) o identificador de conexión exclusivo en cada clave	x	
Reproducción de PDU	Clave independiente por cada conexión de transporte (Kg_tc) y utilización de números de secuencia exclusivos en cada clave o identificador de conexión y número de secuencia exclusivos en cada clave	x	
Reflexión	Indicador de dirección (campo de banderas) en cada SE TPDU	x	x
Usurpación de identidad	ICV y clave de integridad o cifrado exclusiva de una dirección de transporte	x	

5.6.3 Función de etiqueta de seguridad

El etiquetado de seguridad es una función facultativa que puede utilizarse para asociar una etiqueta de seguridad a cada conjunto de TPDU encapsuladas. La etiqueta indica la sensibilidad de los datos. La etiqueta de seguridad admite mecanismos de control de acceso.

La estructura e interpretación del contenido de la etiqueta son definidas por diferentes autoridades definidoras. La autoridad definidora se identifica mediante un identificador de objeto, codificado como una definición de contenido según se especifica en la Rec. X.209 del CCITT | ISO/CEI 8825.

5.6.4 Función de relleno de seguridad

El relleno de seguridad es una función facultativa que puede utilizarse para aumentar la longitud de un conjunto de TPDU encapsuladas, según se requiera. Esta función admite los requisitos de los algoritmos criptográficos a efectos de confidencialidad e integridad.

5.6.5 Función de autenticación de entidad par

Esta función efectúa la autenticación de entidad par intercambiando las PDU de establecimiento de conexión encapsuladas que contienen un identificador de conexión, tal como se muestra en la Figura 3.

Las referencias de origen y destino deben ser:

- de integridad protegida, y
- exclusivas mientras dura la clave de integridad.

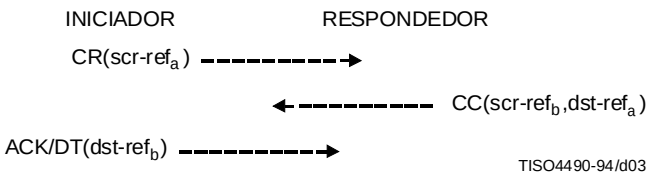


Figura 3 – Ilustración de intercambios para sustentar la autenticación de entidad par

5.6.6 Función SA que utiliza el protocolo SA-P dentro de banda

Este protocolo puede inicializarse mediante los procedimientos definidos en la Rec. UIT-T X.224 | ISO/CEI 8073 para soportar la transferencia de las PDU de SA-P, pero dicha inicialización debe efectuarse antes del establecimiento de la conexión de transporte o a través de canales de gestión local. Si se emplean los procedimientos definidos en la Recomendación UIT-T X.224 | ISO/CEI 8073, deberá utilizarse un número de referencia local para indicar inequívocamente que éste se emplea en la capa de transporte para el establecimiento, mantenimiento y liberación de la SA.

NOTA – Si en los sistemas que aplican la Rec. UIT-T X.234 | ISO 8602 se estima que no se dispone del nivel de fiabilidad que corresponde al establecimiento de una asociación de seguridad, se puede tomar la decisión, en dichos sistemas, de no utilizar el método SA-P dentro de banda para el establecimiento de la asociación de seguridad.

6 Elementos de procedimiento

Los elementos de procedimiento son los indicados en la especificación del protocolo de transporte en modo con conexión (véase la Rec. UIT-T X.224 | ISO/CEI 8073) y en el protocolo para la prestación del servicio de transporte en modo sin conexión (véase la Rec. UIT-T X.234 | ISO 8602), con las siguientes adiciones.

Los mecanismos de protocolo descritos más adelante son los utilizados para la encapsulación de datos. Una SE TPDU contiene:

a) un encabezamiento en texto claro;

b) un contenido longitud y bandera protegidos; si no se emplea confidencialidad, este encabezamiento también es en texto claro;

c) una sola TPDU o un conjunto TPDU concatenadas de acuerdo con las reglas de la Rec. UIT-T X.224 | ISO/CEI 8073;

d) un campo de parámetro ICV, si se emplea la protección de integridad;

e) campos de relleno apropiados para integridad y confidencialidad;

f) una etiqueta de seguridad, si se selecciona el mecanismo de etiqueta.

Una TPDU se protegerá en base a los atributos de la asociación de seguridad y se encapsulará en una SE TPDU. Al recibir una SE TPDU, la entidad de transporte verificará la presencia de toda la protección especificada por los atributos de la clave de asociación de seguridad. Se descartarán las TPDU con protección inadecuada (no protegidas de acuerdo con los atributos de la SA).

NOTA – La recepción de TPDU protegidas inadecuadamente es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

Si se invoca la función de encapsulación de seguridad para una TPDU para la que no existe una SA adecuada, el TLSP puede invocar un protocolo de establecimiento SA, como se especifica en la presente Recomendación | Norma Internacional, o ejecutar cualquier otra acción apropiada.

6.1 Concatenación y separación

El procedimiento de concatenación y separación es el especificado en 6.4 de la especificación de protocolo de transporte en modo con conexión (véase la Rec. UIT-T X.224 | ISO/CEI 8073), con los siguientes cambios:

a) La concatenación sólo se efectuará antes de la encapsulación. Cualquier TPDU definida en la Rec. UIT-T X.224 | ISO/CEI 8073 puede ser transferida después de haber sido encapsulada en una SE TPDU. Sólo se pueden concatenar las TPDU que han de ser protegidas bajo la misma clave de asociación de seguridad.

b) Una SE TPDU nunca será encapsulada en otra SE TPDU.

NOTA – Este procedimiento no se utiliza con el protocolo de transporte en modo sin conexión (Rec. UIT-T X.234 | ISO 8602).

6.2 Confidencialidad

6.2.1 Finalidad

La confidencialidad puede ser utilizada en el modo con conexión y en el modo sin conexión del protocolo de transporte, para la protección de extremo a extremo de TPDU y de la información de control de seguridad en tránsito entre entidades de transporte comunicantes.

6.2.2 TPDU y parámetros utilizados

El procedimiento utiliza la TPDU y los parámetros siguientes:

– SE-TPDU;

– SA-ID;

– sincronización criptográfica;

– relleno de cifrado.

6.2.3 Procedimiento

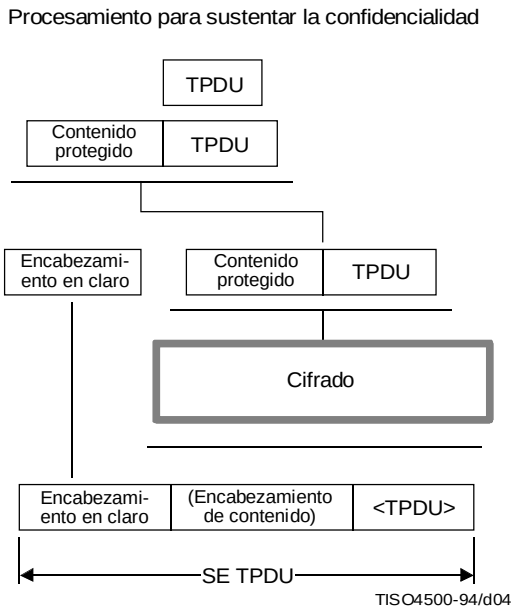
Si se ha especificado confidencialidad para una asociación de seguridad (Conf = verdadero), todas las TPDU deberán estar protegidas mediante su encapsulación dentro de una SE TPDU. Todos los octetos que sigan al SE-ID (encabezamiento protegido y TPDU) deberán estar cifrados. Véase la Figura 4. Si el algoritmo de cifrado necesita un campo de sincronización criptográfica, se adjuntará previamente al contenido protegido, después del encabezamiento en claro.

Antes del cifrado se colocará, si es necesario, un relleno de cifrado al final de la SE-TPDU, de modo que la longitud de contenido protegido (incluido el campo de longitud del contenido protegido) más la longitud del ICV y el campo de relleno del ICV (si se ha solicitado la integridad) más la longitud del relleno de cifrado sea un múltiple entero del tamaño del bloque de cifrado (Atributo Enc_Blk de la SA). En la recepción se utilizará el campo de sincronización criptográfica, si está presente, para la sincronización.

El algoritmo criptográfico es especificado por un atributo de la asociación de la seguridad que se identifica mediante el identificador de asociación de seguridad (SA-ID).

Al recibir una SE TPDU, la entidad de transporte utiliza la clave identificada por el SA-ID en la SE TPDU para identificar el servicio de seguridad y descifrar la SE TPDU. El contenido del campo de relleno de cifrado se pasará por alto en recepción. Si la clave no está disponible, se descarta la SE TPDU.

NOTA – La recepción de una SE-TPDU con un SA-ID no válido es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fueran del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).



NOTA – Las cantidades entre paréntesis son cantidades cifradas.

Figura 4 – Métodos de encapsulación del TLSP (Método del TLSP de encapsulación y cifrado para sustentar la confidencialidad, como se indica en 6.2)

6.3 Procesamiento de la integridad

Los procedimientos que se indican a continuación se utilizan para prestar servicios de integridad en modo sin conexión y en modo con conexión.

6.3.1 Procesamiento del valor de comprobación de integridad (ICV)

6.3.1.1 Finalidad

El procesamiento del ICV puede ser utilizado por el TLSP tanto en el modo con conexión (Rec. UIT-T X.224 | ISO/CEI 8073) como en el modo sin conexión (Rec. UIT-T X.234 | ISO 8602) del protocolo de transporte, para detectar modificaciones no autorizadas de los datos de usuario y de la información de control de seguridad, mientras transita entre entidades de transportes comunicantes.

6.3.1.2 TPDU y parámetros utilizados

El procedimiento utiliza la TPDU y los parámetros siguientes:

- SE TPDU;
- SA-ID;
- PAD de integridad;
- ICV.

6.3.1.3 Procedimiento

Hay dos tipos de procesamiento del ICV: el código de autenticación de mensaje (MAC) y el código de detección de manipulación (MDC). La diferencia entre la utilización de MAC o de MDC está relacionada directamente con lo que se haya especificado: integridad o integridad y confidencialidad. Si se elige sólo integridad se utilizará un MAC basado en

la criptografía. Si se elige integridad y confidencialidad, el ICV puede ser un código de detección de manipulación no basado en la criptografía (MDC), tal como un XOR o una suma de control, o puede estar basado en la criptografía, tal como el MAC. No es preciso que se base en la criptografía, ya que la totalidad del contenido estará cifrado porque se ha elegido también la confidencialidad. Si sólo se elige confidencialidad no hay campo de ICV.

Si se especifica integridad de datos (Integ = verdadero) para una asociación criptográfica, un ICV protegerá todas las SE TPDU. El código de autenticación de mensaje (MAC) se transporta en el parámetro ICV y se produce como el último campo de la SE TPDU. El ICV se calcula en los contenidos protegidos y en la TPDU encapsulada. Si se especifica confidencialidad (Conf = Verdadero) además de integridad, el código de detección de manipulación (MDC) o el MAC basado en la criptografía se calculan antes del cifrado. En los contenidos protegidos se colocará, si hace falta, un relleno de integridad de modo que la longitud del contenido protegido (incluido el campo de contenido protegido) sea un múltiplo entero del tamaño del bloque de ICV (Atributo ICV_Blk de la SA). El contenido del relleno de integridad se pasará por alto en recepción. Véase la Figura 5.

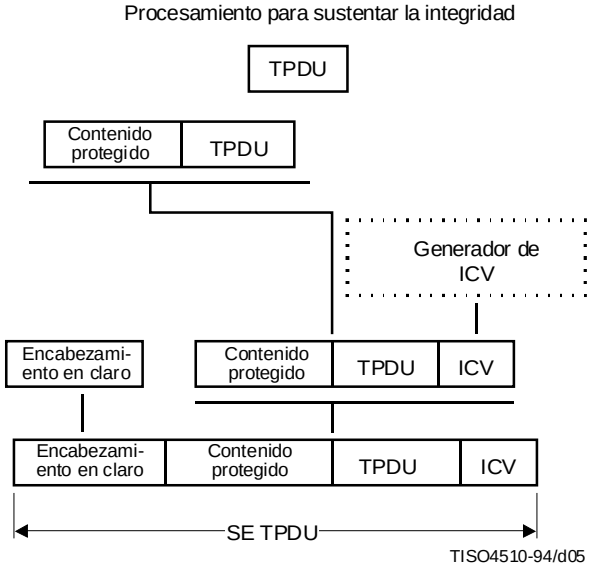


Figura 5 – Métodos de encapsulación del TLSP
(Método del TLSP de encapsulación y generación de ICV para sustentar la integridad, como se indica en 6.3)

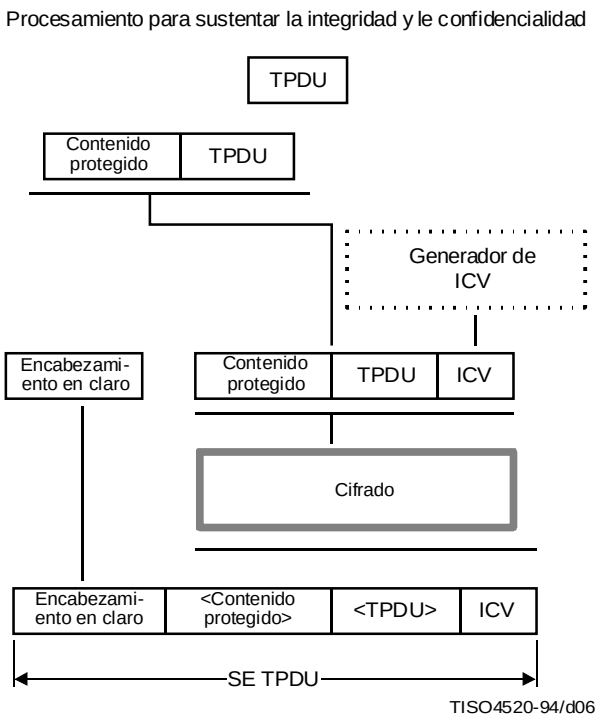
La función de comprobación de integridad y la longitud del campo de ICV son atributos de la asociación de seguridad.

Al recibirse una SE TPDU en una asociación de seguridad con protección de integridad, el campo de ICV se verificará calculando un valor de comprobación de integridad de prueba en los contenidos protegidos y el conjunto de TPDU encapsuladas. Si la asociación de seguridad identificada por el SA-ID no está disponible o el valor de comprobación de integridad de prueba no es igual al campo de ICV, deberá descartarse toda la SE TPDU.

NOTA – El fallo de la comprobación del ICV es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

Si se requiere también descifrado, la verificación del valor de comprobación de integridad se efectuará tras el descifrado.

La Figura 6 describe la integridad y la confidencialidad.



NOTA – Las cantidades entre paréntesis son cantidades cifradas.

Figura 6 – Método de encapsulación del TLSP
(Método del TLSP de encapsulación y generación de ICV para sustentar la «integridad» y la «confidencialidad», como se indica en 6.2 y 6.3)

6.3.2 Procesamiento del indicador de sentido

6.3.2.1 Finalidad

La finalidad del indicador de sentido es proporcionar protección contra la reflexión.

6.3.2.2 TPDU y parámetros utilizados

El procedimiento utiliza la TPDU y los parámetros siguientes:

– SE TPDU

– FLAGS (banderas).

6.3.2.3 Procedimiento

Cada SE TPDU contendrá el bit indicador de sentido (campo FLAGS) que indica el emisor de la TPDU. Los participantes en la asociación de seguridad ya han decidido quién es el respondedor y quién el iniciador. Cuando una SE TPDU es enviada por el iniciador de la asociación de seguridad, el bit indicador de sentido se pondrá a 1. Cuando una SE TPDU es enviada por el respondedor de la asociación de seguridad, el bit indicador de sentido se pondrá a 0. Al recibir una SE TPDU, la entidad de transporte validará el bit indicador de sentido. Si se recibe una SE TPDU con un indicador de sentido incorrecto, se descartará la TPDU.

NOTA – La recepción de una SE TPDU con indicador de sentido incorrecto es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

6.3.3 Procesamiento del número de secuencia de integridad de conexión

La detección de reproducción, inserción y supresión requiere que cada TPDU de una asociación de seguridad tenga un número de secuencia exclusivo. Cuando se especifica integridad en modo con conexión para una conexión (Kg_tc e Integ_yes), la integridad se proporciona utilizando una clave por cada conexión junto con el procedimiento de número de secuencia exclusivo (véase 6.3.3.1). Este procedimiento no se utiliza con la Rec. UIT-T X.234 | ISO 8602.

6.3.3.1 Números de secuencia exclusivos

Los números de secuencia exclusivos son los mismos números de secuencia indicados en la Rec. UIT-T X.224 | ISO/CEI 8073 (véanse 6.10 y 6.11).

6.3.3.2 Finalidad

Los números de secuencia exclusivos constituyen un procedimiento facultativo para identificar de manera única cada DT y ED TPDU (datos de transporte normales y acelerados) dentro de una conexión. Este procedimiento sólo es aplicable a la Rec. UIT-T X.224 | ISO/CEI 8073 (clases 2, 3 y 4).

6.3.3.3 Procedimiento

Si se especifica el servicio de integridad en modo con conexión para una conexión de transporte (Kg_tc e Integ = verdadero), cada TPDU deberá tener números de secuencia exclusivos en una asociación de seguridad. Ninguna entidad de transporte transmitirá una nueva DT o ED TPDU con un número de secuencia (ya sea TPDU NR o ED TPDU NR) que hubiera sido utilizado previamente con esa clave. Las retransmisiones, en tanto que parte del control de errores y la recuperación normales, pueden repetir el número de secuencia de la clave original o utilizar una nueva clave. Cuando se agota el espacio de números de secuencia de DT o ED en una determinada conexión, podrá utilizarse una clave criptográfica distinta de las empleadas previamente para proteger datos utilizando ese identificador de conexión (DST-REF), con el fin de transmitir cualesquiera TPDU de datos ulteriores. Se invocará el procedimiento de sustitución de clave (véase 6.7). Si no existe tal clave podrá liberarse la conexión. Cuando se reciba una DT o ED TPDU que repite un número de secuencia recibido anteriormente en la clave criptográfica vigente, la entidad de transporte deberá descartar la TPDU.

NOTA – La recepción de una DT o ED TPDU con un número de secuencia repetido es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

El número de secuencia exclusivo es el número de secuencia de transporte utilizado en las clases 2, 3 y 4. Se recomienda la utilización de números de secuencia ampliados para evitar la sustitución de claves.

6.4 Procesamiento de la comprobación de la dirección par

6.4.1 Finalidad

Este procedimiento tiene como finalidad contrarrestar las usurpaciones de identidad y sustentar la autenticación del origen de los datos.

6.4.2 Procedimiento

Al recibirse una TPDU, deberá compararse la dirección par asociada a la clave criptográfica con la dirección de origen de la TPDU. Si las direcciones no concuerdan, se descarta la SE TPDU.

NOTA – La recepción de una SE TPDU con dirección no válida es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fueran del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

Para cada tipo de granularidad de clave existe un grado correspondiente de información de dirección par que requiere verificación. Cuando se utiliza la asignación de claves por cada sistema de extremo (Kg-esp), se verifica la dirección del NSAP de la entidad de transporte par con la dirección par negociada. Cuando se utiliza la asignación de claves por cada sistema de extremo y nivel de seguridad (Kg-esp-sr), se verifica la etiqueta de seguridad de la SE TPDU con el conjunto de niveles de seguridad negociado, además de verificar la dirección del NSAP de la entidad de transporte par. Puesto que la etiqueta de seguridad no es, en sentido estricto, una información de seguridad y puede ser utilizada facultativamente con asociaciones de seguridad de un solo nivel, la comprobación de la etiqueta de seguridad se efectúa de manera independiente, según se analiza en otro lugar (véase 6.5, Etiquetas de seguridad para asociaciones de seguridad).

Cuando se utiliza la asignación de claves por cada conexión (Kg_tc), el procedimiento resulta un poco más complejo, ya que deben verificarse los identificadores de conexión de transporte (SRC-REF, DST-REF) llevados dentro de cada TPDU, además de la dirección del NSAP de la entidad de transporte par. La SRC-REF se contrasta con la porción número de referencia de transporte distante del atributo de seguridad de la dirección par y la DST-REF con la referencia local para la conexión. Obsérvese que una entidad de transporte que inicia una conexión puede no conocer la referencia local utilizada por su par y puede no ser capaz de verificar la SRC-REF de una CC TPDU entrante. Esta situación se produce cuando el par determina dinámicamente la referencia local al procesar una CR TPDU, y no se dispone de ningún valor para que el gestor de claves lo transmita en el momento en que se establecen los atributos de seguridad. Siempre que el campo DST-REF de la CC TPDU sea igual que la referencia local para la conexión, la TPDU puede ser aceptada y el valor del campo SRC-REF retenido.

6.5 Etiquetas de seguridad para asociaciones de seguridad

6.5.1 Finalidad

Las etiquetas de seguridad se utilizan para sustentar el control de acceso y la separación de datos en base a la sensibilidad.

6.5.2 TPDU y parámetros utilizados

El procedimiento utiliza la TPDU y los parámetros siguientes:

- SE TPDU;
- SA-ID;
- LABEL.

6.5.3 Procedimiento

Cuando una asociación de seguridad especifica la utilización de una etiqueta de seguridad explícita en todas las TPDU, deberá enviarse la etiqueta en el campo LABEL (ETIQUETA) del encabezamiento protegido de cada SE TPDU. Al recibir una SE TPDU con el parámetro LABEL, la entidad de transporte verificará que el parámetro LABEL se halla dentro del conjunto de niveles de seguridad aceptables para la asociación de seguridad. Si se recibe una SE TPDU con una LABEL inadecuada, se descartará la TPDU.

NOTA – La recepción de una SE TPDU que no pasa la comprobación de etiqueta es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto quedan fuera del ámbito de la presente Recomendación | Norma Internacional (por ejemplo, el relleno de informes de auditoría).

6.6 Liberación de conexión

Si se utiliza el servicio en modo conexión (Kg_tc), se prescindirá de la clave asociada a la conexión como parte del procedimiento de liberación de conexión.

6.7 Sustitución de claves

El procedimiento de sustitución de claves se emplea si expira el periodo de criptografía de una clave. Cuando se utiliza el servicio en modo con conexión (Kg_tc), también podrá emplearse cuando se hayan agotado los espacios de números de secuencia (véase 6.3.3.1).

La sustitución de clave asocia una nueva clase criptográfica a la(s) conexión(es) de transporte en curso. La nueva asociación de seguridad tendrá atributos que son idénticos a los de la antigua asociación de seguridad, salvo la nueva clave. Si no existe tal clave, se notificará a la entidad de gestión de seguridad y no se utilizará la clave criptográfica original para la transmisión. Una vez ejecutado el procedimiento de sustitución, se descartará la antigua clave criptográfica. Si no existe una nueva clave adecuada, este es un evento relacionado con la seguridad; no obstante, las acciones ulteriores al respecto, tales como el relleno de un informe de auditoría, se consideran un asunto local.

NOTA – La nueva clave debe estar disponible en el temporizador de actividad de transporte (para clase 4) o en el tiempo TWR (clase 3); en los demás casos, el protocolo de transporte puede terminar la conexión.

Tras una sustitución de clave, las DT y ED TPDU, sin acuse recibo, que requieren retransmisión, se enviarán con la nueva clave.

6.8 TPDU no protegidas

La política de seguridad puede permitir conexiones de transporte seguras y no seguras entre entidades comunicantes. La manera de conseguir esto es un asunto local.

En transmisión, si el atributo UNProt de la SA es verdadero, la TPDU se transfiere sin protección, sin añadir el procesamiento de la PCI según los procedimientos del TLSP.

En recepción, si el atributo UNProt de la SA es verdadero, la TPDU recibida se transfiere sin ningún procesamiento según los procedimientos del TLSP.

6.9 Identificación de protocolo

Si este protocolo se utiliza en una conexión de red, será identificado explícitamente por los procedimientos de identificación explícita definidos en la Norma ISO/CEI 11570. La propia UN TPDU identificadora puede estar protegida por el protocolo especificado en la presente Recomendación | Norma Internacional. Si la UN TPDU no está protegida y si especifica esta Recomendación | Norma Internacional junto con la Rec. UIT-T X.224 | ISO/CEI 8073 o la Rec. UIT-T X.234 | ISO 8602, las TPDU estarán protegidas tras la compleción satisfactoria del establecimiento de la conexión de red, de conformidad con los atributos de la SA. Si la UN TPDU está protegida y especifica sólo la Rec. UIT-T X.224 | ISO/CEI 8073 o sólo la Rec. UIT-T X.234 | ISO 8602, se utiliza el único protocolo especificado tras la compleción satisfactoria del establecimiento de la conexión de red.

NOTAS

1 La sustentación o no de una comunicación no protegida depende de los atributos de la SA.

2 La sustentación de TC no protegidas, multiplexadas o no con TC protegidas en la misma NC, depende de los atributos de la SA y de la política de seguridad de la entidad.

El procedimiento de identificación explícita definido en la Norma ISO/CEI 11570 no se utiliza si se aplica la Rec. UIT-T X.224 | ISO/CEI 8073 (clase 4) en el servicio de red en modo sin conexión de OSI definido en la Norma ISO 8348.

6.10 Protocolo de asociación de seguridad

Un protocolo de asociación de seguridad (SA-P) se lleva a efecto mediante el intercambio de unidades PDU de SA y tiene por finalidad permitir el establecimiento y la «personalización» de una SA.

Los campos precisos de la PDU de SA utilizados para el intercambio de información de seguridad dependen del mecanismo concreto utilizado para proporcionar la SA. Cualquiera que sea el mecanismo empleado para el SA-P, deberá proporcionar lo siguiente:

a) derivación de todos los atributos SA requeridos para la forma de protección seleccionada;

b) autenticación de claves derivadas;

c) establecimiento de información inicial para fines de autenticación y de integridad, si se requiere;

d) reaplicación de clave;

e) liberación de la asociación de seguridad.

Para esta función puede utilizarse un algoritmo simétrico o asimétrico. Se recomienda la utilización de un algoritmo asimétrico. En el Anexo B se presenta un ejemplo de dicho mecanismo.

Durante la parte del establecimiento de una SA que requiere el intercambio de información en una forma no protegida, deberán utilizarse unidades PDU de SA. Los intercambios de información protegida requeridos para el establecimiento de la SA pueden efectuarse en unidades PDU de SA o TPDU de SE.

Inmediatamente después de recibir la PDU de SA final en el protocolo SA-P, si hay una TPDU en espera de la encapsulación de seguridad, se procesa y se transmite dicha unidad.

NOTA – La última PDU de SA con información de control de seguridad deberá fijar la bandera en el sentido respondedor a iniciador, en el SA-P. Si es necesario, se puede enviar una PDU de SA con SA-ID local y SA-ID de par como único contenido.

Si no se produce la secuencia esperada de unidades PDU dentro de un periodo de temporización especificado, podrá repetirse cualquier número de veces, una PDU de SA utilizada para el intercambio de información de control de seguridad (SCI). La recepción de unidades PDU de SA, habiéndose recibido anteriormente SCI, tendrá por efecto que se retransmitan las PDU de SA que se habían enviado anteriormente como respuesta. Las PDU de SA con SCI que estén fuera de la secuencia esperada deberán ignorarse.

Una entidad TLSP puede abortar un procedimiento de establecimiento de la SA e ignorar las subsiguientes PDU de SA con SCI si fracasa cualquier comprobación.

7 Utilización de elementos de procedimiento

El Cuadro 1 da una visión de conjunto de los elementos de procedimiento que se incluyen en cada clase de la Rec. UIT-T X.224 | ISO/CEI 8073 y en la Rec. UIT-T X.234 | ISO 8602.

Cuadro 1 – Elementos de procedimiento TLSP

Mecanismo de protocolo	Referencia (subcláusula)	Rec. UIT-T X.224 | ISO/CEI 8073, Clase					Rec. UIT-T X.234 | ISO 8602
Confidencialidad criptográfica	6.2	m	m	m	m	m	m
Procesamiento del ICV	6.3.1	m	m	m	m	m	m
Procesamiento del indicador de sentido	6.3.2	*	*	*	*	*	*
Números de secuencia exclusivos	6.3.3.1	NA	NA	o	o	o	NA
Procesamiento de comprobación de dirección par	6.4	*	*	*	*	*	*
Etiquetas de seguridad para asociación criptográfica	6.5	o	o	o	o	o	o
Liberación de conexión	6.6	o	o	o	o	o	NA
Sustitución de clave	6.7	o	o	o	o	o	o

* Procedimiento incluido siempre en la clase.

NA No aplicable.

o Procedimiento negociable cuya implementación en el equipo es facultativa.

m Procedimiento negociable cuya implementación en el equipo es obligatoria.

NOTA – La negociación de este procedimiento queda, actualmente, fuera del ámbito de la presente Recomendación | Norma Internacional. No obstante, el procedimiento del SA-P del 6.10 permite que esta negociación se efectúe en cualquier momento antes de la conexión como parte del TLSP.

8 Estructura y codificación de las TPDU

8.1 Estructura de la TPDU

La estructura de la TPDU, o de TPDU concatenadas, antes de la encapsulación (es decir, situada en el campo «datos protegidos» de una TPDU, véase 8.2) es tal como se define en 13.2 de la Rec. UIT-T X.224 | ISO/CEI 8073.

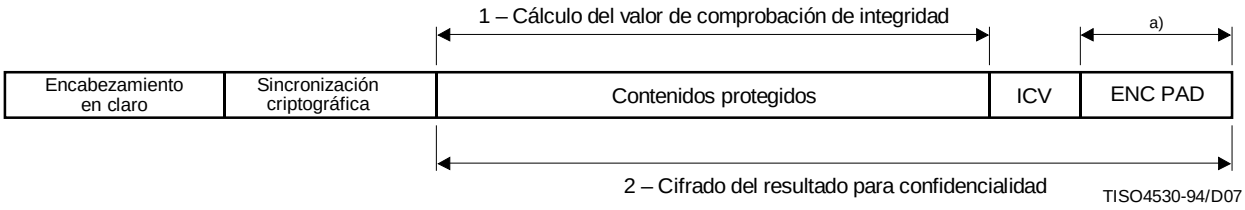
8.2 TPDU de encapsulación de seguridad

Todas las unidades de datos de protocolo de transporte (las SE TPDU) contendrán un número entero de octetos. Los octetos de una SE TPDU se numeran comenzando por uno y aumentando en el orden en que son introducidos en una NSDU. Los bits de un octeto están numerados del 1 al 8, siendo el bit 1 el bit de orden inferior.

Cuando se utilizan octetos consecutivos dentro de la SE TPDU para representar un número binario, el número de octeto más bajo tiene el valor más significativo.

En las Figuras que siguen se indica, debajo de cada campo de longitud fija de la SE TPDU, el número de octetos de ese campo.

La estructura de la TPDU será como sigue:



a) Este campo depende de si el algoritmo de cifrado seleccionado requiere un relleno de cifrado independiente.

Figura 7 – Estructura de la TPDU

8.2.1 Encabezamiento en claro

Véase la Figura 8.

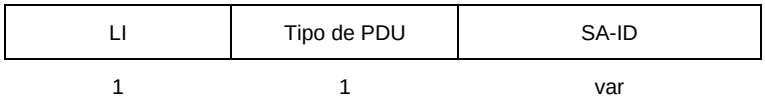


Figura 8 – Formato del encabezamiento en claro

8.2.1.1 Longitud del encabezamiento en claro de la PDU

El campo indicador de longitud (LI) del encabezamiento en claro de la PDU contiene la longitud del tipo de PDU y de la SA-ID en octetos, con exclusión del propio campo indicador de longitud.

8.2.1.2 Tipo de PDU

Este campo contiene el código del tipo de PDU y se utiliza para definir la estructura del encabezamiento restante. El valor del código del tipo de PDU es: 0100 1000.

8.2.1.3 SA-ID

El campo de identificador de asociación de seguridad (SA-ID) contiene el identificador distante de la clave criptográfica utilizada para proteger la TPDU.

8.2.2 Sincronización criptográfica

Este es un campo facultativo que puede contener datos de sincronización para un identificador de algoritmo de cifrado específico, contenido en los atributos de la asociación de seguridad.

NOTA – El tamaño de este campo lo conocerían las entidades participantes y parte de los atributos de la asociación de seguridad.

8.2.3 Contenido protegido

La Figura 9 muestra el formato de contenido protegido de la PDU segura.

Longitud del contenido	Bandera/tipo	Etiqueta	Datos protegidos	INT PAD
1-3	1	(tlv)	(tlv)	(tlv)[a)]

a) Puede ser un relleno de un solo octeto.

Figura 9 – Contenido protegido

8.2.3.1 Estructura del campo de contenido protegido

Los campos de contenido protegido son tipo, longitud y valor (tlv) codificados.

El tipo de campo de contenido tiene la siguiente atribución:

Valor	*Tipo de campo de contenido*
00-7F	Reservado para uso privado
80-BF	Reservado
C0	Datos protegidos
C1-C5	Reservado
C6	Etiqueta
C7-CF	Reservado
D0	Reservado
D1	Relleno de un solo octeto
D2	Reservado
D3	Relleno de integridad
D4	Relleno de cifrado
D5-FF	Reservado para uso futuro

Si se requiere un campo de relleno de dos octetos para PAD (RELLENO) de integridad o de cifrado, el campo de longitud tendrá el valor 0 con el tipo de campo de contenido apropiado.

La longitud del campo de contenido contiene la longitud del valor del campo de contenido en octetos. La longitud del campo de contenido puede ser de uno, dos o tres octetos.

a) Si la longitud es de un octeto, el bit 8 es 0 y los 7 bits restantes definen una longitud de valor de hasta 127 octetos.

b) Si la longitud es de dos octetos, el primer octeto se codifica 1000 0001 y los octetos restantes definen longitudes de campo de hasta 255 octetos.

c) Si la longitud es de tres octetos, el primer octeto se codifica 1000 0010 y los dos octetos restantes definen longitudes de campo de hasta 65, 535 octetos.

Otros valores del primer octeto quedan reservados para uso futuro.

8.2.3.2 Longitud del contenido

El campo de longitud contiene la longitud de los contenidos protegidos en octetos, excluido el campo de longitud de contenido (es decir, bandera, etiqueta, datos protegidos y relleno de ICV). Tiene un valor máximo de 65, 535 ($2^{16} – 1$).

8.2.3.3 Banderas

Véase la Figura 10.

Valor
1

Figura 10 – Campo de banderas

Los bits actualmente definidos en este campo son:

– *bit 1 indicador de sentido*

0 = respondedor a iniciador;

1 = iniciador a respondedor.

– *bit 4 hacia afuera/respuesta*

0 = hacia afuera;

1 = respuesta.

Los bits 2 a 3 y 5 a 8 bits de bandera no utilizados se ponen a cero en transmisión.

8.2.3.4 Etiqueta

Véase la Figura 11.

C6 Hex	Longitud de etiqueta	Longitud de autoridad definidora	Autoridad definidora	Valor
1	1-3	1-3	var	var

Figura 11 – Formato del campo de etiqueta

El formato del campo de valor lo define la autoridad definidora.

NOTA – Se prevé que estas etiquetas se registrarán mediante los procedimientos definidos por UIT-T (antes CCITT) e ISO. Una autoridad definidora se registrará como un valor de identificador de objeto de acuerdo con ISO 8824, codificado de acuerdo con ISO 8825, y mediante los procedimientos definidos en ISO/CEI 9834.

8.2.3.5 Datos protegidos

El campo de datos contiene una TPDU o un conjunto de TPDU concatenadas, según la Rec. UIT-T X.224 | ISO/CEI 8073 o la Rec. UIT-T X.234 | ISO 8602 (véase la Figura 12).

C0 Hex	Longitud	Datos protegidos
1	var	var

Figura 12 – Formato del campo de datos protegidos

8.2.3.6 Relleno de integridad

El campo de valor contiene datos arbitrarios requeridos para los mecanismos de integridad.

La longitud de relleno viene definida por:

a) El relleno que necesita el mecanismo de integridad.

El mecanismo de integridad utilizado tiene características conocidas, entre las que figurarán la longitud de bloque definida para la utilización en la asociación de seguridad (si el mecanismo se utiliza en el modo bloque). El punto de comienzo del proceso de integridad al final del relleno de integridad debe ser un múltiplo entero de la longitud del bloque.

b) El relleno que necesita el mecanismo de cifrado de bloque para llevar el final del ICV hasta el final del tamaño del bloque, si no se requiere un relleno de cifrado separado.

La elección del valor de relleno es un asunto local. Si se necesita un relleno de dos octetos, la longitud es cero sin valor. Si se necesita un relleno de un solo octeto, se utiliza un relleno de un solo octeto (tipo = D1, sin longitud ni valor) en vez del relleno de integridad.

8.2.4 ICV

El campo de ICV contiene el valor de comprobación de integridad. La longitud de este campo viene impuesta por el identificador de algoritmo del ICV contenido en los atributos de la asociación de seguridad.

8.2.5 Relleno de cifrado

El tamaño de bloque para cifrado es una característica conocida del algoritmo de cifrado. El punto de comienzo del proceso de confidencialidad, al final del ICV, debe ser un múltiplo entero de la longitud de bloque. La presencia del relleno de cifrado que sigue al ICV depende de si el algoritmo de cifrado seleccionado requiere un relleno de cifrado independiente.

La elección del valor de relleno es un asunto local. Si se necesita un relleno de dos octetos, la longitud es cero sin valor. Si se necesita un relleno de un solo octeto, se utiliza un relleno de un solo octeto (tipo = D1, sin longitud ni valor) en vez del relleno de cifrado.

8.3 PDU de asociación de seguridad

El formato de la PDU de SA se muestra en la Figura 13.

LI	Tipo de PDU	SA-ID	Tipo de SA-P	Contenido de PDU de SA
1	1	var	tlv	var

Figura 13 – Estructura de la PDU de SA

8.3.1 LI (indicador de longitud)

Este campo contiene la longitud del campo de tipo de PDU más el SA-ID. Si el SA-ID necesita señalar que no conoce el SA-ID de su par (por ejemplo, cuando se establece una nueva SA), el campo de longitud se fijará de tal modo que el campo de SA-ID no esté presente (es decir, al valor 1).

8.3.2 Tipo de PDU

Este campo contiene el valor de tipo de PDU 0100 1001 para indicar una PDU de asociación de seguridad.

8.3.3 SA-ID (identificador de asociación de seguridad)

El campo SA-ID contiene el identificador de asociación de seguridad del receptor (es decir, el atributo SA Peer_SAID). Este campo no es necesario cuando se utiliza para establecer una nueva SA (es decir, cuando el receptor todavía no ha asignado un SA-ID).

8.3.4 Tipo de SA-P

Este campo contiene un identificador de objeto que indica el mecanismo utilizado para proporcionar el protocolo SA, como se expresa más adelante.

El identificador de objeto asignado para intercambio de clave exponencial (definido en el Anexo D) es:

joint-ccitt-iso (2) tlsp (21) sa-p-kte (1) eke (1).

La utilización de otros algoritmos con el SA-P puede indicarse por ulteriores identificadores adjudicados («allocated») de acuerdo con ISO 9834-1 (Procedimientos de registro).

8.3.5 Contenido de la PDU de SA

La estructura interna de este campo depende del mecanismo que proporciona el protocolo SA, especificado en 8.3.4. En el Anexo B se define un protocolo de esta naturaleza que utiliza los mecanismos de intercambio de clave y de firma digital.

9 Conformidad

9.1 Generalidades

Se rellenará un enunciado de conformidad de realización de protocolo (PICS) con respecto a cualquier alegación de conformidad de una realización con esta Recomendación | Norma Internacional. El PICS se elaborará de acuerdo con el formulario PICS pertinente.

9.2 Requisitos de conformidad estática comunes

a) Una realización conforme admitirá por lo menos el TLSP con la Rec. UIT-T X.224 | ISO/CEI 8073 o la Rec. UIT-T X.234 | ISO 8602.

b) Una realización conforme admitirá la aplicación en un sistema de extremo.

c) Todo sistema que alega conformidad con el TLSP será capaz de la encapsulación y la extracción de datos de usuario dentro de una PDU de transferencia de datos segura.

d) Todo sistema que alega prestar servicios de seguridad de confidencialidad admitirá por lo menos el mecanismo de cifrado.

e) Todo sistema que alega prestar servicios de seguridad de integridad admitirá por lo menos el mecanismo de ICV.

9.3 TLSP con requisitos de conformidad estática de la Rec. UIT-T X.234 | ISO 8602

Todo sistema que alega conformidad con el protocolo TLSP prestará por lo menos uno de los siguientes servicios de seguridad:

a) confidencialidad en modo sin conexión;

b) integridad en modo sin conexión.

9.4 TLSP con requisitos de conformidad estática de la Rec. UIT-T X.224 | ISO/CEI 8073

Todo sistema que alega conformidad con el TLSP prestará por lo menos uno de los siguientes servicios de seguridad:

a) confidencialidad en modo con conexión;

b) integridad en modo con conexión sin recuperación;

c) autenticación de identidad par.

9.5 Requisitos de conformidad dinámica comunes

Todo sistema que alega conformidad con la presente Recomendación | Norma Internacional tendrá el siguiente comportamiento:

a) Detección de todos los campos obligatorios y facultativos dentro de una PDU de transferencia de datos segura en una secuencia.

b) Los campos no reconocidos dentro de una PDU de transferencia de datos segura, se tratarán como un error, según se describe en 6.

9.6 TLSP con requisitos de conformidad dinámica de la Rec. UIT-T X.234 | ISO 8602

Todo sistema que alega conformidad con el protocolo TLSP tendrá el siguiente comportamiento:

– Cuando se proporciona autenticación del origen de los datos se invocará el mecanismo de cifrado o un mecanismo de ICV criptográfico.

9.7 TLSP con requisitos de conformidad dinámica de la Rec. UIT-T X.224 | ISO/CEI 8073

Todo sistema que alega conformidad con el protocolo TLSP tendrá el siguiente comportamiento:

– Cuando se proporciona autenticación de entidad par o del origen de los datos se invocará el mecanismo de cifrado o un mecanismo de ICV criptográfico.

10 Enunciado de conformidad de realización de protocolo (PICS)

El suministrador de una realización de protocolo que alega conformidad con la presente Recomendación | Norma Internacional rellenará un ejemplar del formulario de PICS presentado en el Anexo A, incluida la información necesaria para identificar tanto al suministrador como a la realización.

Anexo A

Formulario de PICS[a)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

A.1 Introduction

A.1.1 Background

The supplier of a protocol implementation which is claimed to conform to Recommendation | International Standard 10736 shall complete the Transport Layer Security Protocol (TLSP), Protocol Implementation Conformance Statement (PICS) proforma. A completed PICS proforma becomes the PICS for the implementation in question. The PICS is a statement identifying the capabilities and options of the protocol that have been implemented. The PICS can have a number of uses, including:

- use by the protocol implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;
- use by the supplier and receiver of the implementation, as a detailed indication of its capabilities, stated relative to the common basis of understanding provided by the standard PICS proforma;
- use by the user of the implementation, as a basis for checking the possibility of interworking with another implementation;
- use by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.1.2 Approach

The first part of the PICS proforma, the Implementation Identification and Protocol Summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation. The main part of the PICS proforma is a fixed-format questionnaire divided into subclauses, each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually “Yes” or “No”), or by entering a value or a set or range of values. Note that there are some items where two or more choices from a set of possible answers can apply. Therefore, all relevant choices are to be marked.

Each item is identified by an reference index in the first column; the second column contains the item to be addressed; the third column contains the reference(s) to the location of the item in the main body of the standard. For optional items, additional columns indicate the status of the item (i.e. whether support is mandatory, optional, or conditional), and provide space or a choice or items for the implementation support response.

The following status column notations described in ISO/IEC JTC1/ SC6 N6233, Catalogue of PICS Proforma Notations, are used for this PICS proforma:

Symbol	*Meaning*
m	Mandatory
o	Optional
–	Not applicable (N/A)
o.<n>	Optional, but support of at least one of the group of options labelled by the same numeral <n> is required
<cid>:	Conditional requirement, according to the condition or item index identified by <cid>
<item>::	Simple predicate condition, dependent on the support marked for <item>

---

a) Comunicado sobre derechos de autor del formulario de PICS:

Los usuarios de esta Recomendación pueden reproducir libremente el formulario de PICS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el PICS cumplimentado.

A.2 Implementation identification

See Table A.1.

Table A.1 – TLSP Implementation Identification

Item	Information
Supplier	
Contact point for queries about this PICS	
Implementation Name(s) andVersion(s)	
Other information necessary for full identification [e.g. Names and Version(s) for machines and operating systems, System Name(s)]	

NOTES

1 Only the first three items are required for each implementation. Other information may be completed as appropriate in meeting the requirements for full identification.

2 The terms “Name” and “Version” should be interpreted appropriately to correspond with a supplier’s terminology (e.g. using Type, Series, Model).

A.3 General statement of conformance

Table A.2 codifies the general statement of conformance for the implementation.

Table A.2 – General Conformance Statement

Index Item		Support	
SP	Does the implementation claim conformance with ISO/IEC 10736?	Y	N
SPMAN	Are all mandatory features of ISO/IEC 10736 implemented?	Y	N

A.4 Protocol implementation

Table A.3 identifies common abbreviations used in this PICs, these same abbreviations are found in ITU-T Rec. X.224 | ISO/IEC 8073, but are identified here for help in conforming to this PICS.

Table A.3 – CO and CL Transport Implemented

Index Transport Class Network Service	
C0	Class 0 over cons
C1	Class 1 over cons
C2	Class 2 over cons
C3	Class 3 over cons
C4	Class 4 over cons
C4L	Class 4 over clns
CLTP	Connectionless transport protocol

A.5 Security services supported

Tables A.4 to A.7 identify for each Class of Transport (COTP::), the security services available through the TLSP and their level of support within the implementation. The security services listed are taken from CCITT Rec. X.800 | ISO 7498-2.

Table A.4 – Service Element Proforma for C0

Index Service Element	Status	Support	
TOSE0 Confidentiality	o.1	Y	N
TOSE1 Connection Confidentiality	TOSE0:m	Y	N
TOSE2 Connectionless Confidentiality	–		
TOSE3 Integrity	o.1	Y	N
TOSE4 Connection Integrity w Recovery	–		
TOSE5 Connection Integrity wo Recovery		Y	N
TOSE6 Connectionless Integrity	TOSE3:m		
TOSE7 Peer Entity Authentication	o	Y	N
TOSE8 Access Control	o	Y	N
TOSE9 IN BAND SA-P	o	Y	N

Table A.5 – Service Element Proforma for C1, C2, C3

Index Service Element	Status	Support	
T3SE0 Confidentiality	o.1	Y	N
T3SE1 Connection Confidentiality	T3SE0:m	Y	N
T3SE2 Connectionless Confidentiality	–		
T3SE3 Integrity	o.1	Y	N
T3SE4 Connection Integrity w Recovery	–		
T3SE5 Connection Integrity wo Recovery	T3SE3:o.2	Y	N
T3SE6 Connectionless Integrity	T3SE3:o.2	Y	N
T3SE7 Peer Entity Authentication	o	Y	N
T3SE8 Access Control	o	Y	N

Table A.6 – Service Element Proforma for C4

Index Service Element	Status	Support	
T4SE0 Confidentiality	o.1	Y	N
T4SE1 Connection Confidentiality	T4SE0:m	Y	N
T4SE2 Connectionless Confidentiality	–		
T4SE3 Integrity	o.1	Y	N
T4SE4 Connection Integrity w Recovery	T4SE3:o.2	Y	N
T4SE5 Connection Integrity wo Recovery	–		
T4SE6 Connectionless Integrity	T4SE3:o.2	Y	N
T4SE7 Peer Entity Authentication	o	Y	N
T4SE8 Access Control	o	Y	N

Table A.7 – Service Element Proforma for C4L

Index Service Element	Status	Support	
TLSE0 Confidentiality	o.1	Y	N
TLSE2 Connectionless Confidentiality	TLSE0:m	Y	N
TLSE1 Connection Confidentiality	–		
TLSE3 Integrity	o.1	Y	N
TLSE4 Connection Integrity w Recovery	TLSE3:o.2		
TLSE5 Connection Integrity wo Recovery	–		
TLSE6 Connectionless Integrity	TLSE3:o.2	Y	N
TLSE7 Peer Entity Authentication	o	Y	N
TLSE8 Access Control	o	Y	N

Table A.8 identifies for connectionless Transport (CLTP::), the security services available through the TLSP and their level of support within the implementation.

Table A.8 – Service Element Proforma for CLTP

Index Service Element	Status	Support	
TCSE0 Confidentiality	o.1	Y	N
TCSE1 Connection Confidentiality	–		
TCSE2 Connectionless Confidentiality	TCSE0:m	Y	N
TCSE3 Integrity	o.1	Y	N
TCSE4 Connection Integrity w Recovery	–		
TCSE5 Connection Integrity wo Recovery	–		
TCSE6 Connectionless Integrity	TCSE3:m	Y	N
TCSE7 Data Origination Authentication	o	Y	N
TCSE8 Access Control	o	Y	N

A.6 Supported functions

Tables A.9 to A.16 identify the mandatory and optional functions implemented for each class of Transport (COTP::) supported.

Table A.9 – Mandatory Functions for C0

Index	Function	Reference (subclause)	Status	Support	
T0SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T0SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T0SF3	Security encapsulation	5.6	m	Y	
T0SF4	Reporting of security events	Notes	m	Y	

Table A.10 – Optional Functions for C0

Index	Function	Reference (subclause)	Status	Support	
T0SF5	Data encipherment	6.2	o.1	Y	N
T0SF6	Integrity protection	6.3	o.1	Y	N
T0SF7	Integrity padding	6.3.1.3	o	Y	N
T0SF8	Explicit security labeling	6.5	o	Y	N
T0SF9	Encipherment padding	6.2.2	o	Y	N

Table A.11 – Mandatory Functions for C1

Index	Function	Reference (subclause)	Status	Support	
T1SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T1SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T1SF3	Separation after decapsulation	6.1	m	Y	
T1SF4	Security encapsulation	5.6	m	Y	
T1SF5	Reporting of security events	Notes	m	Y	

Table A.12 – Optional Functions for C1

Index	Function	Reference (subclause)	Status	Support	
T1SF6	Data encipherment	6.2	o.1	Y	N
T1SF7	Integrity protection	6.3	o.1	Y	N
T1SF8	Pre-encapsulation concatenation	6.1	o	Y	N
T1SF9	Integrity padding	6.3.1.3	o	Y	N
T1SF10	Explicit security labeling	6.5	o	Y	N
T1SF11	Encipherment padding	6.2.2	o	Y	N

Table A.13 – Mandatory Fuctions for C2, C3

Index	Function	Reference (subclause)	Status	Support	
T3SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T3SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T3SF3	Separation after decapsulation	6.1	m	Y	
T3SF4	Secure multiplexing	Implicit	m	Y	
T3SF5	Security encapsulation	5.6	m	Y	
T3SF6	Reporting of security events	Notes	m	Y	

Table A.14 – Optional Functions for C2, C3

Index	Function	Reference (subclause)	Status	Support	
T3SF7	Data encipherment	6.2	o.1	Y	N
T3SF8	Integrity protection	6.3	o.1	Y	N
T3SF9	Integrity sequence number space	6.3.3	o	Y	N
T3SF10	Pre-encapsulation concatenation	6.1	o	Y	N
T3SF11	Integrity padding	6.3.1.3	o	Y	N
T3SF12	Explicit security labeling	6.5	o	Y	N
T3SF13	Encipherment padding	6.2.2	o	Y	N

Table A.15 – Mandatory Functions for C4, C4L

Index	Function	Reference (subclause)	Status	Support	
T4SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T4SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T4SF3	Separation after decapsulation	6.1	m	Y	
T4SF4	Secure multiplexing	Implicit	m	Y	
T4SF5	Security encapsulation	5.6	m	Y	
T4SF6	Reporting of security events	Notes	m	Y	

Table A.16 – Optional Functions for C4, C4L

Index	Function	Reference (subclause)	Status	Support	
T4SF7	Data encipherment	6.2	o.1	Y	N
T4SF8	Integrity protection	6.3	o.1	Y	N
T4SF9	Integrity sequence number	6.3.3	o	Y	N
T4SF10	Pre-encapsulation concatenation	6.1	o	Y	N
T4SF11	Integrity padding	6.3.1.3	o	Y	N
T4SF12	Explicit security labeling	6.5	o	Y	N
T4SF13	Encipherment padding	6.2.2	o	Y	N

Tables A.17 and A.18 identify the mandatory and optional functions implemented for connectionless Transport (CLTP::).

Table A.17 – Mandatory Functions for CLTP

Index	Function	Reference (subclause)	Status	Support	
TLF1	Verification of peer address	5.6.2, 6.4	m	Y	
TLF2	Reflection detection	5.6.2, 6.3.2	m	Y	
TLF3	Security encapsulation	5.6	m	Y	
TLF4	Reporting of security events	5.2.1, 6	m	Y	

Table A.18 – Optional Functions for CLTP

Index	Function	Reference (subclause)	Status	Support	
TLF5	Data encipherment	6.2	o.1	Y	N
TLF6	Integrity protection	6.3	o.1	Y	N
TLF7	Integrity padding	6.3.1.3	o	Y	N
TLF8	Explicit security labeling	6.5	o	Y	N
TLF9	Encipherment padding	6.2.2	o	Y	N

A.7 Supported Protocol Data Units (PDUs)

A.7.1 Supported Transport PDUs (TPDUs)

As indicated in Table A.19 the SE TPDU is supported for both transmission and receipt, for both the connection oriented (COTP::) and connectionless Transport Protocol (CLTP::).

Table A.19 – TPDUs Supported

Index	TPDU	Item	Status	Support	
STS1	SE	Transmission COTP or CLTP	m	Y	
STS2	SE	Receipt COTP or CLTP	m	Y	

A.7.2 Supported parameters of issued TPDUs

Tables A.20 and A.21 indicate which parameters are mandatory or optional when a SE TPDU is issued by Transport (COTP:: or CLTP::).

Table A.20 – Mandatory Parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
SPI1	Key Identifier must be present.	6.2, 6.3	m	Y	
SPI2	Bit one of Protected Header Flag must be set as direction indicator.	8.2.3.3	m	Y	

Table A.21 – Optional Parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
SPI3	Label	8.2.3.4	o	Y	N
SPI4	Integrity Pad	8.2.3.6	o	Y	N
SPI5	ICV	8.2.4	o	Y	N
SPI6	Encipherment Pad	8.2.5	o	Y	N

A.7.3 Supported parameters of received TPDUs

Implementations shall be capable of receiving and processing all possible parameters of the SE TPDU as indicated in Table A.22.

Table A.22 – Mandatory parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
SPR1	Key Identifier must be present.	6.2, 6.3	m	Y	
SPR2	Bit one of Protected Header Flag	8.2.3.3	m	Y	
SPR3	Label	8.2.3.4	m	Y	
SPR4	Integrity Pad	8.2.3.6	m	Y	
SPR5	ICV	8.2.4	m	Y	
SPR6	Encipherment Pad	8.2.5	m	Y	

Allowed values of issued TPDU parameters are given in Table A.23.

Table A.23 – Values for Parameters of issued TPDUs for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVI1	SA-ID	2-126 octets	
AVI2	Prot Header Flags	0 or 1	
	Label		
AVI3	Defining Authority	1-n octets	
AVI4	Value	1-m octets	
	ICV Padding		
AVI5	Length	1-254	
AVI6	Value	1-254 octets	
AVI7		ICV 1-indef octets	
	ENC PADDING		
AVI8	Length	1-254	
AVI9	Value	1-254 octets	

A.7.4 Allowed values of issued TPDU parameters

See Table A.24.

Table A.24 – Values for parameters of received TPDUs for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVR1	SA-ID	2-126 octets	
AVR2	Prot Header Flags	0 or 1	
	Label		
AVR3	Defining Authority	1-n octets	
AVR4	Value	1-m octets	
	ICV Padding		
AVR5	Length	1-254	
AVR6	Value	1-254 octets	
AVR7	ICV	1-indef octets	
	ENC PADDING		
AVR8	Length	1-254	
AVR9	Value	1-254 octets	

A.8 Service, function, and protocol relationships

A.8.1 Relationship between services and functions

Table A.25 gives a mapping between OSI security services provided by TLSP and the associated functions needed in an implementation. The consistency between supported functions and security services shall be maintained accordingly.

Table A.25 – Mapping of security services to supported functions

Security Service	Functions
Confidentiality	Data encipherment padding
Connection Integrity	Integrity sequence number space Integrity protection Reflection detection padding
Connectionless Integrity	Integrity protection Reflection detection padding
Peer Entity or	Verification of peer address
Data Orig. Authentication	Security encapsulation Use of either: integrity protection or data encipherment
Access Control	Explicit security labeling Secure meltiplexing Security encapsulation

A.8.2 Relationship between services and protocol

Table A.26 gives a mapping between OSI security services provided by TLSP and the SE TPDU protocol control information (PCI) and parameter fields employed by the underlying security mechanisms. The consistency between supported security parameters and SE TPDU parameter fields shall be maintained accordingly.

Table A.26 – Mapping of security services to SE TPDU parameters

Security Service	TPDU Parameters/PCI
Confidentiality	Encrypted data Confidentiality padding
Connectionless Integrity	Integrity check value Direction indicator Integrity padding
Connection Integrity	Integrity check value Direction indicator Integrity padding DT/ED send sequence number (final sequence number)
Data Orig. Authentication	Peer address
Peer Entity Authentication	Key identifier Key identifier employed in: integrity check value or encrypted data
Access Control	Security labels Key identifier Key identifier employed in: integrity check value or encrypted data

A.9 Supported algorithms

Table A.27 identifies the set of confidentiality and integrity algorithms supported by this implementation.

Table A.27 – Supported algorithms

Index	Item	Reference (subclause)	Algorithm Identifier [a)]
ALG1	Data Encryption	6.2.3	
ALG2	Cryptographichic ICV	6.3.1.3	
ALG3	Non-Cryptographic ICV	6.3.1.3	
[a)] Algorithms supported (if appropriate) under the registration scheme defined in ISO/IEC 9979 or ISO/IEC 9834.			

A.10 Error handling

A.10.1 Security errors

Table A.28 contains the mandatory security error actions to be taken upon receipt of an SE TPDU corresponding to the event description.

A.10.2 Protocol errors

Table A.29 identifies the protocol error actions to be taken upon receipt of an SE TPDU corresponding to the event description.

A.11 Security Association

A.11.1 SA Generic Fields

See Table A.30.

Table A.28 – Mandatory security error actions for COTP, CLTP

Index	Event	Reference (subclause)
SEA1	An improperly protected TPDU received shall be discarded.	6.0
SEA2	A TPDU with an invalid value in the SA-ID identified shall be discarded.	6.2.3
SEA3	A TPDU with an invalid ICV shall be discarded.	6.3.1.3
SEA4	A TPDU with an invalid direction indicator shall be discarded.	6.3.2.3
SEA5	A TPDU with an improper label shall be discarded.	6.5.3
SEA6	A TPDU with an improper Integrity Pad shall be discarded.	6.3.1.3
SEA7	A TPDU with a duplicate sequence number shall be discarded.	6.3.3.3
SEA8	A TPDU with an invalid peer address shall be discarded.	6.4
SEA9	A TPDU with an improper Encipherment Pad shall be discarded.	6.2.2

NOTES

1 In item SEA1, an improperly protected TPDU includes both those SE TPDUs where non-negotiated options are used, and those where negotiated options are not used.

2 Item SEA7 apply only to the connection oriented Transport Protocol (COTP::) when integrity sequence number space and truncation protection have been negotiated for C2-C4, C4L.

Table A.29 – Protocol error actions for COTP, CLTP

Index	Event	Reference (subclause)	Action	
			Allowed	Supported
PEA1	An undefined parameter encountered in the protected contents.	8.2.3		
PEA2	Out of sequence parameters discovered in the protected contents.	8.2.3		

Table A.30

Item	Questions/Features	Reference (subclause)	Status	Support on transmission	Support on receipt
SaLI	Length Indicator field tansmitted in each SA PDU?	8.3.1	SA:M	Yes N/A	Yes N/A
SaPDUType	PDU Type field with value 01001001 in each SA PDU	8.3.2	SA:M	Yes N/A	Yes N/A
SaSAID	SA-ID field	8.3.3	SA:M	Yes N/A	Yes N/A
SA-PType	SA-P TYPE field	8.3.4	SA:M	Yes N/A	Yes N/A
SA-RK	Is the SA REKEY Supported?	B.5.3	SA:O	Yes No N/A	Yes No N/A
SSLYR*	Is the example SA protocol using Key Token Exchange supported?	Annex B	SA:O	Yes No N/A	Yes No N/A

A.11.2 Content Fields Specific to Key Exchange SA-P

See Table A.31.

Table A.31

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on receipt
SAExchId	ExchangeID	B.6.1	SAKTE:M	Yes N/A	Yes N/A
ContLen	Is the Length Indicator field transmitted in each SA PDU?	B.6.2	SAKTE:M	Yes N/A	Yes N/A
MySAID	My SAID Content field	B.6.3.1	SAKTE:M	Yes N/A	Yes N/A
OldYrSAID	Old Your SAID Content field	B.6.3.2	SAKTE:M	Yes N/A	Yes N/A
KeyTokens	Key Token 1 and Key Token 2 Content Fields	B.6.3.3	SAKTE:M	Yes N/A	Yes N/A
AuthFields	Authentication digital signature and Authentication certificate Content fields	B.6.3.4	SAKTE:M	Yes N/A	Yes N/A
ServSel	Service Selection Content field	B.6.3.5	SAKTE:O	Yes No N/A	Yes No N/A
SARejReas	SA Rejection Reason Content field	B.6.3.6	SAKTE:O	Yes No N/A	Yes No N/A
SAAbReas	SA Abort/Release Reason Content field	B.6.3.7	SAKTE:M	Yes No N/A	Yes No N/A
LabDef	Label Definition Content field	B.6.3.8	SAKTE:O	Yes No N/A	Yes No N/A
KeySel	Key Selection Content field	B.6.3.9	SAKTE:O	Yes No N/A	Yes No N/A
KeyUse	Usage Flags sub-field	B.6.3.9.	KeySel:M	Yes No N/A	Yes No N/A
KeySelInfo	Key Selection Information sub-field	B.6.3.9.	KeySel:M	Yes No N/A	Yes No N/A
KeyRefx	Key Reference sub-field	B.6.3.9.	KeySel:O	Yes No N/A	Yes No N/A
SaFlags	SA Flags Content field	B.6.3.10	SAKTE:O	Yes No N/A	Yes No N/A
ASSR	ASSR Content field	B.6.3.11	ServSel:M	Yes No N/A	Yes No N/A

Anexo B

Protocolo de asociación de seguridad que emplea intercambio de testigos de clave y firmas digitales

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

B.1 Visión de conjunto

Este anexo define un protocolo para la utilización de un mecanismo asimétrico con el fin de efectuar el establecimiento, mantenimiento y aborto/liberación de una asociación de seguridad. El protocolo permite a las entidades TLSP comunicantes:

a) autenticar dos entidades (una a la otra);

b) inicializar atributos SA incluidas las claves; y

c) establecer la información inicial que se utilizará para proporcionar la integridad.

Este anexo describe un protocolo SA que efectúa lógicamente las siguientes funciones distintas:

a) Se emplea un intercambio de testigos de clave (KTE, *key token exchange*), para establecer un secreto compartido. Este mecanismo soporta un intercambio de testigos de clave. La forma de estos testigos es específica a cada mecanismo. En el Anexo C se presenta un ejemplo de testigos de clave específicos al mecanismo, que soportan el intercambio de claves exponenciales, conocido también por el intercambio Diffie-Hellman.

b) Para obtener la autenticación se emplean certificados, firmas digitales y elementos obtenidos del intercambio de testigos de clave.

c) Se utilizan intercambios de protocolo para negociar atributos SA.

d) Se utilizan intercambios de protocolo para señalar que se está liberando la SA.

Antes de establecer una asociación de seguridad (SA) mediante este protocolo SA, cada entidad TLSP tiene que haber establecido previamente la siguiente información:

a) El mecanismo que ella soporta, expresado por:

   1) una lista de los conjuntos ASSR soportados, y

   2) el conjunto de servicios de seguridad soportados por cada uno de los ASSR identificados anteriormente.

b) Un par de claves asimétricas para cada algoritmo asimétrico soportado que pueda ser utilizado por la entidad TLSP para firmar datos con fines de autenticación.

c) Un certificado de una autoridad de confianza para cada algoritmo asimétrico soportado que identifica la entidad TLSP, y su clave asimétrica pública, para fines de autenticación.

d) Las claves públicas, y los algoritmos asimétricos implicados, de toda autoridad de certificación de confianza que envíe certificados a entidades TLSP con las que esta entidad TLSP entrará en comunicación.

Este protocolo de asociación de seguridad (brevemente, protocolo SA) establece dinámicamente la siguiente información de seguridad que necesita para asegurar su propia comunicación:

a) negociación del algoritmo de cifrado para proteger la comunicación de protocolo SA;

b) negociación del algoritmo asimétrico y del esquema de firma digital utilizados para proporcionar autenticación de protocolo SA;

c) generación de la información de aplicación de clave que el algoritmo de cifrado necesita para proteger la comunicación de protocolo SA.

Este protocolo SA establece la siguiente información compartida entre las dos entidades TLSP:

a) los identificadores de asociación de seguridad (SA-ID) local y distante;

b) los servicios de seguridad que habrán de utilizarse entre las entidades asociadas para instancias de comunicación;

c) el mecanismo y sus respectivos parámetros de acuerdo con los servicios de seguridad seleccionados;

d) las claves iniciales compartidas para la integridad, el mecanismo de cifrado y la autenticación de una instancia de comunicación;

e) el conjunto de etiquetas de seguridad que puede utilizarse en esta asociación para el control de acceso.

Se puede establecer una SA utilizando los mismos servicios de seguridad seleccionados, los mecanismos y parámetros respectivos, y el conjunto de etiquetas de seguridad procedentes de una SA previamente establecida. En este caso lo único que cambia son los identificadores SA-ID y las claves; todos los demás atributos quedan como estaban.

Cada vez que se establece una nueva SA hay que establecer nuevos valores de clave.

En el caso del protocolo TLSP en modo sin conexión, después de haberse liberado una SA, el SA-ID se pone en estado «congelado». Mientras esté congelado, un SA-ID no podrá utilizarse. El periodo durante el cual estará congelado un SA-ID deberá ser mayor que la duración de vida máxima de una PDU en la red subyacente.

El atributo SA Adr_served (dirección servida) se establece por medios externos a este protocolo.

El atributo SA Initiator (iniciador) se fija a TRUE para el iniciador del intercambio de protocolo SA y a FALSE para el respondedor.

Los intercambios de protocolo para el establecimiento de la SA se ilustran en la Figura D.1.

B.2 Intercambio de testigos de clave (KTE)

Las entidades TLSP comienzan su protocolo SA con un intercambio de testigos de clave para generar un secreto compartido (en forma de una cadena de bits) entre las entidades. Las entidades TLSP utilizan entonces un subconjunto de esta cadena de bits secreta, junto con un algoritmo de clave privada para cifrar el resto de la comunicación entre ellas, con lo que se proporciona la confidencialidad del resto de los intercambios de protocolo SA.

El intercambio de testigos de clave comprende el intercambio de dos valores Key Token 1 (testigo de clave 1) y Key Token 2 (testigo de clave 2) calculados a partir de parámetros específicos al mecanismo junto con números generados localmente mediante algoritmos específicos al mecanismo como los descritos en líneas generales en el Anexo D. Las dos entidades comunicantes emplean entonces los valores intercambiados para generar la cadena de bits secreta compartida.

Un subconjunto de esta cadena de bits se utiliza junto con un algoritmo de clave privada para cifrar el resto del intercambio de protocolo SA que soporta la negociación de la autenticación de protocolo SA y la negociación de atributo SA. Además, un subconjunto de esta cadena de bits se referencia también para utilizarla como clave y como atributos ISN de la asociación de seguridad que se está estableciendo. Esta referenciación se efectúa:

1) sea por el intercambio de información de posición en la negociación de atributo SA;

2) sea por un conocimiento previo.

B.3 Autenticación de protocolo SA

Para que una entidad TLSP pueda autenticar a otra durante el establecimiento de la SA necesita un certificado de autenticación y un par de claves públicas.

Las entidades TLSP intercambian certificados y firmas digitales (como los definidos en la Norma ISO 9594-8) para verificar, cada una de ellas, la identidad de la otra. Un certificado contiene, como mínimo, alguna información de identificación relativa a una TLSPE más la clave pública de la entidad (véase la Figura D.1).

El certificado lo establece una autoridad de confianza y se proporciona al TLSP mediante un procedimiento que está fuera del ámbito del protocolo TLSP. El certificado contiene la firma de autenticación de la autoridad de confianza. Una entidad TLSP que participe en este protocolo SA deberá tener la clave pública de la autoridad de confianza que expidió el certificado. El método utilizado para obtener la clave pública de la autoridad de confianza está fuera del ámbito de esta Recomendación UIT-T | Norma Internacional. Para que una entidad TLSP pueda demostrar que posee un determinado certificado deberá probar que conoce la clave secreta que corresponde a la clave pública en el certificado.

La prueba de que la operación se efectúa en tiempo oportuno y la prevención de ataques por reproducción fraudulenta se consiguen mediante los datos firmados constituidos por los números concretos determinados conjuntamente y específicos a esta operación del protocolo. En el caso de las dos entidades comunicantes A (el iniciador de la SA) y B (el respondedor), esto se efectúa de la manera siguiente:

a) Se crea el contenido de la SA, lo que incluye los campos codificados como TLV, que transportan:

el certificado de A;

la negociación de atributos SA (véase B.4) o los motivos para el aborto/liberación (véase B.6),

el testigo de clave 3, calculado utilizando un algoritmo como el descrito en el Anexo D,

pero excluyendo el identificador de intercambio y la longitud del contenido, después de esto se firma el contenido (por ejemplo, utilizando la firma de autenticación definida en la Norma ISO 9594-8). Seguidamente, el contenido de la SA, con la firma incluida, se codifica como un TLV, y se cifra la longitud del contenido. La clave de cifrado está formada por los n primeros bits de la cadena de bits producida por el intercambio KTE, siendo n el número de bits requeridos por el algoritmo utilizado.

b) Se crea el contenido de la SA, se firma y se cifra utilizando la información equivalente relativa a B y el testigo de clave 4 en vez del testigo de clave 3.

Cada entidad verifica la firma de autenticación de la entidad par: primero decodificando los datos recibidos en el intercambio, y después verificando el testigo de clave para la protección contra ataques por reproducción. Para la verificación hay que utilizar la clave pública de la entidad par, y el proceso convenido para verificación de firma.

B.4 Negociación de atributo SA

B.4.1 Selección de servicio de seguridad

Basándose en su política de seguridad local, la entidad TLSP iniciadora envía un conjunto de uno o más servicios de seguridad aceptables seleccionados. Cada elemento de este conjunto contiene lo siguiente:

a) el identificador del conjunto convenido de reglas de seguridad (ASSR_ID) que define la semántica de los servicios de seguridad seleccionados (reseñados más abajo) para este elemento del conjunto; y

b) valores de selección de servicio (semántica definida por el ASSR_ID), uno para cada uno de los siguientes servicios: confidencialidad, autenticación, control de acceso, integridad, y confidencialidad del flujo de tráfico.

Basándose en su política de seguridad local, la entidad TLSP receptora retornará al originador la siguiente información PCI:

a) Si sólo es aceptable un elemento de servicio del conjunto de servicios propuestos, el receptor retornará el único elemento de servicio seleccionado.

b) Si ninguno de los elementos del conjunto de servicios propuestos es aceptable, el receptor rechazará la SA y retornará un campo Status (estado) que indicará el motivo por el que se rechaza la SA.

NOTA – Esta negociación permite a ambas entidades TLSP seleccionar servicios de seguridad que se ajusten a su política de seguridad local.

B.4.2 Negociación del conjunto de etiquetas

De acuerdo con su política de seguridad local, la entidad TLSP iniciadora envía un conjunto de etiquetas de seguridad y un conjunto de referencias que desea transferir bajo la protección de esta SA. Cada elemento del conjunto contiene la semántica completa de la etiqueta.

Basándose en su política de seguridad local, la entidad TLSP receptora determinará cuál(es) de las etiquetas del conjunto propuesto desea que se transfiera(n) bajo la protección de esta SA. La entidad TLSP receptora retornará al originador la siguiente información PCI:

a) Si una o más etiquetas del conjunto de etiquetas propuesto es aceptable, el receptor retornará un subconjunto del conjunto de referencias propuesto. No se permitirán conjuntos vacíos.

b) Si ninguna de las etiquetas del conjunto propuesto es aceptable, el receptor rechazará la SA y retornará un campo Status que indicará el motivo por el que se rechaza la SA.

NOTA – Esta negociación permite a ambas entidades TLSP seleccionar un conjunto de etiquetas que se ajuste a su política de seguridad local. Lo anteriormente expuesto sólo es aplicable si se ha seleccionado el atributo de etiqueta.

B.4.3 Selección de clave y de ISN

Basándose en su política de seguridad local, la entidad TLSP iniciadora selecciona las porciones de la cadena de bits resultantes del intercambio KTE que habrán de utilizarse como claves y/o ISN durante las comunicaciones (dicho sea con más precisión, comunicaciones TLSP, y no comunicaciones de protocolo SA) con destino a la entidad TLSP receptora. Para la identificación de la clave/ISN se comunica la posición del bit de comienzo en la cadena de bits obtenida como resultado del intercambio KTE. La longitud de la clave/ISN se determina a partir de los parámetros asociados con el servicio seleccionado. Se envía a la entidad TLSP receptora un conjunto de punteros a las claves y datos siguientes:

a) clave de cifrado de datos normales;

b) clave de cifrado de datos acelerados;

c) clave de la generación de comprobación de la integridad de datos normales;

d) clave de la generación de comprobación de la integridad de datos acelerados;

e) «My ISN» para datos normales;

f) «My ISN» para datos acelerados; y

g) clave de la generación de autenticación.

De manera similar, la entidad TLSP receptora determinará localmente qué porciones de la cadena de bits resultantes del intercambio KTE va a utilizar para sus claves/ISN. La entidad TLSP receptora retornará al originador la siguiente información PCI:

a) si el receptor opta por utilizar las mismas posiciones de bit propuestas por la entidad TLSP iniciadora, no retorna PCI explícita;

b) si el receptor rechaza la SA porque ha habido otros fallos en la negociación, no retorna PCI explícita;

c) si el receptor selecciona posiciones de bit diferentes para sus claves/ISN, retornará un conjunto de punteros.

NOTA – Un mismo valor de clave se puede utilizar para varios fines proporcionando el mismo puntero para más de una clave/ISN.

B.4.4 Negociación de diversos atributos SA

Basándose en su política de seguridad local, la entidad TLSP iniciadora determina el valor de los siguientes atributos SA para la SA que se está estableciendo, por ejemplo seleccionando la retención de estos atributos al desconectar (Rec. UIT-T X.224 | ISO/CEI 8073).

La entidad TLSP iniciadora envía a la entidad TLSP receptora este conjunto de atributos SA propuestos, en un campo de banderas diversas.

Basándose en su política de seguridad local, la entidad TLSP receptora retornará al originador la siguiente información PCI:

a) si el receptor acepta todos los atributos SA propuestos, no retorna PCI explícita. El hecho de que el receptor no rechace la SA implica que los atributos son aceptables por la entidad TLSP receptora;

b) si uno cualquiera de estos atributos no es aceptable, el receptor rechaza la SA y retorna un campo Status que indicará los atributos que causaron el rechazo.

B.4.5 Visión de conjunto de la reaplicación de la clave

Si en una SA en curso de establecimiento se dispone que se vuelva a aplicar una SA antigua, sólo se efectúa la selección de clave e ISN. En este caso, en lugar de la negociación del servicio, del conjunto de etiquetas y de los atributos SA diversos, se coloca en «Old_your_SA-ID» la referencia a la antigua SA de la cual habrán de heredarse estos atributos.

B.4.6 Visión de conjunto del aborto/liberación de la SA

Se puede liberar una asociación de seguridad por los siguientes métodos:

a) mediante el intercambio de unidades de datos de protocolo de asociación de seguridad;

b) por medio de mecanismos externos fuera del alcance del protocolo de la capa inferior;

c) implícitamente, cerrando una conexión;

d) implícitamente, al expirar una clave en la SA.

Estos métodos para la liberación de la asociación de seguridad pueden agruparse en dos categorías: el método fuera de banda y el método dentro de banda. En el caso del método dentro de banda es posible liberar la SA mediante la petición de desconexión de la conexión de transporte, o emitiendo una liberación de SA (PDU de SA con un campo de contenido de tipo motivo del aborto/liberación de la SA). Para más detalles, véase B.6.3.

B.5 Correspondencia de funciones de protocolo SA con intercambios de protocolo

Este protocolo SA ejecuta las tres funciones antes descritas durante tres intercambios de protocolo distintos:

a) el primer intercambio comprende el intercambio de testigos de clave (KTE) y el intercambio de certificados, y no tiene aplicado cifrado;

b) el segundo intercambio consiste en una negociación de seguridad protegida para proporcionar autenticación, como se define en B.3;

c) un intercambio separado, iniciado cuando la SA deja de ser necesaria; este intercambio comprende un código de motivo protegido para proporcionar autenticación, como se define en B.3.

B.5.1 (Primer) intercambio KTE

B.5.1.1 Petición de inicio de protocolo SA

La entidad TLSP o la gestión de seguridad local inicia el protocolo SA.

La entidad TLSP iniciadora ejecuta las siguientes funciones y envía al receptor la siguiente información:

a) Se selecciona un SA-ID disponible, que se coloca como «My_SA-ID» del originador.

b) Se da comienzo al intercambio KTE y se envía el testigo de clave 1.

c) Una lista de mecanismos de confidencialidad propuestos, que podrían utilizarse para proteger el segundo intercambio de protocolo SA. Esta lista se expresa como un conjunto de uno o más elementos, que incluye: ASSR_ID y servicios de seguridad de confidencialidad seleccionados. No es necesario enviar esta lista si previamente se han convenido los mecanismos.

d) Una lista de mecanismos de integridad propuestos, uno de los cuales se utilizará para firmar digitalmente el segundo intercambio de protocolo SA. Esta lista se expresa como un conjunto de uno o más elementos, que incluye: ASSR_ID, y servicios de seguridad de integridad seleccionados. No es necesario enviar esta lista si previamente se han convenido los mecanismos.

NOTA – Los servicios de seguridad de confidencialidad seleccionados deben identificar solamente un algoritmo de cifrado simétrico y su modo de funcionamiento. Los servicios de seguridad de integridad seleccionados deben identificar solamente un algoritmo asimétrico y su esquema de firma digital asociada. Los puntos a que se refieren los apartados c) y d) pueden conocerse de antemano.

En el caso del modo con conexión (CO), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU para el primer intercambio, no se establece la SA y no se hacen ulteriores intentos para ello.

En el caso del modo sin conexión (CL), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU para el primer intercambio, la entidad TLSP iniciadora retransmite su PDU del primer intercambio. Las retransmisiones están limitadas a un número finito, que se fija localmente.

B.5.1.2 Recepción de la primera PDU de SA por la entidad receptora

Al recibir la primera PDU de SA, la entidad TLSP receptora ejecuta las siguientes funciones y envía la siguiente información a la entidad iniciadora:

a) El «My_SAID» recibido se coloca en el campo «Your_SAID» del encabezamiento genérico descrito en 8.3.

b) Se selecciona un SAID disponible y se envía como el My_SAID del originador.

c) Basándose en su política de seguridad local, la entidad TLSP receptora retorna al originador la siguiente información PCI:

1) Si el receptor acepta uno de los mecanismos de confidencialidad propuestos, retorna el mecanismo seleccionado. Si el iniciador había propuesto un solo mecanismo, no se retorna PCI explícita.

2) Si ninguno de los mecanismos de confidencialidad es aceptable, el receptor rechaza la SA y retornará un campo Status que indicará la causa del rechazo.

d) Basándose en su política de seguridad local, la entidad TLSP receptora retorna al originador la siguiente información PCI:

   1) Si el receptor acepta uno de los mecanismos de confidencialidad propuestos, retorna el mecanismo seleccionado. Si el iniciador había propuesto un solo mecanismo, no se retorna PCI explícita.

   2) Si ninguno de los mecanismos de confidencialidad es aceptable, el receptor rechaza la SA y retornará un campo Status que indicará la causa del rechazo.

e) En el caso de que se haya seleccionado un mecanismo de confidencialidad y un mecanismo de integridad, se comienza el cálculo de KTE y se envía el testigo de clave 2.

En el caso del modo con conexión (CO), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU del segundo intercambio, no se establece la SA y no se hacen ulteriores intentos para ello.

En el caso del modo sin conexión (CL), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU del segundo intercambio, la entidad TLSP iniciadora retransmite su PDU del primer intercambio. Las retransmisiones están limitadas a un número finito, que se fija localmente.

En el caso del modo sin conexión, si se recibe de nuevo la PDU del primer intercambio, se vuelve a enviar la PDU de retorno.

B.5.2 (Segundo) intercambio para la negociación de autenticación y seguridad

B.5.2.1 Recepción de la primera PDU de SA por la entidad iniciadora

Al recibir la PDU de SA del primer intercambio, la entidad TLSP iniciadora ejecuta las siguientes funciones y envía al receptor la siguiente información:

a) El «My_SAID» recibido se coloca en el campo «Your_SAID» del encabezamiento genérico descrito en 8.3.

b) El certificado del iniciador asociado con el mecanismo de integridad seleccionado se coloca en el campo de contenido certificado.

c) El iniciador genera el testigo de clave 4.

d) Se coloca en el campo de contenido selección de servicio una lista de servicios de seguridad propuestos que podrían utilizarse para proteger la comunicación TLSP.

e) Se coloca en Label_Def un conjunto de etiquetas propuestas que podrían protegerse utilizando esta SA durante una comunicación TLSP.

f) Se coloca en selección de clave un conjunto de las claves/ISN seleccionadas.

g) Se colocan en banderas SA los diversos atributos SA requeridos para esta SA.

h) Si en el establecimiento de la SA se debe volver a aplicar una SA antigua, el Old Your SA-ID (tu ID de SA antiguo) se fija al SA-ID para la SA antigua que se está reaplicando. Si se sigue este procedimiento no deberá ejecutarse lo prescrito en los anteriores apartados d), e) y g).

i) El contenido de la SA se protege como se indica en B.3.

En el caso del modo con conexión (CO), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU del segundo intercambio, no se establece la SA y no se hacen ulteriores intentos para ello.

En el caso del modo sin conexión (CL), si, transcurrido un periodo de temporización, no se ha recibido en retorno ninguna PDU del segundo intercambio, la entidad TLSP iniciadora retransmite su PDU del segundo intercambio. Las retransmisiones están limitadas a un número finito, que se fija localmente.

En el caso del modo sin conexión, si se recibe de nuevo la PDU del segundo intercambio, se vuelve a enviar la PDU del segundo intercambio.

B.5.2.2 Recepción de la PDU del segundo intercambio por la entidad receptora

Al recibir la PDU del segundo intercambio, la entidad TLSP receptora ejecuta las siguientes funciones y envía al iniciador la siguiente información:

a) El My_SAID recibido se coloca en el campo Your_SAID del encabezamiento genérico, como se describe en 8.3.

b) Se comprueban los siguientes puntos. Si la comprobación de cualquiera de los puntos fracasa, se rechaza la SA y se retorna el campo Status de modo que indique la causa del rechazo:

1) Se comprueba la validez de la firma digital recibida.

2) Se comprueba la validez del testigo de clave 3.

3) Se comprueba el conjunto de servicios de seguridad propuestos para determinar si algunos de ellos son aceptables. Sólo podrá seleccionarse uno de los servicios de seguridad propuestos.

4) Se comprueba el conjunto de etiquetas propuestas para determinar si algunas de ellas son aceptables.

5) Se comprueban los diversos atributos SA para determinar si todos son aceptables.

c) Si Old Your SA-ID está presente en la PDU recibida, la SA apropiada se copia desde el SA-ID referenciado. En este caso no pueden enviarse los campos descritos en los apartados c) y d) que siguen.

Siempre que todos estos puntos hayan sido comprobados con éxito, se envía lo siguiente:

a) El certificado del iniciador asociado con el mecanismo de integridad seleccionado.

b) Los servicios de seguridad seleccionados que se utilizarán para proteger la comunicación TLSP. Si el conjunto de servicios propuestos sólo contenía un elemento no se retorna PCI.

c) El receptor (recibiente) genera el testigo de clave 4.

d) El subconjunto seleccionado de etiquetas propuestas que podrían protegerse utilizando esta SA durante la comunicación TLSP.

e) Un conjunto de punteros a clave/ISN. Si los punteros propuestos por el iniciador son aceptables por el receptor, no se envía PCI.

f) El contenido de la SA se protege como se describe en B.3.

En el caso del modo sin conexión (CL), si se vuelve a recibir la PDU del segundo intercambio, el receptor envía de nuevo su PDU del segundo intercambio.

B.5.3 Procedimiento de reaplicación de clave

Las entidades TLSP pueden actualizar claves en cualquier momento durante una asociación de seguridad. Esto se consigue mediante un intercambio de información SCI. Este intercambio es transparente al usuario TLSP y no se definen primitivas de servicio TLSP para invocarlo.

Un posible modo de funcionamiento es a intervalos regulares durante una conexión (por ejemplo, cada hora o cada 10 000 TPDU de SE) para intercambiar SCI. La reaplicación de clave provocará la selección de un nuevo SA-ID; no obstante, los atributos de la SA actual pueden heredarse.

La información de reaplicación de clave puede contener uno de estos elementos:

a) una nueva clave cifrada con un KEK mutuo;

b) una nueva clave cifrada con la clave pública del receptor;

c) una referencia a una clave distribuida previamente;

d) información de reaplicación de clave utilizada por un método de distribución de claves previamente convenido.

Los procedimientos de reaplicación de clave se basan en el intercambio de dos PDU de SA con información de reaplicación de clave (denominada «hacia afuera y respuesta») y TPDU de SE normales, y se efectúan como sigue:

Se prepara de la manera siguiente una PDU de SA que contenga información de reaplicación de clave hacia afuera:

a) la bandera hacia afuera/respuesta en el octeto de bandera se fija a 0;

b) si se ha seleccionado el mecanismo de etiqueta, la referencia de etiqueta se fija a la referencia para la etiqueta apropiada;

c) la información de clave se fija como lo requiera el mecanismo de distribución de claves;

d) el ISN inicial protegido se fija al número secuencial sobre la base del cual se deberá encriptar la TPDU de SE utilizando la clave actualizada;

e) el campo tres de reaplicación de clave de banderas de la SA se fija a 1.

Al recibirse una PDU de SA que contiene información de reaplicación de clave hacia afuera:

a) si se ha seleccionado el mecanismo de etiqueta, se comprueba que el campo de referencia de etiqueta contiene un valor válido para esta SA;

b) se procesa la información de clave como lo requiera el mecanismo de distribución de claves;

c) se comprueba si el ISN inicial es o no apropiado;

d) se comprueba que el campo tres de reaplicación de clave está fijado a 1.

Después de esto, se prepara de la manera siguiente una PDU de SA que contenga información de reaplicación de clave de respuesta:

a) la bandera hacia afuera/respuesta en el octeto de bandera se fija a 1;

b) si se ha seleccionado el mecanismo de etiqueta, la referencia de etiqueta se fija a la etiqueta apropiada;

c) la información de clave se fija como lo requiera el mecanismo de distribución de claves;

d) el ISN inicial protegido se fija al número secuencial sobre la base al cual se deberá encriptar la TPDU de SE utilizando la clave actualizada;

e) el campo tres de reaplicación de clave de banderas de la SA se fija a 1.

Al recibirse una PDU de SA que contiene información de reaplicación de clave de respuesta:

a) si se ha seleccionado el mecanismo de etiqueta, se comprueba que el campo de referencia de etiqueta contiene un valor válido para esta SA;

b) se procesa la información de clave como lo requiera el mecanismo de distribución de claves;

c) se comprueba si el ISN inicial es o no apropiado;

d) se comprueba que el campo tres de reaplicación de clave está fijado a 1.

Tras la comprobación exitosa de la respuesta, si la entidad TLSP no tiene TPDU en espera de encapsulación, se envía, para concluir el procedimiento de reaplicación de clave, una PDU de SA que no contenga datos.

Cuando una entidad TLSP que haya enviado una TPDU de SE con información de reaplicación de clave hacia afuera recibe una TPDU de SE encapsulada mediante la clave anterior, no deberá descartar la TPDU de SE encapsulada por la clave anterior a menos que la política de seguridad indique que se deba proceder de esa manera.

Si fracasa el procedimiento de reaplicación de clave, la asociación se establecerá de nuevo mediante el empleo del SA-P, o por cualquier otro medio adecuado.

B.5.4 Intercambio de liberación/aborto

B.5.4.1 Petición de inicio de la liberación/aborto de una SA

La entidad TLSP o la gestión de seguridad local inicia la liberación/aborto de la SA. El iniciador de un aborto/liberación de la SA no tiene necesariamente que ser el iniciador del establecimiento de la SA.

a) Si la entitad local es la iniciadora del establecimiento de la SA, se genera el testigo de clave 3 o el testigo de clave 4. En cualquier caso, el testigo generado se coloca en el contenido de la SA;

b) se coloca el motivo apropiado en el campo motivo del aborto/liberación de la SA;

c) el contenido de la SA se protege como se describe en B.3.

En el caso del modo con conexión, si, transcurrido un periodo de temporización, no se ha retornado una PDU de confirmación con respecto a la petición de aborto/liberación, no se establece la SA y no se hacen ulteriores intentos para ello.

En el caso del modo sin conexión, si, transcurrido un periodo de temporización, no se ha retornado una PDU de confirmación en el intercambio de aborto/liberación, la entidad TLSP iniciadora retransmite su PDU de petición de liberación/aborto de la SA. Las retransmisiones están limitadas a un número finito que se fija localmente.

B.5.4.2 Recepción de una petición de aborto/liberación de la SA

Al recibir la PDU de confirmación de aborto/liberación de la SA, la entidad TLSP receptora ejecuta las siguientes funciones y envía al iniciador la siguiente información:

a) Si la entitad local es la iniciadora del establecimiento de la SA, se genera el testigo de clave 3 o el testigo de clave 4. En cualquier caso, el testigo generado se coloca en el contenido de la SA.

b) El código de motivo apropiado se coloca en el campo motivo del aborto/liberación de la SA.

c) El contenido de la SA se protege como se describe en B.3.

En el caso del modo sin conexión, si se vuelve a recibir la PDU de la petición de aborto/liberación de la SA, el receptor retransmite su PDU del segundo intercambio, operación que repite un número de veces, hasta un límite fijado.

B.6 Campo Contenido de la SA, de la PDU de SA

Para este protocolo SA específico, el formato del campo contenido de la SA, de la PDU de SA definida en 8.4, se muestra en la Figura B.2.

Figura B.2 – Contenido de la SA

B.6.1 Identificador de intercambio

El campo identificador de intercambio contiene el valor 00000000 si la PDU está asociada con el primer intercambio de testigo de clave (KTE), y el valor 00000001 si la PDU está asociada con el segundo intercambio de autenticación/negociación. Este campo contiene el valor 10000000 si la PDU está asociada con una petición de aborto/liberación de la SA, y un valor 10000001 si la PDU está asociada con una confirmación de aborto/liberación de la SA.

B.6.2 Longitud de contenido

Este campo contiene la longitud en octetos de todos los campos de contenido; no incluye su propia longitud, es decir, la del campo de longitud de contenido.

B.6.3 Campos de contenido

La codificación del tipo de campo de contenido se define en 8.2. A continuación se indican los campos de contenido SA (es decir, A0-BF) utilizados en los procedimientos descritos en este anexo.

Valor	*Tipo de campo de contenido*
A0	My SA-ID (mi ID de SA)
A1	Old Your SA-ID (antiguo Tu Id de SA)
A2	Key Token 1 (testigo de clave 1)
A3	Key Token 2 (testigo de clave 2)
A4	Firma digital de autenticación
A5	Certificado de autenticación
A6	Selección de servicio
A7	Motivo de rechazo de la SA
A8	Motivo de aborto/liberación de la SA
A9	Banderas SA
AA	Selección de clave
AB	ASSR
AC	Iniciador
AD	Algoritmo de integridad
AE	Algoritmo de confidencialidad
AF	Longitud del ICV
B1	Clave de cifrado
B2	Clave de descifrado
B3	Mecanismo de autenticación
B4	Mecanismo de control de acceso
B5	Key Token 3
B6	Key Token 4
B7-BF	Reservados para uso futuro.

NOTA – En 8.2 del cuerpo principal de esta Recomendación UIT-T | Norma Internacional se indican otros códigos reservados para uso privado.

Los campos de selección de servicio, motivo del rechazo de la SA, Label-Def, banderas de SA, y selección de clave son facultativos dentro de esta definición específica del contenido del protocolo SA.

B.6.3.1 My SA-ID (mi identificador de SA)

Este campo obligatorio se utiliza solamente en el primer intercambio. El parámetro es el identificador local para una asociación de seguridad.

B.6.3.2 Old Your SA-ID (antiguo Tu ID de SA)

Este campo se utiliza en el segundo intercambio si se van a heredar de la antigua SA atributos que no sean claves.

B.6.3.3 Key Token 1 (testigo de clave 1), Key Token 2 (testigo de clave 2), Key Token 3 (testigo de clave 3) y Key Token 4 (testigo de clave 4)

Estos campos obligatorios se utilizan para soportar el intercambio KTE y la autenticación, como se ha indicado antes en este anexo.

B.6.3.4 Certificado de autenticación, firma digital de autenticación

Estos campos obligatorios se utilizan para soportar la autenticación, como se ha indicado antes en este anexo.

B.6.3.5 Selección de servicios

Este campo facultativo se utiliza en el primer intercambio y en el segundo intercambio:

a) si se utiliza en el primer intercambio, su finalidad es identificar mecanismos de confidencialidad y/o integridad que se van a utilizar en el segundo intercambio de protocolo SA. En este caso sólo están presentes los primeros dos octetos;

b) si se utiliza en el segundo intercambio, su finalidad es proponer todos los mecanismos que van a utilizarse en las comunicaciones TLSP protegidas por la SA que se está estableciendo.

Este campo se podrá incluir una o más veces en la PDU de primer o de segundo intercambio para formar un conjunto de servicios de seguridad propuesto para negociación. Cada parámetro se relaciona con el parámetro ASSR que le precede inmediatamente.

Este parámetro contiene una secuencia de octetos que indica los niveles de servicios de seguridad seleccionados que se requieren. Las semánticas de los niveles se definen como parte de la política de seguridad. Los octetos para cada uno de los servicios aparecen en el orden indicado más adelante. La secuencia de octetos puede truncarse si todos los octetos que son eliminados al ser truncados se relacionan con los servicios que tienen el valor de calidad de servicio 0. Un octeto único con el valor 255 indica que los servicios de seguridad seleccionados se han establecido previamente.

Octeto	*Significado*
1	Confidencialidad en modo sin conexión/confidencialidad en modo conexión
2	Integridad en modo sin conexión/integridad en modo conexión con o sin recuperación
3	Autenticación del origen de datos/autenticación de entidad par
4	Control de acceso
5	Protección de sistemas de extremo
6	Protección conexión por conexión

B.6.3.6 Motivo del rechazo de la SA

Este campo puede estar presente en la PDU del primer o del segundo intercambio. Su presencia indica el rechazo de la SA en su fase de establecimiento. Contiene el motivo del rechazo, que puede ser uno de los siguientes:

Valor	*Significado*
1	Mecanismo de confidencialidad no soportado
2	Mecanismo de integridad no soportado
3	Mecanismo de control de acceso no soportado
4	Mecanismo de autenticación no soportado
5	Sistema de extremo no soportado
6	Conexión por conexión no soportada
7	Mecanismo de confidencialidad rechazado
8	Mecanismo de integridad rechazado
9	Mecanismo de control de acceso rechazado

10	Mecanismo de autenticación rechazado
11	Firma de autenticación inválida
12	Certificado inválido
13	Conjunto de etiquetas propuesto rechazado
14	Retención al desconectar rechazada
15	Protección de parámetros rechazada
16	Sistema de extremo rechazado
17	Conexión por conexión rechazada

B.6.3.7 Motivo del aborto/liberación de la SA

Este campo obligatorio está presente en la petición y en la indicación de aborto/liberación de la SA. Se utiliza para indicar el motivo del aborto o la liberación de la SA.

Se fija a 0 para indicar aborto y a 1 para liberación normal. Los valores de 2 a 127 están reservados para uso futuro. Pueden utilizarse otros valores para códigos de motivo definidos privadamente.

B.6.3.8 Etiqueta

Este campo facultativo sólo se utiliza en la PDU del segundo intercambio y su uso se indica en 8.2.3.4. El originador propondrá un conjunto de etiquetas de seguridad. El receptor puede seleccionar el conjunto completo o un subconjunto de lo que envió el originador. Si el conjunto original no es aceptable, el receptor puede proponer un conjunto diferente de etiquetas.

B.6.3.9 Selección de clave

Este campo facultativo sólo se utiliza en la PDU del segundo intercambio. Puede aparecer cualquier número de veces en el contenido de SCI.

Este campo se subdivide en tres subcampos:

a) bandera de utilización;

b) información de selección de clave;

c) referencia de clave.

B.6.3.9.1 Banderas de utilización

Este campo contiene hasta siete valores que indican la posición, dentro de la cadena de bits resultante del intercambio KTE, en la cual ciertas claves toman su valor. La longitud de la clave se determina por el servicio de seguridad asociado seleccionado, que identifica el logaritmo asociado. Múltiples claves pueden utilizar la misma posición de bit (es decir, vienen a ser una misma clave). Las combinaciones admisibles dependerán de la política de seguridad local.

Octeto	*Posición correspondiente de clave/ISN en la cadena de bits EKE*
1-2	Clave de cifrado de datos normales
3-4	Clave de cifrado de datos acelerados
5-6	Clave de generación de comprobación de la integridad de datos normales
7-8	Clave de generación de comprobación de la integridad de datos acelerados
9-10	My ISN para datos normales
11-12	My ISN para datos acelerados
13-14	Clave de generación de autenticación

Si el receptor desea utilizar las mismas claves que el originador, este campo no estará presente en la PDU de segundo intercambio del receptor.

B.6.3.9.2 Información de selección de clave

Este campo indica la posición dentro de la cadena de bits que se obtiene como resultado de un intercambio KTE donde las claves seleccionadas deberán tomar su valor. La longitud de la clave se determina de acuerdo con los servicios de seguridad asociados seleccionados, con lo que se identifica el algoritmo asociado. Múltiples claves pueden utilizar la misma posición de bit (por lo que vienen a ser la misma clave). Las combinaciones admisibles dependerán de la política de seguridad local.

B.6.3.9.3 Referencia de clave

Este subcampo facultativo puede utilizarse para hacer posible una ulterior referencia a la clave. Puede emplearse, por ejemplo, para fines de auditoría, o para la selección de una nueva clave para una conexión en que se emplee la PDU de SA. El valor de esta referencia deberá ser único para la asociación de seguridad.

B.6.3.10 Banderas de la SA

Las siguientes posiciones de bit se utilizan para señalar los atributos SA identificados. El valor 0 significa falso y el valor 1 verdadero.

Bit	*Atributo SA*
1	Retener al desconectar (Retain-on-Disconnect)
2	Protección de parámetro (Param_Protect)
3	Reaplicación de clave (Rekey)
4	Hacia afuera/Respuesta (Outward/Response)
5-8	Reservados para uso futuro

Los bits 5-8 se ponen a 0 en transmisión y no se tienen en cuenta en recepción.

B.6.3.11 ASSR

Este campo tiene que estar presente si lo está el campo de selección de servicio. El identificador de objeto (definido en ISO/CEI 9834) identifica el conjunto de reglas de seguridad que definen el mecanismo que va a aplicarse para una determinada calidad de servicio de protección seleccionada.

Anexo C

Ejemplo de un conjunto convenido de reglas de seguridad (ASSR)

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

Un conjunto convenido de reglas de seguridad (ASSR) establece los mecanismos de seguridad que deben utilizarse, incluidos todos los parámetros necesarios para definir el funcionamiento del mecanismo para una calidad de servicio (QOS) de protección dada.

ASSR-ID { joint-iso-ccitt (2) identified organization (3) oiw (14) secsig (3) oiwsecsigassrobjectidentifier (5) rule (1) } (Object Identifier)

SA-ID Length 4 Octets

Protection QOS Definition Module

PE Auth:	low
AC:	none
Confid:	high
Integ:	high
Security Label:	none

Protection of all service parameters

For Protection QOS: Integ = high Confid = high

Mechanism Module – Security Labels for Access Control

For Protection QOS: AC = high or Conf = high

Label_Def_Auth XYZ

Explicit indication: Yes

Mechanism Module – Integrity Check Value

For Protection QOS: Integ .none or Auth = High
or Mechanism for Security Labels

ICV_Alg_ID	XYZ
ICV_Block_size	8 octets
Rekey after	15 000 PDUs
Key Distribution mech	Asymmetric

Mechanism Module – Integrity Sequence Number

For Protection QOS: Integ = high Auth = high

ISN_Len 4 octets

Mechanism Module – Encipherment

For Protection QOS: Conf > low

Enc_Alg_ID	XYZ
Mode	Chained
Enc_Block_Size	8 octets
Rekey after	10 000 PDUs
Key Distribution mech	Asymmetric

Mechanism Module – Connection Authentication

For Protection QOS: AC > low or PE Auth > Low

Enc_Alg_ID XYZ

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID RSA

Mechanism Module – Symmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID DES (X9.17)

Anexo D

Visión de conjunto del algoritmo EKE

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

El algoritmo EKE requiere dos parámetros. Uno es un número primo p que deberá ser grande (de modo que p-1 tenga un factor que también sea un número primo grande), y el otro es un número «a» comprendido en la gama 1, a, p-1.

Sean A y B los dos partícipes en la comunicación (véase la Figura C.1). EKE comienza haciendo que A seleccione un número aleatorio grande, X, y que B seleccione un número aleatorio grande, Y. Seguidamente A calcula (a** X mod p) y envía a, p y (a**X mod p) a B, quien calcula (a**Y mod p) y lo envía a A. Ambos partícipes, A y B, calculan (a**XY mod p). Un «intruso» sólo ve (a**X mod p) y (a**Y mod p). Dicho intruso no puede determinar X ni Y, y por tanto no puede calcular (a**XY mod p).

Después de esto, A y B pueden utilizar como claves subconjuntos de los bits en (a**XY mod p).

Los valores descritos en el protocolo SA definido en el Anexo B son los siguientes:

- La cadena de bits compartida EKE es (a**XY mod p).
- El testigo de clave 1 es a, p, (a**X mod p), donde ‘a’, ‘p’, y (a**X mod p) se codifican como cadenas de bits concatenadas.
- El testigo de clave 2 es (a**Y mod p).
- El testigo de clave 3 es información derivada de la cadena de bits compartida KTE (a**XY mod p) para contrarrestar los ataques de reproducción.
- El testigo de clave 4 es información derivada de la cadena de bits compartida KTE (a**XY mod p) para contrarrestar los ataques de reproducción.

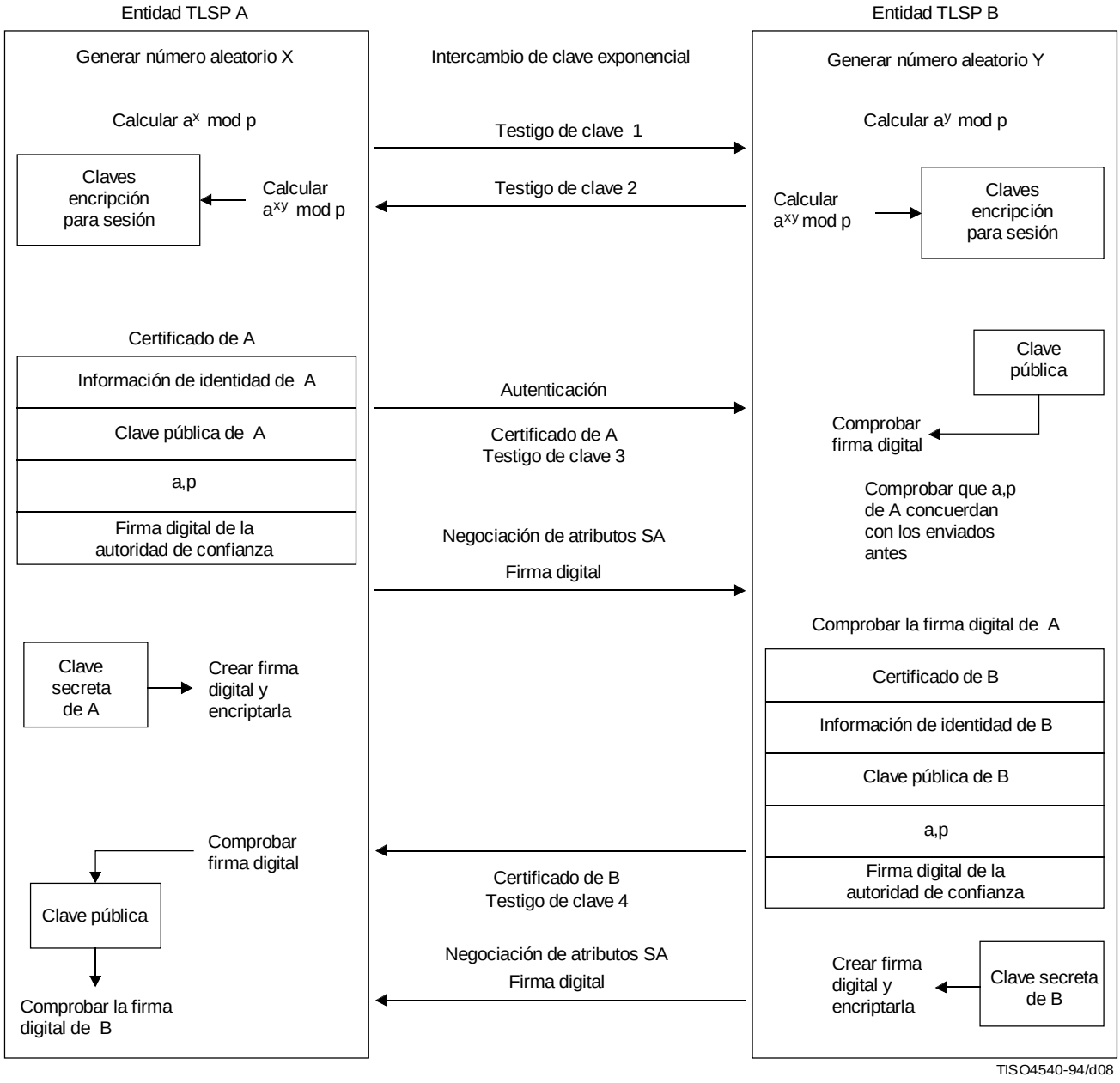


Figura D.1 – Ilustración de la derivación de claves «en línea» y de la firma digital mediante el algoritmo EKE