UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.273

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 – INTERCONEXIÓN DE SISTEMAS ABIERTOS – PROTOCOLO DE SEGURIDAD DE LA CAPA DE RED

Recomendación UIT-T X.273

(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.273 se aprobó el 1 de julio de 1994. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 11577.

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 COMUNICACIÓN 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 con conexión	X.220-X.229
Especificación de los protocolos en modo sin conexión	X.230-X.239
Formularios PICS	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de red	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Consideraciones generales	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 OSI Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta N.° 1 (ASN.1)	X.680-X.699
GESTIÓN OSI	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES OSI	
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

Página

Página

Sumario

Esta Recomendación | Norma Internacional especifica el protocolo que sustenta todos los servicios de integridad, confidencialidad, autenticación y control de acceso que, según el modelo de seguridad OSI, son aplicables a los protocolos de capa de red en los modos con conexión y sin conexión. El protocolo sustenta estos servicios mediante el empleo de mecanismos criptográficos, etiquetas de seguridad y atributos de seguridad asignados, tales como claves criptográficas.

Introducción

El protocolo definido por esta Recomendación UIT-T | Norma Internacional se utiliza para proporcionar servicios de seguridad como soporte de una instancia de comunicación entre entidades de capas más bajas. Este protocolo está ubicado con respecto a otras normas por la estructura estratificada definida en la Rec. X.200 del CCITT | ISO 7498 y por la organización de la capa de red definida en ISO 8648 y ampliado por la Rec. UIT-T X.802 | TR 13595 (Modelo de seguridad de capa inferior). Se proporcionan servicios de seguridad para el soporte de servicios de red en modo conexión y en modo sin conexión. En particular, este protocolo está situado en la capa de red y tiene interfaces funcionales e interfaces de servicio claramente definidos en sus fronteras superior e inferior.

Para evaluar la conformidad de una implementación particular es necesario disponer de un enunciado en el que se indiquen las capacidades y opciones que han sido implementadas para un determinado protocolo OSI. Este enunciado se denomina Enunciado de conformidad de implementación de protocolo (PICS, *protocol implementation conformance statement*).

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – PROTOCOLO DE SEGURIDAD DE LA CAPA DE RED

1 Alcance y campo de aplicación

Esta Recomendación UIT-T | Norma Internacional especifica un protocolo que será utilizado por sistemas de extremo y sistemas intermedios para proporcionar servicios de seguridad en la capa de red, que se define en la Rec. X.213 del CCITT | ISO 8348 AD2 e ISO 8648. El protocolo definido en esta Recomendación UIT-T | Norma Internacional se denomina protocolo de seguridad de la capa de red (NLSP, *network layer security protocol)*.

Esta Recomendación UIT-T | Norma Internacional especifica:

1) El soporte para los siguientes servicios de seguridad definidos en la Rec. X.800 del CCITT | ISO 7498-2:
   a) autenticación de la entidad par;
   b) autenticación del origen de datos;
   c) control de acceso;
   d) confidencialidad en modo conexión;
   e) confidencialidad en modo sin conexión;
   f) confidencialidad del flujo de tráfico;
   g) integridad de la conexión sin recuperación (incluida la integridad de las unidades de datos, con lo cual quedan protegidas las unidades de servicio de datos (SDU) individuales en una conexión);
   h) integridad en el modo sin conexión.
2) Los requisitos funcionales que deben cumplir las implementaciones que pretenden ser conformes con esta Recomendación UIT-T | Norma Internacional.

Los procedimientos de este protocolo se definen en términos de:

a) requisitos que deben cumplir las técnicas criptográficas que pueden utilizarse en una instancia de este protocolo;

b) los requisitos que debe cumplir la información transportada en la asociación de seguridad utilizada en una instancia de comunicación.

Aunque el grado de protección proporcionado por algunos organismos de seguridad depende del uso de algunas técnicas criptográficas específicas, el funcionamiento correcto de este protocolo no depende de la elección de un algoritmo particular de cifrado o descifrado: esta cuestión deberán resolverla los sistemas comunicantes como un asunto local.

Por otra parte, ni la elección ni la implementación de una política de seguridad concreta están comprendidas en el ámbito de esta Recomendación UIT-T | Norma Internacional. La elección de una política de seguridad concreta, y en consecuencia el grado de protección que se alcanzará, es un asunto local que habrán de resolver los sistemas que están utilizando una determinada instancia de comunicaciones seguras. Esta Recomendación UIT-T | Norma Internacional no requiere que las múltiples instancias de comunicaciones seguras en que interviene un sistema abierto dado tengan que utilizar el mismo protocolo de seguridad.

El Anexo D proporciona la proforma (o formulario) PICS para el protocolo de seguridad de la capa de red de acuerdo con las orientaciones pertinentes impartidas en ISO/CEI 9646-2.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación UIT-T | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, con lo que se preconiza que los participantes en acuerdos basados en esta Recomendación UIT-T | Norma Internacional

investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas citadas a continuación. Miembros de la CEI y la ISO llevan un registro 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 X.213 del CCITT (1992) | ISO 8348:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de red*.
- Recomendación UIT-T X.233 (1993) | ISO/CEI 8473:1994, *Tecnología de la información – Protocolo para proporcionar el servicio de red sin conexión OSI: Especificación del protocolo*.
- Recomendación UIT-T X.802 (1994) | ISO/CEI TR 13594:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de las capas inferiores*.
- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de las capas superiores*.

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación X.200 del CCITT (1988), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: el modelo básico.*

  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 X.210 del CCITT (1988), *Tecnología de la información – Interconexión de sistemas abiertos – Convenios para la definición de servicios OSI*.

  ISO TR 8509:1987, *Information processing systems – Open Systems Interconnection – OSI service conventions.*

- Recomendación X.209 del CCITT (1988), *Especificación de las reglas de codificación básica para la notación de sintaxis abstracta uno (ASN.1).*

  ISO/CEI 8825:1990, *Information technology – Open Systems Interconnection – Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)*.

- Recomendación X.223 del CCITT (1988), *Utilización de la Recomendación X.25 para proporcionar el servicio de red OSI en modo conexión*.

  ISO/CEI 8878:1992, *Information technology – Telecommunications and information exchange between systems – Use of X.25 to provide the OSI connection-mode network service*.

- Recomendación X.290 del CCITT (1992), *Metodología de las pruebas de conformidad OSI y marco para las Recomendaciones de protocolo para aplicaciones del CCITT – Conceptos generales.*

  ISO/CEI 9646-1:1991, *Information technology – Open Systems Interconnection – Conformation testing methodology and framework – Part 1: General concepts*.

- Recomendación X.291 del CCITT (1992), *Metodología de las pruebas de conformidad OSI y marco para las Recomendaciones de protocolo para aplicaciones del CCITT – Especificación de series de pruebas abstractas*.

  ISO/CEI 9646-2:1991, *Information technology – Open Systems Interconnection – Conformation testing methodology and framework – Part 2: Abstract test suite specification*.

- Recomendación X.509 del CCITT (1988), *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: marco de autenticación*.

  ISO/CEI 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*

2.3 Referencias adicionales

- ISO/CEI 7498/AD1:1987, *Information processing systems – Open Systems Interconnection – Basic Reference Model Addendum 1 – Connectionless-mode transmission*.
- ISO 8648:1988, *Information Processing Systems – Open Systems Interconnection – Internal organization of the Network Layer*.
- ISO/CEI 8208:1990, *Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment*.
- 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*.
- ISO/CEI 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.
- Recomendación X.25 del CCITT (1993), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para terminales que funcionan en el modo paquete y conectados a redes públicas de datos por circuitos especializados*.

3 Definiciones

3.1 Definiciones del modelo de referencia

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. X.200 del CCITT | ISO 7498:

a) sistema de extremo;
b) entidad de red;
c) capa de red;
d) protocolo de red;
e) unidad de datos de protocolo de red;
f) relevo de red;
g) servicio de red;
h) punto de acceso al servicio de red;
i) dirección de punto de acceso al servicio de red;
j) unidad de datos del servicio de red;
k) unidad de datos de protocolo;
l) encaminamiento;
m) servicio;
n) unidad de datos de servicio.

3.2 Definiciones de la arquitectura de seguridad

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. X.800 del CCITT | ISO 7498-2:

a) control de acceso;
b) confidencialidad;
c) integridad de la conexión sin recuperación;
d) confidencialidad en el modo sin conexión;
e) integridad en el modo sin conexión;
f) autenticación del origen de datos;
g) descifrado;

h) firma digital (o signatura digital);

i) cifrado;

j) autenticación de entidad par;

k) etiqueta de seguridad;

l) servicio de seguridad;

m) confidencialidad del flujo de tráfico.

3.3 Definiciones de convenios de servicio

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. X.210 del CCITT | ISO/TR 8509:

a) proveedor de servicio;

b) usuario de servicio.

3.4 Definiciones del servicio de red

En esta Recomendación | Norma Internacional se utiliza el siguiente término definido en la Rec. X.213 del CCITT | ISO 8348:

– punto de unión de subred (o punto de conexión de subred)

3.5 Definiciones de la organización interna de la capa de red

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en ISO 8648:

a) sistema intermedio;

b) sistema de relevo (o sistema relevador);

c) subred;

d) protocolo de acceso a subred;

e) protocolo de convergencia dependiente de la subred;

f) protocolo de convergencia independiente de la subred.

3.6 Definiciones de protocolo de red en modo sin conexión

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. X.233 del CCITT | ISO 8473:

a) PDU inicial;

b) asunto local;

c) reensamblado;

d) segmento.

3.7 Definiciones del modelo de seguridad de capa superior

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. UIT-T X.803 | ISO/CEI 10745:

a) política de interacción segura;

b) relación de seguridad.

3.8 Definiciones de las pruebas de conformidad

En esta Recomendación | Norma Internacional se utilizan los siguientes términos definidos en la Rec. X.290 del CCITT | ISO/CEI 9646-1:

a) proforma PICS (o formulario PICS);

b) enunciado de conformidad de implementación de protocolo;

c) visión de conjunto de la conformidad estática.

3.9 Definiciones adicionales

A efectos de esta Recomendación | Norma Internacional se aplican las siguientes definiciones:

3.9.1 **SA-ID congelado**: Un SA-ID que no está disponible para asignación a una asociación de seguridad porque es necesario evitar su reutilización.

3.9.2 **clave por pares**: Un par de valores de clave relacionados (clave pública) o idénticos (clave secreta) para uso entre dos participantes determinados.

3.9.3 **información de control de seguridad**: Información de control de protocolo (PCI) intercambiada por un protocolo de seguridad con el fin de establecer o mantener una asociación de seguridad.

3.9.4 **atributos de SA**: La colección de información requerida para controlar la seguridad de las comunicaciones entre una entidad y su(s) entidad(es) par(es) distante(s).

3.9.5 **asociación de seguridad**: Una relación de seguridad entre entidades comunicantes de capa inferior para la que existen atributos SA correspondientes.

3.9.6 **integridad de la unidad de datos**: Una forma de integridad de la conexión en la cual se protege la integridad de unidades de datos de servicio (SDU) individuales, pero los errores en la secuencia de SDU no son detectados.

3.9.7 **dentro de banda (o en banda)**: Significa que la operación ha sido efectuada por un mecanismo utilizando la unidad de datos de protocolo (PDU) de la asociación de seguridad (SA) definida en esta Recomendación UIT-T | Norma Internacional.

3.9.8 **fuera de banda**: Significa que la operación se ha efectuado por otros medios que no son la unidad de datos de protocolo de la asociación de seguridad.

3.9.9 **reglas de seguridad**: Información de seguridad que, una vez seleccionados ciertos servicios de seguridad, especifica el mecanismo de seguridad que habrá de utilizarse, incluidos todos los parámetros necesarios para el funcionamiento del mecanismo.

NOTA – Esta información puede formar parte de unas Reglas de Interacción de Seguridad definidas en la Rec. X.803 del CCITT | ISO 10745.

3.9.10 **Etiqueta**: Véase «Etiqueta de seguridad» (Rec. X.800 del CCITT | ISO 7498-2).

4 Abreviaturas

4.1 Unidades de datos

NPDU	Unidad de datos de protocolo de red (*network protocol data unit*)
NSDU	Unidad de datos de servicio de red (*network service data unit*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
SDU	Unidad de datos de servicio (*service data unit*)

4.2 Campos de la unidad de datos de protocolo

LI	Indicador de longitud (*length indicator*)

4.3 Parámetros

QOS	Calidad de servicio (*quality of service*)

4.4 Diversos

ASSR	Conjunto acordado de reglas de seguridad (*agreed set of security rules*)
CL	Modo sin conexión (*connectionless-mode*)
CLNP	Protocolo de red en modo sin conexión (*connectionless-mode network protocol*)
CLNS	Servicio de red en modo sin conexión (*connectionless-mode network service*)
CO	Modo con conexión (*connection mode*)
CSC PDU	PDU de control de seguridad de conexión (*connection security control PDU*)

DU	Unidad de datos (*data unit*)
EKE	Intercambio de clave exponencial (*exponential key exchange*) (véase el Anexo H)
ES	Sistema de extremo (*end system*)
ICV	Valor de verificación de integridad (*integrity check value*)
IS	Sistema intermedio (*intermediate system*)
ISN	Número secuencial para la integridad (*integrity sequence number*)
KEK	Clave de cifrado de clave (*key enciphering key*)
NLSP	Protocolo de seguridad de la capa de red (*network layer security protocol*)
NLSP-CO	NLSP para el modo conexión (*NLSP for connection mode*)
NLSP-CL	NLSP para el modo sin conexión (*NLSP-connectionless mode*)
NLSPE	Entidad NLSP (*NLSP entity*)
NS	Servicio de red (*network service*)
NSAP	Punto de acceso al servicio de red (*network service access point*)
PCI	Información de control de protocolo (*protocol control information*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
SA	Asociación de seguridad (*security association*)
SA-ID	Identificador de asociación de seguridad (*security association identifier*)
SA-P	Protocolo de asociación de seguridad (*security association protocol*)
SA PDU	PDU de asociación de seguridad (*security association PDU*)
SCI	Información de control de seguridad (*security control information*)
SDT PDU	PDU de transferencia de datos segura (*secure data transfer PDU*)
SN	Subred (*subnetwork*)
SNAcP	Protocolo de acceso a subred (*subnetwork access protocol*)
SNICP	Protocolo de convergencia independiente de la subred (*subnetwork independent convergence protocol*)
SNPA	Punto de unión de subred (*subnetwork point of attachment*)
UN	Red subyacente (*underlying network*)

5 Visión de conjunto del protocolo

5.1 Introducción

Hay dos modos básicos de operación del protocolo NLSP; estos dos modos son:

a) NLSP-CL – Utilizado para proporcionar un servicio de red seguro en modo sin conexión.

b) NLSP-CO – Utilizado para proporcionar un servicio de red seguro con conexión.

Ambos modos de NLSP funcionan como una subcapa de la capa de red. El servicio proporcionado a la entidad superior se denomina el servicio NLSP, y el servicio asumido para proporcionarlo a NLSP se denomina el servicio de red subyacente (UN, *underlying network*). Las primitivas y los parámetros van acompañados de las abreviaturas NLSP o UN para distinguir claramente el servicio al cual se está haciendo referencia. Los servicios UN y NLSP son «interfaces nocionales», es decir, servicios que se describen como si fueran servicios de capa, pero que pueden residir enteramente en la capa de red, lo que depende de la ubicación de la subcapa NLSP (véase el Anexo E).

Ambos modos de NLSP pueden implementarse en sistemas de extremo y en sistemas intermedios. Ambos modos permiten la utilización de la dirección NLSP de origen y de destino así como, facultativamente, la protección de otros parámetros de NLSP-CONEXIÓN. El protocolo NLSP en el modo conexión (NLSP-CO) puede emplearse en cualquier lugar dentro de la capa de red. El protocolo NLSP para el modo sin conexión (NLSP-CL) puede emplearse en cualquier lugar dentro de la capa de red por encima del protocolo de convergencia dependiente de la subred (véase ISO 8648).

El protocolo ha sido diseñado de tal manera que pueda optimizarse para satisfacer una serie de requisitos que los entornos en los que la principal preocupación es la alta seguridad imponen a los entornos en los que la principal preocupación es un rendimiento optimizado. En particular, en NLSP-CO se proporciona una opción «sin encabezamiento» con la cual se consigue un impacto mínimo en la eficiencia de las comunicaciones, aunque pudiera sufrirse una disminución de la seguridad.

El protocolo NLSP utiliza el concepto de una asociación de seguridad (SA) que puede existir fuera de una primitiva DATO UNIDAD sin conexión específica, o de una conexión. Para la SA se define un conjunto de atributos que a su vez definen parámetros para seguridad (por ejemplo, algoritmo, claves etc.).

El protocolo proporciona el mismo modo de servicio (CO o CL) en sus fronteras superior e inferior.

Este protocolo soporta el uso de una amplia gama de mecanismos específicos de seguridad (normalizados y no normalizados). Los usuarios e implementadores deben elegir, para utilizarlo con este protocolo, un mecanismo de seguridad que sea apropiado para obtener el servicio de seguridad y el nivel de protección requeridos. Las cláusulas 9 a 12 y el Anexo C definen el soporte de un conjunto de mecanismos específicos para todos los servicios de seguridad requeridos para el NLSP.

La protección de la seguridad que el protocolo NLSP trata de proporcionar se deriva de los requisitos de servicio de seguridad establecidos por la administración del dominio de seguridad.

NOTA – La utilización del parámetro QOS de la protección, del servicio NLSP, es un asunto local y queda fuera del ámbito de esta Recomendación UIT-T | Norma Internacional.

5.2 Visión de conjunto de los servicios proporcionados

El protocolo NLSP proporciona los servicios de seguridad definidos en la Rec. X.800 del CCITT | ISO 7498-2 que serán apropiados para la capa de red, junto con los servicios capa de red OSI definidos en ISO 8348 y en la Rec. X.213 del CCITT | ISO 8348/AD1.

NLSP-CL soporta los siguientes servicios de seguridad si se seleccionan:

a) Autenticación del origen de datos.

b) Control de acceso.

c) Confidencialidad en el modo sin conexión. Esta protección incluye facultativamente todos los parámetros del servicio NLSP que dependen de los servicios de seguridad seleccionados.

d) Confidencialidad del flujo de tráfico.

e) Integridad en el modo sin conexión. Esta protección incluye facultativamente todos los parámetros del servicio NLSP que dependen de los servicios de seguridad seleccionados.

El NLSP-CO soporta los siguientes servicios de seguridad si, se seleccionan:

a) Autenticación de la entidad par.

b) Control de acceso.

c) Confidencialidad de la conexión. Esta protección incluye facultativamente todos los parámetros de la conexión NLSP que dependen de los servicios de seguridad seleccionados.

d) Confidencialidad del flujo de datos.

e) Integridad de la conexión sin recuperación. Esta protección incluye facultativamente todos los parámetros de la conexión NLSP que dependen de los servicios de seguridad seleccionados. Esta protección incluye, también facultativamente, la integridad de la secuencia de SDU.

5.3 Visión de conjunto de los servicios asumidos

Los servicios asumidos por debajo del NLSP se conocen como el servicio (de red) subyacente (UN). Los servicios subyacentes asumidos por el NLSP-CL utilizan las mismas primitivas que las definidas en el servicio de red sin conexión (Rec. X.213 del CCITT | ISO 8348/AD1).

Para el NLSP-CO, el interfaz UN se modela en dos partes:

a) un servicio que utiliza las mismas primitivas de la Rec. X.213 del CCITT | ISO 8348, con la adición de un parámetro denominado parámetro de autenticación UN;

b) la correspondencia de este servicio ya sea con el servicio de red estándar o directamente con las primitivas de la Rec. X.25 del CCITT | ISO 8208.

La dirección de red transportada en las primitivas del protocolo NLSP se denomina la dirección NLSP. Este parámetro de servicio identifica la entidad de usuario NLSP, que puede o no ser una entidad de transporte, lo que dependerá de que se utilicen o no otros protocolos de capa de red por encima del NLSP y de que la entidad NLSPE esté situada en un sistema de extremo o en un sistema intermedio. La dirección de red que se pasa a la red subyacente se denomina la dirección UN. Este parámetro UN es equivalente a la dirección SNPA si, y únicamente si, ningún protocolo está operando entre la entidad NLSP y la entidad de acceso a la subred.

5.4 Asociaciones de seguridad y reglas de seguridad

5.4.1 Asociaciones de seguridad

El funcionamiento del NLSP se controla mediante una colección de información de gestión de seguridad (por ejemplo, información de selección de servicios de seguridad, identificador de algoritmo de seguridad, claves criptográficas) denominada atributos de asociación de seguridad (atributos SA). La existencia de la colección de atributos de asociación de seguridad requeridos para gobernar la provisión de servicios de seguridad entre entidades comunicantes se denomina una asociación de seguridad.

Las asociaciones de seguridad se describen con más detalle en Rec. UIT-T X.802 | ISO/CEI TR 13594 (Lower Layers Security Model).

Los atributos SA requeridos por el protocolo NLSP en modo sin conexión (NLSP-CL) y por el protocolo NLSP en modo conexión (NLSP-CO) se definen en 6.2. Los atributos SA requeridos por el NLSP-CL se definen en 7.4. Los atributos requeridos por el NLSP-CO se definen en 8.4. Otros atributos específicos a los mecanismos se definen en 10.2, 11.2 y 12.2.

A fin de proteger una instancia de comunicación (una SDU en modo sin conexión o una conexión) se utiliza una SA adecuada existente, o si no existe una SA adecuada es necesario establecer una entre las partes comunicantes.

La asociación de seguridad puede establecerse fuera de banda o utilizando el protocolo de asociación de seguridad (SA-P) dentro de banda del NLSP. El SA-P del NLSP intercambia información de control de seguridad (SCI) mediante la utilización de PDU de SA y/o PDU de SDT con el contenido tipo de datos SA-P. Se utilizarán las PDU de SA si la información SCI se va a transportar en la forma ordinaria. Deberá utilizarse o bien la PDU de SA o la PDU de SDT si la información SCI va a protegerse. Esta SCI se utiliza para completar la formación de atributos SA en cualesquiera atributos de SA y reglas de seguridad.

El NLSP-CO soporta también el intercambio de información para actualizar atributos SA «dinámicos» (por ejemplo, con claves de trabajo, véase el Anexo G) durante el establecimiento de la conexión y después de establecida la conexión. Una actualización de los atributos SA dinámicos no modificará los servicios de seguridad proporcionados.

La utilización de un SA-P dentro de banda junto con el NLSP-CL se define en 7.5. La utilización de un SA-P dentro de banda con un NLSP-CO se define en 8.5 (durante el establecimiento de la conexión) y en 8.11.1 (durante la transferencia de datos). En el Anexo C se define un protocolo para realizar el SA-P dentro de banda. En el Anexo H se presenta un ejemplo de un mecanismo que establece una clave para uso con este protocolo.

5.4.2 Reglas de seguridad

La fijación de los valores de cierto número de atributos SA será impuesta por la política de seguridad. Esta parte de la política de seguridad se denomina el conjunto de reglas de seguridad para la entidad de protocolo. El conjunto de reglas de seguridad para una entidad de protocolo puede forzar a atributos SA tales como las longitudes de campos, los algoritmos de cifrado, etc., a tener un solo valor o un conjunto de valores, que podrán ser limitados aún más por otros medios (por ejemplo, por la gestión de sistemas OSI o mediante el empleo de un intercambio SA-P).

Cuando se ofrezcan otros niveles de protección, el conjunto de reglas de seguridad definirá otras constricciones para tener en cuenta el caso en que se requieran diferentes calidades de protección.

Cuando esos conjuntos de reglas de seguridad se utilicen para la operación entre entidades NLSP, deberá establecerse un identificador único para ellos; dicho identificador se llama un «conjunto convenido de reglas de seguridad» (ASSR, *agreed set of security rules*). El identificador ASSR puede intercambiarse como parte del establecimiento de la asociación de seguridad.

Las reglas de seguridad se describen con más detalle en TR 13594 (Lower Layers Security Model).

5.5 Visión de conjunto del protocolo – Funciones de protección

5.5.1 Alcance de la protección

Tanto el NLSP-CO como el NLSP-CL tienen tres modos diferentes de operación que soportan tres grados básicos de protección:

a) *Protección de todos los parámetros de servicio del NLSP*

En este modo se protegen todos los parámetros de servicio del NLSP, incluidas las direcciones y todos los datos de usuario, salvo los que se negocian con el proveedor del servicio (calidad de servicio, selección de confirmación de la recepción, selección de datos acelerados).

Este modo se selecciona dándole al atributo SA Param_Prot (véase 6.2) el valor TRUE.

b) *Protección de datos de usuarios del NLSP*

En este modo se protegen los datos de usuario, pero no otros parámetros de servicio del NLSP.

Este modo se selecciona dándole al atributo SA Param_Prot el valor FALSE.

Para el protocolo NLSP-CO hay otros submodos de protección de los datos de usuario NLSP, o bien:

1) se protegen todos los datos de usuario del NLSP (incluidos los datos de usuario en las primitivas de servicio NLSP-CONEXIÓN, NLSP-DATOS y NLSP-DESCONEXIÓN);

2) o bien se protegen los datos de usuario NLSP en la primitiva de servicio NLSP-DATOS.

Los submodos para el NLSP se seleccionan ulteriormente por un atributo SA Protect_Connect_Params (véase 8.3). Si Protect_Connect_Params es TRUE, se protegen todos los datos de usuario del NLSP, y en caso contrario sólo se protegen los datos de usuario NLSP en NLSP-DATOS. Protect_Connect_Params deberá forzarse a TRUE (es decir, a que se protejan todos los datos de usuario NLSP) si Param_Prot es TRUE.

c) *Ausencia de protección*

En este modo, todos los parámetros de servicio NLSP se copian directamente a los parámetros de servicio UN equivalentes. Se contornean todos los procedimientos del NLSP.

Este modo se selecciona localmente en base a las direcciones de las entidades pares comunicantes y de las exigencias del servicio de seguridad a nivel local.

5.5.2 Calidad de protección

La realización de la calidad de servicio (QOS) de la seguridad (protección) en las capas inferiores OSI se consigue mediante implementaciones que seleccionan los servicios de seguridad que habrán de aplicarse mediante una política de seguridad controlada localmente. Toda indicación dentro de banda de servicios de seguridad seleccionados se transporta en un protocolo de asociación de seguridad que es independiente de una instancia de comunicación, implícitamente mediante la utilización de una etiqueta de seguridad, o explícitamente por otros medios. En consecuencia, toda modificación relativa a la selección de servicios de seguridad es independiente de que el parámetro de calidad de servicio se transporte a través de las fronteras del interfaz del servicio.

NOTA – Es posible que se deba también indicar a las capas superiores los servicios de seguridad. Sin embargo, hasta el presente no existe la exigencia inmediata de que se definan requisitos específicos de la calidad del servicio de protección.

5.5.3 Funciones de protección de datos

5.5.3.1 Funciones de protección basadas en la PDU de SDT

Tanto el NLSP-CO como el NLSP-CL pueden proteger los parámetros de servicio NLSP mediante la utilización de una unidad de datos de protocolo de transferencia de datos segura (PDU de SDT). El NLSP-CO puede utilizar aún otro posible método para la protección de los datos de usuario NLSP el cual se selecciona dándole al atributo SA sin encabezamiento (No_Header) (véase 8.3) el valor TRUE.

Los procedimientos basados en la PDU de SDT protegen los parámetros de servicio NLSP mediante:

a) la codificación de los parámetros de servicio NLSP como una cadena de octetos antes de la encapsulación;

b) si se selecciona el etiquetado de seguridad explícito (el atributo SA etiqueta fijado a TRUE), la colocación de una etiqueta de seguridad en la cadena de octetos antes de la encapsulación;

c) la aplicación de una función de encapsulación (y la consiguiente desencapsulación) que soporta los siguientes mecanismos:

– confidencialidad del flujo de tráfico

– la integridad y la autenticación del origen de datos

– la confidencialidad

como corresponda a los servicios de seguridad seleccionados. Esta función proporciona una cadena de octetos protegida.

Las subcláusulas 6.4.1.1 y 6.4.2.1 definen procedimientos genéricos, independientes del mecanismo, para la utilización de la PDU de SDT con el fin de proteger los datos. La cláusula 11 define el soporte para una clase de mecanismo de encapsulación basado en la PDU de SDT. Pueden utilizarse con la PDU de SDT otros procedimientos de encapsulación definidos privadamente.

5.5.3.2 Sin encabezamiento (NLSP-CO solamente)

El modo sin encabezamiento del NLSP-CO protege a los usuarios de datos NLSP mediante una función de encapsulación que no cambia la longitud de los datos protegidos. El protocolo NLSP no agrega ninguna información de control de protocolo a los datos protegidos. Los servicios de seguridad soportados dependerán del mecanismo utilizado, pero la función de encapsulación deberá, por lo menos, proporcionar confidencialidad. El modo sin encabezamiento sólo puede utilizarse para proteger un parámetro de servicio único (usuarios de datos NLSP) por lo que sólo puede emplearse si Param_Prot es FALSE.

Las subcláusulas 6.4.1.2 y 6.4.2.2. definen procedimientos genéricos independientes del mecanismo para el uso del modo sin encabezamiento, para proteger datos. La cláusula 12 define el soporte de una clase de mecanismo para encapsulación sin encabezamiento. Con el modo sin encabezamiento pueden utilizarse otros procedimientos de encapsulación definidos privadamente.

5.5.4 Control de la seguridad de la conexión (NLSP-CO solamente)

Cuando se establece una conexión de control de la seguridad de la conexión se intercambian PDU para señalar el modo de establecimiento de la conexión NLSP (es decir, si se emplea o no un SA-P dentro de banda, y si las primitivas de NLSP-CONEXIÓN se hacen o no corresponder con primitivas de UN-CONEXIÓN o de UN-DATOS). Además, la PDU de CSC puede soportar la autenticación de entidad par y establecer valores para atributos SA dinámicos tales como claves y números secuenciales para la integridad. Esto tiene por finalidad permitir la reutilización de una SA previamente establecida sin tener que sufrir la tara del SA-P. También puede utilizarse en cualquier momento durante la existencia de una conexión para reautenticar (probar el conocimiento compartido de) la SA o actualizar atributos dinámicos.

La PDU de CSC sólo se utiliza en el NLSP en modo conexión. La cláusula 8 define los procedimientos generales, independientes del mecanismo, para la utilización de la PDU de CSC. La cláusula 10 define el soporte para una clase de mecanismo para la autenticación y gestión de claves. Con la PDU de CSC pueden utilizarse otros procedimientos, definidos privadamente para el soporte de otras clases de mecanismos.

NOTA – Cuando se utilizan otros mecanismos para la autenticación, si se está utilizando el mecanismo definido en la cláusula 11, este otro mecanismo deberá establecer un valor inicial para el ISN.

5.5.5 PDU utilizadas por el NLSP

El NLSP utiliza las siguientes PDU:

a) *PDU de transferencia de datos segura* – Para proteger los parámetros de las primitivas de servicio NLSP y otros datos mediante la encapsulación descrita en 5.5.3.1. La estructura de esta PDU se define en 13.3.

b) *PDU de control de la seguridad de la conexión* – Para controlar el modo de establecimiento de la conexión NLSP-CO y facultativamente para proporcionar la autenticación de la entidad par, así como modificar atributos SA dinámicos, como se describe en 5.5.4. La estructura de esta PDU se define en 13.5.

NOTA – La PDU de CSC sólo es aplicable al NLSP-CO.

c) *PDU de SA* – PDU que permite el intercambio dentro de banda de información de control de seguridad para fines de gestión de la SA, como se describe en 5.4.1. La estructura de esta PDU se define en 13.4.

Además, con el protocolo NLSP-CO, se pueden proteger facultativamente los datos sin la adición de una información de control de protocolo suplementaria (es decir, sin utilizar la PDU de SDT) como se describe en 5.5.3.2, en lugar de la PDU de SDT.

5.6 Visión de conjunto del protocolo – NLSP-CL

5.6.1 Cláusulas que definen el NLSP-CL

Los procedimientos para el protocolo NLSP-CL se definen en las cláusulas 6 y 7, y los procedimientos facultativos específicos al mecanismo para la encapsulación en la cláusula 11. Estos procedimientos utilizan la PDU de SDT definida en 13.3 y facultativamente la PDU de SA definida en 13.4.

Las siguientes subcláusulas sólo proporcionan una visión de conjunto del funcionamiento del protocolo NLSP-CL; las cláusulas específicas identificadas más arriba definen el funcionamiento del NLSP-CL.

5.6.2 Funciones del NLSP-CL

El NLSP permite transferir datos protegidos o no protegidos en modo sin conexión entre usuarios NLSP pares si así lo permiten las reglas de control de acceso en el ASSR. La entidad NLSP (NLSPE) determina localmente (utilizando servicios de seguridad seleccionados, la dirección NLSP de destino y otras informaciones de gestión) si se necesita o no protección. La transferencia de datos protegidos puede efectuarse con la protección de todos los parámetros de servicio NLSP o con la sola protección de los datos de usuario NLSP según los determine el atributo SA Param_Prot.

Al recibirse una petición NLSP-DATO UNIDAD:

- La entidad NLSP comprueba la SA y determina si se permite la comunicación no protegida con la dirección de destino y, de ser así, se requiere o no protección.
- Si no se requiere protección, la entidad NLSP copiará todas las primitivas y parámetros NLSP a las correspondientes primitivas y parámetros UN sin modificación.
- Si se requiere protección, la entidad NLSP encapsula los parámetros de servicio, forma una PDU de SDT y la transfiere como los datos de usuario UN de una petición UN-DATO UNIDAD junto con la dirección de origen UN, la dirección de destino UN y parámetros de calidad de servicio UN. De esta forma pueden quedar protegidos sólo los datos de usuario NLSP, o todos los parámetros de servicio NLSP.

Al recibir una indicación UN-DATO UNIDAD, la entidad NLSP:

- Utiliza la dirección de origen UN e información local para determinar si se permite la comunicación con la dirección de destino y, de ser así, si se requiere o no protección.
- Si no se requiere protección, los parámetros de servicio UN se copian a los parámetros NLSP sin modificación.
- Si se requiere protección, la entidad NLSP comprueba la PDU de SDT, extrae los datos de usuario NLSP y, facultativamente, otros parámetros de servicio NLSP, utilizando la función de desencapsulación. Los datos de usuario, la dirección de origen, la dirección de destino y los parámetros de calidad de servicio se pasan al usuario NLSP en la indicación NLSP-DATO UNIDAD.

NOTA – En transmisión, el NLSP puede funcionar después (o antes, o a la recepción) de funciones de protocolo (CLNP) de la Rec. UIT-T X.233 | ISO/CEI 8473, protegiendo las PDU de CLNP. Asimismo, en transmisión, el NLSP puede funcionar después (o antes, o a la recepción) de funciones de protocolo, transportándose las PDU de CLNP en campos de datos de PDU de CLNP.

Dado que algunos de los parámetros CLNP pueden tener importancia para la seguridad, la selección de esos parámetros, después del NLSP en transmisión, debe considerarse en función de la política de seguridad local. Algunos de los parámetros facultativos que deben considerarse son el registro de ruta, el encaminamiento parcial y completo desde el origen, y el conteo de los saltos. Cualquiera de estos parámetros podría dar información, sobre la red en cuestión, que no debiera ser perceptible por el observador de la red.

Para determinar que una PDU de CLNP ha transportado una PDU del NLSP-CL en recepción, el receptor deberá, o bien comprobar que el selector de la dirección de destino tiene un valor de todos ceros, o que el identificador de protocolo NLSP en el campo de datos de la PDU de CLNP es lo definido en 13.3. Cualquiera de estas dos comprobaciones puede utilizarse para indicar que esta PDU debe ser procesada por la capa de red, o de lo contrario enviarse directamente a la capa de transporte.

5.7 Visión de conjunto del protocolo – NLSP-CO

5.7.1 Cláusulas que definen el NLSP-CO

Los procedimientos para el NLSP-CO basados en No_Header (sin encabezamiento) se definen en las cláusulas 6 y 8, y los procedimientos facultativos específicos al mecanismo, en la cláusula 12 para la encapsulación y en la cláusula 10 para el control de la seguridad de la conexión. Estos procedimientos utilizan la PDU de CSC definida en 13.5 y facultativamente la PDU de SA definida en 13.4.

Los procedimientos para el NLSP-CO basados en la utilización de la PDU de SDT se definen en las cláusulas 6 y 8, y los procedimientos facultativos específicos al mecanismo, en la cláusula 11 para la encapsulación y en la cláusula 10 para el control de la seguridad de la conexión. Estos procedimientos utilizan la PDU de SDT definida en 13.3, la PDU de CSC definida en 13.5 y facultativamente la PDU de SA definida en 13.4.

Las subcláusulas que siguen proporcionan solamente una visión de conjunto del funcionamiento del protocolo NLSP-CO; las cláusulas específicas identificadas anteriormente definen la operación del NLSP-CO.

5.7.2 Conexiones no protegidas en el NLSP-CO

Si se permiten comunicaciones no protegidas entre las direcciones llamante y llamada, todos los parámetros de servicio NLSP/UN se copian directamente hacia/desde el interfaz de servicio NLSP desde/hacia el interfaz de servicio UN.

5.7.3 NLSP-CONEXIÓN

Al recibir una petición de NLSP-CONEXIÓN, la NLSPE comprueba si existe o no en ese momento una SA con las características requeridas. Si existe, puede utilizarse para proteger la conexión. Si no existe, se establece una nueva SA dentro de banda como parte de las funciones NLSP-CONEXIÓN o fuera de banda dentro de un periodo de temporización dado. Si no se puede ejecutar ninguna de estas dos acciones, se retorna una NLSP-DESCONEXIÓN.

Se soportan dos modos básicos de establecimiento de una conexión NLSP. En el primero, los parámetros de la NLSP-CONEXIÓN se transportan en las primitivas de servicio UN-CONEXIÓN. En el segundo, los parámetros de NLSP-CONEXIÓN, después de encapsulados en una PDU de SDT, se transportan en una primitiva de UN-DATOS después de establecida la conexión UN. Existen variantes de ambos modos de establecimiento de la conexión NLSP: uno para uso con intercambios SA-P dentro de banda (empleando la PDU de SA y/o PDU de SDT con tipo de datos de contenido de SA-P) transportados en una primitiva UN-DATOS, y el otro para uso con una SA que se ha establecido fuera de banda.

La PDU de control de la seguridad de la conexión (PDU de CSC) se utiliza para señalar el modo de establecimiento de la conexión y, si no se está transportando SA-P dentro de banda, el intercambio de PDU de CSC se utiliza también para:

a) establecer atributos de seguridad específicos al mecanismo para uso en la protección de la conexión (por ejemplo, claves, números secuenciales para la integridad);

b) efectuar la autenticación de entidad par.

En la cláusula 10 se define el soporte facultativo de mecanismos para una autenticación simple basada en desafío-respuesta, y la gestión de claves.

Cuando la primitiva de NLSP-CONEXIÓN se transporta en una primitiva de UN-CONEXIÓN con el SA-P dentro de banda, se establece una conexión UN para transportar el SA-P, la que se libera posteriormente, antes de ejecutar el intercambio de UN-CONEXIÓN en que se transportan los parámetros NLSP-CONEXIÓN. Las PDU de CSC se utilizan en el segundo intercambio de UN-CONEXIÓN para reautenticar las entidades NLSP pares.

El establecimiento de la SA se consigue mediante un intercambio de unidades PDU de SA o PDU de SDT que transportan la información necesaria para establecer los atributos SA requeridos. En el Anexo C se define un protocolo SA para este fin.

Si los parámetros de la NLSP-CONEXIÓN deben ser protegidos, se encapsularán antes de transferirlos.

5.7.4 NLSP-DATOS

Al recibirse una petición NLSP-DATOS:

a) Si se selecciona la protección basada en PDU de SDT, la entidad NLSP encapsula los parámetros de servicio apropiados, forma una PDU de SDT y la transfiere como los datos de usuario UN de una petición UN-DATOS.

b) Si se selecciona la protección basada en sin encabezamiento, los datos de usuario NLSP se cifran y se transfieren a los datos de usuario UN de una petición UN-DATOS.

Al recibirse una indicación UN-DATOS:

a) Si se ha seleccionado la protección basada en PDU de SDT, la entidad NLSP verifica la PDU y extrae los datos de usuario NLSP, y posiblemente una confirmación/petición NLSP, utilizando la función de desencapsulación.

b) Si se selecciona la protección basada en sin encabezamiento, los datos de usuario UN se descifran para obtener los datos de usuario NLSP.

c) Los parámetros de servicio NLSP se pasan al usuario NLSP en la indicación NLSP-DATOS.

5.7.5 NLSP-DATOS ACELERADOS

Estos datos se procesan de manera similar a una petición NLSP-DATOS.

NOTA – Cuando se utiliza la PDU de SDT, por efecto de la función de encapsulación el tamaño de los datos puede aumentar. En consecuencia, al haberse limitado el tamaño del campo de datos de usuario puede ser necesario que los datos acelerados sufran una ulterior segmentación y sean reensamblados cuando atraviesen la red subyacente.

5.7.6 NLSP-REINICIACIÓN

El NLSP pasa esta primitiva directamente a la red subyacente. Se reautentica la conexión segura y los atributos específicos al mecanismo se restablecen utilizando PDU de CSC transportadas en UN-DATOS.

NOTA – También puede ser necesario reinicializar algunos mecanismos de seguridad, ya que pueden haberse perdido datos. En particular, el mecanismo de secuenciación para la integridad deberá poder evitar ataques por reproducción fraudulenta incluso tras una pérdida de datos.

5.7.7 NLSP-ACUSE DE DATOS

Si se van a proteger todos los parámetros de servicio NLSP (es decir, si Param_Prot es TRUE), el NLSP encapsula esta información, la coloca en una PDU de SDT, y la pasa a la subcapa UN. En otro caso, esta primitiva de servicio se hace corresponder directamente a UN-ACUSE DE DATOS.

5.7.8 NLSP-DESCONEXIÓN

Al recibir una petición NLSP-DESCONEXIÓN, si de acuerdo con el modo de protección seleccionado (véase 5.5.1) se requiere la protección de los parámetros de servicio, la entidad NLSP construye una PDU de transferencia de datos de seguridad que contiene la petición NLSP-DESCONEXIÓN, los datos de usuario NLSP, y facultativamente los otros parámetros. Esta PDU se transporta, o bien en UN-DATOS antes de que se libere la conexión UN, o, si cabe, la PDU de SDT puede transportarse en el parámetro datos de usuario UN de una UN-DESCONEXIÓN.

Si no se requiere la protección de los parámetros de la petición NLSP-DESCONEXIÓN, dichos parámetros se envían en una petición UN-DESCONEXIÓN.

5.7.9 Otras funciones

El NLSP soporta también otras funciones que se inician por temporizaciones u otros sucesos externos:

a) Intercambio de PDU de CSC para modificar atributos SA dinámicos tales como claves.

b) Intercambio de prueba de seguridad para comprobar que los aspectos criptográficos de la SA están bien establecidos.

c) Transmisión de PDU de SDT que contienen solamente un campo de relleno de tráfico para la confidencialidad del flujo de tráfico.

6 Funciones de protocolo comunes al NLSP-CL y al NLSP-CO

6.1 Introducción

En esta cláusula se describen funciones de protocolo comunes al NLSP en modo conexión y en modo sin conexión. Estas funciones son invocadas como se describe en las cláusulas 7 y 8.

6.2 Atributos SA comunes

Los siguientes atributos SA controlan el funcionamiento del protocolo NLSP en modo conexión y en modo sin conexión. En su descripción se han incluido los nemónicos utilizados para hacer referencia a estos atributos en esta Especificación.

NOTA – Cuando un atributo SA esté «constreñido por el ASSR», esta constricción puede definir un valor único o un conjunto de valores. Cuando el conjunto convenido de reglas de seguridad (ASSR, agreed set of security rules) define una gama de valores, el valor del atributo puede establecerse por la gestión de sistemas OSI, por un intercambio SA-P, o por otros medios que están fuera del ámbito de esta Especificación.

a) *Identificación de la SA:*

My_SA-ID: Entero en la gama
0 a (256 ** maxlength) – 1

El identificador local de la SA. El valor de este atributo se fijará al establecerse la SA.

Your_SA-ID: Entero en la gama
0 a (256 ** maxlength) – 1

El identificador distante de la SA. El valor de este atributo se fijará al establecerse la SA.

maxlength es un entero comprendido en la gama de 2 a 126.

NOTA 1 – Sería un grave error que hubiera más de una SA con el mismo identificador local.

b) *Indicador que señala si la NLSPE inició o respondió al establecimiento de la SA:*

Iniciador: Booleano

Este atributo indica la forma de establecer la bandera iniciador a respondedor para detectar las PDU reflejadas.

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

c) *Dirección UN de entidad NLSP par:*

Peer_Adr: Cadena de octetos con el formato definido en la Rec. X.213 del CCITT | ISO 8348/AD2.

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

d) *Dirección NLSP de entidades servidas a través de la entidad par distante:*

Adr_Served: Conjunto de cadenas de octeto con el formato definido en la Rec. X.213 del CCITT | ISO 8348/AD2.

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

e) *Servicios de seguridad seleccionados para la SA:*

AC: Entero en la gama constreñida por el ASSR

TF_Conf: Entero en la gama constreñida por el ASSR

f) *Protección de parámetros:*

Param_Prot: Booleano

Protege todos los parámetros de servicio NLSP salvo los que pueden ser modificados por la red subyacente (es decir, calidad de servicio, selección de confirmación de recepción y selección de datos acelerados).

g) *Atributo del mecanismo de etiqueta:*

Label: Booleano

Etiquetado explícito de las PDU en modo conexión/sin conexión.

Label_Set: Set of (Conjunto de)

{Label_Ref:	Entero
Label_Auth:	Identificador de objeto
Label_Content:	Según el formato definido por Label_Auth}

Los valores de estos atributos se fijan al establecerse la SA, o están preestablecidos.

NOTA 2 – Se espera que estas etiquetas serán registradas de acuerdo con los procedimientos definidos por UIT-T e ISO/CEI.

6.3 Funciones comunes ejecutadas al recibirse una petición para una instancia de comunicación

6.3.1 Comprobaciones iniciales

Una NLSPE que recibe una petición de una instancia de comunicación (es decir, una petición NLSP-CONEXIÓN o una petición DATO-UNIDAD) verificará que:

a) La dirección llamante o de origen NLSP es una dirección NLSP servida por esta NLSPE.

b) Los servicios de seguridad requeridos pueden ser proporcionados por esta NLSPE.

6.3.2 Identificación de la asociación de seguridad

Una NLSPE que recibe una petición de una instancia de comunicación (es decir, una petición NLSP-CONEXIÓN o una petición DATO-UNIDAD) identifica, entre todas las SA de que ella dispone, una SA cuyos atributos satisfagan las siguientes condiciones:

a) toda exigencia de servicio de seguridad obtenido localmente concuerda con los servicios de seguridad seleccionados para la SA;

b) la dirección llamada o de destino NLSP está contenida en el conjunto de direcciones NLSP en Adr_Served;

c) ninguna conexión NLSP está utilizando en ese momento la SA en cuestión (NLSP-CO solamente).

El procedimiento que se sigue cuando más de una SA satisface estas condiciones es un asunto local. Si no existe tal SA, y si el establecimiento de SA dentro de banda está soportado, se puede seleccionar la opción SA-P (protocolo de SA) como se define en las cláusulas 7 y 8. De no ser así, pueden seguirse procedimientos de establecimiento de la SA fuera de banda. Si ninguno de estos procedimientos puede seguirse con éxito dentro de un periodo de temporización definido localmente, se aplicarán los procedimientos de recuperación tras error adecuados para el modo de comunicación, como se indica en 7.4 y 8.4.

6.4 Funciones de protocolo de transferencia de datos segura

6.4.1 Generación

6.4.1.1 Generación basada en la PDU de SDT

Para la utilización indicada en las cláusulas 7 y 8 se efectúa lo siguiente:

a) El campo tipo de datos de 8 bits se fijará al valor del atributo SA iniciador.

b) Si estos procedimientos son invocados en base a 8.6 (DATOS-NLSP), el campo tipo de datos de 7 bits se fijará de acuerdo con esos procedimientos; de lo contrario, este bit se fija a un valor que indique «último».

c) Los bits 1-6 del campo tipo de datos se fijarán a un valor definido en 13.3.4.2 como convenga a los procedimientos de las cláusulas 7 y 8.

d) Los datos relacionados con los parámetros de servicio NLSP o con otros intercambios de protocolo (por ejemplo, datos de prueba) se colocan en los campos de contenido apropiados (véase 13.3.4.3), en la forma requerida, de acuerdo con los procedimientos descritos en las cláusulas 7 y 8.

e) Si (Label es TRUE), y en el caso de NLSP-CO, ésta es la primera PDU de SDT enviada en la conexión actual, entonces, o bien:

   1) se colocará una etiqueta de seguridad, incluida la autoridad definidora, en un campo de contenido etiqueta y se insertará en la PDU; o bien

   2) se colocará una referencia de etiqueta de seguridad en un campo de contenido referencia de etiqueta y se insertará en la PDU.

   La etiqueta seleccionada será uno de los valores en el atributo SA Label_Set.

   NOTA 1 – En el caso de NLSP-CO, si Protect_Connect_Params está presente, sólo será etiquetada la PDU de SDT que transporta parámetros de NLSP-CONEXIÓN; de lo contrario, será etiquetada la PDU de SDT enviada en cualquiera de los dos sentidos de transmisión durante la fase de transferencia de datos NLSP.

f) Deberá invocarse una función de encapsulación (por ejemplo, la descrita en la cláusula 11) a la cual se pasarán los siguientes argumentos:

   1) SA-ID se fijará a My_SA-ID;

   2) unit-data-type (tipo de dato unidad) se fijará a:

      - «acelerados» si los datos que han de protegerse provienen de una primitiva NLSP-DATOS ACELERADOS;
      - «normales» en otro caso;

   3) la cadena de octetos antes de la encapsulación se fijará al valor de los campos PDU construidos.

g) La función de encapsulación retornará, sea un error, sea una cadena de octetos encapsulada. Tras una ejecución exitosa de la función de encapsulación, el encabezamiento no protegido de la PDU de SDT se creará como se define en 13.3.2 con la cadena de octetos encapsulada agregada al final del encabezamiento.

   NOTA 2 – El SA-ID no está presente en NLSP-CO.

6.4.1.2 Ausencia de encabezamiento (NLSP-CO solamente)

Para la utilización indicada en la cláusula 8 se efectuará lo siguiente:

a) Deberá llamarse una función de encapsulación que no cambie el tamaño de los datos (por ejemplo, una función descrita en la cláusula 12) a la cual se pasarán los siguientes argumentos:

   1) SA-ID se fijará a My_SA-ID;

   2) el tipo de dato unidad se fijará a:

      - «acelerados», si los datos que han de protegerse provienen de una primitiva NLSP-DATOS ACELERADOS;
      - «normales» en otro caso;

   3) la cadena de octetos antes de la encapsulación deberá fijarse al valor del parámetro datos de usuario NLSP.

b) La función de encapsulación retornará, sea un error, sea una cadena de octetos encapsulada.

6.4.2 Comprobación

6.4.2.1 Comprobación basada en la PDU de SDT

Para la utilización indicada en las cláusulas 7 y 8 se efectuará lo siguiente:

a) El encabezamiento no protegido se retirará de la PDU, y se descartará.

b) Se invocará una función de desencapsulación (por ejemplo, una de las descritas en la cláusula 11) a la cual se pasarán los siguientes argumentos:

   1) SA-ID se fijará a My_SA-ID;

   2) el tipo dato unidad se fijará a:

      - «acelerados» si los datos que habrán de ser desencapsulados provienen de una primitiva UN-DATOS ACELERADOS;
      - «normales» en otro caso;

   3) la cadena de octetos encapsulada se fijará al resto de la PDU.

c) La función de desencapsulación retornará, sea un error, sea una cadena de octetos antes de la encapsulación. Tras una ejecución exitosa de la función de desencapsulación se efectuará el siguiente procesamiento.

d) Se comprobará que la bandera (iniciador a respondedor) constituida por el bit 8 del campo de tipo de datos no es igual al valor del atributo SA iniciador.

e) Los bits 1-6 y el bit 7 del campo de tipo de datos se examinarán para comprobar que tienen el valor apropiado para los procedimientos indicados en las cláusulas 7 y 8.

f) Si Label es TRUE, y, en el caso de NLSP-CO, ésta es la primera PDU de SDT recibida en la conexión en curso, se comprobará la PDU para cerciorarse de que hay únicamente presente un campo de contenido etiqueta o referencia de etiqueta. Si está presente, el valor de la etiqueta deberá comprobarse para cerciorarse de que está contenido en el conjunto Label_Set.

g) Los campos de contenido relacionados con los parámetros de servicio NLSP u otras funciones del protocolo se comprobarán para cerciorarse de que están presentes, como se requiere en los procedimientos de las cláusulas 7 y 8. Los datos se toman de estos campos y se tratan de acuerdo con los procedimientos de las cláusulas 7 y 8.

6.4.2.2 Sin encabezamiento presente (NLSP-CO solamente)

Para la utilización indicada en la cláusula 8 se efectuará lo siguiente:

a) Se invocará la función de desencapsulación definida que se utilizará para esta SA (por ejemplo, la descrita en la cláusula 12), a la que se pasarán los siguientes argumentos:

   1) SA-ID se fijará a My_SA-ID;

   2) el tipo de dato unidad se fijará a:

      - «acelerados» si los datos que habrán de desencapsularse provienen de una primitiva UN-DATOS ACELERADOS;
      - «normales» en todos los demás casos;

3) la cadena de octetos encapsulada se fijará al valor del parámetro datos de usuario UN.

b) La función de desencapsulación deberá retornar, sea un error, sea una cadena de octetos antes de la encapsulación.

6.5 Utilización de un protocolo de asociación de seguridad

Cuando dos NLSPE no tienen establecida una SA, pueden establecer una SA utilizando un protocolo de asociación de seguridad (SA-P) o algún otro método. Un SA-P intercambia PDU de SA, o PDU de SDT con el contenido tipo de datos fijado a SA-P, entre las NLSPE, para establecer, modificar, o terminar una SA.

Las cláusulas 7 y 8 sobre el protocolo NLSP definen la forma en que SA-P podría invocarse, pero no los procedimientos del SA-P. Los procedimientos del SA-P, y la información PCI contenida en la PDU de SA/PDU de SDT, dependen del mecanismo específico utilizado para proporcionar el SA-P (en el Anexo C se define un mecanismo de protocolo adecuado). Todo SA-P proporcionará las prestaciones siguientes:

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

b) claves provenientes de una fuente autenticada;

c) establecimiento de la información inicial para fines de autenticación e integridad, si se requiere.

Una NLSPE deberá descartar las PDU SA si el SA-P específico no está soportado.

Un SA-P puede basarse en algoritmos simétricos o asimétricos. Se recomienda la utilización de un algoritmo asimétrico. El Anexo C contiene un ejemplo de ese mecanismo.

7 Funciones de protocolo para el NLSP-CL

7.1 Servicios proporcionados por el NLSP-CL

Los servicios proporcionados por el NLSP se indican por el prefijo «NLSP». Las primitivas son las siguientes:

Primitivas	*Parámetros*
Petición NLSP-DATO UNIDAD	Dirección de destino NLSP
Indicación NLSP-DATO UNIDAD	Dirección de origen NLSP
	Calidad de servicio NLSP
	Datos de usuario NLSP

Las primitivas de servicio y los parámetros son equivalentes a los definidos en la Rec. X.213 del CCITT | ISO 8348/AD1.

7.2 Servicios asumidos

Los servicios asumidos por NLSP en su frontera inferior se señalan con el prefijo «UN» (*underlying network*», red subyacente). Estas primitivas son:

Primitivas	*Parámetros*
Petición UN-DATO UNIDAD	Dirección llamada UN
Indicación UN-DATO UNIDAD	Dirección llamante UN
	Calidad de servicio UN
	Datos de usuario UN

Las primitivas de servicio y los parámetros asumidos son equivalentes a los del CLNS de la ISO (Rec. X.213 del CCITT | ISO 8348/AD1).

7.3 Atributos de la asociación de seguridad

Los siguientes atributos controlan el funcionamiento del NLSP-CL. Su descripción incluye los nemónicos utilizados para hacer referencia a estos atributos en esta Especificación:

NOTA – Cuando un atributo SA está «constreñido por el ASSR», esta constricción puede definir un solo valor o un conjunto de valores. Cuando el ASSR define una gama de valores, el valor de atributo puede ser establecido por la gestión de sistemas OSI, un intercambio SA-P o por otros medios fuera del ámbito de esta Especificación.

– Servicios de seguridad seleccionados para la SA:

DOAuth: Entero en la gama constreñida por el ASSR para el nivel de autenticación del origen de datos.

El valor de este atributo será preestablecido o fijado al establecerse la SA.

CLConf: Entero en la gama constreñida por el ASSR para el nivel de confidencialidad en el modo sin conexión.

El valor de este atributo será preestablecido o fijado al establecerse la SA.

CLInt: Entero en la gama constreñida por el ASSR para el nivel de integridad en el modo sin conexión.

El valor de este atributo será preestablecido o fijado al establecerse la SA.

7.4 Comprobaciones

En muchos puntos de las siguientes descripciones, la entidad NLSP-CL comprueba que se ha cumplido alguna condición. A menos que se especifique otra cosa, cada vez que fracasa una comprobación, la entidad NLSP-CL descartará los datos que se están procesando en ese momento. Facultativamente, la entidad puede también registrar en un fichero un informe de auditoría. Los fallos que deberán ser verificados por auditoría se consideran un asunto local.

7.5 Establecimiento de la SA dentro de banda

Una SA puede establecerse dentro de banda utilizando un protocolo de asociación de seguridad (SA-P). En el Anexo C se define un protocolo SA-P.

NOTA – Actualmente el protocolo SA-P no incluye procedimientos de recuperación, por lo que debe tenerse cuidado de que se proporcione la fiabilidad requerida cuando se utilice este protocolo con NLSP-CL.

7.6 Procesamiento de la petición NLSP-DATO UNIDAD

7.6.1 Comprobaciones iniciales e identificación de la SA

Al recibirse una petición NLSP-DATO UNIDAD, la NLSPE comprueba si se permiten comunicaciones no protegidas basadas en exigencias locales del servicio de seguridad y el par de direcciones de origen/destino. Si se permiten comunicaciones no protegidas, los parámetros de servicio NLSP se copian directamente a los parámetros de servicio UN equivalentes en una petición UN-DATO UNIDAD y la NLSP no ejecuta ninguna otra acción.

Si se requiere que las comunicaciones estén protegidas, se deberán realizar las comprobaciones iniciales y la identificación de los procedimientos SA descritas en 6.3, a lo que seguirán los siguientes procedimientos:

7.6.2 Protección de NLSP-DATO UNIDAD

La NLSPE efectuará las «funciones de generación basadas en la PDU de SDT» definidas en 6.4.1.1, con el tipo de datos «pet/ind NLSP-DATO UNIDAD» que contiene:

a) si Param_Prot es TRUE, la dirección NLSP de origen;

b) si Param_Prot es TRUE, la dirección NLSP de destino;

c) el parámetro de datos usuario NLSP.

La «bandera última/no última» se pondrá en «última» (por ejemplo, el bit 7 del campo tipo de datos = 0)

7.6.3 Petición de red

La PDU de SDT se pasará al protocolo inferior siguiente como el parámetro datos de usuario UN de una petición UN-DATO UNIDAD.

Si Param_Prot es TRUE, la dirección de origen UN será la dirección UN de la entidad NLSP local, y en caso contrario la dirección de origen NLSP se copiará a la dirección de origen UN.

Si Param_Prot es TRUE, la dirección de destino UN será Peer_Adr, y en caso contrario la dirección de destino NLSP se copiará a la dirección de destino UN.

UN QOS se determinará de acuerdo con la política local, pero puede copiarse del parámetro QOS del NLSP.

NOTA – Si los parámetros de ruta de registro y de ruta de origen se encuentran en parámetros QOS del NLSP y no se han pasado como parámetros QOS de UN, la calidad de servicio (QOS) especificada no podrá proporcionarse para la parte de la ruta entre las entidades NLSP-CL de origen y de destino.

7.7 Procesamiento de la indicación UN-DATO UNIDAD

7.7.1 Comprobaciones iniciales y procesamiento

Si no está presente ninguna PDU de SDT, la NLSPE comprueba si se permiten comunicaciones no protegidas en base a las exigencias locales del servicio de seguridad y el par de direcciones de origen/destino. Si se permiten comunicaciones no protegidas, los parámetros de servicio UN se copian directamente a los parámetros de servicio NLSP equivalentes en una petición NLSP-DATO UNIDAD, y la NLSPE no ejecuta ninguna otra acción. Si no se permiten comunicaciones no protegidas, se siguen los procedimientos descritos en 7.4. La NLSPE no ejecuta ninguna otra acción.

Si está presente una PDU de SDT, la NLSPE identificará, entre las SA de que dispone, una SA en la que My_SA-ID sea igual al campo SA-ID de la PDU de SDT recibida. Toda ulterior operación se referirá a esta SA identificada.

La NLSPE efectuará el procesamiento común descrito en 6.4.2.1. Además, se efectuarán las siguientes comprobaciones:

a) Si el campo tipo de datos indica «no relacionado con ninguna primitiva de servicio NLSP», la PDU de SDT no será procesada ulteriormente de acuerdo con estos procedimientos. En otro caso, se comprobará el campo tipo de datos para determinar si es una NLSP-DATO UNIDAD.

NOTAS

1 Puede ignorarse el valor de «bandera última/no última» (por ejemplo, el bit 7 del campo tipo de datos = 0).

2 El soporte del relleno de tráfico y de los intercambios de prueba en el modo sin conexión queda fuera del ámbito del NLSP.

b) Si Param_Prot es TRUE, deberá comprobarse la PDU de SDT para asegurarse de que los siguientes campos están presentes:

1) dirección de destino;

2) dirección de origen.

Se pasará una indicación NLSP-DATO UNIDAD al usuario NLSP con los parámetros fijados y la dirección comprobada como se prescribe en 7.7.2

7.7.2 Parámetros de la indicación NLSP-CL

7.7.2.1 Parámetros de la dirección

Si Param_Prot es TRUE, la NLSPE fijará los parámetros de servicio NLSP a los valores contenidos en la PDU de SDT.

Si Param_Prot es FALSE, los valores se tomarán de los parámetros de la indicación UN de la manera siguiente:

a) dirección de origen NLSP = dirección de origen UN, y

b) dirección de destino NLSP = dirección de destino UN.

La dirección de destino NLSP, fijada como se ha descrito anteriormente, se comprobará para determinar que es la dirección NLSP servida por esta entidad NLSP, de acuerdo con la política de seguridad local.

La dirección de origen NLSP, fijada como se ha descrito anteriormente, se comprobará para determinar que es una dirección NLSP contenida en el atributo SA Adr_Served.

7.7.2.2 QOS (calidad de servicio)

Los parámetros de calidad de servicio se copian del servicio UN al servicio NLSP.

7.7.2.3 Datos de usuario

Los datos en el campo datos de usuario de la cadena de octetos antes de la encapsulación de la PDU de SDT se pasarán al usuario NLSP en el parámetro datos de usuario NLSP de la indicación NLSP-DATO UNIDAD.

8 Funciones de protocolo para el NLSP-CO

8.1 Servicios proporcionados por el NLSP-CO

Las primitivas de los servicios proporcionados por el NLSP-CO son las siguientes:

Primitivas		*Parámetros*
Petición	NLSP-CONEXIÓN	Dirección llamada NLSP
Indicación	NLSP-CONEXIÓN	Dirección llamante NLSP
		Selección de confirmación de recepción NLSP
		Selección de datos acelerados NLSP
		Conjunto de parámetros QOS NLSP
		Datos de usuario NLSP
Respuesta	NLSP-CONEXIÓN	Dirección respondedora NLSP
Confirmación	NLSP-CONEXIÓN	Selección de confirmación de recepción NLSP
		Selección de datos acelerados NLSP
		Conjunto de parámetros QOS NLSP
		Datos de usuario NLSP
Petición	NLSP-DATOS	Datos de usuario NLSP
Indicación	NLSP-DATOS	Petición de confirmación NLSP
Petición	NLSP-ACUSE DE DATOS	
Indicación	NLSP-ACUSE DE DATOS	
Petición	NLSP-DATOS ACELERADOS	Datos de usuario NLSP
Indicación	NLSP-DATOS ACELERADOS	
Petición	NLSP-REINICIACIÓN	Motivo NLSP
Indicación	NLSP-REINICIACIÓN	Originador NLSP
		Motivo NLSP
Respuesta	NLSP-REINICIACIÓN	
Confirmación	NLSP-REINICIACIÓN	
Petición	NLSP-DESCONEXIÓN	Originador NLSP
Indicación	NLSP-DESCONEXIÓN	Motivo NLSP
		Datos de usuario NLSP
		Dirección respondedora NLSP

NOTA – El parámetro Originador no se aplica a la primitiva petición.

Las primitivas de servicio y los parámetros son equivalentes a los definidos en la Rec. X.213 del CCITT | ISO 8348.

8.2 Servicios asumidos

El servicio asumido por NLSP en su frontera inferior se designará por el prefijo «UN» (*underlying network*, red subyacente). Este es un interfaz nocional (véase 5.1).

El interfaz UN se modela en dos partes:

a) una definición de las primitivas y parámetros del servicio UN (véase más adelante);

b) una tabla de correspondencia desde el servicio UN (véase 5.1), o bien con un servicio de red normalizado, o directamente con la Rec. X.25 del CCITT | ISO 8208.

Los Anexos A y B definen la correspondencia desde la interfaz del servicio nocional con el servicio de red y con las primitivas de la Rec. X.25 o ISO 8208.

Las primitivas UN asumidas para NLSP-CO son las siguientes:

Primitivas		*Parámetros*
Petición	UN-CONEXIÓN	Dirección llamada UN
Indicación	UN-CONEXIÓN	Dirección llamante UN Selección de confirmación de recepción UN Selección de datos acelerados UN Conjunto de parámetros QOS UN Datos de usuario UN Autenticación UN[1)]
Respuesta	UN-CONEXIÓN	Dirección respondedora UN
Confirmación	UN-CONEXIÓN	Selección de confirmación de recepción UN Selección de datos acelerados UN Conjunto de parámetros QOS UN Datos de usuario UN Autenticación UN[1)]
Petición	UN-DATOS	Datos de usuario UN
Indicación	UN-DATOS	Petición de confirmación UN
Petición	UN-ACUSE DE DATOS	
Indicación	UN-ACUSE DE DATOS	
Petición	UN-DATOS ACELERADOS	Datos de usuario UN
Indicación	UN-DATOS ACELERADOS	
Petición	UN-REINICIACIÓN	Motivo UN
Indicación	UN-REINICIACIÓN	Originador UN Motivo UN
Respuesta	UN-REINICIACIÓN	
Confirmación	UN-REINICIACIÓN	

1) El parámetro autenticación UN se utiliza para transportar la PDU de CSC. Esto permite una codificación eficiente cuando el NLSP se utiliza conjuntamente con la Rec. X.25 o la Norma ISO 8208 en aquellos casos en que el parámetro autenticación UN pueda transportarse por el campo facilidad de protección DTE (véase el Anexo B).

Petición	UN-DESCONEXIÓN	Motivo UN
		Datos de usuario UN
		Dirección respondedora UN
Indicación	UN-DESCONEXIÓN	Originador UN
		Motivo UN
		Datos de usuario UN
		Dirección respondedora UN

Los Anexos A y B definen la correspondencia de la autenticación UN con la Rec. X.213 del CCITT | ISO 8348 y con la Rec. X.25 o ISO 8208.

NOTA – Cuando el NLSP se utiliza estrechamente acoplado con la Rec. X.25 | ISO 8208 se pueden emplear otras codificaciones que permiten aprovechar plenamente el protocolo subyacente, mientras que la correspondencia variable con la Rec. X.213 del CCITT | ISO 8348 presupone solamente la utilización de un servicio de red subyacente.

8.3 Atributos de la asociación de seguridad

Los siguientes atributos controlan el funcionamiento de NLSP-CO. Su descripción incluye los nemónicos utilizados para hacer referencia a estos atributos en esta Especificación:

NOTA 1 – Cuando un atributo SA está «constreñido por el ASSR», esta constricción puede definir un solo valor o un conjunto de valores. Cuando el ASSR define una gama de valores, el valor de atributo puede ser establecido por la gestión de sistemas OSI, un intercambio SA-P, o por otros medios que están fuera del ámbito de esta Especificación.

a) *Servicios de seguridad seleccionados para la SA:*

PE Auth: Entero en la gama constreñida por el ASSR para el nivel de autenticación de la entidad par.

CO Conf: Entero en la gama constreñida por el ASSR para el nivel de confidencialidad de la conexión.

CO Int: Entero en la gama constreñida por el ASSR para la integridad de la conexión sin recuperación.

Los valores de estos atributos estarán preestablecidos o se fijarán al establecerse la SA.

b) *Atributos relacionados con el protocolo CO:*

Retain_On_Disconnect: Booleano

Determina si los atributos SA deben retenerse cuando se produce una desconexión.

El valor de este atributo estará preestablecido o se fijará al establecerse la SA.

Protect_Connect_Params: Booleano

Protege los datos de usuario NLSP en NLSP-CONEXIÓN y NLSP-DESCONEXIÓN, así como otros parámetros de servicio en NLSP-CONEXIÓN y NLSP-DESCONEXIÓN si Param_Prot es también TRUE.

El valor de este atributo deberá estar constreñido por el ASSR.

NOTA 2 – Param_Prot no puede ser TRUE si Protect_Connect_Params es FALSE.

No_Header: Booleano

Si es TRUE, deberá utilizarse la forma de protección basada en sin encabezamiento para proteger datos (por ejemplo, mediante los procedimientos definidos en la cláusula 12).

El valor de este atributo deberá ser constreñido por el ASSR.

8.4 Comprobaciones y otras funciones comunes

En muchos puntos de las siguientes descripciones se expresa que se satisface alguna condición. A menos que se especifique otra cosa, cada vez que fracasa una comprobación durante los procedimientos de NLSP-CONEXIÓN o NLSP-DESCONEXIÓN, deberá emitirse una petición UN-DESCONEXIÓN y una indicación NLSP-DESCONEXIÓN,

según proceda. Si esto ocurre después del establecimiento de la conexión, la NLSPE descartará los datos que se están procesando en ese momento y, como una decisión local, invocará o bien:

- uno de los procedimientos UN-REINICIACIÓN iniciada por el NLSP, definida en 8.8.5;
- una petición UN-DESCONEXIÓN y una indicación NLSP-DESCONEXIÓN.

Facultativamente, la entidad puede también registrar en un fichero un informe de auditoría. Es un asunto local la decisión de la información de auditoría que habrá de registrarse.

De manera similar, en los procedimientos descritos a continuación se presenta una secuencia esperada de sucesos. Si no se cumple esta secuencia y aparece un suceso inesperado, deberá tratarse de la misma forma que el fracaso de una comprobación.

Cuando las descripciones siguientes se refieren a la generación o comprobación de PDU de CSC, o PDU de transferencia de datos segura, deberán aplicarse procedimientos apropiados específicos al mecanismo, por ejemplo, los descritos en las cláusulas 9 a 12 de esta Especificación.

8.5 Funciones de NLSP-CONEXIÓN

8.5.1 Procedimientos iniciales

8.5.1.1 Comprobaciones iniciales – Petición NLSP-CONEXIÓN

Al recibir una petición NLSP-CONEXIÓN, la NLSPE comprobará si las exigencias locales del servicio de seguridad permiten comunicaciones no protegidas y verificará el par direcciones llamante/llamada. Si se permiten comunicaciones no protegidas, los parámetros de servicio NLSP y UN se copian directamente a los parámetros de servicio UN y NLSP equivalentes, para todas las primitivas de servicio NLSP y UN subsiguientes, hasta que se reciba una indicación UN-DESCONEXIÓN. La NLSPE no ejecutará más ninguna otra acción durante la conexión.

Si se requiere que las comunicaciones estén protegidas, la NLSPE seguirá los procedimientos para comprobaciones iniciales e identificación de la asociación de seguridad descritos en 6.3.1 y 6.3.2, respectivamente. Esto se efectúa siguiendo los procedimientos definidos en 8.5.2, 8.5.3 u 8.5.4. Los procedimientos apropiados que se apliquen dependen del modo de establecimiento de la conexión seleccionado, definido en 8.5.1.2. La misma cláusula se utiliza entonces para las subsiguientes primitivas de servicio UN-CONEXIÓN y NLSP-CONEXIÓN, para esa conexión UN.

8.5.1.2 Modo de establecimiento de la conexión NLSP

Si en un momento dado existe una SA que reúne las características requeridas, esa SA puede utilizarse para proteger la conexión. De lo contrario, hay que establecer una nueva SA dentro de banda como parte de las funciones NLSP-CONEXIÓN, o fuera de banda dentro de un determinado periodo de temporización. Si no se puede ejecutar ninguna de estas dos acciones, deberá devolverse NLSP-DESCONEXIÓN.

Hay dos modos básicos de establecimiento de una conexión NLSP, con variantes para soportar el establecimiento de la SA dentro de banda; se procede como sigue:

a) **NLSP-CONEXIÓN en UN-CONEXIÓN,** donde los intercambios de protocolo para proporcionar autenticación y el intercambio de parámetros NLSP-CONEXIÓN se transportan en los parámetros UN-CONEXIÓN;

b) **NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P**, donde el establecimiento de la SA dentro de banda se transporta en UN-DATOS en una conexión previa al establecimiento de una segunda conexión UN, transportándose la autenticación y los parámetros NLSP-CONEXIÓN en la UN-CONEXIÓN como se ha dicho anteriormente en a);

c) **NLSP-CONEXIÓN en UN-DATOS**, donde se efectúa un intercambio de autenticación en la UN-CONEXIÓN, seguido del intercambio de los parámetros NLSP-CONEXIÓN en UN-DATOS;

d) **NLSP-CONEXIÓN en UN-DATOS con SA-P**, donde se transporta un intercambio SA-P en UN-DATOS, seguido del intercambio de parámetros NLSP-CONEXIÓN en UN-DATOS.

La selección del modo más apropiado es una decisión local que tomará la NLSPE llamante basada en las exigencias (presentes o previstas) del establecimiento de la conexión NLSP y el entorno de perfiles en los que funciona el NLSP.

La selección de un SA-P se indica por la bandera SA-P en la CSC PDU. La selección de NLSP-CONEXIÓN en UN-CONEXIÓN, o NLSP-CONEXIÓN en UN-DATOS se indica a la NLSPE distante por la bandera UNC-UND (véase el Cuadro 8-2 más adelante).

En los dos últimos modos (NLSP-CONEXIÓN en UN-DATOS con o sin SA-P), los parámetros NLSP-CONEXIÓN se codifican en una PDU de SDT, por lo que estos modos no pueden utilizarse en el modo sin encabezamiento (No_Header).

En los dos primeros modos (NLSP-CONEXIÓN en UN-CONEXIÓN con o sin SA-P) los parámetros NLSP-CONEXIÓN serán protegidos en una PDU de SDT si No_Header es FALSE y Protect_Connect_Params es TRUE. Sin embargo, estos modos no pueden utilizarse si la PDU de SDT resultante es mayor que el espacio disponible en los datos de usuario UN de la primitiva UN-CONEXIÓN.

El Cuadro 8-1 indica las limitaciones impuestas a los diversos modos de establecimiento de la conexión definidos más arriba. Este cuadro puede utilizarse para determinar qué procedimientos de establecimiento de la llamada son apropiados para un perfil dado:

Cuadro 8-1 – Cuadro indicativo de las limitaciones del modo de establecimiento de la conexión NLSP

SA-P	No_Header	Protect_ Connect_ Params	Límites de la longitud de la PDU de SDT (véanse las Notas)	Modo	Procedimientos de establecimiento de la conexión
TRUE	TRUE	TRUE or FALSE		NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P	8.5.3 seguido de 8.5.2.2 a 8.5.2.4
TRUE	FALSE	TRUE	SDT <= Datos de usuario UN	NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P	8.5.3 seguido de 8.5.2.2 a 8.5.2.4
TRUE	FALSE	FALSE		NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P	8.5.3 seguido de 8.5.2.2 a 8.5.2.4
TRUE	FALSE	TRUE or FALSE		NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P	8.5.4
FALSE	TRUE	TRUE or FALSE		NLSP-CONEXIÓN en UN-CONEXIÓN	8.5.2
FALSE	FALSE	TRUE	SDT <= Datos de usuario UN	NLSP-CONEXIÓN en UN-CONEXIÓN	8.5.2
FALSE	FALSE	FALSE		NLSP-CONEXIÓN en UN-CONEXIÓN	8.5.2
FALSE	FALSE	TRUE or FALSE		NLSP-CONEXIÓN en UN-DATOS	8.5.4

NOTAS

1 SDT se refiere a la longitud máxima posible de la PDU de SDT que puede generarse durante el establecimiento de la conexión para el entorno de perfil en que está funcionando el NLSP.

2 Se supone que los límites aplicables a la longitud de los datos de usuario NLSP son los mismos aplicables a los datos de usuario UN.

3 Para una correspondencia con la Rec. X.213 del CCITT | ISO 8348, «max UN Userdata» es la longitud máxima de los datos de usuario que pueden transportarse en las primitivas de servicio N-CONEXIÓN del servicio de red (por ejemplo, 128 para la Rec. X.223 del CCITT | ISO 8878 y la Rec. X.25 | ISO 8208) menos la longitud de la PDU de CSC.

4 Para una correspondencia directa con la Rec. X.25 | ISO 8208 «max UN Userdata» es 128.

8.5.1.3 Comprobaciones iniciales – Indicación UN-CONEXIÓN

Al recibirse una indicación UN-CONEXIÓN sin que esté presente ninguna PDU de CSC en el parámetro autenticación UN, la NLSPE comprobará si se permiten comunicaciones no protegidas basándose en las exigencias locales del servicio de seguridad y en el par de direcciones llamante y llamada. Si se permiten comunicaciones no protegidas, los parámetros de servicio NLSP y UN se copian directamente a los parámetros de servicio UN y NLSP equivalentes para todas las primitivas de servicio NLSP y UN subsiguientes, hasta que se reciba una indicación UN DESCONEXIÓN. La NLSPE no ejecuta ninguna otra acción más durante la conexión.

Si no se permiten comunicaciones no protegidas y no está presente ninguna PDU de CSC, se siguen los procedimientos definidos en 8.4 para el caso de fracaso de la comprobación.

Si está presente una PDU de CSC, se siguen los procedimientos definidos en 8.5.2, 8.5.3 u 8.5.4, lo que depende del valor de las banderas SA-P y UNC-UND en el campo de tipo de PDU indicado en el Cuadro 8-2. La bandera SA-P puesta indica que los intercambios SA-P dentro de banda los efectúa el NLSP. La bandera UNC-UND puesta indica que la NLSP-CONEXIÓN debe transportarse en UN-DATOS y no en UN-CONEXIÓN. Esta misma cláusula se aplica entonces a las primitivas de servicio UN-CONEXIÓN y NLSP-CONEXIÓN subsiguientes para esa conexión UN.

Cuadro 8-2 – Banderas de la PDU de CSC que identifican los procedimientos de establecimiento de la conexión NLSP

Bandera UNC-UND	Bandera SA-P	Procedimientos de establecimiento de la conexión NLSP
Puesta	Puesta	8.5.4 (NLSP-CONEXIÓN en UN-DATOS)
Puesta	Anulada	8.5.4 (NLSP-CONEXIÓN en UN-DATOS)
Anulada	Puesta	8.5.3 (NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P)
Anulada	Anulada	8.5.2 (NLSP-CONEXIÓN en UN-CONEXIÓN)

8.5.2 NLSP-CONEXIÓN en UN-CONEXIÓN

La secuencia esperada de sucesos para el establecimiento de la conexión NLSP con los parámetros de NLSP-CONEXIÓN en UN-CONEXIÓN se ilustra en la Figura 8-1.

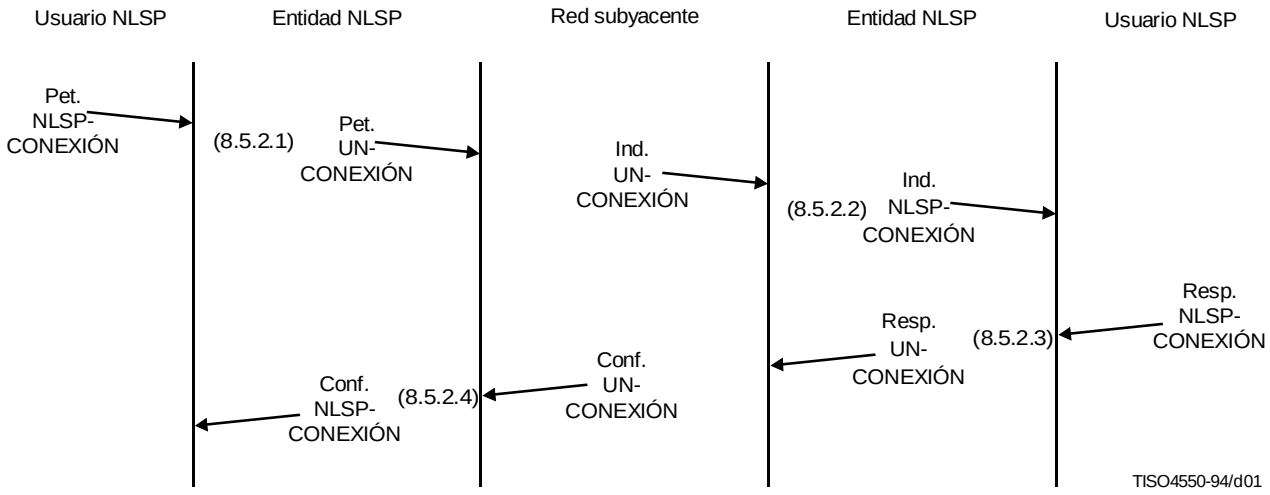


Figura 8-1 – Cronograma de las primitivas de servicio para NLSP-CONEXIÓN en UN-CONNEXIÓN

8.5.2.1 Petición NLSP-CONEXIÓN

En una petición NLSP-CONEXIÓN, si los parámetros NLSP-CONEXIÓN deben transportarse en UN-CONEXIÓN, deberá seguirse el siguiente procedimiento:

a) Si Protect_Connect_Params es TRUE y No_Header es TRUE, los datos de usuarios NLSP deberán encapsularse como se describe en 6.4.1.2. Estos datos se colocan en datos de usuario UN.

b) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es TRUE, se genera una PDU de SDT que contiene la dirección llamada NLSP, la dirección llamante NLSP, y datos de usuario NLSP como se describe en 6.4.1.1, con tipo de datos «pet/ind NLSP-CONEXIÓN». Estos datos se colocan en datos de usuario UN.

c) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es FALSE, se genera una PDU de SDT que contiene datos de usuario NLSP, si hay algunos presentes, como se describe en 6.4.1.1, con tipo de datos «pet/ind NLSP-CONEXIÓN». Estos datos se colocan en datos de usuario UN.

d) Si Protect_Connect_Params es FALSE, se coloca datos de usuario NLSP en datos de usuario UN.

e) Se prepara una PDU de CSC con:

   1) La bandera UNC-UND anulada;

   2) El SA-ID de la SA actual se coloca en el campo SA-ID;

   3) Se anula la bandera SA-P;

   4) El contenido CSC se fija a lo que dé el primer intercambio CSC, como se requiera para los procedimientos específicos al mecanismo como son los descritos en 10.3.

f) Se invocará una petición UN-CONEXIÓN con:

   1) si Param_Prot, la dirección llamada UN fijada a Peer_Adr, y de lo contrario a la dirección llamada NLSP;

   2) si Param_Prot, la dirección llamante fijada a la dirección UN de la NLSPE local, y en caso contrario a la dirección llamante NLSP;

   3) selección de confirmación de recepción UN y selección de datos acelerados fijados a los valores determinados localmente a partir de la selección de confirmación de recepción NLSP y la selección de datos acelerados NLSP;

   4) el parámetro de calidad de servicio (QOS) UN fijado a un valor determinado localmente a partir del parámetro QOS NLSP;

   5) los datos de usuario UN fijados como se indica en los anteriores apartados a) a d);

   6) autenticación UN fijada a la PDU de CSC como se indicó en el anterior apartado e).

g) La NLSPE llamante espera una confirmación UN-CONEXIÓN como se describe en 8.5.2.4, o una indicación UN-DESCONEXIÓN como se describe en 8.10.

8.5.2.2 Indicación UN-CONEXIÓN – UNC-UND anulada y SA-P anulada

Al recibir una indicación UN-CONEXIÓN con una autenticación UN que contiene una PDU de CSC con la bandera UNC-UND anulada y la bandera SA-P anulada:

a) La NLSPE identificará, entre las SA de que dispone, una SA con SA-ID igual al campo SA-ID de la PDU de CSC recibida. Todas las operaciones ulteriores se referirán a esta SA identificada.

b) Se verificará el contenido de la PDU de CSC como se requiera para los procedimientos específicos al mecanismo tales como los descritos en 10.3. El contenido de la PDU de CSC de respuesta retornado se retendrá para uso en el procesamiento de la respuesta NLSP-CONEXIÓN como se describe en 8.5.2.3.

c) Si Protect_Connect_Params es TRUE y No_Header es TRUE, todo dato de usuario UN será desencapsulado como se describe en 6.4.2.2. Estos datos se colocan en datos de usuario NLSP. Otros parámetros de la indicación NLSP-CONEXIÓN se copian a partir de los parámetros de indicación UN-CONEXIÓN.

d) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es TRUE, la PDU de SDT de los datos de usuario UN se verifica como se indica en 6.4.2.1. Se comprobará el campo tipo de datos para determinar que es pet/ind NLSP-CONEXIÓN. La dirección llamada NLSP, la dirección llamante NLSP, y los campos de contenido de datos de usuario NLSP de la PDU de SDT se colocan en los parámetros de la indicación NLSP-CONEXIÓN. La selección de confirmación de recepción UN y la selección de datos acelerados UN, así como el conjunto de parámetros de calidad de servicio (QOS) UN se copiarán a los parámetros equivalentes de la indicación NLSP-CONEXIÓN.

e) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es FALSE, entonces, si está presente, la PDU de SDT en datos de usuario UN se comprueba como se indica en 6.4.2.1. Se comprobará que el campo tipo de datos es pet/ind NLSP-CONEXIÓN. El campo de contenido datos de usuario de la PDU de SDT se colocará en los datos de usuario NLSP. Otros parámetros de la indicación NLSP-CONEXIÓN deberán copiarse a partir de los parámetros de la indicación UN-CONEXIÓN.

f) Si Protect_Connect_Params es FALSE, todos los parámetros de la indicación UN-CONEXIÓN se copian a los parámetros de la indicación NLSP-CONEXIÓN.

g) Se comprobará que la dirección llamada NLSP, fijada como se ha dicho anteriormente, es una dirección NLSP servida por esta entidad NLSP, determinada localmente.

h) Se comprobará que la dirección llamante NLSP, fijada como se ha dicho anteriormente, es una dirección NLSP en el atributo SA Adr_Served.

i) Si se establece alguna etiqueta de seguridad para la conexión, deberá comprobarse que pertenece al conjunto de etiquetas autorizadas en el atributo SA Label_Set (conjunto de etiquetas).

j) La indicación NLSP-CONEXIÓN se pasará al usuario NLSP.

NOTA – La selección de confirmación de recepción NLSP, selección de datos acelerados NLSP, y el conjunto de parámetros de calidad de servicio NLSP pueden modificarse dándoles un valor determinado localmente, antes de pasarlos al usuario NLSP.

k) La NLSPE llamada espera una respuesta NLSP-CONEXIÓN como se indica en 8.5.2.3, o una petición NLSP-DESCONEXIÓN o una indicación UN-DESCONEXIÓN como se indica en 8.10.

8.5.2.3 Respuesta NLSP-CONEXIÓN

Al recibirse una respuesta NLSP-CONEXIÓN:

a) Si Protect_Connect_Params es TRUE, y No_Header es TRUE, todo dato de usuario NLSP deberá encapsularse como se prescribe en 6.4.1.2. Estos datos se colocan en los datos de usuario UN.

b) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es TRUE, se genera una PDU de SDT que contiene la dirección respondedora NLSP, y los datos de usuario NLSP como se describe en 6.4.1.1, con tipo de datos «resp/conf NLSP-CONEXIÓN». Estos datos se colocan en datos de usuario UN.

c) Si Protect_Connect_Params es TRUE, No_Header es FALSE, Param_Prot es FALSE, y datos de usuario NLSP están presente, se genera una PDU de SDT que contiene datos de usuario NLSP, como se describe en 6.4.1.1, con tipo de datos «resp/conf NLSP-CONEXIÓN». Estos datos se colocan en datos de usuario UN.

d) Si Protect_Connect_Param es FALSE, los datos de usuario NLSP se colocan en datos de usuario UN.

e) Si los datos generados como se indica en los anteriores apartados a) a d) no es posible acomodarlos en los datos de usuario UN, se abortarán estos procedimientos como se define en 8.4.

f) Se generará una PDU de CSC con:

1) Las banderas SA-P y UNC-UND anuladas;

2) El SA-ID fijado al SA-ID de la PDU de CSC recibida en la indicación UN-CONEXIÓN.

3) El contenido de CSC fijado al valor retornado por la anterior invocación de los procedimientos específicos al mecanismo descritos en 8.5.2.2 b).

g) Se enviará una respuesta UN-CONEXIÓN con:

1) si Param_Prot es TRUE, la dirección respondedora UN se fija a la dirección UN de la entidad NLSP local, y en caso contrario al parámetro dirección respondedora NLSP;

2) selección de confirmación de recepción UN y selección de datos acelerados UN se fijan a los valores determinados localmente a partir de selección de confirmación de recepción NLSP y selección de datos acelerados NLSP;

3) el parámetro de calidad de servicio (QOS) UN se fija a un valor determinado localmente a partir del parámetro QOS NLSP;

4) los datos de usuario UN se fijan como se indica en los anteriores apartados a) a d);

5) autenticación UN se fija a la PDU de CSC como se indicó en el apartado g) anterior.

h) Si así se requiere de acuerdo con los procedimientos específicos al mecanismo para la autenticación y el intercambio de CSC (por ejemplo, los descritos en 10.3), la NLSPE llamada puede esperar una PDU de SDT en UN-DATOS antes de concluir el establecimiento de la conexión NLSP, y procesa las primitivas NLSP-DATOS procedentes del usuario NLSP. De lo contrario, la NLSPE llamada tendrá entonces concluidos sus procedimientos de establecimiento de la conexión NLSP y podrá pasar a la fase de transferencia de datos.

NOTA – Si el mecanismo de intercambio de CSC requiere que se intercambien más de dos PDU de CSC, se intercambian estas unidades en UN-DATOS antes de concluir el establecimiento de la conexión.

8.5.2.4 Confirmación UN-CONEXIÓN – Banderas UNC-UND y SA-P anuladas

Al recibirse una confirmación de UN-CONEXIÓN con una autenticación UN que contiene una PDU de CSC con las banderas UNC-UND y SA-P anuladas:

a) Se comprueba el contenido de la PDU de CSC utilizando los procedimientos específicos al mecanismo descritos en 10.3.

b) Si Protect_Connect_Params es TRUE, y No_Header es TRUE, todo dato de usuario NLSP deberá desencapsularse como se prescribe en 6.4.2.2. Estos datos se colocan en los datos de usuario NLSP. Otros parámetros de la confirmación NLSP-CONEXIÓN se copian a partir de los parámetros de la confirmación UN-CONEXIÓN.

c) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es TRUE, se comprueba la PDU de SDT como se indica en 6.4.2.1. Se comprobará que el campo tipo de datos es «resp/conf NLSP-CONEXIÓN». La dirección respondedora NLSP y los campos de contenido de datos de usuario NLSP de la PDU de SDT se colocarán en los parámetros de la confirmación NLSP-CONEXIÓN. La selección de confirmación de recepción UN y la selección de datos acelerados UN, y los parámetros de calidad de servicio UN se copiarán a los parámetros de la confirmación NLSP-CONEXIÓN.

d) Si Protect_Connect_Params es TRUE, No_Header es FALSE, Param_Prot es FALSE, entonces, si la PDU de SDT está presente en los datos de usuario UN, se comprueba como se describe en 6.4.2.1. Se comprobará que el campo tipo de datos es «resp/conf NLSP-CONEXIÓN». El campo de contenido datos de usuario de la PDU de SDT se colocará en los datos de usuario NLSP. Otros parámetros de la confirmación NLSP-CONEXIÓN se copiarán a partir de los parámetros de la confirmación UN-CONEXIÓN.

e) Si Protect_Connect_Params es FALSE, todos los parámetros de la confirmación UN-CONEXIÓN se copiarán a los parámetros de la confirmación NLSP-CONEXIÓN.

f) Si la dirección respondedora NLSP está presente se comprobará para determinar que es una dirección NLSP contenida en el atributo SA Adr_Served.

g) La confirmación NLSP-CONEXIÓN se pasará al usuario NLSP.

h) Si así se requiere de acuerdo con los procedimientos específicos al mecanismo para la autenticación e intercambio de CSC (por ejemplo, los descritos en 10.3), se puede crear una PDU de SDT como se describe en 6.4.1.1 con tipo de datos «no relacionado con ninguna primitiva de servicio», y que no comprenda otros campos de contenido que los requeridos de acuerdo con la cláusula 6. Esta unidad se enviará como datos de usuario UN de una primitiva UN-DATOS.

NOTA – Si el mecanismo de intercambio de CSC requiere que se intercambien más de dos PDU de CSC, se intercambian estas unidades en UN-DATOS antes de concluir el establecimiento de la conexión.

Los procedimientos de establecimiento de la conexión NLSP estarán entonces completos.

8.5.3 NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P

La secuencia esperada de sucesos se ilustra en la Figura 8-2.

8.5.3.1 Petición NLSP-CONEXIÓN

En una petición NLSP-CONEXIÓN, si la NLSP-CONEXIÓN debe transportarse en UN-CONEXIÓN y se ha seleccionado el establecimiento de la SA dentro de banda, deberá seguirse el siguiente procedimiento:

a) Se preparará una PDU de CSC con:

   1) la bandera UNC-UND anulada;

   2) la bandera SA-P puesta, y SA-ID, la longitud de contenido y el contenido de CSC de PDU ausentes.

b) Se enviará una petición UN-CONEXIÓN con:

   1) la dirección llamada UN fijada a Peer_Adr;

   2) la dirección llamante UN fijada a la dirección UN de la entidad NLSP local;

   3) la selección de confirmación de recepción UN fijada a un valor determinado localmente;

   4) la selección de datos acelerados UN fijada a un valor determinado localmente;

   5) el parámetro de calidad de servicio UN fijado a un valor determinado localmente;

   6) datos de usuario UN vacíos;

   7) la autenticación UN fijada a la PDU de CSC.

c) La NLSPE llamante deberá esperar una confirmación UN-CONEXIÓN como se describe en 8.5.3.3 o una indicación UN-DESCONEXIÓN como se describe en 8.10.

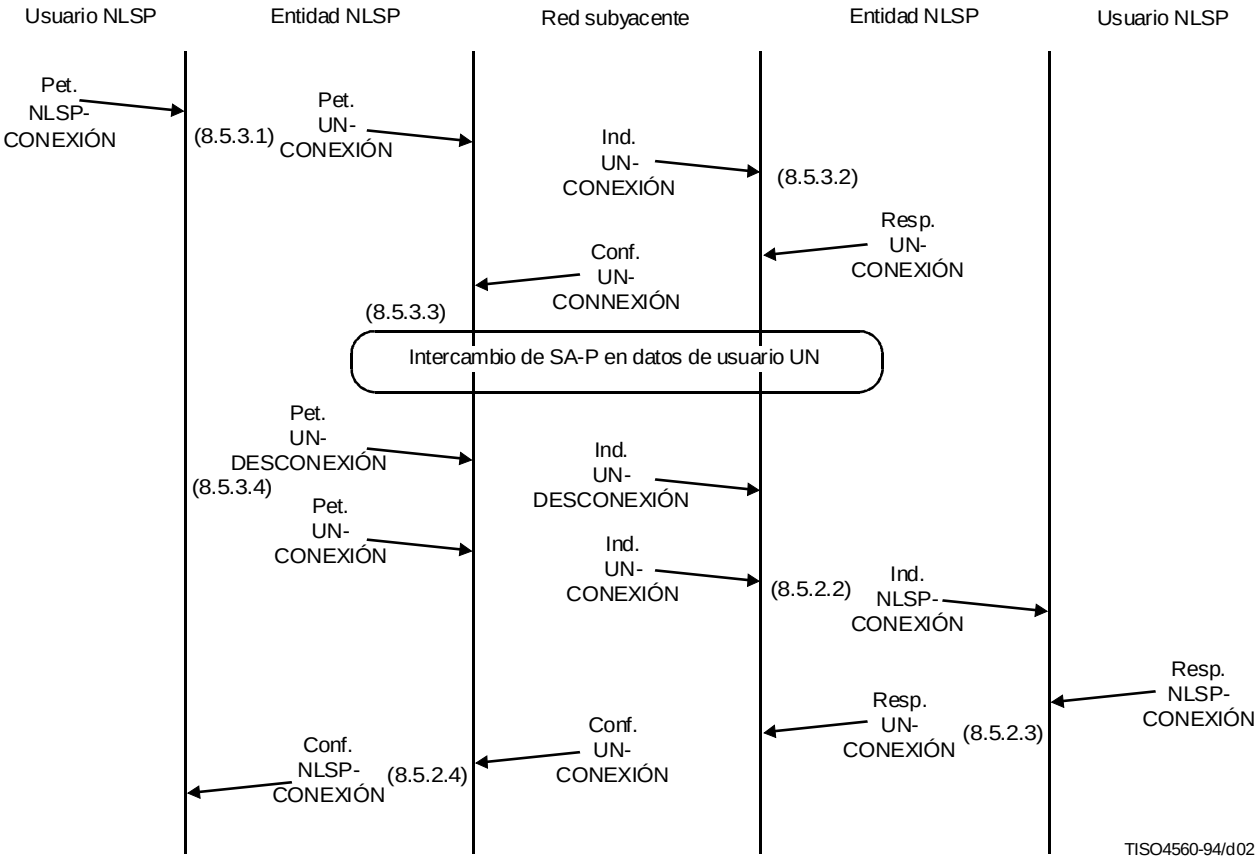


Figura 8-2 – Cronograma de las primitivas de servicio para NLSP-CONEXIÓN en UN-CONEXIÓN con SA-P

8.5.3.2 Indicación UN-CONEXIÓN – La bandera UNC-UND anulada y la SA-P puesta

Al recibirse una indicación UN-CONEXIÓN con una autenticación UN que contiene una PDU de CSC con la bandera UNC-UND anulada y la bandera SA-P puesta:

a) La NLSP preparará una PDU de CSC con:

   1) la bandera UNC-UND anulada;

   2) la bandera SA-P puesta;

   3) el contenido de CSC vacío.

b) La NLSPE responderá enviando una respuesta UN-CONEXIÓN con:

   1) la dirección respondedora UN fijada a la dirección UN local;

   2) la selección de confirmación de recepción UN y la selección de datos acelerados UN fijadas a valores determinados localmente a partir de los parámetros de la indicación UN-CONEXIÓN;

   3) el parámetro de calidad de servicio UN fijado a un valor determinado localmente a partir del parámetro de calidad de servicio UN de la indicación UN-CONEXIÓN;

   4) los usuarios de datos UN vacíos;

   5) la autenticación UN fijada a la PDU de CSC.

La NLSPE llamada esperará un intercambio SA-P o una indicación UN-DESCONEXIÓN como se describe en 8.10. Todo error en el SA-P se tratará como un error según se indica en 8.4.

8.5.3.3 Confirmación UN-CONEXIÓN – La bandera UNC-UND anulada y la SA-P puesta

Al recibirse una confirmación UN-CONEXIÓN con una autenticación UN que contiene una unidad PDU de CSC con la bandera UNC-UND anulada y la bandera SA-P puesta:

a) se aplicará el protocolo SA-P dentro de banda;

b) la NLSPE llamante espera la conclusión del protocolo SA-P como se describe en 8.5.3.4 o una UN-DESCONEXIÓN como se describe en 8.10.

8.5.3.4 Conclusión del SA-P

Al concluirse el protocolo SA-P como se describe en 8.5.3.3, la NLSPE llamante seguirá los siguientes procedimientos:

a) La NLSPE llamante enviará una petición UN-DESCONEXIÓN con el motivo fijado a «condición normal de desconexión», seguida de una petición UN-CONEXIÓN con los parámetros de servicio fijados como sigue.

b) Si Protect_Connect_Params es TRUE y No_Header es TRUE, los datos de usuario NLSP se encapsularán como se describe en 6.4.1.2. Estos datos se colocan en datos de usuario UN.

c) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es TRUE, se genera una PDU de SDT que contiene la dirección llamada NLSP, la dirección llamante NLSP, y los datos de usuario NLSP como se describe en 6.4.1.1 con el tipo de datos «pet/ind NLSP-CONEXIÓN». Esta unidad se coloca en los datos de usuario UN.

d) Si Protect_Connect_Params es TRUE, No_Header es FALSE y Param_Prot es FALSE, se genera una PDU de SDT que contiene datos de usuario, si hay alguno presente, como se describe en 6.4.1.1, con el tipo de datos «pet/ind NLSP-CONEXIÓN». Esta unidad se coloca en los datos de usuario UN.

e) Si Protect_Connect_Params es FALSE, los datos de usuario NLSP se colocan en datos de usuario UN.

f) Se prepara una PDU de CSC con:

   1) la bandera UNC-UND anulada;

   2) el SA-ID de la SA actual colocada en el campo SA-ID;

   3) la bandera SA-P anulada;

   4) el contenido de CSC fijado al primer intercambio de CSC según lo requieran los procedimientos específicos al mecanismo como los descritos en 10.3.

g) Se invocará una petición UN-CONEXIÓN con:

1) si Param_Prot es TRUE, la dirección llamada UN fijada a Peer_Adr, y en caso contrario a la dirección llamada NLSP;

2) si Param_Prot es TRUE, la dirección llamante UN fijada a la dirección UN de entidad NLSP local, y en caso contrario a la dirección llamante NLSP;

3) la selección de confirmación de recepción UN y la selección de datos acelerados UN puestas a los valores determinados localmente a partir de la selección de confirmación de recepción NLSP y de la selección de datos acelerados NLSP;

4) un parámetro de calidad de servicio UN fijado a un valor determinado localmente a partir del parámetro de calidad de servicio NLSP;

5) datos de usuario UN fijados como se describe en los anteriores apartados a) a d);

6) la autenticación UN fijada a la PDU de CSC como se describe en el anterior apartado e).

h) La NLSPE llamante espera una confirmación UN-CONEXIÓN como la descrita en 8.5.2.4 o una indicación UN-DESCONEXIÓN como la descrita en 8.10.

Al concluir el SA-P, la NLSP espera una UN-DESCONEXIÓN con el motivo fijado a «condición normal de desconexión». Al recibirse esta indicación UN-DESCONEXIÓN, la NLSPE llamada espera una indicación UN-CONEXIÓN como se describe en 8.5.2.2.

Las NLSPE llamante y llamada procesarán entonces las subsiguientes primitivas de NLSP-CONEXIÓN y UN-CONEXIÓN como se describe en 8.5.2.2 a 8.5.2.4

8.5.4 NLSP-CONEXIÓN en UN-DATOS

La secuencia esperada de sucesos se ilustra en la Figura 8-3.

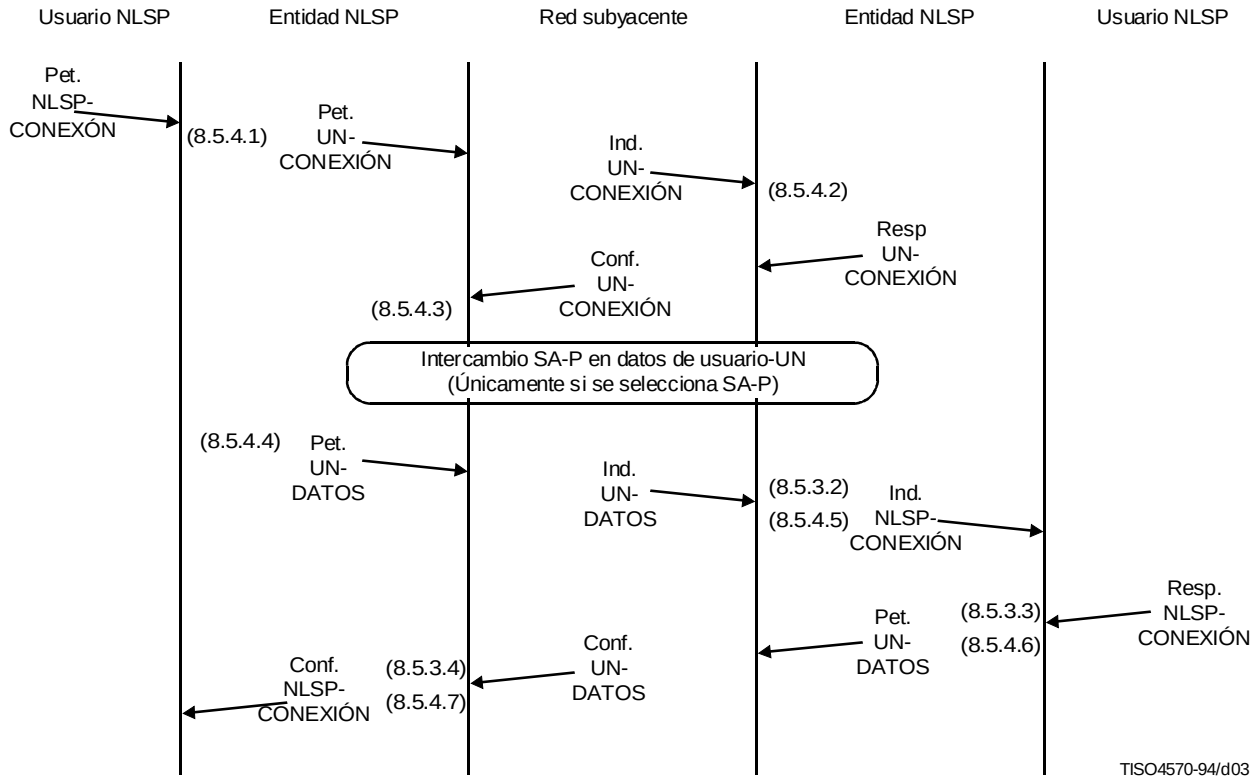


Figura 8-3 – Cronograma de las primitivas de servicio para NLSP-CONEXIÓN en UN-DATOS

8.5.4.1 Petición NLSP-CONEXIÓN

Al recibirse una petición NLSP-CONEXIÓN, si los parámetros NLSP-CONEXIÓN van a transportarse en UN-DATOS deberán seguirse los siguientes procedimientos:

a) Se preparará una PDU de CSC con:
   1) la bandera UNC-UND fijada;
   2) si se selecciona SA-P dentro de banda, la bandera SA-P fijada, y SA-ID, longitud de contenido y los campos de contenido de la PDU de CSC ausentes;
   3) si no se selecciona SA-P dentro de banda, la bandera SA-P anulada, el SA-ID fijado a Your_SA-ID y el contenido de la PDU de CSC fijado al primer intercambio CSC según lo requieran los procedimientos específicos al mecanismo, como los descritos en 10.3.

b) Se enviará una petición UN-CONEXIÓN con:
   1) la dirección llamada UN fijada a Peer_Adr;
   2) la dirección llamante UN fijada a la dirección UN de la entidad NLSP local;
   3) la selección de confirmación de recepción UN fijada a un valor determinado localmente a partir de la confirmación de recepción NLSP;
   4) la selección de datos acelerados UN fijada a un valor determinado localmente a partir de la selección de datos acelerados NLSP;
   5) el parámetro de calidad de servicio UN fijado a un valor determinado localmente a partir de la calidad de servicio NLSP;
   6) datos de usuario UN vacíos;
   7) la autenticación UN fijada a la PDU de CSC;

c) La NLSPE llamante esperará una confirmación UN-CONEXIÓN como se describe en 8.5.4.3 o una indicación UN-DESCONEXIÓN como se describe en 8.10.

8.5.4.2 Indicación UN-CONEXIÓN – UNC-UND fijada

Al recibirse una indicación UN-CONEXIÓN con una autenticación UN que contiene una PDU de CSC con la bandera UNC-UND fijada:

a) si la bandera SA-P está anulada:
   1) la NLSPE identificará, entre las SA de que dispone, una SA con My_SA-ID igual al campo SA-ID de la PDU de CSC recibida. Todas las demás operaciones se referirán a esta SA identificada;
   2) el contenido de la PDU de CSC se verificará según lo requieran los procedimientos específicos al mecanismo tales como los descritos en 10.3.

Los procedimientos que se indican en esta subcláusula se aplicarán sin tener en cuenta que la bandera SA-P esté fijada o anulada.

b) La NLSPE preparará entonces una PDU de CSC con:
   1) la bandera UNC-UND fijada;
   2) si se selecciona SA-P dentro de banda, deberá estar ausente el campo SA-ID, de lo contrario deberá fijarse al SA-ID recibido en la PDU de CSC;
   3) si se selecciona SA-P dentro de banda, se fija la bandera SA-P, y en caso contrario se anula;
   4) si se selecciona SA-P dentro de banda, los campos de contenido de PDU de CSC y de longitud de contenido no están presentes; de lo contrario, el contenido de la PDU de CSC se fija al intercambio de CSC según lo retornado por los procedimientos específicos al mecanismo como los definidos en 10.3.

      NOTA – Los procedimientos actuales no están previstos para trabajar con mecanismos de intercambio de CSC que requieran más de un intercambio bidireccional de PDUs de CSC, seguidos facultativamente de una PDU de SDT.

c) La NLSPE responderá entonces con una respuesta UN-CONEXIÓN con:
   1) la dirección respondedora UN fijada a la dirección UN-local;
   2) la selección de confirmación de recepción UN y la selección de datos acelerados UN fijadas a valores determinados localmente a partir de los parámetros de la indicación UN-CONEXIÓN;
   3) el parámetro de calidad de servicio UN fijado a un valor determinado localmente a partir del parámetro de calidad de servicio UN en la indicación UN-CONEXIÓN;

4) datos de usuario UN vacíos;

5) la autenticación UN fijada a la PDU de CSC.

d) La NLSPE llamada deberá esperar un intercambio de SA-P o una indicación UN-DATOS que contenga una PDU de SDT como se describe en 8.5.4.5 o una indicación UN-DESCONEXIÓN como se describe en 8.10 o una UN-REINICIACIÓN como se describe en 8.9.

8.5.4.3 Confirmación UN-CONEXIÓN – Bandera UNC-UND fijada

Al recibirse una confirmación UN-CONEXIÓN con una autenticación UN que contiene una PDU de CSC de respuesta con la bandera UNC-UND fijada:

a) Se comprueba que la bandera SA-P en la PDU de CSC concuerda con la selección SA-P dentro de banda;

b) Si no se selecciona SA-P:

1) se comprueba el contenido de la PDU de CSC utilizando procedimientos específicos al mecanismo como los descritos en 10.3;

2) se continúan los procedimientos como se describe en 8.5.4.4 c).

NOTA – Si no se selecciona SA-P y el mecanismo de intercambio de CSC requiere el intercambio de más de dos PDU de CSC, se intercambian estas unidades en UN-DATOS antes de continuar con los procedimientos de establecimiento de la conexión.

c) Se selecciona SA-P dentro de banda:

1) se efectúa el intercambio SA-P;

2) la NLSPE espera la conclusión del protocolo SA-P como se describe en 8.5.4.4 o una indicación UN-DESCONEXIÓN como se describe en 8.10, o una indicación UN-REINICIACIÓN como se describe en 8.9. Todo error en el SA-P deberá tratarse como un error, como se describe en 8.4.

8.5.4.4 Conclusión del SA-P/ausencia de SA-P

Al concluirse el SA-P:

a) si el SA-P tiene éxito, la SA establecida se utiliza subsiguientemente para la conclusión del establecimiento de la conexión NLSP y las comunicaciones seguras como se describe en las subcláusulas siguientes;

b) si el SA-P no tiene éxito, la NLSPE llamante, o la llamada, invocará una UN-DESCONEXIÓN y deberán abortarse los procedimientos de establecimiento de la conexión NLSP.

Al concluirse el SA-P o después de una confirmación UN-CONEXIÓN sin SA-P como la descrita en 8.5.4.3 b):

c) los siguientes parámetros de NLSP-CONEXIÓN, pasados al NLSP llamante en el caso descrito en 8.5.4.1, deberán colocarse en una PDU de SDT como se describe en 6.4.1.1 con tipo de datos «pet/ind NLSP-CONEXIÓN»:

- dirección llamante NLSP;
- dirección llamada NLSP;
- datos de usuario NLSP.

NOTA 1 – Los parámetros de dirección NLSP se transportan en forma protegida incluso si Param_Prot es FALSE.

d) la PDU de SDT deberá pasarse al proveedor de servicio UN en datos de usuario UN de una petición UN-DATOS.

NOTA 2 – Con esto se puede proporcionar la tercera parte del intercambio de autenticación de la entidad par.

e) la NLSPE llamante espera una indicación UN-DATOS que contenga una PDU de SDT como se describe en 8.5.4.7, o una indicación UN-DESCONEXIÓN como se describe en 8.10, o una indicación UN-REINICIACIÓN como se describe en 8.9.

Al concluirse el SA-P, la NLSPE llamada esperará una indicación UN-DATOS que contenga una PDU de SDT como se describe en 8.5.4.5, o una indicación UN-DESCONEXIÓN como se describe en 8.10, o una indicación UN-REINICIACIÓN como se describe en 8.9.

8.5.4.5 UN-DATOS que contienen una PDU de SDT, recibida en la NLSPE llamada

Al recibirse una indicación UN-DATOS que contiene una PDU de transferencia de datos segura en la NLSPE llamada, se verificará como se describe en 6.4.2.2.

NOTA – De esta forma se puede proporcionar la tercera parte del intercambio de autenticación de la entidad par.

Se comprobará que el campo tipo de datos en la PDU de SDT es una pet/ind NLSP-CONEXIÓN.

Se comprobará que la dirección llamada NLSP es una dirección NLSP servida por esta entidad NLSP, como se determinó localmente.

Se comprobará que la dirección llamante NLSP es una dirección NLSP contenida en un atributo SA Adr_Served.

Si se establece alguna etiqueta de seguridad para la conexión, se comprobará esta etiqueta cotejándola con el conjunto de etiquetas autorizadas en el atributo SA Label_Set.

La indicación NLSP-CONEXIÓN se pasará al usuario NLSP llamado con los parámetros fijados como sigue:

a) la dirección llamante NLSP, la dirección llamada NLSP, los datos de usuario NLSP se fijan como lo están en los campos de contenido de la PDU de SDT recibida;

b) la selección de confirmación de recepción NLSP y la selección de datos acelerados NLSP se fijan a los valores de los parámetros UN equivalentes en la respuesta UN-CONEXIÓN enviada de acuerdo con los procedimientos descritos en 8.5.4.2;

c) la calidad de servicio NLSP «disponible» se fija a la calidad de servicio UN «seleccionada» por la NLSPE llamada en la respuesta UN-CONEXIÓN enviada de acuerdo con los procedimientos descritos en 8.5.4.2, con «target» (valor deseado) y «lowest acceptable» (valor más bajo aceptable) sin especificar.

La NLSPE esperará una respuesta NLSP-CONEXIÓN como se describe en 8.5.4.6 o una petición NLSP-DESCONEXIÓN como se describe en 8.10, o una indicación UN-DESCONEXIÓN como se describe en 8.10, o una indicación UN-REINICIACIÓN como se describe en 8.9.

8.5.4.6 Respuesta NLSP-CONEXIÓN

Al recibirse una respuesta NLSP-CONEXIÓN, la dirección respondedora NLSP y los parámetros datos de usuario NLSP deberán colocarse en la PDU de SDT como se describe en 6.4.1.1 con el tipo de datos «res/conf NLSP-CONEXIÓN».

Esta PDU de SDT deberá pasarse al proveedor de servicio UN en datos de usuario UN de la petición UN-DATOS.

Con esto, la NLSPE llamada habrá concluido sus procedimientos de establecimiento de la conexión NLSP.

8.5.4.7 UN-DATOS que contienen una PDU de SDT, recibida en la NLSPE llamante

Al recibirse una indicación UN-DATOS que contiene una PDU de SDT se comprobará esta unidad en la forma prescrita en 6.4.2.1. Se comprobará que el campo tipo de datos es una resp/conf NLSP-CONEXIÓN.

Se comprobará que la dirección respondedora NLSP es una dirección NLSP contenida en el atributo SA Adr_Served.

Se envía una confirmación NLSP-CONEXIÓN al usuario NLSP con los parámetros fijados como sigue:

a) la dirección respondedora NLSP, los usuarios de datos NLSP, si están presentes, se fijan como en los campos de contenido de la PDU de SDT recibida;

b) la selección de confirmación de recepción NLSP y la selección de datos acelerados NLSP se fijan a los valores de los parámetros UN equivalentes en la confirmación UN-CONEXIÓN enviada de acuerdo con los procedimientos descritos en 8.5.4.3;

c) la calidad de servicio NLSP se fija a la calidad de servicio UN recibida en la confirmación UN-CONEXIÓN recibida de acuerdo con los procedimientos descritos en 8.5.3.

Con esto, la NLSPE llamante habrá concluido sus procedimientos de establecimiento de la conexión NLSP.

8.6 Funciones de NLSP-DATOS

8.6.1 Petición NLSP-DATOS

Al recibirse una petición NLSP-DATOS, si No_Header es TRUE, los usuarios de datos NLSP deberán encapsularse como se describe en 6.4.1.2. Estos datos se colocan en datos de usuario UN de una petición UN-DATOS y el parámetro petición de confirmación NLSP se copia al parámetro UN-DATOS equivalente. La primitiva UN-DATOS se pasará entonces al proveedor de servicio UN.

Al recibirse una petición NLSP-DATOS, si No_Header es FALSE, se procede de la manera siguiente.

a) Como un asunto local, la NLSPE segmentará los datos de usuario NLSP (si lo exige la SA).

b) Para cada segmento se generará una PDU de SDT como se describe en 6.4.1.1 con tipo de datos «pet/ind NLSP-DATOS» que contiene:

   1) el segmento datos de usuario NLSP;

   2) la bandera último/no último puesta a 0 para el último segmento, y a 1 para todos los segmentos precedentes;

   3) El campo de contenido petición de confirmación NLSP si:

      i) la petición de confirmación NLSP está presente e indica «solicitada la confirmación de recepción» en la petición NLSP-DATOS; y

      ii) éste es el último segmento; y

      iii) param_Prot es TRUE.

c) La PDU de SDT para cada segmento se colocará en el parámetro datos de usuario UN de la petición UN-DATOS.

d) El parámetro petición de confirmación UN de la UN-DATOS estará presente e indicará «solicitada la confirmación de recepción», si:

   1) la petición de confirmación NLSP se indica en la petición NLSP-DATOS; y

   2) éste es el último segmento; y

   3) Param_Prot es FALSE,

   de lo contrario, el parámetro petición de confirmación UN deberá indicar «no solicitada la confirmación de recepción».

e) La primitiva de petición UN-DATOS para cada segmento se pasará al proveedor de servicio UN.

8.6.2 Datos protegidos en una indicación UN-DATOS tras el establecimiento de la conexión

Al recibirse una indicación UN-DATOS, si No_Header es TRUE, los datos de usuario UN se desencapsularán como se describe en 6.4.2.2. Estos datos se colocan en los datos de usuario NLSP de una indicación NLSP-DATOS y el parámetro petición de confirmación UN se copia al parámetro equivalente de la indicación NLSP-DATOS. La indicación NLSP-DATOS se pasará entonces al usuario de servicio NLSP.

Al recibirse una indicación UN-DATOS, si No_Header es FALSE, se procede de la manera siguiente:

a) Se comprobará la PDU de SDT en los datos de usuario UN como se describe en 6.4.2.1.

b) Si el campo tipo de datos es «no relacionado con ninguna primitiva de servicio NLSP», la PDU de SDT se procesa como se indica en 8.11, y no como se describe más abajo.

c) Si el campo tipo de datos es pet/ind NLSP-ACUSE-DE-DATOS, la PDU de SDT se procesará como se indica en 8.9.2, y no como se describe más abajo.

d) Si el campo tipo de datos es pet/ind NLSP-DESCONEXIÓN, la PDU de SDT se procesará como se indica en 8.10.2, y no como se describe más abajo.

e) De no ser así, se comprobará que el campo tipo de datos concuerda con el NLSP-DATOS y se procesará como sigue.

f) Si la bandera último/no último en la PDU de SDT está fijada a 1 (no último), el campo contenido de datos de usuario NLSP en la PDU de SDT se agrega al final de cualesquiera datos de usuario NLSP precedentes que formen parte de la misma petición/indicación NLSP-DATOS y serán retenidos por la NLSPE para ulterior utilización.

g) Si la bandera último/no último en la PDU de SDT está fijada a 0 (último) se procede como sigue:

1) El campo contenido de datos de usuario NLSP en la PDU de SDT se añade al final de cualesquiera datos de usuario NLSP precedentes que formen parte de la misma petición/indicación NLSP-DATOS y se colocará en el parámetro datos de usuario NLSP de una indicación NLSP-DATOS.

2) Si Param_Prot es TRUE, la petición de confirmación NLSP en la indicación NLSP-DATOS señalará «solicitada la confirmación de la recepción» si el campo de contenido petición de confirmación está presente en la PDU de SDT.

3) Si Param_Prot es FALSE, la petición de confirmación UN en la indicación UN-DATOS se copia al parámetro equivalente en la indicación NLSP-DATOS.

4) La indicación NLSP-DATOS se pasa al usuario NLSP.

8.7 Funciones de NLSP-DATOS-ACELERADOS

8.7.1 Petición NLSP-DATOS-ACELERADOS

Al recibirse una petición NLSP-DATOS-ACELERADOS, si No_Header es TRUE los datos de usuario NLSP se encapsularán como se describe en 6.4.1.2. Estos datos se colocan en datos de usuario UN de una petición UN-DATOS-ACELERADOS. La petición UN-DATOS-ACELERADOS se pasará entonces al proveedor de servicio UN.

Al recibirse una petición NLSP-DATOS-ACELERADOS, si No_Header es FALSE se procede como sigue:

a) Como un asunto local, la NLSPE segmentará los datos de usuario NLSP (si así lo requiere la SA):

b) Para cada segmento se generará una PDU de SDT como se describe en 6.4.1.1 con tipo de datos «pet/ind NLSP-DATOS-ACELERADOS» que contiene:

1) el segmento de datos de usuario NLSP;

2) la bandera último/no último puesta a 0 para el último segmento y a 1 para todos los segmentos precedentes;

3) la PDU de SDT para cada segmento se colocará en el parámetro datos de usuario UN de una primitiva de UN-DATOS-ACELERADOS.

c) La primitiva de petición UN-DATOS-ACELERADOS para cada segmento se pasará al proveedor de servicio UN.

NOTA – Cuando se utiliza la PDU de SDT, por efecto de la función de encapsulación puede aumentar el tamaño de los datos. En consecuencia de la restricción impuesta a la longitud del campo de datos de usuario, es posible que haya que segmentar aún más los datos acelerados protegidos cuando atraviesen la red subyacente.

8.7.2 Indicación UN-DATOS-ACELERADOS

Al recibirse una indicación UN-DATOS-ACELERADOS, si No_Header es TRUE los datos de usuario UN se desencapsularán como se describe en 6.4.2.2. Estos datos se colocan en los datos de usuario NLSP de una indicación NLSP-DATOS-ACELERADOS. La indicación NLSP-DATOS-ACELERADOS se pasará entonces al proveedor de servicio NLSP.

Al recibirse una indicación UN-DATOS-ACELERADOS, si No_Header es FALSE:

NOTA – Cuando se utiliza la PDU de SDT, por efecto de la función de encapsulación puede aumentar el tamaño de los datos. Como consecuencia de la restricción impuesta a la longitud del campo de datos de usuario, es posible que haya que reensamblar la PDU de SDT de varias peticiones NLSP-DATOS-ACELERADOS antes de procesarlas completamente.

a) La PDU de SDT en los datos de usuario UN se comprobarán como se describe en 6.4.2.1. Se comprobará que el tipo de datos en la PDU de SDT es pet/ind NLSP-DATOS-ACELERADOS.

b) Si la bandera último/no último en la PDU de SDT está puesta a 1 (no último), el campo de contenido de datos de usuario NLSP en la PDU de SDT se agrega al final de cualesquiera datos de usuario NLSP anteriores que formen parte de la misma petición/indicación NLSP-DATOS-ACELERADOS y serán retenidos por la NLSPE para ulterior uso.

c) Si la bandera último/no último en la PDU de SDT está fijada a 0 (último) se procede como sigue:

1) el campo de contenido de datos de usuario de NLSP en la PDU de SDT se agrega al final de cualesquiera datos de usuario NLSP precedentes que formen parte de la misma petición/indicación NLSP-DATOS-ACELERADOS y se colocarán en el parámetro datos de usuario NLSP de una indicación NLSP-DATOS-ACELERADOS;

2) la primitiva de servicio indicación NLSP-DATOS-ACELERADOS se pasará al usuario NLSP.

8.8 Funciones de REINICIACIÓN

Cualquiera de los sucesos relacionados con el NLSP o con la UN-REINICIACIÓN, que se indican a continuación, tienen precedencia sobre cualquier intercambio de PDU de CSC, intercambio de SA-P, o intercambio de prueba que estén en curso.

8.8.1 Petición NLSP-REINICIACIÓN

Al recibirse una petición NLSP-REINICIACIÓN se enviará una petición UN-REINICIACIÓN con los mismos valores de parámetros.

Se descartará todo dato de usuario NLSP segmentado, retenido de acuerdo con los procedimientos descritos en 8.6 u 8.7.

La NLSPE esperará una confirmación UN-REINICIACIÓN como se describe en 8.8.2, o una petición NLSP-DESCONEXIÓN, o una indicación UN-DESCONEXIÓN como se describe en 8.10. La NLSPE descartará todas las primitivas de UN-DATOS y UN-ACUSE-DE-DATOS hasta que reciba una confirmación UN-REINICIACIÓN o una primitiva de DESCONEXIÓN.

8.8.2 Confirmación UN-REINICIACIÓN tras una petición NLSP-REINICIACIÓN

Al recibirse una confirmación UN-REINICIACIÓN, tras una petición NLSP-REINICIACIÓN como se ha dicho en 8.8.1, se enviará una confirmación NLSP-REINICIACIÓN con los mismos valores de parámetros.

NOTA – Puede ser necesario reinicializar algunos mecanismos de seguridad, ya que pueden haberse perdido datos. En particular, el mecanismo de secuenciación para la integridad deberá poder evitar ataques por reproducción fraudulenta, incluso después de haberse perdido datos. Esto puede conseguirse mediante el intercambio de PDU de CSC descrito a continuación.

Si el atributo SA iniciador es TRUE, la NLSPE iniciará un intercambio de CSC como se describe en 8.12.1. De lo contrario, la NLSPE esperará una primitiva UN-DATOS que contenga una PDU de CSC como se describe en 8.12.2.

8.8.3 Indicación UN-REINICIACIÓN

Al recibirse una indicación UN-REINICIACIÓN durante los procedimientos de establecimiento de la conexión NLSP descritos en 8.5, se enviará una petición UN-DESCONEXIÓN y una indicación NLSP-DESCONEXIÓN de acuerdo con el servicio de red OSI y se abortarán los procedimientos de establecimiento de la conexión.

Cuando se recibe una indicación NLSP-REINICIACIÓN se efectúa lo siguiente para el establecimiento de la conexión NLSP:

a) Se envía una indicación NLSP-REINICIACIÓN con los mismos valores de parámetros.

b) Se descartan cualesquiera datos de usuario NLSP segmentados que hayan sido retenidos de acuerdo con los procedimientos descritos en 8.6 y 8.7.

c) La NLSPE esperará una respuesta NLSP-REINICIACIÓN como se indica en 8.8.4, o una petición NLSP-DESCONEXIÓN o una indicación UN-DESCONEXIÓN como se expresa en 8.10. La NLSPE descartará todas las primitivas de UN-DATOS y de UN-ACUSE-DE-DATOS hasta que se reciba una respuesta NLSP-REINICIACIÓN o una primitiva de DESCONEXIÓN.

8.8.4 Respuesta NLSP-REINICIACIÓN tras una indicación UN-REINICIACIÓN

Al recibirse una respuesta NLSP-REINICIACIÓN tras una indicación UN-REINICIACIÓN como se describe en 8.8.3, deberá enviarse una respuesta UN-REINICIACIÓN.

NOTA – Puede ser necesario reinicializar algunos mecanismos de seguridad, ya que pueden haberse perdido datos. En particular, el mecanismo de secuenciación para la integridad deberá poder evitar ataques por reproducción fraudulenta, incluso después de haberse perdido datos. Esto puede conseguirse mediante el intercambio de PDU de CSC descrito a continuación.

Si el atributo SA iniciador es TRUE, la NLSPE iniciará un intercambio de CSC como se describe en 8.12.1. De lo contrario, la NLSPE esperará una primitiva de UN-DATOS que contengan una PDU de CSC como se describe en 8.12.2.

8.8.5 Reiniciación iniciada por el NLSP

Cuando se produce una reiniciación iniciada como consecuencia de un suceso relacionado con el protocolo NLSP (por ejemplo, el fracaso de una comprobación, como se describe en 8.4):

a) Se descartan cualesquiera datos segmentados que hayan sido retenidos de acuerdo con los procedimientos descritos en 8.6 y 8.7.

b) Se transmitirá una indicación NLSP-REINICIACIÓN al usuario de servicio NLSP con los parámetros originador NLSP y motivo NLSP fijados a un valor determinado localmente.

c) Se transmitirá una petición UN-REINICIACIÓN al proveedor de servicio UN con el motivo UN fijado a un valor determinado localmente.

d) La NLSPE esperará una respuesta NLSP-REINICIACIÓN como se describe en 8.8.6 y una confirmación UN-REINICIACIÓN como se describe en 8.8.7. Puede recibirse también una petición NLSP-DESCONEXIÓN o una indicación UN-DESCONEXIÓN como se consigna en 8.10.

e) La NLSPE descartará todas las primitivas de UN-DATOS y UN-ACUSE-DE-DATOS, hasta que reciba una confirmación UN-REINICIACIÓN o cualquier primitiva de DESCONEXIÓN.

f) La NLSPE descartará todas las primitivas de NLSP-DATOS y de NLSP-ACUSE-DE-DATOS hasta que se reciba una respuesta NLSP-REINICIACIÓN o cualquier primitiva de DESCONEXIÓN.

8.8.6 Respuesta NLSP-REINICIACIÓN tras una petición iniciada por el NLSP

Cuando se recibe una primitiva de NLSP-REINICIACIÓN tras una reiniciación iniciada por NLSP no se necesita ninguna acción ulterior.

8.8.7 Confirmación UN-REINICIACIÓN tras una petición iniciada por el NLSP

NOTA – Puede ser necesario reinicializar algunos mecanismos de seguridad, ya que pueden haberse perdido datos. En particular, el mecanismo de secuenciación para la integridad deberá poder evitar ataques por reproducción fraudulenta, incluso después de haberse perdido datos. Esto puede conseguirse mediante el intercambio de PDU de CSC descrito a continuación.

Al recibirse una confirmación UN-REINICIACIÓN después de una reiniciación iniciada por NLSP, si el atributo SA iniciador es TRUE, la NLSPE iniciará un intercambio de CSC como se describe en 8.12.1. De lo contrario, la NLSPE esperará una primitiva de UN-DATOS que contenga una PDU de CSC como se expresa en 8.12.2.

8.9 NLSP-ACUSE-DE-DATOS

8.9.1 Petición NLSP-ACUSE-DE-DATOS

Al recibirse una petición NLSP-ACUSE-DE-DATOS, si No_Header es TRUE o Param_Prot es FALSE, se transmite una petición UN-ACUSE-DE-DATOS al proveedor de servicio UN.

Al recibirse una primitiva de NLSP-ACUSE-DE-DATOS, si No_Header es FALSE y Param_Prot es TRUE:

a) se generará una PDU de SDT como se describe en 6.4.1.1, con el tipo de datos «pet/ind NLSP-ACUSE-DE-DATOS» que no comprenda campos de contenido adicionales;

b) la PDU de SDT se pasará al proveedor de servicio UN como una primitiva de petición UN-DATOS.

8.9.2 NLSP-ACUSE-DE-DATOS protegida en una indicación UN-DATOS

Si se recibe una PDU de SDT en una indicación UN-DATOS con el tipo de datos fijado a NLSP-ACUSE-DE-DATOS, como se describe en 8.6.2 apartado c):

a) se comprobará que la PDU SDT no comprende ningún campo de contenido relacionado con parámetros de servicio NLSP;

b) se transmite una indicación NLSP-ACUSE-DE-DATOS al usuario NLSP.

8.9.3 Indicación UN-ACUSE-DE-DATOS

Al recibirse una primitiva de UN-ACUSE-DE-DATOS:

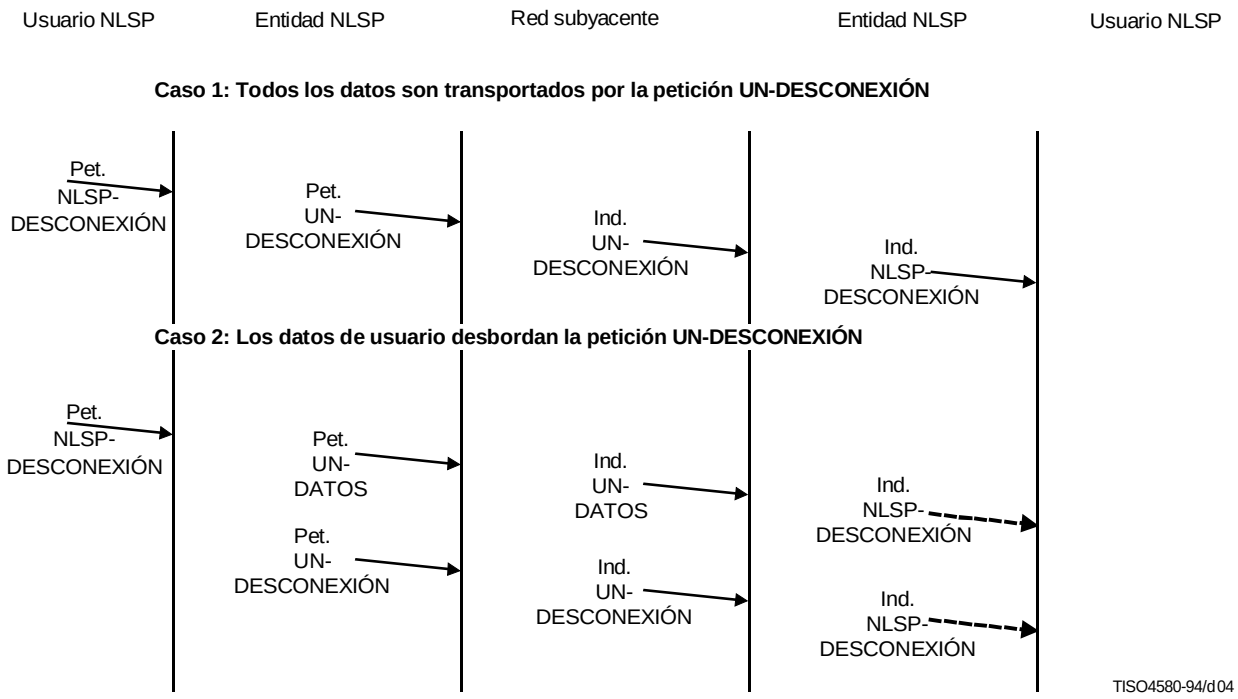
a) la NLSPE comprobará que No_Header es TRUE o Param_Prot es FALSE;

b) se transmitirá una indicación NLSP-ACUSE-DE-DATOS al usuario NLSP.

8.10 NLSP-DESCONEXIÓN

Cualquiera de los sucesos relacionados con NLSP o UN-DESCONEXIÓN indicados más adelante tiene precedencia sobre cualquier intercambio de PDU de CSC, intercambio de SA-P, o intercambio de prueba que se encuentren en curso.

Los procedimientos para la desconexión iniciada por el usuario NLSP se ilustran en la Figura 8-4.



NOTA – NLSP-DESCONEXIÓN puede aparecer en cualquiera de los puntos indicados.

Figura 8-4 – Cronograma de las primitivas de servicio para NLSP-DESCONEXIÓN

8.10.1 Petición NLSP-DESCONEXIÓN

Al recibirse una petición NLSP-DESCONEXIÓN durante los procedimientos de establecimiento de la conexión NLSP descritos en 8.5 se enviará una petición UN-DESCONEXIÓN de acuerdo con el servicio de red OSI (es decir, si ha comenzado el establecimiento de una conexión UN) y se abortarán los procedimientos de establecimiento de la conexión. Si Protect_Connect_Params es TRUE, los parámetros de cualquier petición UN-DESCONEXIÓN se determinarán localmente, y, de lo contrario, los parámetros de la petición NLSP-DESCONEXIÓN se copiarán íntegramente a través de los parámetros equivalentes de la petición UN-DESCONEXIÓN.

NOTA – Si en el curso del establecimiento de la conexión aparece una petición NLSP-DESCONEXIÓN y se ha seleccionado Protect_Connect_Params, se descartarán los parámetros de la petición NLSP-DESCONEXIÓN.

Al recibirse una petición NLSP-DESCONEXIÓN después del establecimiento de la conexión NLSP:

a) Si Protect_Connect_Params es TRUE y No_Header es TRUE, cualesquiera datos usuario NLSP se encapsularán como se describe en 6.4.1.2. Estos datos se colocan en los datos de usuario UN de una petición UN-DESCONEXIÓN. Los otros parámetros de la petición NLSP-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la petición UN-DESCONEXIÓN.

b) Si Protect_Connect_Params es TRUE, No_Header es FALSE, y Param_Prot es TRUE, se genera una PDU de SDT que contiene todos los parámetros de la petición NLSP-DESCONEXIÓN, como se describe en 6.4.1.1, con tipo de datos «pet/ind NLSP-DESCONEXIÓN». Estos datos se colocan en los datos de usuario UN. Los otros parámetros de la UN-DESCONEXIÓN se determinan localmente.

c) Si están presentes datos de usuario NLSP, Protect_Connect_Params es TRUE, No_Header es FALSE, y Param_Prot es FALSE, se genera una PDU de SDT que contiene los datos de usuario descritos en 6.4.1.1 con tipo de datos «pet/ind NLSP-DESCONEXIÓN». Estos datos se colocan en los datos de usuario UN. Los otros parámetros de la UN-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la petición UN-DESCONEXIÓN.

d) Si Protect_Param es FALSE, todos los parámetros de NLSP-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la petición UN-DESCONEXIÓN.

NOTA – Se supone que los mismos límites impuestos a la longitud de los datos de usuario NLSP se aplican a los datos de usuario UN.

e) Si después de lo prescrito en los anteriores apartados b) o c) el parámetro datos de usuario UN resultante es mayor que la longitud máxima de los datos de usuario UN de la petición UN-DESCONEXIÓN, entonces, estos datos de usuario se enviarán, en cambio, en un parámetro datos de usuario UN de una petición UN-DATOS y se pasarán al proveedor de servicio UN. Los datos de usuario UN para la petición UN-DESCONEXIÓN deberán estar vacíos:

NOTA – Una implementación debe esperar a que estos UN-DATOS atraviesen la red subyacente antes de continuar con la UN-DESCONEXIÓN, como se describe en el párrafo siguiente. La duración de esta espera se determina localmente.

f) Deberá enviarse una petición UN-DESCONEXIÓN con los parámetros fijados como se ha expresado anteriormente.

8.10.2 NLSP-DESCONEXIÓN protegida en una indicación UN-DATOS

Si se recibe una PDU de SDT en una indicación UN-DATOS con el tipo datos fijado a NLSP-DESCONEXIÓN, como se describe en 8.6.2 apartado d):

a) la NLSPE comprueba que Protect_Connect_Params es TRUE y que No_Header es FALSE;

b) todo campo de contenido que comprenda parámetros de servicio NLSP se copia a los parámetros equivalentes de NLSP-DESCONEXIÓN, y originador NLSP se fija a usuario NS;

c) la NLSPE retiene los parámetros NLSP-DESCONEXIÓN fijados como se ha expresado antes, espera una indicación UN-DESCONEXIÓN, o envía inmediatamente una indicación NLSP-DESCONEXIÓN. Esta es una decisión local.

8.10.3 Indicación UN-DESCONEXIÓN

Al recibirse una indicación UN-DESCONEXIÓN durante los procedimientos de establecimiento de la conexión NLSP descritos en 8.5, deberá enviarse una indicación NLSP-DESCONEXIÓN de acuerdo con el servicio de red OSI y se abortarán los procedimientos de establecimiento de la conexión. Los parámetros de la indicación UN-DESCONEXIÓN se copiarán íntegramente a los parámetros equivalentes de la indicación NLSP-DESCONEXIÓN o, si Protect_Connect_Params es TRUE, se fijarán como se determine localmente.

En otro caso, al recibirse una indicación UN-DESCONEXIÓN tras el establecimiento de una conexión NLSP con datos de usuario UN no vacíos:

a) Si Protect_Connect_Params es TRUE y No_Header es TRUE, los datos de usuario NLSP deberán desencapsularse como se describe en 6.4.2.2. Estos datos se colocan en los datos de usuario NLSP de una indicación NLSP-DESCONEXIÓN. Los otros parámetros de la indicación NLSP-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la indicación UN-DESCONEXIÓN.

b) Si Protect_Connect_Params es TRUE, No_Header es FALSE, y Param_Prot es TRUE, entonces una PDU de SDT en los datos de usuario UN se comprobará como se expresa en 6.4.2.1. Se comprobará que el tipo de datos es «pet/ind NLSP-DESCONEXIÓN». Todo campo de contenido relacionado con los parámetros de la NLSP-DESCONEXIÓN se copia íntegramente a estos parámetros.

c) Si Protect_Connect_Params es TRUE, No_Header es FALSE, y Param_Prot es FALSE, una PDU de SDT en los datos de usuario UN se comprueba como se describe en 6.4.2.1. Se comprueba que el tipo de datos es NLSP-DESCONEXIÓN. Se comprobará la presencia del campo de contenido datos de usuario y dichos datos se copiarán íntegramente a los datos de usuario NLSP de una indicación NLSP-DESCONEXIÓN. Los otros parámetros de la indicación UN-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la indicación NLSP-DESCONEXIÓN.

d) Si Protect_Param es FALSE, todos los parámetros de UN-DESCONEXIÓN se copian íntegramente a los parámetros equivalentes de la indicación NLSP-DESCONEXIÓN.

e) La indicación NLSP-DESCONEXIÓN deberá pasarse al usuario NLSP.

De lo contrario, al recibirse una indicación UN-DESCONEXIÓN después del establecimiento de la conexión NLSP con datos de usuario NLSP vacíos:

a) Si la NLSPE está esperando una indicación UN-DESCONEXIÓN tras una primitiva de NLSP-DESCONEXIÓN protegida, en una indicación UN-DATOS [véase 8.10.2.c)], los campos de los parámetros NLSP protegidos deberán colocarse en la indicación NLSP-DESCONEXIÓN. Los otros parámetros de la indicación NLSP-DESCONEXIÓN se fijarán a los parámetros equivalentes de la indicación UN-DESCONEXIÓN.

b) En otro caso, los parámetros de la indicación UN-DESCONEXIÓN se copiarán íntegramente a los parámetros equivalentes de la indicación NLSP-DESCONEXIÓN.

c) La indicación NLSP-DESCONEXIÓN se pasará al usuario NLSP a menos que ya se le haya enviado una.

Los atributos SA pueden suprimirse localmente después de cualquier UN-DESCONEXIÓN, si Retain_On_Disconnect (retener al desconectar) es FALSE.

8.10.4 Desconexión iniciada por el NLSP

Cuando fracasa un SA-P o cualquier otra comprobación, se pasan indicaciones NLSP-DESCONEXIÓN y peticiones UN-DESCONEXIÓN al usuario NLSP y a la red subyacente, como se consigna en 8.4.

La Figura 8-5 presenta un ejemplo ilustrativo de una desconexión iniciada por el NLSP como consecuencia del fracaso de un SA-P.

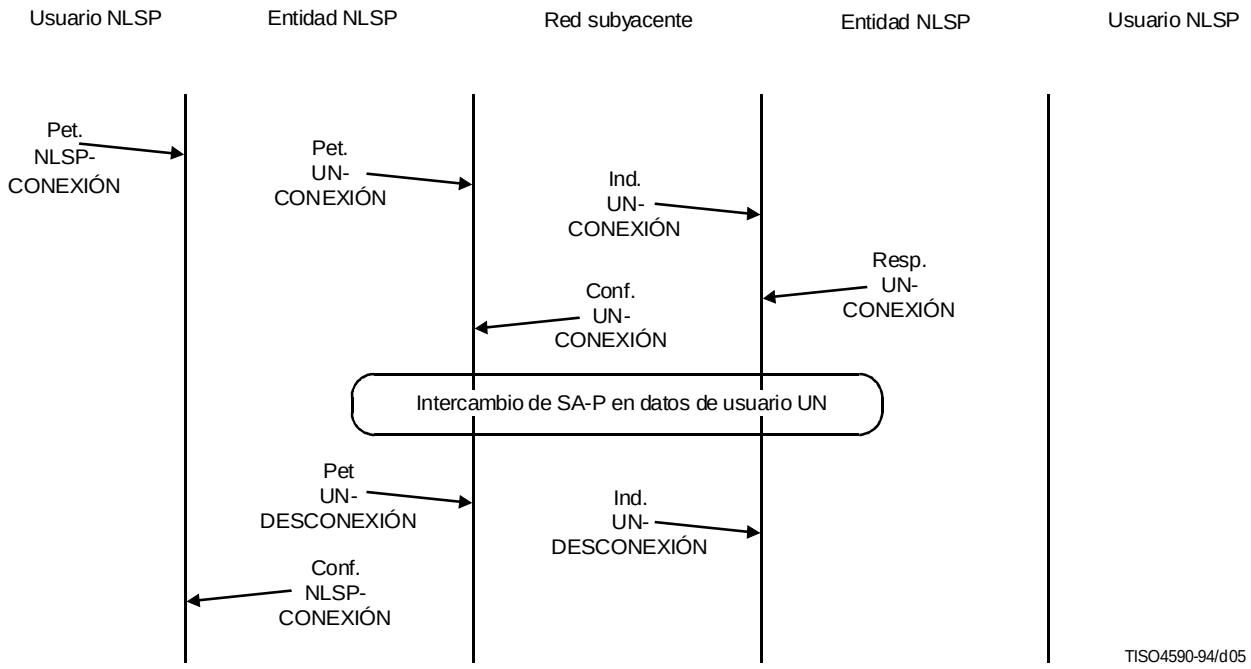


Figura 8-5 – Desconexión iniciada por el NLSP como consecuencia de un fracaso del SA-P

8.11 Otras funciones

Los siguientes procedimientos se inician cuando ocurren sucesos temporizados o externos.

8.11.1 Modificación de atributos SA dinámicos

La NLSPE puede modificar atributos SA dinámicos (véase el Anexo G) en cualquier momento durante la existencia de una conexión. Un cambio cualquiera de los atributos SA dinámicos no deberá traer consigo una modificación de los servicios de seguridad proporcionados. Esto se obtiene por medio de un intercambio de PDU de CSC o de un intercambio SA-P (mediante el empleo de PDU de SA o de PDU de SDT con el tipo de datos de contenido protocolo SA) en datos de usuario de UN-DATOS o por medios externos. Este intercambio es transparente al usuario NLSP y no se definen primitivas NLSP para invocarlo.

NOTA – Por ejemplo, este intercambio podría tener lugar a intervalos regulares durante una conexión (por ejemplo, cada hora, o cada 10 000 PDU de datos seguros) con el fin de intercambiar claves.

Cuando se está efectuando una transferencia de datos habiéndose seleccionado «sin encabezamiento», se enviará una primitiva de UN-REINICIACIÓN antes del intercambio de PDU de CSC como se consigna en 8.8.5.

Los procedimientos para el intercambio de PDU de CSC serán los descritos en 8.12. En el Anexo C se presenta un ejemplo de SA-P que incluye procedimientos para la modificación de los atributos SA.

8.11.2 Intercambio de prueba de seguridad

Estos procedimientos se utilizarán para probar la operación de los aspectos criptográficos de una SA.

Sólo pueden invocarse en aquellos estados en que pueden enviarse primitivas de NLSP-DATOS en UN-DATOS (por ejemplo, después de concluido el establecimiento de una conexión, antes de cualquier procedimiento de desconexión, pero no durante procedimientos de reiniciación).

El intercambio de prueba tiene un orden de precedencia inferior al de cualquier primitiva de DESCONEXIÓN, REINICIACIÓN, o intercambio de unidades PDU de CSC, o intercambio de SA-P.

NOTA – La utilización de esta facilidad se manejará localmente. Son posibles los siguientes modos:

a) optar por no emplearla;

b) utilizarla después de un intercambio de claves;

c) utilizarla periódicamente, en momentos determinados localmente.

8.11.2.1 Invocación de un intercambio de prueba

Al invocarse un intercambio de prueba:

a) se crea un campo de datos de prueba con la bandera de sentido de transmisión anulada (o sea, puesta a 0) y datos de prueba fijados a datos aleatorios;

b) se genera una PDU de SDT como se describe en 6.4.1.1, con tipo de datos «no relacionado con ninguna primitiva de servicio NLSP», que contiene el campo de datos de prueba;

c) esta PDU se enviará en datos de usuario UN de UN-DATOS con una confirmación de recepción UN que indica «confirmación de recepción no requerida».

8.11.2.2 UN-DATOS con una PDU de SDT que contiene datos de prueba

Al recibirse una primitiva UN-DATOS que contiene una PDU de SDT con tipo de datos puesto a 0 (no relacionado con ninguna primitiva de servicio NLSP) como se describe en 8.6.2 b), si la PDU de SDT contiene datos de prueba se procesará como sigue:

a) Si la bandera de sentido de transmisión en el campo de datos de prueba está anulada, deberá generarse una nueva PDU de SDT como se describe en 6.4.1.1 con tipo de datos «no relacionado con ninguna primitiva de servicio NLSP» y que contenga un campo de datos de prueba con la bandera de sentido de transmisión puesta y los datos fijados a los datos aleatorios recibidos. Estos datos deberán devolverse en datos de usuario UN de una primitiva UN-DATOS con una confirmación de recepción que indique «confirmación de recepción no requerida».

b) Si la bandera de sentido de transmisión en los datos de prueba está puesta, se comprobará que los datos de prueba son idénticos a los datos de prueba enviados anteriormente. Si no lo son, la NLSPE ejecutará funciones de error como se define en 8.4.

8.11.3 Relleno de tráfico

Para ocultar la presencia de datos de usuario se pueden enviar primitivas UN-DATOS adicionales que contengan PDU de transferencia de datos segura con tráfico de relleno solamente.

Todas las entidades NLSP deberán ser capaces de recibir PDU de transferencia de datos segura con ese relleno de tráfico.

La utilización de esta facilidad queda a la discreción de la entidad NLSP local y es transparente al usuario de servicio NLSP.

8.11.3.1 Invocación de relleno de tráfico

Cuando se invoca relleno de tráfico:

a) se genera una PDU de SDT como se describe en 6.4.1.1, con tipo de datos «no relacionado con ninguna primitiva de servicio NLSP», que no comprenda otros campos de contenido adicionales diferentes de los requeridos en 6.4.1.1;

b) esta PDU se envía en datos de usuario UN de la primitiva UN-DATOS con una confirmación de recepción UN que indica «confirmación de recepción no requerida».

8.11.3.2 UN-DATOS con una PDU que no comprende campos de contenido adicionales

Al recibirse una primitiva UN-DATOS que contiene una PDU de SDT con el tipo de datos puesto a 0 (no relacionado con ninguna primitiva de servicio NLSP) como se describe en 8.6.2 b), si la PDU de SDT no comprende ningún campo de contenido, aparte de los requeridos de manera general en la cláusula 6, se hará caso omiso de dicha PDU de SDT.

8.12 Autenticación de la entidad par

Pueden invocarse los procedimientos definidos en 8.12.1 y 8.12.2:

- después de una UN-REINICIACIÓN o de una NLSP-REINICIACIÓN, como se describe en 8.8;
- a intervalos de tiempo determinados localmente,

con el fin de efectuar la autenticación de la entidad par o modificar atributos SA dinámicos.

El intercambio de PDU de CSC durante el establecimiento de la conexión se describe en 8.5.

Las peticiones NLSP-DATOS o NLSP-DATOS-ACELERADOS no serán atendidas hasta que se haya realizado íntegramente un intercambio de CSC.

El intercambio de CSC tiene un orden de precedencia inferior al de cualquier primitiva de REINICIACIÓN o DESCONEXIÓN.

8.12.1 Invocación de un intercambio de CSC

Cuando se invoca un intercambio de CSC deberá crearse una PDU de CSC con:

a) las banderas UNC-UND y SA-P anuladas;

b) SA-ID puesto a Your_SA-ID;

c) el contenido fijado al primer intercambio de CSC, de acuerdo con los procedimientos específicos al mecanismo como los descritos en 10.3.

Esta PDU de CSC se enviará en datos de usuario UN de una primitiva de UN-DATOS con «petición de confirmación no requerida».

La NLSPE que invoca el intercambio de CSC esperará una primitiva de UN-DATOS que contenga una PDU de CSC. Otra posibilidad es que el intercambio de CSC tenga un orden de precedencia inferior al de UN-REINICIACIÓN o de una NLSP-REINICIACIÓN, como se describe en 8.8 o al de una UN-DESCONEXIÓN o de una NLSP-DESCONEXIÓN como se describe en 8.10.

8.12.2 UN-DATOS que contiene una PDU de CSC

Al recibirse una primitiva de UN-DATOS que contiene una PDU de CSC (por el iniciador o por el respondedor del intercambio de CSC), se comprueba el contenido de acuerdo con los procedimientos específicos al mecanismo, como se describe en 10.3.

En función de los procedimientos específicos al mecanismo, la NLSPE podrá:

a) Retornar un contenido de PDU de CSC e indicar que se requiere un ulterior intercambio de CSC.

   En tal caso, la bandera UNC-UND de la PDU de CSC y la bandera del SA-P deberán fijarse a Your_SA-ID, y el Contenido deberá fijarse como lo requieran los procedimientos específicos al mecanismo. La PDU de CSC deberá enviarse en datos de usuario UN-DATOS. La NLSPE esperará otra primitiva de UN-DATOS que contenga una PDU de CSC. Otra posibilidad es que el intercambio de CSC

tenga un orden de precedencia inferior al de una UN-REINICIACIÓN o de una NLSP-REINICIACIÓN como se describe en 8.8, o al de una UN-DESCONEXIÓN o de una NLSP-DESCONEXIÓN como se describe en 8.10.

b) Retornar un contenido de PDU de CSC e indicar que se requiere una PDU de SDT para completar el intercambio.

En tal caso, la bandera UNC-UND de la PDU de CSC y la bandera del SA-P deberán anularse, SA-ID deberá fijarse a Your_SA-ID, y el Contenido deberá fijarse como lo requieran los procedimientos específicos al mecanismo. La PDU de CSC deberá enviarse en datos de usuario UN-DATOS. La NLSPE esperará otra primitiva de UN-DATOS que contenga una PDU de CSC, la que se procesa como se describe en 8.6. Otra posibilidad es que el intercambio de CSC tenga un orden de precedencia inferior al de una UN-REINICIACIÓN o de una NLSP-REINICIACIÓN como se describe en 8.8, o al de una UN-DESCONEXIÓN o de una NLSP-DESCONEXIÓN como se describe en 8.10.

NOTA 1 – No se considera que la autenticación está completa, por lo que las peticiones UN-DATOS (o NLSP-DATOS-ACELERADOS) no serán procesadas en esta NLSPE hasta que se reciba una PDU de SDT. Esta PDU de SDT puede, o bien contener una primitiva NLSP-DATOS del usuario NLSP distante, o no estar relacionada con ninguna primitiva de servicio NLSP.

NOTA 2 – Esta opción no puede ser soportada si No_Header es TRUE.

c) Retornar un contenido de PDU de CSC e indicar que el intercambio está completo.

En este caso, la bandera UNC-UND de la PDU de CSC y la bandera del SA-P deberán anularse, SA-ID deberá fijarse a Your_SA-ID, y el contenido deberá fijarse como lo requieran los procedimientos específicos al mecanismo. La PDU de CSC deberá enviarse en datos de usuario UN-DATOS.

d) Indicar que se debe enviar una PDU de SDT para completar el intercambio de CSC.

En tal caso, si se está esperando para enviar la petición NLSP-DATOS (o NLSP-DATOS-ACELERADOS), y No_Header es FALSE, deberá procesarse dicha petición como se describe en 8.6 y 8.7. De lo contrario, se creará una PDU de SDT como se describe en 6.4.1.1 con el tipo de datos «no relacionado con ninguna primitiva de servicio», que no comprenda campos de contenido salvo los requeridos de una manera general en la cláusula 6, y se enviará en datos de usuario UN de una primitiva UN-DATOS.

e) Indicar que el intercambio de CSC está completo.

En este caso no es necesario ejecutar acciones ulteriores.

NOTA 3 – No se han definido procedimientos generales para resolver las colisiones entre dos intercambios de CSC iniciados al mismo tiempo.

NOTA 4 – Con el mecanismo de autenticación definido en la cláusula 10, si la utilización de funciones de encapsulación/desencapsulación, como la descrita en la cláusula 11, no incluye ISN, no se proporciona la plena autenticación de la entidad par. Por otra parte, tampoco se proporciona la plena autenticación de la entidad par si se utiliza un mecanismo de encapsulación basado en la ausencia de encabezamiento, como el descrito en la cláusula 12.

9 Visión de conjunto del mecanismo utilizado

Las cláusulas 9 a 12 definen mecanismos específicos para ser utilizados con los protocolos genéricos definidos en las cláusulas 1 a 8. Estos mecanismos no son los únicos que pueden utilizarse para proporcionar seguridad dentro del NLSP genérico. Otros mecanismos podrán normalizarse en el futuro, y es posible utilizar mecanismos privados con el NLSP.

9.1 Servicios y mecanismos de seguridad

El NLSP-CL soporta los siguientes servicios de seguridad, si se seleccionan, con el mecanismo descrito:

a) *Autenticación del origen de datos* – El mecanismo utilizado para proporcionar este servicio es un ICV junto con la gestión de claves;

b) *Control de acceso* – Los mecanismos utilizados para proporcionar este servicio son etiquetas de seguridad y/o el control de claves y/o el uso de direcciones autenticadas.

c) *Confidencialidad en modo sin conexión* – El mecanismo utilizado para proporcionar este servicio es el cifrado. Esta protección incluye facultativamente todos los parámetros de servicio NLSP, que dependen de los servicios de seguridad seleccionados.

d) *Confidencialidad del flujo de tráfico* – Los mecanismos utilizados para este servicio son el relleno de tráfico y/o la ocultación de la dirección NLSP.

e) *Integridad (en modo) sin conexión* – El mecanismo utilizado para proporcionar este servicio es un ICV. Esta protección incluye facultativamente todos los parámetros de servicio NLSP, que dependen de los servicios de seguridad seleccionados.

El NLSP-CO soporta los siguientes servicios de seguridad, si se seleccionan, con los mecanismos descritos:

a) *Autenticación de la entidad par* – El mecanismo utilizado para proporcionar este servicio es un intercambio de números secuenciales para la integridad, cifrados, junto con la gestión de claves.

b) *Control de acceso* – Los mecanismos utilizados para proporcionar este servicio son etiquetas de seguridad y/o el control de claves y/o el uso de direcciones autenticadas.

c) *Confidencialidad en modo sin conexión* – El mecanismo utilizado para proporcionar este servicio es el cifrado. Esta protección incluye facultativamente todos los parámetros de conexión NLSP, que dependen de los servicios de seguridad seleccionados.

d) *Confidencialidad del flujo de tráfico* – Los mecanismos utilizados para este servicio son el relleno de tráfico y/o la ocultación de la dirección.

e) *Integridad en modo sin conexión, sin recuperación* – Los mecanismos utilizados para proporcionar este servicio son un valor de comprobación de la identidad y números secuenciales para la integridad. Esta protección incluye facultativamente todos los parámetros de conexión NLSP, que dependen de los servicios de seguridad seleccionados.

9.2 Funciones soportadas

Los elementos esenciales de los mecanismos soportados por el NLSP son:

a) Una función de autenticación de la conexión que soporta la autenticación de la entidad par y establece valores iniciales para los atributos SA «dinámicos» que soportan la transferencia de datos segura. Esta función sólo la utiliza el NLSP-CO.

b) Una función de encapsulación basada en la PDU de SDT, que soporta la transferencia segura de datos mediante el empleo de los siguientes mecanismos:

   1) número secuencial para la integridad;

   2) relleno para la confidencialidad del flujo de tráfico, algoritmos de integridad de bloque, y algoritmos de cifrado de bloque;

   3) valor de comprobación de la integridad;

   4) cifrado.

c) Una función de encapsulación basada en la forma de protección sin encabezamiento, (No_header) la cual emplea un mecanismo de cifrado que no cambia la longitud de los datos.

Los mecanismos actúan en el mismo orden en que se han enumerado.

10 Control de la seguridad de la conexión (NLSP-CO solamente)

10.1 Visión de conjunto

El procedimiento «control de la seguridad de la conexión» utiliza un intercambio de unidades de datos de protocolo (PDU) de control de la seguridad de la conexión (CSC, *connection security control*) para:

a) facultativamente, especificar una nueva clave para el cifrado/la integridad;

b) efectuar la autenticación de la entidad par;

c) establecer un número secuencial para la integridad.

El soporte de un mecanismo para la autenticación mediante el intercambio de números secuenciales se especifica en esta Recomendación | Norma Internacional. Para la entidad iniciadora, la autenticación mediante este mecanismo queda completada cuando se ejecuta íntegramente el intercambio bidireccional. Para la entidad respondedora, si se selecciona la integridad de la secuencia de manera que proteja contra los ataques por reproducción fraudulenta (es decir, si ISN es TRUE), la autenticación queda completada solamente cuando se recibe de la entidad iniciadora la primera PDU de datos, o de datos de prueba.

10.2 Atributos SA

Se utilizan los siguientes atributos de seguridad para soportar los procedimientos de control de la seguridad de la conexión:

a) *Mecanismos seleccionados por la SA:*

Autenticación: Booleano

Indica si se va o no a utilizar la autenticación de la entidad par mediante ISN cifrado.

Los valores de estos atributos lo define el ASSR en base a los servicios de seguridad seleccionados.

b) *Atributos de los mecanismos de distribución de claves:*

kdm: Modo que va a utilizarse con esta SA

El valor de este atributo lo define el ASSR en base a los servicios de seguridad seleccionados.

Puede tener los siguientes valores:

kdm_mutual:	distribución por claves simétricas;
kdm_asymmetric_single:	distribución mediante el empleo de la clave pública de receptores;
kdm_asymmetric_double:	distribución mediante el empleo de la clave pública y de la clave privada local;
kdm_distributed:	distribución por referencia a una clave predistribuida o a una clave distribuida por otros medios;
kdm_other:	utilización de un mecanismo de distribución definido privadamente.

c) *Atributos de los mecanismos de autenticación:*

Auth_Alg: Identificador de objeto adjudicado según ISO/CEI 9979

El valor de este atributo lo define el ASSR en base a los servicios de seguridad seleccionados.

Enc_Auth_len: Longitud del campo datos de autenticación para el cifrado en la PDU de CSC

El valor de este atributo lo define el ASSR en base a los servicios de seguridad seleccionados.

Auth_Gen_Key: Forma constreñida por el ASSR

El valor inicial de este atributo se fija al establecerse la SA y se puede cambiar durante la existencia de la asociación.

Auth_Check_Key: Forma constreñida por el ASSR

El valor inicial de este atributo se fija al establecerse la SA y se puede cambiar durante la existencia de la asociación.

El mecanismo de autenticación de la conexión puede establecer los siguientes atributos, que son utilizados por el mecanismo de transferencia de datos segura:

a) *Atributos del mecanismo ISN:*

Data_My_ISN

Data_Your_ISN

Exp_My_ISN

Exp_Your_ISN

b) *Atributos del mecanismo de cifrado:*

Data_Enc_Key

Data_Dec_Key

Exp_Enc_Key

Exp_Dec_Key

c) *Atributos del mecanismo ICV:*

Data_ICV_Gen_Key

Data_ICV_Check_Key

Exp_ICV_Gen_Key

Exp_ICV_Check_Key

NOTA – En futuras versiones de esta Recomendación | Norma Internacional podrán identificarse atributos adicionales específicos al mecanismo; también podrán identificarse atributos adicionales para mecanismos privados.

10.3 Procedimientos

Las entidades NLSP intercambian PDU de control de la seguridad de la conexión (CSC, *connection security control*) al establecerse cada conexión, o después de una reiniciación, o cuando ocurren sucesos temporizados externamente, con el fin de:

a) facultativamente, especificar la clave para el cifrado o la integridad;

b) efectuar la autenticación de la entidad par;

c) establecer el número secuencial para la integridad.

La autenticación de la entidad par puede proporcionarse como se define más adelante. Cualquier método alternativo debe proporcionar un número secuencial para la integridad si se requiere la integridad de la conexión.

La clave para el cifrado/la integridad se especifica, o bien:

a) por una indicación de que se va a utilizar la clave existente; o

b) pasando una nueva clave, cifrada con una clave que a su vez cifra una clave mutua; o

c) pasando una nueva clave cifrada con la clave pública del receptor; o

d) por referencia a una clave previamente distribuida.

NOTA 1 – La derivación de una clave de cifrado proporciona una pequeña cantidad de verificación de la integridad por el hecho de que impide una reproducción fraudulenta de texto en lenguaje cifrado, protegido con una clave diferente. El algoritmo de derivación de clave debe ser específico a cada algoritmo de cifrado, para prevenir la derivación accidental de las claves débiles.

El NLSP utiliza un método de autenticación de la entidad par basado en el intercambio de números secuenciales iniciales, para la integridad, cifrados mediante una clave de autenticación. Este método puede utilizarse incluso si no se emplean números secuenciales para el servicio de integridad.

Los procedimientos de la seguridad de la conexión se basan en el intercambio de dos UPD de CSC y una PDU de transferencia de datos segura, de la manera siguiente:

Una PDU de CSC la prepara el iniciador del intercambio de seguridad:

a) Los Auth-Data cifrados fijados a un valor seleccionado localmente de My-Initial-ISN y un valor 0 para Your-Initial-ISN, ambos cifrados por medio de la clave Auth_Gen_Key. El ISN seleccionado tiene que ser único para las claves de autenticación e integridad.

b) La información de clave fijada como lo exige el mecanismo de distribución de claves.

Al recibirse una PDU de CSC por una entidad NLSP que todavía no es el iniciador de un intercambio de PDU de CSC:

a) los Auth-Data cifrados se descifran utilizando Auth_Check_Key;

b) se comprueba que el campo Your-Initial-ISN es 0;

c) los atributos SA locales Data_Your_ISN y Exp_Your_ISN se fijan al campo My-Initial-ISN recibido;

d) se procesa la información de clave como lo exige el mecanismo de distribución de claves.

Se prepara entonces una PDU de CSC con:

a) Los Auth-Data cifrados fijados a un valor seleccionado localmente de My-Initial-ISN y Your-Initial-ISN con el valor del My-Initial-ISN recibido, ambos cifrados mediante la clave Auth_Gen_Key. El ISN seleccionado tiene que ser único para las claves de autenticación e integridad.

b) La información de clave fijada como lo exige el mecanismo de distribución de claves.

Al recibirse una PDU de CSC por el iniciador del intercambio de CSC:

a) los Auth-Data cifrados se descifran mediante Auth_Check_Key;

b) el campo Your-Initial-ISN se coteja con el My-Initial-ISN enviado anteriormente;

c) los atributos SA locales Data_Your_ISN y Exp_Your_ISN se fijan al campo My-Initial-ISN recibido;

d) la información de clave se procesa como lo exige el mecanismo de distribución de claves.

Tras la comprobación exitosa de la respuesta, si la entidad NLSP no tiene datos en espera y se ha seleccionado el mecanismo ISN para la encapsulación de las PDU de SDT (véase la cláusula 11), se enviará, para completar la autenticación, una PDU de transferencia de datos segura que no contenga datos, pero que incluya un ISN.

NOTA 2 – La PDU de SDT puede enviarse, incluso si no hay datos en espera, para completar los procedimientos de autenticación, sin necesidad de seguir los procedimientos normales de transferencia de datos.

Si la autenticación fracasa, entonces, en base a una decisión local, la asociación de seguridad podrá establecerse de nuevo, dentro o fuera de banda; se podrá asimismo seguir los procedimientos de recuperación tras error descritos en 8.4.

10.4 Campos de PDU de CSC utilizados

Los procedimientos descritos en esta subcláusula utilizan los siguientes campos de contenido CSC específicos al mecanismo, definidos en 13.5.6:

a) Auth-Data cifrado;

b) información de clave.

11 Función de encapsulación basada en la PDU de SDT

11.1 Visión de conjunto

El protocolo NLSP-CL, y facultativamente el NLSP-CO, protegen los datos de usuario y la correspondiente información de control de protocolo por medio de una función de encapsulación basada en la PDU de SDT. Esta cláusula define esa función de encapsulación. Dicha función de encapsulación se basa en cuatro funciones:

– ISN (número secuencial para la integridad);

– relleno;

– ICV (valor de comprobación para la integridad); y

– cifrado.

La decisión de emplear una determinada función ha de basarse en los atributos de la SA.

Si se selecciona numeración secuencial deberá añadirse un campo ISN.

NOTA 1 – No se tiene prevista la utilización de este mecanismo de protección con el protocolo NLSP-CL.

Si se selecciona relleno para el tráfico puede añadirse un campo de relleno para el tráfico.

Si se utiliza un algoritmo de integridad de bloque puede añadirse un campo de relleno para la integridad.

Si se selecciona comprobación de la identidad se podrá calcular un ICV y añadirlo al final de cada uno de los campos antes mencionados.

NOTA 2 – El valor ICV puede también utilizarse para proporcionar autenticación del origen de datos.

Si hay que utilizar un algoritmo de cifrado de bloque se puede añadir un campo de relleno para el cifrado.

Si se selecciona cifrado, los campos antes mencionados se cifran utilizando la clave de cifrado para la asociación de seguridad.

El proceso antes descrito encapsula datos de usuario y otros parámetros del protocolo NLSP para dar protección a la transferencia por la red. En el extremo distante, el receptor de una PDU de transferencia de datos segura retira la protección, y la comprueba, invirtiendo el orden del procedimiento.

11.2 Atributos de la SA

a) *Mecanismos seleccionados para la SA:*

ISN: Booleano

Números secuenciales para la integridad que se incluyen en cada cadena de octetos encapsulada.

Padd: Booleano

Relleno en la cadena de octetos encapsulada, para soportar el mecanismo de relleno para el tráfico.

ICV: Booleano

Integridad y/o autenticación del origen de datos del contenido de la cadena de octetos encapsulada, utilizando un valor de comprobación de la integridad.

Encipher: Booleano

Cifrado de una cadena de octetos encapsulada para proporcionar confidencialidad.

Los valores de estos atributos se definen en el ASSR, dados los servicios de seguridad seleccionados que se desean.

b) *Atributos del mecanismo ISN:*

ISN_Len: Entero

El valor de este atributo será definido por el ASSR dados los servicios de seguridad seleccionados.

Data_My-ISN: ISN para los últimos datos normales enviados.

Data_Your_ISN: ISN para los últimos datos normales recibidos.

Exp_My_ISN: ISN para los últimos datos acelerados enviados.

Exp_Your_ISN: ISN para los últimos datos acelerados recibidos.

Los valores iniciales de estos atributos «de clave» se fijarán al establecerse la SA y se podrá cambiarlos durante la existencia de la asociación.

NOTA 1 – Los atributos ISN datos acelerados son aplicables al NLSP-CO solamente.

c) *Atributos del mecanismo de relleno:*

Traff_Padd: Forma constreñida por el ASSR

Exigencias de relleno de tráfico.

d) *Atributos del mecanismo ICV:*

ICV_Alg: Identificador de objeto

El valor de este atributo estará constreñido por el ASSR, dados los servicios de seguridad seleccionados. Este atributo implica ciertos atributos del mecanismo de integridad, tales como algoritmos separados de generación y comprobación de algoritmos, vectores de inicialización, etc.

ICV_Blk: Entero

Tamaño de bloque básico sobre el que actúa el algoritmo ICV.

El valor de este atributo estará constreñido por el ASSR, dados los servicios de seguridad seleccionados.

ICV_Len: Entero

La longitud de la salida del mecanismo ICV.

El valor de este atributo será definido por el ASSR, dados los servicios de seguridad seleccionados.

No es necesario que ICV_Len sea igual a ICV_Blk.

Data_ICV_Gen_Key: Forma constreñida por el ASSR

Referencia de clave de generación de ICV para datos normales.

Data_ICV_Check_Key: Forma constreñida por el ASSR

Referencia de clave de comprobación de ICV para datos normales.

Exp_ICV_Gen_Key: Forma constreñida por el ASSR

Referencia de clave de generación de ICV para datos acelerados.

Exp_ICV_Check_Key: Forma constreñida por el ASSR

Referencia de clave de comprobación de ICV para datos acelerados.

Los valores iniciales de estos atributos «de clave» se fijarán al establecerse la SA y se podrá cambiarlos durante la existencia de la asociación.

NOTA 2 – Los atributos de clave de datos acelerados son aplicables al NLSP-CO solamente.

e) *Atributos del mecanismo de cifrado:*

Enc_Alg: Identificador de objeto adjudicado según ISO/CEI 9979

El valor de este atributo estará constreñido por el ASSR, dados los servicios de seguridad seleccionados. Este atributo implica ciertos atributos del mecanismo de cifrado, tales como la forma y longitud de cualquier campo de sincronización, algoritmos separados de cifrado y descifrado, vectores de inicialización, etc.

Enc_Blk: Entero

Tamaño de bloque del algoritmo de cifrado.

El valor de este atributo estará constreñido por el ASSR, dados los servicios de seguridad seleccionados.

Data_Enc_Key: Forma constreñida por el ASSR

Referencia de clave de cifrado para datos normales.

Data_Dec_Key: Forma constreñida por el ASSR

Referencia de clave de descifrado para datos normales.

Exp_Enc_Key: Forma constreñida por el ASSR

Referencia de clave de cifrado para datos acelerados.

NOTA 3 – Este atributo sólo lo utiliza el NLSP-CO.

Exp_Dec_Key: Forma constreñida por el ASSR

Referencia de clave de descifrado para datos acelerados.

NOTA 4 – Este atributo sólo lo utiliza el NLSP-CO.

Los valores iniciales de estos atributos «de clave» se fijarán al establecerse la SA y se podrá cambiarlos durante la existencia de la asociación.

NOTA 5 – En futuras versiones de esta Recomendación | Norma Internacional podrán identificarse atributos adicionales específicos al mecanismo; también podrán identificarse atributos adicionales para mecanismos privados.

11.3 Procedimientos

Cuando se efectúa la encapsulación, se formará una PDU añadiéndole campos al final o al principio. Estos campos pueden ser facultativos. Una PDU parcialmente formada se designará en el texto que sigue como «campos existentes». Durante la desencapsulación, se descompondrá una PDU retirándole los campos. Una PDU parcialmente descompuesta se designará en el texto que sigue como «datos restantes».

NOTAS

1 La descripción de la adición de campos al final o al principio no tiene por finalidad constreñir las implementaciones del NLSP, sino especificar inequívocamente el protocolo.

2 Esta función de encapsulación no trata la opción sin encabezamiento (No_Header). Esta opción se trata en los procedimientos definidos en la cláusula 12.

11.3.1 Función de encapsulación

Deberá utilizarse el SA-ID para referenciar una asociación de seguridad. Si la asociación de seguridad no existe, se retornará el error SA no disponible y el valor de la cadena de octetos encapsulada será indeterminado.

Si (ISN es TRUE) entonces, o bien:

a) Si (tipo de dato unidad = normal), Data_Su_ISN será avanzado y colocado en el campo de contenido número secuencial, y añadido al final de los campos existentes en la cadena de octetos antes de la encapsulación.

b) Si (tipo de dato unidad = acelerado), Exp_Su_ISN será avanzado y colocado en el campo de contenido número secuencial, y añadido al final de los campos existentes en la cadena de octetos antes de la encapsulación.

NOTAS

1 El ISN puede avanzarse incrementando un número secuencial o eligiendo el número siguiente en una secuencia no repetitiva. Los sellos de tiempo pueden también considerarse una secuencia no repetitiva.

2 No se tiene prevista la utilización de este mecanismo de protección con el protocolo NLSP-CL.

3 Exp_Su_ISN sólo es aplicable al NLSP-CO.

Si (Padd es TRUE), una cantidad y una forma de relleno, determinadas localmente por las reglas del ASSR a que se hace referencia en Traff_Padd, se colocará en un campo de contenido relleno para el tráfico y añadirá al final de los campos existentes en la cadena de octetos antes de la encapsulación. Si se requiere un solo octeto de relleno deberá utilizarse el campo de contenido relleno de un solo octeto.

Si (ICV es TRUE) e (ICV_Blk > 1), entonces, si es necesario, se agrega al final de los campos existentes un campo de relleno para la integridad, de manera que la longitud de los campos existentes con el campo de relleno para la integridad (incluido el campo de contenido protegido) sea un múltiplo entero del tamaño de bloque ICV (es decir, ICV_Blk). Si está presente, un relleno de una cantidad y de una forma determinadas localmente se colocará en el campo de contenido relleno para la integridad. Si se requiere un solo octeto de relleno, deberá utilizarse el campo de contenido relleno de un solo octeto. El valor longitud de contenido se aumentará en la misma cantidad de relleno añadida.

Se colocará un campo longitud de contenido antes de los campos existentes. Se determinará la longitud de todos los campos existentes y su valor se colocará en el campo longitud de contenido.

Si (ICV es TRUE), se calculará un ICV de longitud ICV_Len, y se añadirá al final de los campos existentes. El algoritmo utilizado será el identificado por ICV_Alg, y la clave utilizada será o bien:

a) Data_ICV_Gen_Key si tipo de dato unidad = normal, o bien

b) Exp_ICV_Gen_Key si tipo de dato unitario = acelerado.

Si (Encipher es TRUE), deberá generarse un campo de sincronización criptográfica con una forma y una longitud determinadas por Enc_Alg, y se añadirá al final de los campos existentes.

Si (Encipher es TRUE), se añadirá al final de los campos existentes un relleno para el cifrado de manera que la longitud de los campos existentes (es decir, los campos de longitud de datos protegidos, cadena de octetos antes de la encapsulación, ISN, relleno para la integridad, e ICV) más la longitud de un relleno para el cifrado, sea un múltiplo entero del tamaño de bloque de cifrado (es decir, Enc_Blk). Si está presente, un relleno de una cantidad y de una forma determinadas localmente se colocará en un campo de contenido relleno para el cifrado. Si se requiere un solo octeto de relleno deberá utilizarse el campo de contenido relleno de un solo octeto.

Si (Encipher es TRUE), se cifran los campos existentes. El algoritmo utilizado será el identificado por Enc_Alg, y la clave utilizada será o bien:

a) Data_Enc_Key si tipo de dato unidad = normal, o bien

b) Exp_Enc_Key si tipo de dato unitario = acelerado.

La PDU construida se retornará como el resultado de la cadena de octetos encapsulada.

11.3.2 Función de desencapsulación

Si fracasa cualquiera de las comprobaciones siguientes, todas las informaciones de «status» (es decir, estado, situación) pertinentes se fijan a la información de status de seguridad antes de la recepción de este mensaje, con excepción de la información de alarma, auditoría, y/o contabilidad.

Deberá utilizarse el argumento SA-ID para referenciar una asociación de seguridad. Si la asociación de seguridad no existe, se retornará el error «SA no disponible» y el valor de la cadena de octetos encapsulada será indeterminado.

Si (Encipher es TRUE) se siguen los pasos siguientes:

a) Se decriptará la cadena de octetos encapsulada. El algoritmo de descifrado utilizado será el identificado por Enc_Alg, y la clave utilizada será o bien:

   1) Data_Dec_Key si el tipo de unidad de datos = normal, o bien

   2) Exp_Dec_Key si el tipo de unidad de datos = acelerado.

b) El campo de sincronización criptográfica se suprimirá descartando un número de octetos, determinado por Enc_Alg, a partir de la posición inicial de los datos descifrados.

c) El campo de contenido relleno para el cifrado o relleno de un solo octeto se suprimirá añadiendo la longitud de contenido e ICV_Len, y descartando entonces todo octeto en los datos descifrados restantes que esté más allá de la longitud calculada.

Si (ICV es TRUE) se siguen los pasos siguientes:

a) Se verifica el campo ICV comprobando los últimos ICV_Len octetos de los datos restantes. El algoritmo utilizado deberá ser el identificado por ICV_Alg y, si tiene un fundamento criptográfico, la clave utilizada para calcular ICV será:

   1) Data_ICV_Check_Key si el tipo de unidad de datos = normal, o

   2) Exp_ICV_Check_Key si el tipo de unidad de datos = acelerado.

b) Si fracasa la verificación ICV se retornará el error de fallo de la integridad de la unidad de datos, y el valor de la cadena de octetos antes de la encapsulación será indeterminado.

El ICV se suprimirá descartando todo octeto en los datos restantes que esté situado más allá de la longitud contenida en longitud de contenido, después del campo longitud de contenido.

El campo longitud de contenido se suprimirá descartando los dos primeros octetos de los datos restantes.

Todo campo de contenido de relleno para el tráfico, relleno para la integridad, o relleno de un solo octeto se retirará de los datos restantes suprimiendo los datos que estén situados más allá de la cadena de octetos antes de la encapsulación.

NOTA 1 – Los campos de contenido se localizan decodificando el contenido de la cadena de octetos antes de la encapsulación, que es un campo de tipo de un solo octeto seguido de un número de campos TLV.

Si (ISN es TRUE), los datos restantes se comprobarán para cerciorarse de que sólo está presente un campo de contenido ISN, y sólo uno; de lo contrario, se comprobarán los datos restantes para cerciorarse de que no está presente ningún campo de contenido ISN. Si está presente y:

a) Si (tipo de unidad de datos = normal) entonces Data_Su_ISN se avanzarán y se comprobará el valor de la ISN recibida con la ventana de valores esperados determinados por Data_Su_ISN;

b) Si (tipo de unidad de datos = expedidos) entonces se avanzará Exp_Su_ISN y se comprobará el valor de la ISN recibida con la ventana de valores esperados determinados por Exp_Su_ISN.

Tanto en a) como en b), se avanzará la ISN antes de comprobar.

NOTA 2 – El avance de la ventana se obtendrá incrementando un número secuencial o eligiendo el número siguiente de una secuencia seudoaleatoria no repetitiva.

El valor de la cadena de octetos antes de la encapsulación se retornará como el resultado en la cadena de octetos antes de la encapsulación.

11.4 Campos de PDU utilizados

En estos procedimientos se utilizan los siguientes campos de una PDU de SDT como se indica en 13.3:

a) cadena de octetos encapsulada;

b) sincronización criptográfica;

c) ICV;

d) campos de contenido:

   1) relleno para el cifrado;

   2) número secuencial;

   3) relleno de un solo octeto;

   4) relleno para el tráfico;

   5) relleno para la integridad.

12 Función de encapsulación sin encabezamiento (NLSP-CO solamente)

12.1 Visión de conjunto

El NLSP-CO sólo puede proporcionar la confidencialidad de los datos de usuario mediante el empleo de una opción Sin encabezamiento. Esta opción utiliza una función de encapsulación como la descrita en esta cláusula. Esta función de encapsulación se basará en un mecanismo de cifrado.

La utilización de la opción sin encabezamiento implica que el mecanismo de cifrado actúa sobre una longitud de bloque de un octeto, y que el algoritmo no modifica el tamaño de los datos cifrados.

12.2 Atributos SA

a) Mecanismo seleccionado para la SA:

Encipher: Booleano

Cifrado de una cadena de octetos encapsulada para proporcionar confidencialidad.

Los valores de este atributo deberán ser definidos por el ASSR dados los servicios de seguridad seleccionados.

b) Atributos del mecanismo de cifrado:

Enc_Alg: Identificador de objeto adjudicado según ISO/CEI 9979

El valor de este atributo será definido por el ASSR, dados los servicios de seguridad seleccionados. Este atributo implica ciertos atributos del mecanismo de cifrado, tales como la forma y longitud de cualquier campo de sincronización, algoritmos separados de cifrado y descifrado, vectores de inicialización, etc.

Data_Enc_Key: Forma constreñida por el ASSR

Referencia de clave de cifrado para datos normales.

Data_Dec_Key: Forma constreñida por el ASSR

Referencia de clave de descifrado para datos normales.

Exp_Enc_Key: Forma constreñida por el ASSR

Referencia de clave de cifrado para datos acelerados.

Exp_Dec_Key: Forma constreñida por el ASSR

Referencia de clave de descifrado para datos acelerados.

Los valores iniciales de estos atributos «de clave» se fijarán al establecerse la SA y se podrá cambiarlos durante la existencia de la asociación.

NOTA – En futuras versiones de esta Recomendación | Norma Internacional podrán identificarse atributos adicionales específicos al mecanismo; también podrán identificarse atributos adicionales para mecanismos privados.

12.3 Procedimientos

12.3.1 Función de encapsulación

Deberá utilizarse el SA-ID para referenciar una asociación de seguridad. Si la asociación de seguridad no existe, se retornará el error «SA no disponible» y el valor de la cadena de octetos encapsulada será indeterminado.

Si (Encipher es TRUE) se cifrará la cadena de octetos antes de la encapsulación. El algoritmo utilizado será el identificado por Enc_Alg, y la clave utilizada será o bien:

a) Data_Enc_Key si el tipo de unidad de datos = normal, o bien

b) Exp_Enc_Key si el tipo de unidad de datos = acelerado.

Los datos cifrados se retornarán como el resultado de la cadena de octetos encapsulada.

12.3.2 Función de desencapsulación

Si fracasa cualquiera de las comprobaciones siguientes, todas las informaciones de «status» (es decir, estado, situación) pertinentes se fijan a la información de status de seguridad antes de la recepción de este mensaje, con excepción de la información de alarma, auditoría, y/o contabilidad.

Deberá utilizarse el SA-ID para referenciar una asociación de seguridad. Si la asociación de seguridad no existe, se retornará el error «SA no disponible» y el valor de la cadena de octetos encapsulada será indeterminado.

Si (Encipher es TRUE) se descifrará la cadena de octetos encapsulada. El algoritmo de descifrado utilizado será el identificado por Enc_Alg, y la clave utilizada será o bien:

a) Data_Dec_Key si el tipo de unidad de datos = normal, o bien

b) Exp_Dec_Key si el tipo de unidad de datos = acelerado.

El valor de los datos descifrados se retornará como resultado de la cadena de octetos antes de la encapsulación.

13 Estructura y codificación de las PDU

13.1 Introducción

El protocolo NLSP utiliza tres tipos de PDU:

a) PDU de transferencia de datos segura (PDU de SDT);

b) PDU de asociación de seguridad (PDU de SA);

c) PDU de control de la seguridad de la conexión (PDU de CSC).

Se utiliza además un formato de datos no estructurados, sin información PCI, cuando se elige la opción sin encabezamiento para datos protegidos.

Todas las PDU contendrán un número entero de octetos. Los octetos de la PDU se numeran comenzando por el uno (1) y el número aumenta a medida que los octetos se van colocando en la petición de «red subyacente» apropiada. Cuando se utilizan octetos consecutivos para representar un número binario, el octeto de número inferior tiene el valor más significativo. Los bits de un octeto se numeran del uno (1) al ocho (8), siendo el bit uno (1) el de orden inferior.

Cuando, en esta cláusula, se representa una PDU mediante un diagrama:

a) los octetos se muestran con el octeto de número más bajo a la izquierda, o arriba;

b) dentro de un octeto, los bits se muestran con el bit ocho (8) a la izquierda y el bit uno (1) a la derecha.

Los números que aparecen debajo de las casillas indican la longitud de los respectivos campos, en octetos; «var» indica que la longitud del campo es variable.

La presencia o ausencia de un campo «facultativo» (u «opcional») se especificará por los atributos contenidos en la asociación de seguridad.

NOTA – A los efectos de los campos facultativos, el calificativo de facultativo (u opcional) habrá de entenderse en el sentido de que una asociación de seguridad dada podrá requerir la presencia de ciertos campos y la ausencia de otros. Una vez decidida la asociación de seguridad, la presencia o ausencia de cada campo viene determinada por los atributos SA.

13.2 Formato del campo de contenido

El campo de contenido es un formato de campo general para los valores de datos que habrán de colocarse en las PDU definidas en ésta y otras subcláusulas de la presente especificación (véase la Figura 13-1).

Tipo	Longitud	Valor
1	1-3	var

Figura 13-1 – Campo de contenido

El tipo del campo de contenido se fijará a uno de los valores siguientes:

Valor	*Tipo del campo de contenido*
00-5F	Reservado para uso privado
60-9F	Reservado para uso futuro
A0-BF	Reservado para uso del SA-P (véase el Anexo C)
C0-CF	Reservado para uso independiente del mecanismo (véase 13.3.4.3)
D0-FF	Reservado para uso dependiente del mecanismo (véase 13.3.5)

El campo longitud de campo de contenido contendrá la longitud del valor de campo de contenido, en octetos. La longitud de campo de contenido será de uno, dos, o tres octetos:

a) si la longitud es de un octeto, el bit 8 será 0 y los siete bits restantes definirán una longitud de hasta 127 octetos;

b) si la longitud es de dos octetos, el primer octeto se codificará 1000 0001 y el octeto restante definirá la longitud de los campos hasta 255 octetos;

c) si la longitud es de tres octetos, el primer octeto se codificará 1000 0010 y los dos octetos restantes definirán la longitud de los campos hasta 65 535 octetos.

Otros valores del primer octeto están reservados para uso futuro.

El valor del campo de contenido contendrá datos para el campo PDU.

13.3 Datos protegidos

Esta subcláusula describe las PDU utilizadas para transferir datos protegidos. Incluye dos aspectos de las PDU: los que son independientes del mecanismo usado (señalados como genéricos), y los que son específicos al mecanismo soportado por los procedimientos de encapsulación definidos en la cláusula 11 (señalados como específicos al mecanismo). Los que incluyen aspectos tanto genéricos como específicos al mecanismo se señalan como mixtos.

13.3.1 Estructuras de PDU básicas (genéricas)

Se definen dos estructuras de datos para la transferencia de datos segura. La primera es obligatoria para el NLSP-CL; una de las dos debe ser soportada para el NLSP-CO:

a) la PDU de transferencia de datos segura (PDU de SDT) formatada se muestra en la Figura 13-2.

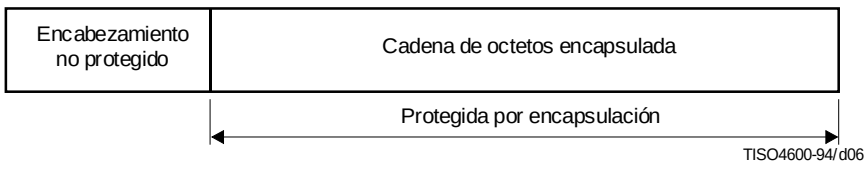


Figura 13-2 – Estructura genérica de la PDU de transferencia de datos segura

La estructura del encabezamiento no protegido se define en 13.3.2. El campo cadena de octetos encapsulada contendrá los datos de salida de una función de encapsulación (por ejemplo, como se describe en la cláusula 11 mediante el empleo de la estructura definida en 13.3.3) que actúa sobre la cadena de octetos antes de la encapsulación, estructurada como se describe en 13.3.4.

Las condiciones (obligatorias, facultativas, etc.) para el soporte de los campos que constituyen esta PDU se definen en D.5.3, D.5.4 (campos específicos al mecanismo), D.6.4 (NLSP-CL solamente) y D.7.6 (NLSP-CO solamente).

b) Una cadena de bits no estructurada, para la opción de confidencialidad sin encabezamiento solamente, formatada como se muestra en la Figura 13-3. No se añade PCI.

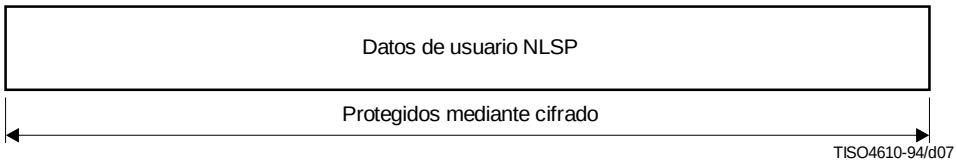


Figura 13-3 – Confidencialidad mediante el uso solamente de la opción sin encabezamiento

La opción sin encabezamiento sólo se utilizará cuando se cumplan todas las condiciones siguientes:

a) No_Header (sin encabezamiento) es TRUE;

b) Label (etiqueta) es FALSE;

c) ICV es FALSE;

d) ISN es FALSE;

e) Encipher (cifrar) es TRUE;

f) Enc_Sync_Len = 0;

g) Enc_Blk = 1;

h) Pad (Relleno) es FALSE.

13.3.2 Encabezamiento no protegido (genérico)

El formato del encabezamiento no protegido será el mostrado en la Figura 13-4.

Id de protocolo	LI	Tipo de PDU	SA-ID
1	1	1	var

Figura 13-4 – Encabezamiento no protegido

13.3.2.1 Identificador de protocolo (genérico)

Este campo contendrá el identificador de protocolo NLSP, valor 1000 1011.

13.3.2.2 LI (indicador de longitud) (genérico)

Este campo contiene la longitud del campo tipo de PDU, más el SA-ID.

Para NLSP-CO no se requiere el campo SA-ID. Por tanto, a este campo se le dará un valor que signifique que el campo SA-ID no está presente (es decir, el valor 00000001).

13.3.2.3 Tipo de PDU (genérico)

Este campo contendrá el valor de tipo de PDU de 01001000 para indicar una PDU de transferencia de datos segura.

13.3.2.4 SA-ID (genérico)

El campo SA-ID contendrá el identificador de la asociación de seguridad de la entidad distante (es decir, el atributo SA Your_SA-ID). Este campo no se necesita en el NLSP-CO.

13.3.3 Cadena de octetos encapsulada (específico al mecanismo)

La estructura de la PDU de SDT que utiliza los procedimientos específicos definidos en la cláusula 13 será la mostrada en la Figura 13-5.

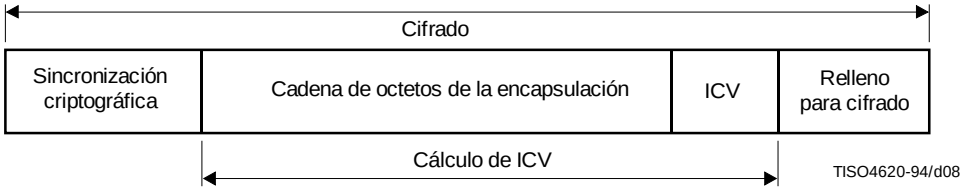


Figura 13-5 – Estructura de la cadena de octetos encapsulada

13.3.3.1 Sincronización criptográfica (específico al mecanismo)

Este es un campo facultativo que puede contener datos de sincronización para algoritmos de cifrado específicos. Su presencia, forma y longitud se obtienen implícitamente de Enc-Alg.

13.3.3.2 Valor de comprobación de la integridad (específico al mecanismo)

Este campo contiene un valor de comprobación de la integridad (ICV, *integrity check value*). La longitud de este campo la definirá el identificador de algoritmo ICV contenido en los atributos de asociación de seguridad.

13.3.3.3 Relleno para el cifrado (específico al mecanismo)

Este campo contiene relleno para el cifrado, destinado a soportar los algoritmos de cifrado de bloque para proporcionar confidencialidad. La elección del valor de relleno es un asunto local. Todas las NLSPE deberán poder descartar este campo. El formato de este campo se codificará sea como se define en 13.2, sea como se define para el algoritmo de cifrado. El código tipo de este campo de TLV será el definido en 13.3.5. Si se requiere un relleno de dos octetos, la longitud será cero con ningún valor. Si se requiere un relleno de un solo octeto, se utilizará un campo de relleno de un solo octeto en lugar de un campo de relleno para el cifrado.

La utilización de este campo depende de que el algoritmo de cifrado requiera o no un relleno para el cifrado independiente.

13.3.4 Cadena de octetos antes de la encapsulación (mixto)

La Figura 13-6 muestra el formato de la cadena de octetos antes de la encapsulación. Contiene un número cualquiera de campos de contenido genéricos y específicos al mecanismo.

Por lo menos los campos longitud de contenido y tipo de datos deberán estar presentes.

Longitud de contenido	Tipo de datos	Campo de contenido (genérico)	. .	Campo de contenido (específico al mecanismo)	. .
2	1	var		var	

Figura 13-6 – Cadena de octetos antes de la encapsulación

13.3.4.1 Longitud de contenido (genérico)

Este campo contendrá la longitud combinada de todos los campos de contenido y del tipo de datos.

NOTA – No incluye los campos ICV ni relleno para el cifrado.

13.3.4.2 Tipo de datos (genérico)

El bit 8 de este campo es la bandera «iniciador a respondedor». El valor 1 indica el sentido de iniciador a respondedor, y el valor 0 el de respondedor a iniciador.

El bit 7 de este campo es la bandera «último/no último», este bit tomará el valor 0 cuando la PDU de SDT contenga el último segmento de una secuencia. De lo contrario tomará el valor 1. Así, para NLSP-CL siempre tomará el valor 0.

Los bits 1-6 de este campo se codifican de modo que indiquen los siguientes parámetros de servicio:

Valor	*Primitiva de servicio*
000000	No relacionado con ninguna primitiva de servicio (por ejemplo, datos de prueba)
000001	pet/ind NLSP-DATOS UNIDAD
000010	pet/ind NLSP-CONEXIÓN
000011	resp/conf NLSP-CONEXIÓN
000100	pet/ind NLSP-DATOS
000101	pet/ind NLSP-ACUSE-DE-DATOS
000110	pet/ind NLSP-DATOS-ACELERADOS
000111	pet/ind NLSP-DESCONEXIÓN
001000	Protocolo SA
001001-011111	Reservados para uso futuro
100000-111111	Reservados para uso privado

13.3.4.3 Campos de contenido (genéricos)

La codificación del tipo de campo de contenido se define como prescribe 13.2. A continuación se indican los campos de contenido independientes del mecanismo (es decir, C0-CF) utilizados por los procedimientos de las cláusulas 6, 7 y 8:

Valor	*Tipo de campo de contenido*
00-BF	Reservado
C0	Datos de usuario
C1	Datos de prueba
C2	Dirección NLSP llamante/de origen
C3	Dirección NLSP llamada/de destino
C4	Dirección NLSP respondedora
C5	No utilizado
C6	Etiqueta
C7	Referencia de etiqueta
C8	Petición de confirmación
C9	Motivo de la desconexión
CA-CF	Reservado para uso futuro
D0-FF	Reservado

13.3.4.3.1 Datos de usuario NLSP

Este campo contiene los datos de usuario NLSP de la primitiva de servicio.

13.3.4.3.2 Datos de prueba

La estructura de los datos de prueba será la mostrada en la Figura 13-7.

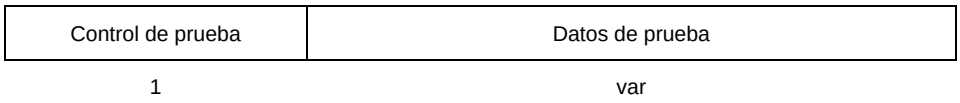


Figura 13-7 – Datos de prueba

El campo control de prueba contiene un conjunto de bits adjudicados como sigue:

a) Bit 1 – Bandera del sentido de transmisión. 0 indica datos de prueba originales y 1 datos de prueba reflejados.

b) Bits 2-4 – Reservados para uso futuro.

c) Bits 5-8 – Reservados para uso privado.

13.3.4.3.3 Dirección NLSP llamante/de origen

Este campo contiene una dirección de capa de red codificada en una de las formas descritas en la Rec. X.213 del CCITT | ISO 8348/AD2.

13.3.4.3.4 Dirección NLSP llamada/de destino

Este campo contiene una dirección de capa de red codificada en una de las formas descritas en la Rec. X.213 del CCITT | ISO 8348/AD2.

13.3.4.3.5 Dirección NLSP respondedora

Este campo contiene una dirección de capa de red codificada en una de las formas descritas en la Rec. X.213 del CCITT | ISO 8348/AD2.

13.3.4.3.6 Etiqueta

Este campo se utiliza para transportar la etiqueta de seguridad de una PDU. No está presente si el campo de contenido referencia de etiqueta está presente (véase la Figura 13-8).

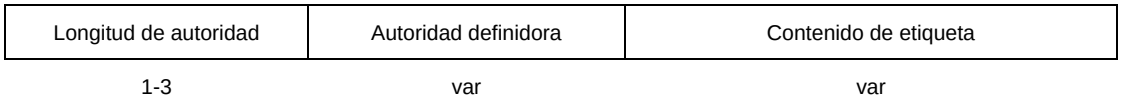


Figura 13-8 – Valor de etiqueta

La autoridad definidora se codificará como el contenido de un valor de identificador de objeto mediante las reglas de codificación básica de un identificador de objeto definido en la cláusula 22 de la Rec. X.209 del CCITT | ISO 8825.

La estructura y la interpretación del contenido de la etiqueta se definen por diversas autoridades definidoras.

NOTA – Se espera que estas etiquetas se registren de acuerdo con los procedimientos definidos por la UIT-T y la ISO/CEI. Una autoridad definidora se registrará como un identificador de objeto mediante los procedimientos definidos en ISO/CEI 9834.

13.3.4.3.7 Referencia de etiqueta

Este procedimiento identifica una de las etiquetas que forman un conjunto de etiquetas de seguridad definido en el atributo de SA Label_Set (conjunto de etiquetas). Cuando está presente, este campo se codifica siempre de modo que la parte del campo referente al valor sea dos octetos. Este campo no estará presente si está presente un campo de contenido de etiqueta.

13.3.4.3.8 Petición de confirmación

Cuando está presente, este campo indica que se ha solicitado la confirmación de la recepción. Este campo se codificará como un código de tipo de un octeto (sin longitud ni valor).

13.3.4.3.9 Motivo de la desconexión

Este campo transporta el parámetro de servicio motivo de la NLSP-DESCONEXIÓN, con la misma codificación que tiene cuando se transporta en la red subyacente.

NOTA – Cuando la red subyacente es una red conforme a la Rec. X.25 del CCITT | ISO 8208, el primer octeto del valor es la causa y, si está presente, el segundo octeto es el código de diagnóstico obtenido por la correspondencia con el motivo de la NLSP-DESCONEXIÓN definido en la Rec. X.223 del CCITT | ISO 8878.

13.3.5 Campos de contenido (específicos al mecanismo)

La codificación de los campos de contenido se efectuará como se define en 13.2. A continuación se indica la codificación de tipo de campo de contenido para los campos de contenido específicos al mecanismo:

Valor	*Tipo de campo de contenido*
00-CF	Reservado
D0	Número secuencial
D1	Relleno de un solo octeto
D2	Relleno para el tráfico
D3	Relleno para la integridad
D4	Relleno para el cifrado
D5-FF	Reservado para uso futuro

13.3.5.1 Número secuencial

Este campo contiene Your_ISN (es decir, un número secuencial para la integridad de la PDU) que será único dentro de la clave actual para ese tipo de datos (acelerados o normales).

NOTA – En el protocolo NLSP CO, la unicidad entre los flujos de datos acelerados y los flujos de datos normales (y en consecuencia la protección contra la reproducción fraudulenta) la proporciona el hecho de que el campo tipo de datos es diferente (véase 13.3.4.2).

13.3.5.2 Relleno de un solo octeto

Este campo será un campo de tipo de un octeto (sin longitud ni valor) para el relleno general (por ejemplo, para soportar un solo octeto de relleno para la integridad). Este octeto puede utilizarse una o más veces, en lugar de un campo de relleno para integridad, cifrado o tráfico, con codificación TLV, para proporcionar relleno para la integridad, el cifrado, o el tráfico. Todas las NLSPE deberán detectar y descartar este campo.

13.3.5.3 Relleno para el tráfico

Este campo contiene relleno para fines de confidencialidad del flujo de tráfico. La elección del valor de relleno es un asunto local. Todas las NLSPE deberán detectar y descartar este campo. Si se requiere un relleno de dos octetos, la longitud será cero con ningún valor. Si se requiere un relleno de un solo octeto se utilizará un campo de relleno de un solo octeto, y no el campo de relleno para el tráfico.

13.3.5.4 Relleno para la integridad

Este campo contiene el relleno para soportar algoritmos de integridad de bloque. La elección del valor de relleno es un asunto local. Todas las NLSPE deberán detectar y descartar este campo. Si se requiere un relleno de dos octetos, la longitud será cero con ningún valor. Si se requiere un relleno de un solo octeto se utilizará un campo de relleno de un solo octeto, y no el campo de relleno para la integridad.

Este campo puede utilizarse también para satisfacer las exigencias de relleno para el cifrado.

13.4 PDU de asociación de seguridad

El formato de la PDU de asociación de seguridad será el indicado en la Figura 13-9.

Las condiciones (obligatorias/facultativas, etc.) para uso con los campos que constituyen esta PDU se definen en D.5.5 y D.5.6 (campos específicos al mecanismo).

Identificador de protocolo	LI	Tipo de PDU	SA-ID	Tipo de SA-P	Contenido de PDU de SA
1	1	1	var	1	var

Figura 13-9 – Estructura de la PDU de asociación de seguridad

13.4.1 Identificador de protocolo

Este campo contendrá el identificador de protocolo NLSP, valor 10001011.

13.4.2 Indicador de longitud (LI)

Este campo contendrá la longitud del campo tipo de PDU más el campo SA-ID.

Si el SA-P necesita señalar que no conoce el SA-ID de su entidad par (por ejemplo, al establecer una SA), este campo se fijará al valor 00000001 para indicar que el campo SA-ID no está presente.

13.4.3 Tipo de PDU

Este campo contendrá el valor 01001001 para indicar una PDU de asociación de seguridad.

13.4.4 SA-ID

Este campo contendrá el identificador de asociación de seguridad de la entidad distante (es decir, el atributo SA Your_SA-ID). Este campo no se requiere cuando se está utilizando el SA-P para establecer una nueva SA (es decir, cuando todavía no se ha asignado un SA-ID al receptor).

13.4.5 Tipo de SA-P

Este campo contendrá un identificador de objeto que indica el mecanismo utilizado para proporcionar el protocolo SA. Este identificador de objeto será codificado como el contenido del valor de identificador de objeto mediante las reglas de codificación básica definidas en la cláusula 22 de la Rec. X.209 del CCITT | ISO/CEI 8825.

El siguiente identificador de objeto se asigna para uso del SA-P genérico con procedimientos de intercambio de testigos de clave, definidos en el Anexo C, junto con el algoritmo de intercambio de clave exponencial descrito en el Anexo H:

joint-ccitt-iso nlsp (22) sa-p-kte (1) eke (1)

La utilización de otros protocolos o algoritmos con el SA-P definido en el Anexo C se puede indicar por otros identificadores de objeto adjudicados de acuerdo con ISO/CEI 9834-1.

13.4.6 Contenido de la PDU de SA

La estructura interna de este campo depende del mecanismo que proporciona el protocolo SA, como se especifica en 13.4.5. En el Anexo C se define tal protocolo SA.

13.5 PDU de control de la seguridad de la conexión

El formato de la PDU de control de la seguridad de la conexión se muestra en la Figura 13-10.

Las condiciones (obligatorias/facultativas, etc.) para el soporte de los campos que constituyen esta PDU se definen en D.7.7 y D.7.8 (campos específicos al mecanismo).

Identificador de protocolo	LI	Tipo de PDU	SA-ID	Longitud de contenido	Contenido de la PDU de CSC
1	1	1	var	1	var

Figura 13-10 – PDU de control de la seguridad de la conexión

13.5.1 Identificador de protocolo

Este campo contiene el identificador de protocolo NLSP, valor 1000 1011.

13.5.2 Identificador de longitud (LI)

Este campo contiene la longitud del campo tipo de PDU más la del campo SA-ID.

13.5.3 Tipo de PDU

Este campo contiene el valor de tipo de PDU de xx111111 para indicar una PDU de control de la conexión de seguridad. Los valores de los bits de este campo son los siguientes:

a) Los bits 1-6 contienen el valor de tipo de PDU de 111111 para indicar una PDU de control de la conexión de seguridad.

b) El bit 7 contiene la bandera UNC-UND; si está puesta, indica que la NLSP-CONEXIÓN está transportándose en UN-DATOS; en caso contrario, es decir, si está anulada, indica que la NLSP-CONEXIÓN se está transportando en la UN-CONEXIÓN.

c) El bit 8 contiene la bandera SA-P e indica que se está invocando SA-P en una conexión; si está puesta, no hay más ningún otro campo presente en esta PDU.

13.5.4 SA-ID

Este campo contiene el identificador de asociación de seguridad de la entidad distante (es decir, el atributo SA Your_SA-ID). Este campo no estará presente si está puesta la bandera SA-P.

13.5.5 Longitud de contenido

Este campo contiene la longitud del contenido de la PDU de CSC, en octetos. Este campo no estará presente si está puesta la bandera SA-P.

13.5.6 Contenido de la PDU de CSC

La estructura interna de este campo depende del mecanismo que soporta la autenticación de la conexión. Este campo no estará presente si está puesta la bandera SA-P. Los campos requeridos para el mecanismo de control de seguridad específico descrito en la cláusula 10 son los siguientes (véase la Figura 13-11):

Datos de autenticación cifrados	Información de clave
(Nota 1)	(Nota 2)

NOTAS

1 El contenido de los datos de autenticación cifrados (Enciphered-Auth-Data) depende del algoritmo de cifrado utilizado, definido por el Atributo SA Enc_Auth_len.

2 La longitud de la información de clave depende del método utilizado para la distribución de las claves. No se incluye si no se cambia la clave.

Figura 13-11 – Contenido de la PDU de CSC

13.5.7 Datos de autenticación cifrados (específico al mecanismo)

Véase la Figura 13-12.

Este campo contiene un número que se utiliza para autenticación y, si se selecciona, como un número secuencial para la integridad, su longitud se define como parte de los atributos SA. Cuando se envía de la entidad NLSP llamante a la llamada, Your-Initial-ISN es 0.

Figura 13-12 – Datos de autenticación cifrados

13.5.8 Información de clave (específico al mecanismo)

Según el método de distribución de claves («kdm», *key distribution method*) seleccionado para uso en la asociación de seguridad, este parámetro, o bien no está presente, lo que indica que no se va a utilizar una clave existente, o está presente y adopta una de las modalidades siguientes, que dependen del kdm atribuido a la SA:

kdm_mutual:	Una clave cifrada utilizando KEK mutuo.
kdm_asymmetric_single:	Una clave cifrada con la clave pública del receptor.
kdm_asymmetric_double:	Una clave cifrada con la clave privada del emisor de la clave pública del receptor.
kdm_distributed:	Una referencia de clave.
kdm_other:	Contenido definido privadamente.

La presencia de este campo se obtiene implícitamente de la comparación de longitud de contenido con el atributo SA Enc_Auth_len.

14 Conformidad

14.1 Requisitos de conformidad estática

14.1.1 Clases de conformidad

El sistema soportará una de las dos clases de conformidad siguientes, o las dos:

a) NLSP en modo sin conexión (NLSP-CL);

b) NLSP en modo conexión (NLSP-CO).

El soporte de estas clases de conformidad se define atendiendo a las capacidades definidas en 14.1.2 y 14.1.3.

El soporte de cada una de estas clases de conformidad se proporcionará mediante el empleo de los mecanismos de seguridad especificados en esta Recomendación | Norma Internacional.

La utilización de mecanismos de seguridad especificados en esta Recomendación | Norma Internacional se define sobre la base de los requisitos que deben cumplir los mecanismos de seguridad de acuerdo con lo prescrito en 14.1.5.

14.1.2 Capacidades del NLSP en modo sin conexión (NLSP-CL)

14.1.2.1 Servicios de seguridad

Un sistema conforme con el NLSP en modo sin conexión (NLSP-CL) soportará los siguientes servicios:

a) Uno o más de los siguientes servicios:

1) confidencialidad en modo sin conexión;

2) integridad en modo sin conexión;

3) autenticación del origen de datos.

b) Facultativamente, control de acceso.

c) Facultativamente, confidencialidad del flujo de tráfico.

14.1.2.2 Alcance de la protección

Un sistema que pretende la conformidad con el NLSP-CL deberá soportar:

a) la protección de todos los parámetros del servicio NLSP; y/o

b) la protección de los datos de usuario NLSP.

Un sistema que pretenda la conformidad con el NLSP-CL podrá soportar facultativamente:

c) la ausencia de protección.

14.1.2.3 Otras capacidades

Cuando un sistema soporta el modo NLSP-CL deberá poder transmitir y/o recibir una PDU de SDT.

14.1.3 Capacidades del modo NLSP-CO

14.1.3.1 Servicios de seguridad

Un sistema conforme con el NLSP en modo conexión (NLSP-CO) soportará los siguientes servicios de seguridad:

a) Uno o más de los siguientes servicios:

1) confidencialidad de la conexión;

2) integridad de la conexión sin recuperación;

3) autenticación de la entidad par.

b) Facultativamente, control de acceso.

c) Facultativamente, confidencialidad del flujo de tráfico.

14.1.3.2 Alcance de la protección

Un sistema que pretende la conformidad con el NLSP-CO deberá soportar:

a) la protección de todos los parámetros del servicio NLSP; y/o

b) la protección de los datos de usuario NLSP, incluidos los datos de usuario en NLSP-CONEXIÓN y NLSP-DESCONEXIÓN;

c) la protección de los datos de usuario durante la transferencia de datos.

Un sistema que pretenda la conformidad con el NLSP-CL podrá soportar facultativamente:

d) la ausencia de protección.

14.1.3.3 Otras capacidades

Cuando un sistema soporta el modo NLSP-CO podrá:

a) iniciar y/o aceptar una conexión;

b) transmitir y recibir una PDU de CSC;

c) transmitir y/o recibir datos de por lo menos una de estas dos cosas:

1) datos protegidos mediante el mecanismo de encapsulación basado en sin encabezamiento, definido en 6.4.1.2 y 6.4.2.2;

2) datos protegidos por la encapsulación basada en la PDU de SDT, según lo definido en 6.4.1.1 y 6.4.2.1;

d) funcionar en, por lo menos, uno de los modos de establecimiento de la conexión NLSP definidos en 8.5;

e) facultativamente, soportar intercambios de prueba;

f) facultativamente, soportar un protocolo SA dentro de banda.

14.1.4 Soporte de las PDU

El Cuadro 14-1 muestra si el soporte de distintas PDU es obligatorio o facultativo para un modo de operación dado.

Cuadro 14-1 – Soporte del NLSP para las distintas PDU

PDU	Condiciones para el soporte
UPD de SDT	Obligatorio en el modo sin conexión Obligatorio si se trata del modo conexión y se soporta la encapsulación basada en la PDU de SDT
PDU de SA	Facultativo si se soporta el SA-P
PDU de CSC	Obligatorio en el caso de NLSP-CO

14.1.5 Requisitos de conformidad estática con respecto al mecanismo seleccionado

Un sistema que pretenda soportar los mecanismos de seguridad definidos en esta Recomendación | Norma Internacional deberá cumplir los siguientes requisitos con respecto al mecanismo seleccionado:

a) Todo sistema que pretenda soportar servicios de seguridad de confidencialidad en el modo conexión o sin conexión proporcionará esos servicios mediante el empleo de un mecanismo de cifrado.

b) Todo mecanismo que pretenda soportar servicios de seguridad para la integridad en modo sin conexión, o en modo con conexión sin recuperación, proporcionará esos servicios mediante el empleo de un mecanismo que utilice el campo ICV definido en 13.3.3.2 y, facultativamente, el campo ISN definido en 13.3.5.1.

c) Todo sistema que pretenda soportar el servicio de seguridad de confidencialidad del flujo de tráfico proporcionará ese servicio mediante el empleo de un mecanismo que utilice el campo de relleno de tráfico definido en 13.3.5.3.

d) Todo sistema que pretenda soportar el servicio de seguridad de autenticación del origen de datos proporcionará dicho servicio, o bien mediante el empleo de un mecanismo de cifrado, o de un mecanismo criptográfico que utiliza el campo ICV definido en 13.3.3.2.

e) Todo sistema que pretenda soportar el servicio de seguridad de autenticación de la entidad par soportará el campo de datos de autenticación cifrados, definido en 13.5.7.

14.2 Requisitos de conformidad dinámica

14.2.1 Requisitos generales

a) El sistema generará, aceptará y responderá correctamente a todos los elementos de protocolo válidos que soportan cada clase y cada modo de operación con respecto a los cuales se pretende la conformidad.

b) El sistema responderá correctamente a todas las secuencias incorrectas de elementos de protocolo NLSP.

14.2.2 Requisitos específicos

Para cada clase de conformidad con respecto a la cual se pretenda la conformidad y para cada opción de los requisitos de conformidad estática implementada, el sistema exhibirá un comportamiento externo consecuente con el hecho de haber implementado lo siguiente:

a) las funciones de protocolo comunes definidas en la cláusula 6;

b) para el modo NLSP-CL, las funciones de protocolo definidas en la cláusula 7;

c) para el modo NLSP-CO, las funciones de protocolo definidas en la cláusula 8;

d) para los sistemas NLSP-CL que soportan procedimientos específicos al mecanismo, las funciones de protocolo definidas en la cláusula 11;

e) para los sistemas NLSP-CO que soportan procedimientos específicos al mecanismo, las funciones de protocolo para el control de seguridad de la conexión definidas en la cláusula 10, y las funciones de protocolo para la encapsulación definidas en la cláusula 11 o en la 12;

f) la estructura y la codificación de las PDU descritas en la cláusula 13, estructura y codificación de las PDU.

14.3 Enunciado de conformidad de implementación de protocolo

Deberá establecerse un enunciado de conformidad de implementación de protocolo (PICS), descrito en el Anexo D, con respecto a toda pretensión de conformidad de una implementación con esta Recomendación | Norma Internacional. El enunciado PICS se establecerá de acuerdo con el formulario (o proforma) PICS apropiado.

Anexo A

Correspondencia de las primitivas UN con las de la Rec. X.213 del CCITT | ISO 8348

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

Cuadro A.1

Primitiva UN	Transportada por	Comentarios
UN-DATO UNIDAD (UN-UNITDATA)	N-DATO UNIDAD (N-UNITDATA)	Correspondencia simple de la primitiva UN con la primitiva N-DATO UNIDAD de la Rec. X.213 del CCITT | ISO 8348 AD1
UN-CONEXIÓN (UN-CONNECT)	N-CONEXIÓN (N-CONNECT)	Los parámetros se han hecho corresponder con parámetros de la Rec. X.213 del CCITT | ISO 8348 equivalentes, excepto: – UN autenticación concatenada con UN datos de usuario, que se ha hecho corresponder con datos de usuario en las primitivas N-CONEXIÓN
UN-DATOS (UN-DATA)	N-DATOS (N-DATA)	Correspondencia simple: todos los parámetros se han hecho corresponder con parámetros equivalentes de la Rec. X.213 del CCITT | ISO 8348
UN-DATOS ACELERADOS (UN-EXPEDITED-DATA)	N-DATOS ACELERADOS (N-EXPEDITED-DATA)	Correspondencia simple
UN-ACUSE DE DATOS (UN-DATA-ACKNOWLEDGE)	N-ACUSE DE DATOS (N-DATA-ACKNOWLEDGE)	Correspondencia simple
UN-DESCONEXIÓN (UN-DISCONNECT)	N-DESCONEXIÓN (N-DISCONNECT)	Correspondencia simple

Anexo B

Correspondencia de las primitivas UN con las de la Rec. X.25 del CCITT | ISO 8208

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

En los entornos OSI, la correspondencia entre las primitivas de servicio UN y el protocolo de la Rec. X.25 del CCITT o ISO 8208 se define en ISO 8878 para las primitivas de los servicios de capa de red equivalentes, con excepción del parámetro autenticación UN de la primitiva UN-CONEXIÓN, que se transporta en la «facilidad de protección» del DTE.

En el Cuadro B.1, la columna central describe los paquetes X.25 o ISO 8208 utilizados para transportar las primitivas UN. En este caso se puede utilizar la X.25 o ISO 8208 de cualquier manera permitida por la presente Recomendación | Norma Internacional y, por ejemplo, se puede invocar el bit Q. Tales prestaciones específicas X.25 o ISO 8208 pasan a través del protocolo NLSP sin sufrir cambios.

Cuadro B.1

Primitiva UN	Transportada por	Comentarios
UN-DATO UNIDAD (UN-UNITDATA)	N/A	
UN-CONEXIÓN (UN-CONNECT)	LLAMADA (CALL)	Todos los parámetros se han hecho corresponder con facilidades equivalentes del paquete LLAMADA X.25 | ISO 8208, excepto el parámetro autenticación UN, que se transporta en la «facilidad de protección» del DTE
UN-DATOS (UN-DATA)	DATOS (DATA)	Correspondencia simple
UN-DATOS ACELERADOS (UN-EXPEDITED-DATA)	INTERRUPCIÓN (INTERRUPT)	Correspondencia simple
UN-ACUSE DE DATOS (UN-DATA-ACKNOWLEDGE)	RR o RNR	Correspondencia simple
UN-DESCONEXIÓN (UN-DISCONNECT)	LIBERACIÓN (CLEAR)	Correspondencia simple

Anexo C

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)

C.1 Visión de conjunto

Este anexo define un protocolo para la utilización de un mecanismo asimétrico con el fin de efectuar el establecimiento y el aborto/liberación de una asociación de seguridad. El protocolo permite a las entidades NLSP 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 para establecer un secreto compartido. Se soporta así un intercambio de testigos de clave. La forma de estos testigos es específica a cada mecanismo. En el Anexo H 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 NLSP 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 soportado 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 NLSP para firmar datos con fines de autenticación.

c) Un certificado de una autoridad de confianza para cada algoritmo asimétrico soportado que identifica la entidad NLSP, 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 NLSP con las que esta entidad NLSP 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 utilizado 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 NLSP:

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 NLSP 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.

C.2 Intercambio de testigos de clave (KTE)

Las entidades NLSP 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 NLSP 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 (KTE, *key token exchange*) 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 H. 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.

C.3 Autenticación de protocolo SA

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

Las entidades NLSP intercambian certificados y firmas digitales (como los definidos en la Rec. X.509 del CCITT | ISO/CEI 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 NLSPE más la clave pública de la entidad.

El certificado lo establece una autoridad de confianza y se proporciona al NLSP mediante un procedimiento que está fuera del ámbito del protocolo NLSP. El certificado contiene la firma de autenticación de la autoridad de confianza. Una entidad NLSP 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 | Norma Internacional. Para que una entidad NLSP 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 incluyendo el certificado de A y Key-Token-3 (calculado utilizando un algoritmo como el descrito en el Anexo H) y luego se firma (utilizando por ejemplo, la firma de autenticación definida en la Rec. X.509 del CCITT | ISO/CEI 9594-8). Esta firma excluye el ID de intercambio y la longitud del contenido. Se cifra entonces el contenido de la CA, incluyendo la firma y la longitud del contenido, pero excluyendo el ID de intercambio. La clase de cifrado consiste en los *n* primeros bits de la cadena de bits producida por el cambio de KTE, donde *n* es el número de bits requeridos para el algoritmo utilizado.

b) Se crea el contenido de la SA de modo que transporte la negociación de atributo SA (véase C.4) o los motivos para el aborto/liberación (véase C.5). Este contenido se firma y cifra entonces como se ha indicado en a) utilizando la información equivalente relativa a B y Key-Token-4 en vez de Key-Token-3.

Cada entidad verifica la firma de autenticación de la entidad par descifrando primero los datos recibidos en el intercambio, y luego verificando el Key-Token para protección contra los ataques de respuesta. La verificación requiere la utilización de la clave pública de la entidad par, y el proceso convenido para verificación de firma.

C.4 Negociación de atributo SA

C.4.1 Selección de servicio de seguridad

Como una decisión local, la entidad NLSP 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.

Como una decisión local, la entidad NLSP 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 que indicará el motivo por el que se rechaza la SA.

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

C.4.2 Negociación de conjunto de etiquetas

De acuerdo con su política de seguridad local, la entidad NLSP iniciadora envía un conjunto de etiquetas de seguridad y un conjunto de referencias que desea que se transfieran bajo la protección de esta SA. Cada elemento del conjunto contiene lo siguiente:

a) una referencia que se puede transportar posteriormente en lugar de la etiqueta durante la existencia de la SA, por razones de eficiencia; y

b) la semántica completa de la etiqueta.

De acuerdo con su política de seguridad local, la entidad NLSP receptora determinará cuál o cuáles de las etiquetas del conjunto propuesto desea que se transfieran bajo la protección de esta SA. La entidad 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 NLSP seleccionar un conjunto de etiquetas que se ajuste a su política de seguridad local.

C.4.3 Selección de clave y de ISN

Como una decisión local, la entidad NLSP iniciadora selecciona las porciones de la cadena de bits resultante del intercambio KTE que habrán de utilizarse como claves y/o ISN durante las comunicaciones (dicho sea con más precisión, comunicaciones NLSP, y no comunicaciones de protocolo SA) con destino a la entidad NLSP 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 EKE. La longitud de la clave/ISN se determina a partir de los parámetros asociados con el servicio seleccionado. Se envía a la entidad NLSP receptora un conjunto de punteros, para lo siguiente:

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 NLSP receptora determinará localmente qué porciones de la cadena de caracteres resultante del intercambio EKE va a utilizar para sus claves/ISN. La entidad NLSP receptora retornará al originador la siguiente información PCI:

a) si el receptor opta por utilizar las mismas posiciones de bit propuestas por la entidad NLSP 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.

NOTAS

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

2 No es necesario emplear este procedimiento si se conocen de antemano las posiciones para seleccionar las claves e ISN.

C.4.4 Negociación de diversos atributos SA

Como una decisión local, la entidad NLSP iniciadora determina el valor de los siguientes atributos SA para la SA que se está estableciendo:

a) retener estos atributos SA cuando se efectúe la desconexión (NLSP-CO solamente);

b) proteger los parámetros del modo conexión (NLSP-CO solamente);

c) se debe utilizar la opción «sin encabezamiento» (NLSP-CO solamente);

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

Como una decisión local, la entidad NLSP 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 NLSP 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.

C.4.5 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 del servicio, el conjunto de etiquetas y la negociación de atributos SA diversos, se coloca en «Old-your-SA-ID» la referencia a la antigua SA de la cual habrán de heredarse estos atributos.

C.5 Aborto/liberación de la SA

Una entidad puede indicar que ya no está utilizando una asociación de seguridad mediante un intercambio bidireccional de PDU de SA, con un código de motivo firmado y cifrado según los procedimientos definidos en C.3.

C.6 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 EKE 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 C.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 C.3.

C.6.1 (Primer) Intercambio KTE

C.6.1.1 Petición de inicio de protocolo SA

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

La entidad NLSP 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.

NOTAS

1 Los servicios de seguridad de confidencialidad seleccionados deben identificar solamente un algoritmo de cifrado simétrico y su modo de operación. Los servicios de seguridad de integridad seleccionados deben identificar solamente un algoritmo asimétrico y su esquema de firma digital asociada.

2 La información a que se refieren los anteriores apartados c) y d) puede 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 NLSP iniciadora retransmite su PDU del primer intercambio. Las retransmisiones están limitadas a un número finito, que se fija localmente.

C.6.1.2 Recepción de la primera PDU de SA por la entidad receptora

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

a) El «My_SA-ID» recibido se coloca en el campo «Your_SA-ID» del encabezamiento genérico descrito en 13.4.

b) Se selecciona un SA-ID disponible y se envía como el My_SA-ID del originador.

c) Como una decisión local, la entidad NLSP 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) Como una decisión local, la entidad NLSP receptora retorna al originador la siguiente información PCI:

1) Si el receptor acepta uno de los mecanismos de integridad 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 integridad 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 NLSP 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.

C.6.2 (Segundo) Intercambio para la negociación de autenticación y seguridad

C.6.2.1 Recepción de la primera PDU de SA por la entidad iniciadora

Al recibir la primera PDU de SA, la entidad NLSP iniciadora ejecuta las siguientes funciones:

a) el «My_SA-ID» recibido se coloca en el campo «Your_SA-ID» del encabezamiento genérico descrito en 13.4;

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

c) la entitad iniciadora genera Key-Token-1;

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 NLSP;

e) se coloca en Label_Def un conjunto de etiquetas propuestas que podrían protegerse utilizando esta SA durante una comunicación NLSP;

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 C.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 NLSP 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.

C.6.2.2 Recepción de la PDU del segundo intercambio por la entidad receptora

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

a) El My_SA-ID recibido se coloca en el campo Your_SA-ID del encabezamiento genérico, como se describe en 13.4.

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 de Key-Token-3 recibida.

   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, se copia la SA apropiada desde el SA-ID referenciado. En este caso no puede enviarse la utilización de los campos descritos a continuación en los apartados c) y d).

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 NLSP. Si el conjunto de servicios propuestos sólo contenía un elemento no se retorna PCI.

c) La entitad receptora genera Key-Token-4.

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

e) Un conjunto de punteros a clave/ISN. Si las claves propuestas por el iniciador para uso por el respondedor son aceptables no se envía nuevos valores.

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

C.6.3 Intercambio de liberación/aborto

C.6.3.1 Petición de inicio de la liberación/aborto de una SA

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

a) Si la entitad local es el iniciador del establecimiento de la SA, se genera Key-Token-3 o bien Key-Token-4. En ambos casos el testigo (*token*) 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 C.3.

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

C.6.3.2 Recepción de una petición de aborto/liberación de la SA

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

a) Si la entitad local es el iniciador del establecimiento de la SA, se genera Key-Token-3 o bien Key-Token-4. En ambos casos 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 C.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.

C.7 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 13.4, se muestra en la Figura C.1.

Identificador de intercambio	Longitud de contenido	Campo de contenido	Campo de contenido	. . .
1	2	var	var	var

Figura C.1 – Contenido de la SA

C.7.1 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, 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.

C.7.2 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.

C.7.3 Campos de contenido

La codificación del tipo de campo de contenido se define en 13.2. A continuación se indican los campos de contenido SA-P (es decir, A0-BF) utilizados en los procedimientos descritos en este anexo de la especificación.

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	Autenticación de firma digital	
A5	Certificado de autenticación	
A6	Selección de servicio	
A7	Motivo de rechazo de la SA	
A8	Motivo de aborto/liberación de la SA	
A9	Label-Def	
AA	Banderas de SA	
AB	Selección de clave	
AC	ASSR	
AD	Key-Token-3	
AE	Key-Token-4	
AD-BF	Reservados para uso futuro	

NOTA – En 13.2 del cuerpo principal de esta Recomendación | 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.

C.7.3.1 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.

C.7.3.2 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.

C.7.3.3 Key-Token-1, Key-Token-2, Key-Token-3 y Key-Token-4

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

C.7.3.4 Certificado de autenticación, firma digital de autenticación

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

C.7.3.5 Selección de servicios

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

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

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

Este campo deberá seguir a una aparición del parámetro ASSR y 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 desaparecen están relacionados con los servicios que tienen el valor 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 sin recuperación
3	Autenticación del origen de datos/autenticación de entidad par
4	Control de acceso
5	Confidencialidad del flujo de tráfico

C.7.3.6 Motivo del rechazo

Este campo puede estar presente en la PDU del primer o del segundo intercambio. Su presencia indica el rechazo de la SA en la 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	Confidencialidad del flujo de tráfico no soportada
6	Mecanismo de confidencialidad rechazado
7	Mecanismo de integridad rechazado
8	Mecanismo de control de acceso rechazado
9	Mecanismo de autenticación rechazado
10	Confidencialidad del flujo de tráfico rechazada
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	«Sin encabezamiento» rechazado

C.7.3.7 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.

C.7.3.8 Label-Def

Este campo facultativo sólo se utiliza en la PDU del segundo intercambio. Puede incluirse una o más veces para:

a) Proponer un conjunto de etiquetas de seguridad, si lo utiliza el originador. El iniciador deberá siempre utilizar los dos subcampos.

b) Seleccionar un subconjunto del subconjunto de etiquetas propuesto, si lo utiliza el receptor. El receptor sólo utilizará el subcampo Label_Ref.

El campo Label-Def se divide en dos subcampos:

a) un subcampo Label_Ref de dos octetos (no se utilizará el valor FF FF hex por estar reservado para una referencia nula);

b) un subcampo Label, cuyo contenido se define en 13.3.4.3.7.

Label_Ref es un número asociado con la etiqueta de seguridad definida en el subcampo Label. Label_Ref se utiliza en otras PDU como una alternativa a llevar la etiqueta de seguridad asociada.

C.7.3.9 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 (dos octetos);

b) información de selección de clave (dos octetos);

c) referencia de clave (longitud variable).

C.7.3.9.1 Banderas de utilización

Este subcampo contiene banderas que indican los fines de seguridad para los cuales se va a utilizar la clave definida en los subcampos precedentes. Los bits se codifican de modo que el valor 0 signifique FALSE (falso) y el valor 1 TRUE (verdadero). La clave puede utilizarse para cualquier combinación de los fines siguientes. Las combinaciones admisibles dependerán de la política de seguridad local.

Bit N.º	*Servicio*	*Datos*	*Origen de los datos*
Octeto 1:			
1	Confidencialidad	Normales	Iniciador SA
2	Confidencialidad	Normales	Respondedor SA
3	Confidencialidad	Acelerados	Iniciador SA
4	Confidencialidad	Acelerados	Respondedor SA
5	Generación de ICV	Normales	Iniciador SA
6	Generación de ICV	Normales	Respondedor SA
7	Generación de ICV	Acelerados	Iniciador SA
8	Generación de ICV	Acelerados	Respondedor SA
Octeto 2:			
1	Autenticación		Iniciador SA
2	Autenticación		Respondedor SA
3	ISN	Normales	Iniciador SA
4	ISN	Normales	Respondedor SA
5	ISN	Acelerados	Iniciador SA
6	ISN	Acelerados	Respondedor SA

El respondedor puede contraordenar selecciones para uso propio.

C.7.3.9.2 Información de selección de clave

Este campo indica la posición dentro de la cadena de bits que se obtiene como resultado de un intercambio EKE donde un bit seleccionado deberá 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.

C.7.3.9.3 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 de una conexión en que se emplee la PDU de control de la seguridad de la conexión. El valor de esta referencia deberá ser único para la asociación de seguridad.

C.7.3.10 Banderas de la SA

Este campo facultativo sólo se utiliza en la PDU del segundo intercambio. 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_Prot)
3	Sin encabezamiento (No_Header)
4-8	Reservados para uso futuro

Los bits 4-8 se ponen a 0 en transmisión y no se tienen en cuenta en recepción.

C.7.3.11 ASSR

Este campo tiene que estar presente si lo está el campo de selección de servicio. El identificador de objeto (definido en ISO/CEI 9834-3) identifica el conjunto de reglas de seguridad que definen el mecanismo que va a aplicarse para una determinada calidad de servicio de protección seleccionada.

Este campo puede aparecer más de una vez, en cuyo caso los parámetros de selección de servicio que siguen a cada aparición se relacionan con el parámetro ASSR que le precede inmediatamente.

Anexo D

Formulario PICS NLSP [2)]

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

D.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this ITU-T Recommendation | International Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

- by the protocol implementor, as a check-list to reduce the risk of failure to conform to the standard through oversight;
- by the supplier and acquirer – or potential acquirer – of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- by the user – or potential user – of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);

---

2) Comunicado sobre derechos de autor del formulario de PICS.

Los usuarios de esta Recomendación | Norma Internacional 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.

- by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

D.2 Abbreviations and Special Symbols

D.2.1 Status Symbols

M Mandatory

O Optional

O.<n> Optional, but support of at least one of the group of options labelled by the same numeral <n> is required

X Prohibited

<item> Conditional-item symbol, dependent upon the support marked for <item> (see D.3.4)

D.2.2 General Abbreviations

N/A Not applicable

PICS Protocol Implementation Conformance Statement

D.3 Instructions for Completing the PICS Proforma

D.3.1 General Structure of the PICS Proforma

The first part of the PICS proforma – 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 three major subclauses covering features common to NLSP-CL and NLSP-CO, followed by clauses specific to each of these two modes of operation; these are divided into further 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: all relevant choices are to be marked.

Each item is identified by an item reference in the first column; the second column contains the question to be answered; the third column contains the reference or references to the material that specifies the item in the main body of this ITU-T Recommendation | International Standard. The remaining columns record the status of the item – whether support is mandatory, optional, prohibited or conditional – and provide the space for the answers: see also D.3.4 below.

A supplier may also provide, or can be required to provide, further information, categorised as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i> respectively for cross-referencing purposes, where i is any unambiguous identification for the item (e.g. simply a numeral): there are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformance Statement for the implementation in question.

NOTE – Where an implementation is capable of being configured in more than one way according, for example, to the items in D.5.1, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer presentation of the information.

D.3.2 Additional Information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations; or a brief rationale – based perhaps upon specific application needs – for the exclusion of features which, although optional, are nonetheless commonly present in implementations of the network layer security protocol.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

D.3.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this: instead, the supplier shall write the missing answer into the Support column, together with an X<i> reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to ITU-T Recommendation | International Standard.

NOTE – A possible reason for the situation described above is that a defect in this ITU-T Recommendation | International Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

D.3.4 Conditional Status

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply – mandatory, optional or prohibited – are dependent upon whether or not certain other items are supported.

Individual conditional items are indicated by a conditional symbol of the form <item>:<s> in the status column, where <item> is an item reference that appears in the first column of the table for some other item, and <s> is one of the status symbols M, O, O.n or X.

If the item referred to by the conditional symbol is supported, the conditional item is applicable, its status is given by <s> and the support column is to be completed in the usual way. Otherwise, the conditional item is not relevant and the Not applicable (N/A) answer is to be marked.

Each item whose reference is used in a conditional symbol is indicated by an asterisk in the Item column.

D.4 Identification

D.4.1 Implementation Identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification – e.g. name(s) and version(s) of machines and or operating systems; system names	

NOTES

1 Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

2 The terms Name and Version should be interpreted appropriately to correspond with the supplier's terminology (e.g. Type, Series, Model).

D.4.2 Protocol Summary

Identification of protocol specification	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:1994
Identification of amendments and corrigenda to this PICS proforma which have been completed as part of this PICS	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:1994 Am. : Corr. : Am. : Corr. : Am. : Corr. : Am. : Corr. :

Have any exception items been required (see D.3.3)? NOTE – The answer **Yes** means that the implementation does not conform to this ITU-T Recommendation | International Standard.	Yes ☐ No ☐

Date of statement	

D.5 Features Common to NLSP-CO and NLSP-CL

D.5.1 Major Capabilities (Common)

Item	Questions/Features	Reference (subclause)	Status	Support
CO*	Is the connection-mode supported?	5.1	O.1	Yes ☐ No ☐
CL*	Is the connectionless-mode supported?	5.1	O.1	Yes ☐ No ☐
AC	Is Access Control supported?	5.2	O	Yes ☐ No ☐
TFC*	Is Traffic Flow Confidentiality supported?	5.2	O	Yes ☐ No ☐
ParamProt*	Is protection of all NLSP service parameters supported?	5.5.1a	O.2	Yes ☐ No ☐
UserDatProt	Is protection of NLSP Userdata supported?	5.5.1b	O.2	Yes ☐ No ☐
NoProt*	Is no protection supported?	5.5.1c	O	Yes ☐ No ☐
SdtBase*	Is any SDT PDU based encapsulation function supported?	5.5.3	CO:O.3 CL:M ParamProt:M	Yes ☐ No ☐
NoHead	Is any No Header encapsulation function supported?	5.5.3	CO:O.3 CL:X ParamProt:X	Yes ☐ No ☐ N/A ☐
SA-P*	Is any in-band SA-P supported?	5.4.1	O	Yes ☐ No ☐
LabMech*	Is the label mechanism supported?	6.2g, 6.4.1.1e, 6.4.2.1f	SdtBase:O	Yes ☐ No ☐ N/A ☐
SDTMech*	Is the standardised SDT PDU based encapsulation function supported?	11	SdtBase:O	Yes ☐ No ☐ N/A ☐
NoHeadMech	Is the standardised No Header encapsulation function supported?	12	NoHead:O	Yes ☐ No ☐ N/A ☐

D.5.2 PDUs (Common)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SDT*	Is the Secure Data Transfer PDU supported on transmision/receive?	6.4.1.1 13.3	SdtBase:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA*	Is the Security Association PDU supported on transmission/receive?	5.4.1, 13.4	SA-P:O	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.3 SDT PDU Fields Common to CO and CL and Generic to Mechanisms

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SdtPID	PID field value 10001011 in each SDT PDU	13.3.2.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtLI	Length Indicator field in each SDT PDU	13.3.2.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtPDUType	PDU Type field with value 01001000 in each SDT PDU	13.3.2.3	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtContLen	Content Length in each SDT PDU	13.3.4.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
DataType	Data Type field in each SDT PDU	13.3.4.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UserData	Content field type CO – Userdata	13.3.4.3	SDT:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
CSAddr	Content field type C2 – Calling/Source NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CDAddr	Content field type C3 – Calling/Destination NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
Label	Content field type C6 – Label	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabRef	Content field type C7 – Label Reference	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabelExc	Is the mutual exclusion of label and label reference in any SDT PDU enforced?	13.3.4.3	LabMech:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.4 SDT PDU Fields Common to CO and CL with Specific SDT Based Encapsulation Mechanisms

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Receipt
Synch	Crypto synchronisation	11.3, 13.3.3.1	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ICV	ICV field	11.3, 13.3.3.2	COInteg:M CLInteg:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
EncPad	Padding for Encipherment	11.3, 13.3.3.3	COConf:O CLConf:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SeqNo	Sequence Number Content field	11.3, 13.3.5.1	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SinglePad	Single octet general padding field	11.3, 13.3.5.2	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
TFCPad	Traffic padding	11.3, 13.3.5.3	TFC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
IntegPad	Padding for Integrity	11.3, 13.3.5.4	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the above fields are conditional on SDTMech selected.					

D.5.5 SA PDU Fields Generic to SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SaPID	PID field value 10001011 in each SA PDU	13.4.1	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaLI	Is the Length Indicator field transmitted in each SA PDU?	13.4.2	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaPDUType	PDU Type field with value 01001001 in each SA PDU	13.4.3	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaSA-ID	SA-ID field	13.4.4	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PType	SA-P Type field	13.4.5	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SAKTE*	Is the example SA protocol using Key Token Exchange supported?	Annex C	SA:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

D.5.6 SA PDU Content Fields Specific to Key Token Exchange SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SAExchId	Exchange ID	C.7.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ContLen	Is the Length Indicator field transmitted in each SA PDU?	C.7.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
MySA-ID	My SA-ID Content field	C.7.3.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
OldYrSA-ID	Old Your SA-ID Content field	C.7.3.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyTokens	Key-Token-1, Key-Token-2, Key-Token-3 and Key-Token-4 Content fields	C.7.3.3	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
AuthFields	Authentication digital signature and Authentication certificate Content fields	C.7.3.4	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ServSel*	Service Selection Content field	C.7.3.5	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SARejReas	SA Rejection Reason Content field	C.7.3.6	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAAbReas	SA Abort/Release Reason Content field	C.7.3.7	SAKTE:M	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabDef	Label Definition Content field	C.7.3.8	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeySel*	Key Selection Content field	C.7.3.9	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeyUse	Usage Flags sub-field	C.7.3.9.1	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeySelInfo	Key Selection Information sub-field	C.7.3.9.2	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyRefx	Key Reference sub-field	C.7.3.9.3	KeySel:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAFlags	SA Flags Content field	C.7.3.10	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ASSR	ASSR Content field	C.7.3.11	ServSel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.7 Algorithms Supported

Item	Questions/Features	Reference (subclause)	Status	Support
RegKTE	List of registered Key Token Exchange algorithms supported	–	O	Names: Object Identifers:
UnRegKTE	List the unregistered Exponential Key Exchange algorithms supported	–	O	Names:
RegICV	List the registered names of ICV algorithms supported	–	O	Names: Object Identifers:
UnRegICV	List the unregistered ICV algorithms supported	–	O	Names:
RegConf	List the registered names of Confidentiality algorithms supported	–	O	Names: Object Identifers:
UnRegConf	List the unregistered Confidentiality algorithms supported	–	O	Names:

D.6 Features Specific to NLSP-CL

D.6.1 Major Capabilities (NLSP-CL)

Item	Questions/Features	Reference (subclause)	Status	Support
CLConf*	Is connectionless confidentiality supported?	5.2	CL:O.5	Yes □ No □ N/A □
CLInteg*	Is connectionless integrity supported?	5.2	CL:O.5	Yes □ No □ N/A □
DOA	Is Data Origin Authentication supported?	5.2	CL:O.5	Yes □ No □ N/A □

D.6.2 Initiator/Responder (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CLXmtProt	Is the implementation capable of transmitting protected connectionless data units?	7.6	CL:O.6	Yes ☐ No ☐ N/A ☐
CLRcvProt	Is the implementation capable of accepting incoming protected connectionless data units?	7.7	CL:O.6	Yes ☐ No ☐ N/A ☐
CLXmt	Is the implementation capable of transmitting unprotected connectionless data units?	7.6.1	NoProt:M	Yes ☐ N/A ☐
CLRcv	Is the implementation capable of accepting incoming unprotected connectionless data units?	7.7.1	NoProt:M	Yes ☐ N/A ☐

D.6.3 Environment (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CL1	Are the mandatory elements of IS 8348 AD1 supported?	5.2	CL:M	Yes ☐ N/A ☐

D.6.4 SDT PDU Fields (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
SdtSA-ID	SA-ID field transmitted in each SDT PDU?	13.3.2.4	CL:M	Yes ☐ N/A ☐

D.7 Features Specific to NLSP-CO

D.7.1 Major Capabilities (NLSP-CO)

Item	Questions/Features	Reference (subclause)	Status	Support
SNAcP	Is the protocol mapping directly onto CCITT Rec. X.25 | ISO 8208?	5.3, Annex B	CO:O.7	Yes ☐ No ☐
SNISP*	Is the protocol mapping onto CCITT Rec. X.213 | ISO 8348?	5.3, Annex A	CO:O.7	Yes ☐ No ☐
COConf*	Is connection confidentiality supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
COInteg*	Is connection integrity without recovery supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
PEA	Is peer entity authentication supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
ExCSC*	Is Example CSC PDU procedures defined in NLSP supported?	10	CO:O	Yes ☐ No ☐ N/A ☐

D.7.2 PDUs (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CSC*	Connection Security Control PDU	8.5, 13.5	CO:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.7.3 Modes of Connection Establishment/Release

Item	Questions/Features	Reference (subclause)	Status	Support as Calling entity	Support as Called entity
UNConn	NLSP-CONNECT in UN-CONNECT	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNConnSAP	NLSP-CONNECT in UN-CONNECT with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNData	NLSP-CONNECT in UN-DATA	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNDataSAP	NLSP-CONNECT in UN-DATA with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNDisc	NLSP-DISCONNECT in UN-DISCONNECT	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNData	NLSP-DISCONNECT in UN-DATA	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

D.7.4 Environment (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CO1	Are the mandatory elements of IS 8348 supported?	5.3	SNISP:M	Yes ☐ N/A ☐
ConOpt1	Does the implementation provide Expedited Data?	8.7	CO:O	Yes ☐ No ☐ N/A ☐
ConOpt3	Does the implementation provide Receipt Confirmation?	8.9	CO:O	Yes ☐ No ☐ N/A ☐

D.7.5 Timers and Parameters (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
T1	Is the timer between transmitting NLSP-DISCONNECT and issuing UN-DISCONNECT supported?	8.10	CO:O	Yes ☐ No ☐ N/A ☐

D.7.6 SDT PDU Fields (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Recceipt
TestData	Content field type C1 – Testdata	13.3.4.3	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
RAddr	Content field type C4 – Responding NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ConfReq	Content field type C8 – Confirmation Request	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
Reason	Content field type C9 – Disconnect Reason	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the items in D.7.6 are conditional on SDT being supported.					

D.7.7 CSC PDU Fields – Generic (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CscPID	PID field value 10001011 in each CSC PDU	13.5.1	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscLI	Length Indicator field in each CSC PDU	13.5.2	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscPTyp	PDU Type field with a value of xx111111 in each CSC PDU	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UNC-UNDFlg	Is the UNC-UND flag in PDU Type field transmitted in each CSC PDU?	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PFlg	Is the SA-P flag in PDU Type field transmitted in each CSC PDU?	13.5.3c	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscSA-ID	SA-ID field	13.5.4	CSC:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ContLen	Content Length field in each CSC PDU	13.5.5	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.7.8 Example CSC PDU Content (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CscInit	Is the implementation capable of initiating a CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
CscResp	Is the implementation capable of responding to a peer initiated CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
EncAuth	Enciphered AUTH-DATA field	13.5.7	ExCSC:M	Yes ☐ N/A ☐
KeyInfox	Key Information field	13.5.8	ExCSC:O	Yes ☐ No ☐ N/A ☐

Anexo E

Explicación de algunos conceptos básicos del protocolo de seguridad de la capa de red

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

E.1 Base para la protección

La base para la protección de los datos de usuario en el protocolo de seguridad de la capa de red (NLSP) es la unidad de datos de protocolo (PDU) de transferencia de datos segura (SDT, *secure data transfer*), brevemente, la PDU de SDT. La PDU de SDT protege los datos por medio de una función de encapsulación que añade al final un valor de comprobación de la integridad (ICV, *integrity check value*) que es seguidamente cifrado para proporcionar confidencialidad. Se pueden colocar campos de relleno con los datos protegidos para proporcionar el soporte del mecanismo de confidencialidad del flujo de datos y del mecanismo de ICV de bloque. Se puede colocar un campo de relleno individual después del ICV para el mecanismo de cifrado de bloque.

Antes de protegerla en una PDU de SDT, se puede colocar información adicional de control de seguridad (por ejemplo etiqueta, número secuencial) junto con los datos de usuario para producir la cadena de octetos antes de la encapsulación (Octet-String-Before-Encapsulation). Después de esto, la cadena de octetos antes de la encapsulación se protege por medio de una función de encapsulación, como ya se ha dicho. Se coloca un encabezamiento en blanco antes de la PDU para identificar el tipo de PDU y el conjunto de «atributos de seguridad» (claves, etc.; véase la cláusula 5) utilizado para proteger la unidad de datos. La Figura E.1 ilustra la constitución de una PDU de SDT.

El NLSP en modo conexión (NLSP-CO) soporta una segunda forma de protección de los datos de usuario en el NLSP; esta segunda forma de protección es facultativa y se denomina «sin encabezamiento» (No_Header). En este método, los datos NLSP se encriptan directamente sin añadirles ninguna información de control de seguridad ni encabezamiento en blanco.

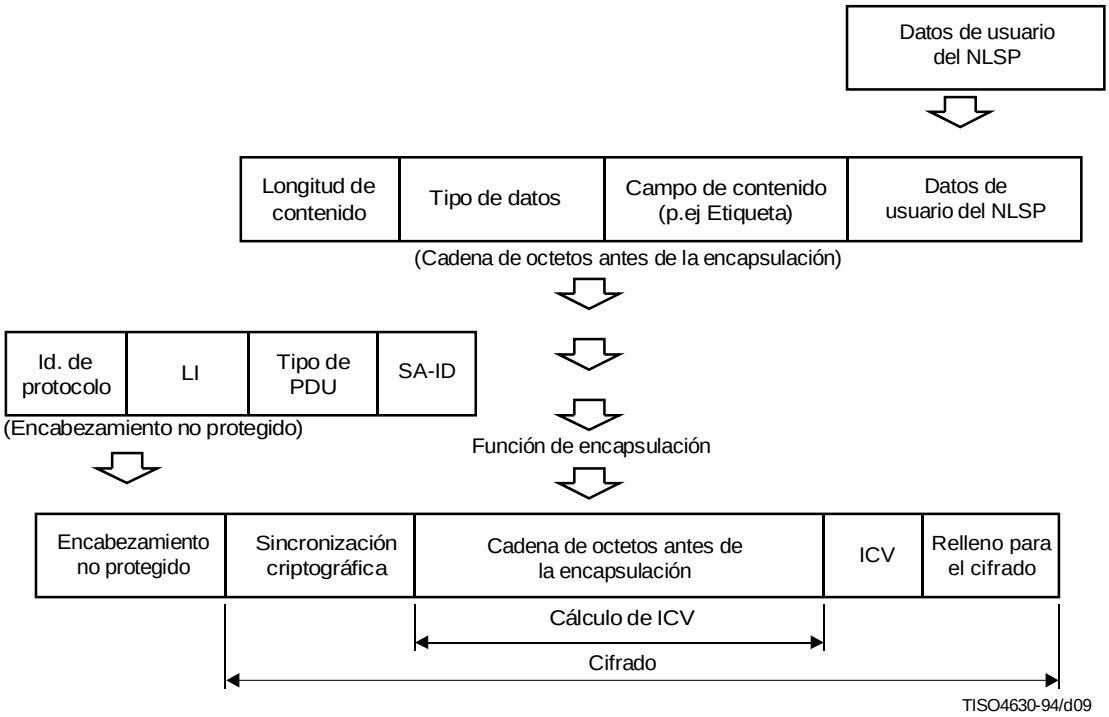


Figura E.1 – Constitución de una PDU de transferencia de datos segura

E.2 Servicio de red subyacente por oposición a servicio NLSP

El protocolo NLSP tiene dos interfaces de servicio nacionales. Una, denominada el servicio NLSP, es la interfaz proporcionada a protocolos situados «por encima del NLSP» (esto es, protocolos que utilizan las comunicaciones protegidas). La otra denominada servicio de red subyacente, o brevemente servicio UN (*underlying network*), la utiliza el protocolo NLSP para invocar los protocolos de comunicación subyacentes. El NLSP puede añadirse transparentemente sin que ello afecte al funcionamiento de los protocolos por encima y por debajo de él. La interfaz del NLSP da una «imagen de espejo» del servicio esperado por los protocolos situados por encima, y el servicio UN se hace corresponder con la forma de servicio proporcionada por los protocolos subyacentes.

Los datos de usuario en la interfaz de servicio del NLSP son protegidos (por ejemplo encapsulándolos en una PDU de SDT) antes de pasarlos a la interfaz de servicio de red subyacente (UN).

La interfaz de servicio NLSP y la interfaz de servicio UN son similares al servicio de red OSI, del que sólo difieren en un aspecto importante. La entidad servida por el NLSP no siempre es una entidad de transporte y el servicio UN nunca interconecta directamente con una entidad de transporte. Como se indicará más adelante, en algunos casos (véase la Figura E.2), el servicio NLSP puede interconectar con una función de relevo y encaminamiento dentro de un sistema intermedio o incluso con una entidad que soporta un protocolo de capa de red (véanse las Figuras). Con el servicio UN, desde la perspectiva de los protocolos subyacentes, la interfaz de servicio puede aparecer como si fuera el servicio de red, pero desde la perspectiva de la totalidad de la pila (de protocolos) OSI, interconecta con una entidad NLSP dentro de la capa de red, por lo que no es un servicio de red OSI puro.

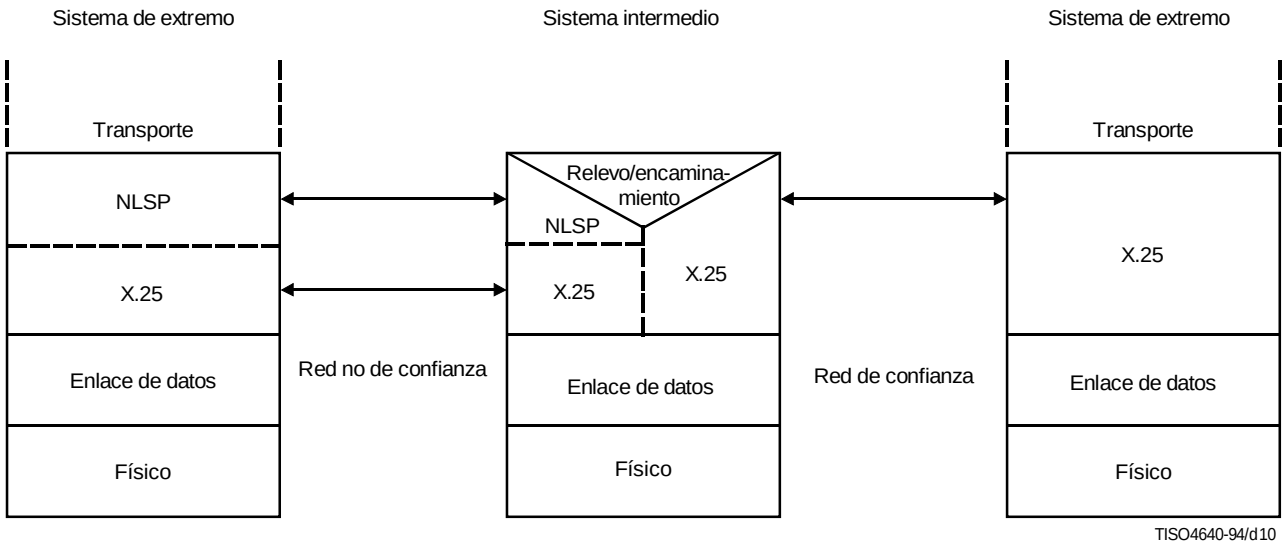
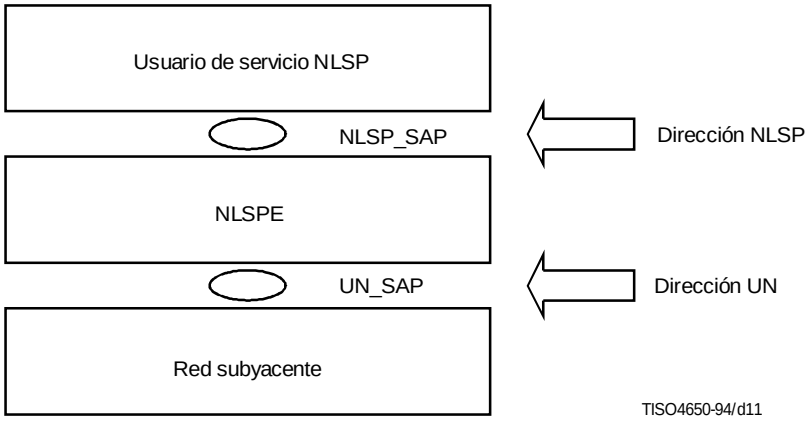


Figura E.2 – Ilustración de un NLSP-CO con sistema intermedio

E.3 Direccionamiento del NLSP

La entidad NLSP (NLSPE) está situada entre el usuario de servicio NLSP y la red subyacente. Los correspondientes puntos de acceso al servicio son el NLSP_SAP y el UN_SAP. En configuraciones actualmente soportadas por el NLSP (véase la la Figura E.3-1 y la nota), la dirección que identifica la entidad unida al NLSP_SAP, por ejemplo el usuario de servicio NLSP, es la dirección NLSP. La dirección que identifica la entidad unida al UN_SAP, por ejemplo la NLSPE, es la dirección UN. Las NLSPE pares forman una subcapa dentro de la capa de red. Las fronteras superior e inferior son puntos de interacción en los que se intercambian direcciones. La figura siguiente representa puntos de acceso al servicio y las direcciones correspondientes.



NOTA – En las configuraciones que relevan servicios N en modo conexión, la dirección NLSP puede identificar una dirección de punto de acceso al servicio de red (NSAP) en un sistema de extremo y no la de un punto de acceso al protocolo de seguridad de la capa de red (NLSP_SAP) en un sistema intermedio (véanse también las cláusulas E.4 y E.5).

Figura E.3-1 – Puntos de acceso al servicio superior e inferior y direcciones correspondientes

El NLSP está situado en la capa de red. Puede ser colocado en la frontera inferior, en la frontera superior, o en cualquier emplazamiento entre ambas. El NLSP y su frontera inferior de servicio UN desempeñan papeles diferentes, que dependen del emplazamiento. De manera similar, las direcciones utilizadas tienen semánticas diferentes en función de este emplazamiento. La Figura E.3-2 muestra los posibles emplazamientos de la NLSPE en la capa de red.

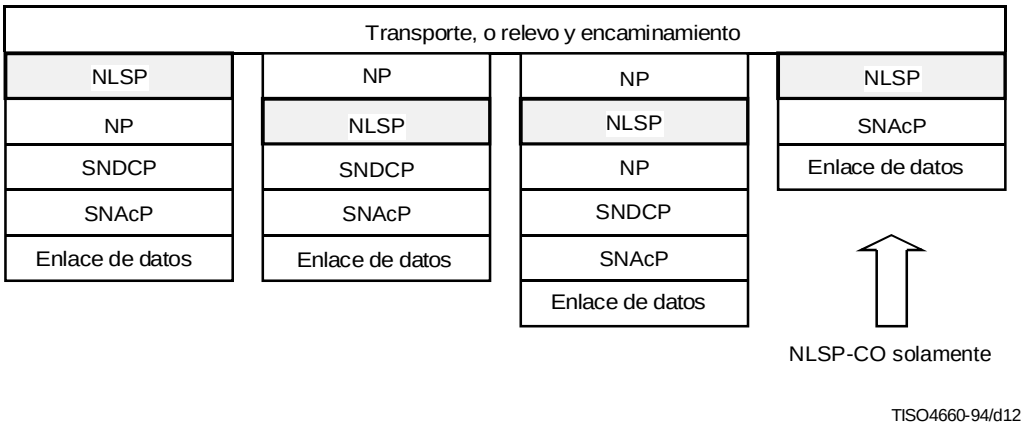


Figura E.3-2 – Emplazamiento del NLSP en la capa de red

Las Figuras E.3-3 y E.3-4 identifican la forma de las direcciones utilizadas en una capa de red que contiene una subcapa NLSP en diferentes emplazamientos.

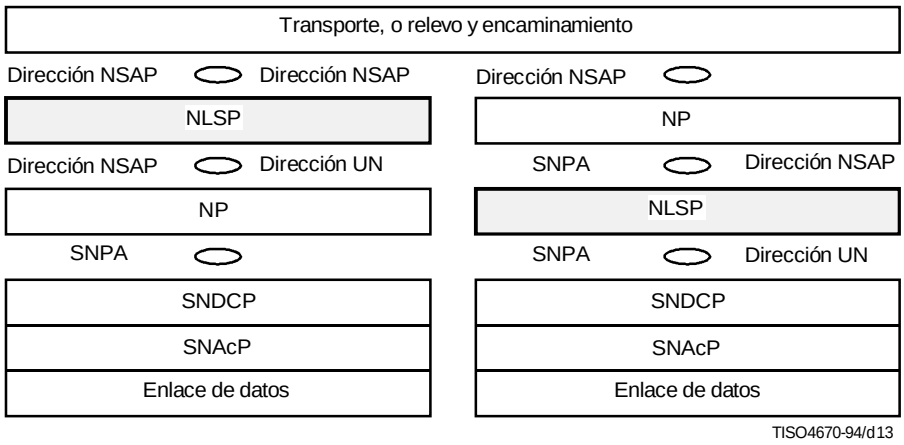


Figura E.3-3 – Direcciones en una capa de red que contiene una subcapa NLSP – Con un protocolo de red por encima/debajo del NLSP

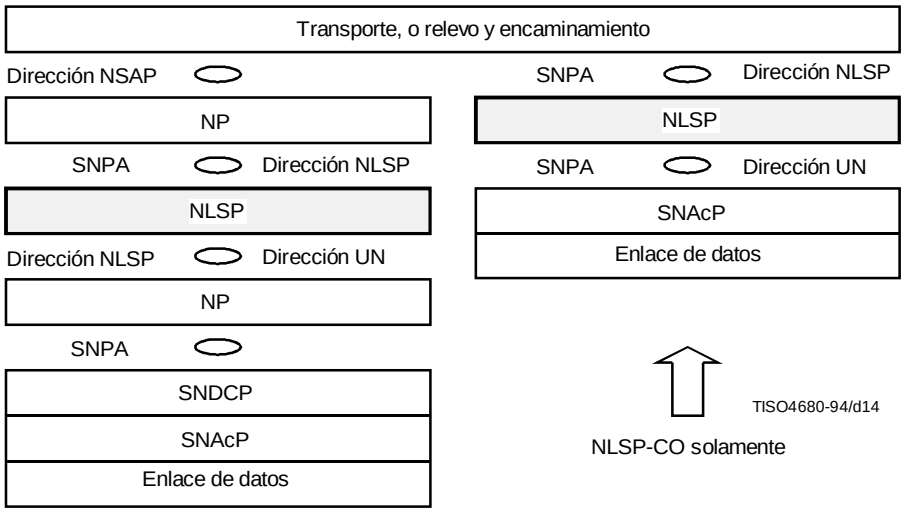


Figura E.3-4 – Direcciones en una capa de red que contiene una subcapa NLSP – Con protocolo de red (NP) por encima y por debajo del NLSP, sin protocolo de red

La dirección NSAP-adr (Un-adr) la utiliza el NLSP para direccionar («addressing») dentro de una red subyacente en los casos en que un protocolo de red (en modo conexión o sin conexión) está situado debajo de la subcapa NLSP. Las direcciones NSAP forman un dominio de direccionamiento encapsulado, cerrado por la subcapa NLSP. Las direcciones NSAP tienen una sintaxis idéntica a la de las direcciones NSAP y se registran mediante el procedimiento de registro de dirección NSAP. Las direcciones NSAP que forman un dominio de red de confianza («*trusted network domain*») se utilizan solamente dentro de un dominio protegido por subcapas NLSP.

El SNPA puede ser idéntico al SNPA (punto de unión al servicio de red) determinado por la entidad NP situada encima. Sin embargo, la dirección SNPA puede ser diferente, en función de la ubicación de la NLSPE par.

El dominio de direccionamiento encapsulado puede considerarse como una subred virtual dentro del entorno OSI (el OSIE). Está confinado por un grupo de entidades NLSP en un sistema de extremo (ES) o en un sistema intermedio (IS), cada uno de los cuales contiene una pila (de protocolos) de capa N idéntica por encima de los protocolos de subred dependientes de la tecnología [Protocolo SNAcP (protocolo de acceso a subred), Protocolo de convergencia dependiente de la subred]. Estas NLSPE tienen por tanto, todas ellas, el mismo emplazamiento dentro de la capa de red.

La Figura E.3-5 muestra un posible escenario de un OSIE que contiene una red subyacente (UN) cerrada por entidades NLSP dentro de sistemas de extremo (ES) y sistemas intermedios (IS):

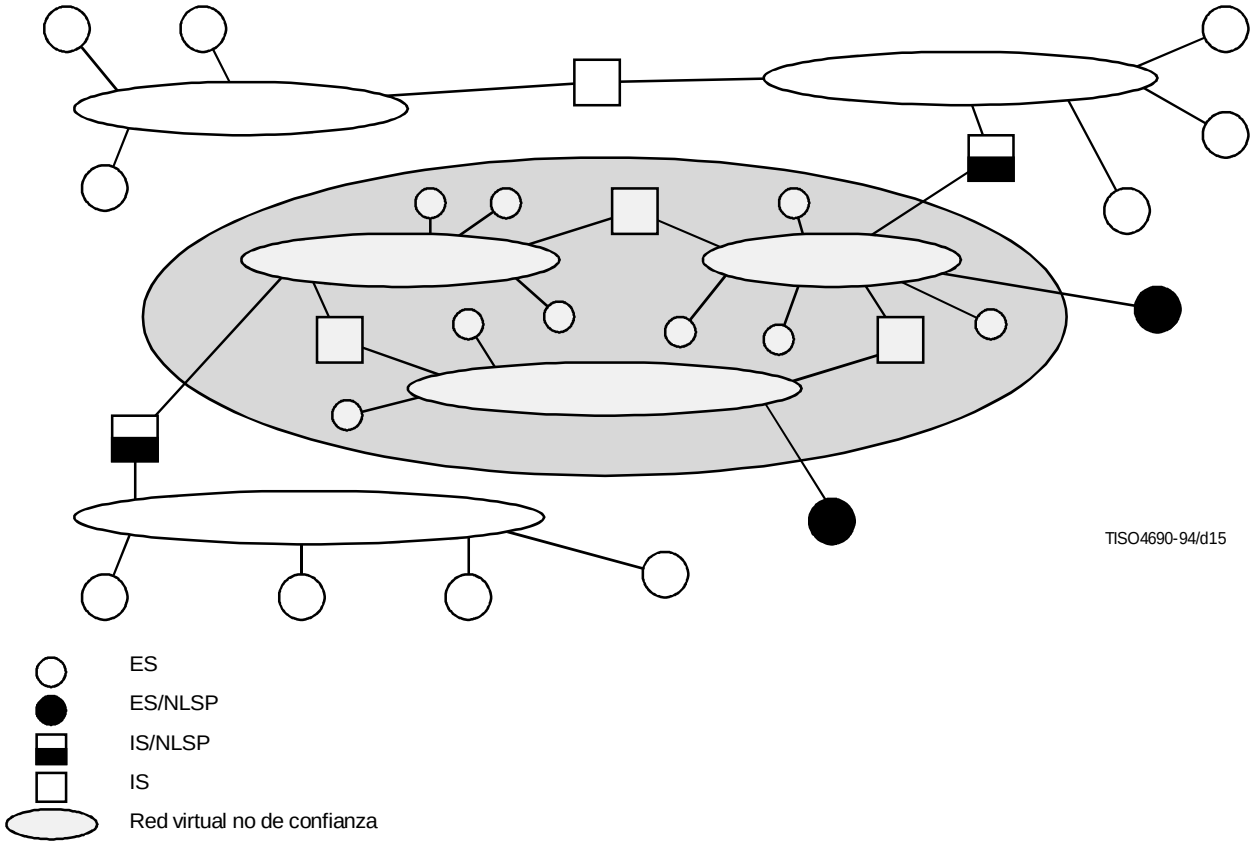


Figura E.3-5 – Red subyacente virtual en un entorno OIS

Las pilas de protocolos de la capa de red y el emplazamiento de las entidades NLSP dependen de los protocolos utilizados en las subredes y de su configuración. El proceso de selección lo efectúa una «autoridad» que define una configuración estática de una combinación de subredes de confianza y no de confianza. Para ello se requieren funciones adicionales de gestión y de encaminamiento seguros, las cuales están fuera del ámbito de esta Recomendación UIT-T | Norma Internacional.

En función del emplazamiento de la NLSPE en el interior de la capa de red, la dirección NLSP y la dirección UN tendrán semánticas diferentes. Conceptualmente, se distinguen dos emplazamientos (véase la Figura E.3-6).

– *Emplazamiento A* – El NLSP_SAP corresponde al NSAP en OSI. El usuario del servicio NLSP es una entidad de transporte. La dirección que identifica la entidad de transporte se define como dirección NSAP y es idéntica a la dirección NLSP.

  La red subyacente se considera un dominio de red no protegido, que es en realidad la red OSI. La dirección que identifica la NLSPE corresponde por eso a la dirección de NSAP en OSI. Sin embargo, los parámetros transferidos en primitivas de servicio a través de las fronteras del NLSP_SAP y del UN_SAP pueden ser diferentes si los parámetros de servicio NLSP están protegidos (Param_Prot es TRUE).

– *Emplazamiento B* – La NLSPE está situada entre dos subcapas de red. La subcapa más alta delimita un dominio de red protegido, en tanto que la subred subyacente representa un dominio de red no protegido.

Dentro de un sistema de extremo, la dirección NSAP identifica diferentes usuarios de servicio de red ubicados, todos ellos, en el sistema de extremo. La dirección NLSP identifica la entidad de encaminamiento del sistema de extremo, que es responsable de las funciones de encaminamiento del sistema de extremo.

Dentro de un sistema intermedio, la dirección NSAP contiene información de encaminamiento para el relevo de NPDU dentro del dominio de red protegido. La dirección NLSP identifica la entidad de encaminamiento ES/IS dentro del sistema intermedio. La dirección UN identifica la NLSPE unida a la UN.

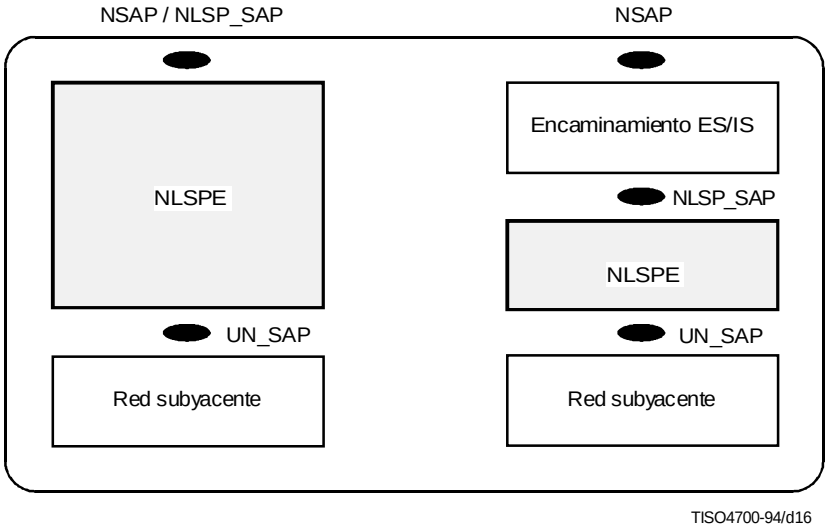


Figura E.3-6 – Emplazamientos de la NLSPE en la capa de red

La(s) dirección(es) NLSP servida(s) por una NLSPE distante se retiene(n) en un atributo SA Adr_Served. La dirección UN de una NLSPE distante se retiene en un atributo SA Peer_Adr.

– Si Param_Prot es FALSE

Las funciones NLSP están limitadas al establecimiento de la correspondencia de las primitivas de servicio del NLSP_SAP al UN_SAP. La dirección NSAP se hace corresponder directamente a la dirección UN. El atributo SA Adr_Served del NLSP tiene el mismo valor que el atributo SA Peer_Adr.

– Si Param_Prot es TRUE

Modo protegido. Las correspondencias de direcciones dependen del emplazamiento de la NLSPE y se proporcionan mediante el empleo de atributos Adr_Served y Peer_Adr.

El Cuadro E.1 presenta las funciones de correspondencia de direcciones de la NLSPE en función de sus diversos emplazamientos y la correspondencia entre los atributos Peer_Adr y Adr_Served. El Cuadro E.1 comprende solamente las direcciones de destino.

E.4 NLSP en modo conexión

E.4.1 Funcionamiento básico

La mayor parte de la complejidad del protocolo NLSP está relacionada con el tratamiento del establecimiento de la conexión en el caso de las comunicaciones en modo conexión.

Cuadro E.1

Emplazamiento	Param_Prot	Dirección NLSP	Dirección UN	Dirección NLSP vs UN
A	FALSE	Dirección NSAP	Dirección NSAP	La misma
A	TRUE	Dirección NSAP	Dirección UN par	Diferente
B: Sistema de extremo	FALSE	Dirección NLSP (Nota)	Dirección UN par	La misma
B: Sistema de extremo	TRUE	Dirección NLSP (Nota)	Dirección UN par	Diferente
B: Sistema intermedio	FALSE	Dirección NLSP (Nota)	Dirección UN par	La misma
B: Sistema intermedio	TRUE	Dirección NLSP (Nota)	Dirección UN par	Diferente
NOTA – El establecimiento de la correspondencia, en ambos sentidos, de la dirección NLSP a la dirección NSAP la establecen funciones de encaminamiento relacionadas con el protocolo situado por encima del NLSP.				

Se soportan dos modos básicos de establecimiento de la conexión NLSP. En uno de ellos, los parámetros de NLSP-CONEXIÓN se transportan en las primitivas de servicio UN-CONEXIÓN. En el otro, los parámetros de NLSP-CONEXIÓN, después de encapsulados en una PDU de SDT, se transportan en una primitiva UN-DATOS después de establecida la conexión UN. Los dos modos de establecimiento de la conexión NLSP tienen variantes, una para uso con SA-P y dentro de banda, y la otra para uso con una SA que se ha establecido fuera de banda.

La PDU de control de la seguridad de la conexión (CSC, *connection security control*) se utiliza para señalar el modo de establecimiento de la conexión, y, si el SA-P dentro de banda no se está transportando en la conexión UN, el intercambio de PDU de CSC se utiliza también para:

a) establecer atributos de seguridad específicos al mecanismo para usarlos en la protección de la conexión (por ejemplo, claves, números secuenciales para la integridad);

b) efectuar la autenticación de la entidad par.

Cuando una NLSP-CONEXIÓN se está transportando en una UN-CONEXIÓN con SA-P dentro de banda, se establece una conexión UN para transportar el SA-P, la cual se libera después, antes de efectuar el intercambio de UN-CONEXIÓN que lleva los parámetros de NLSP-CONEXIÓN. Las PDU de CSC se utilizan en el segundo intercambio de UN-CONEXIÓN para reautenticar las entidades NLSP pares.

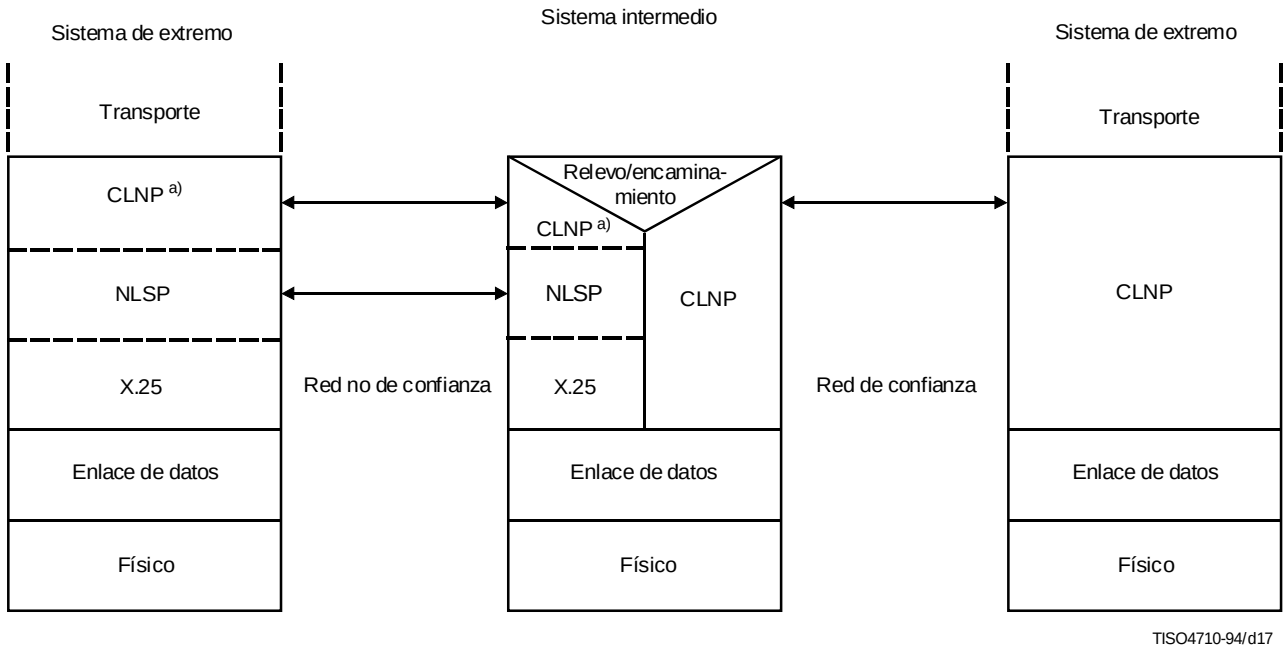
El establecimiento de la SA se obtiene mediante el intercambio de PDU de SA o de PDU de SDT que transportan la información necesaria para establecer los atributos SA requeridos. En el Anexo C se define un protocolo SA para este fin.

Si se requiere que los parámetros de NLSP-CONEXIÓN estén protegidos, o bien se encapsularán en una UPD de SDT o se encriptarán (se selecciona el modo «sin encabezamiento») antes de la transferencia.

Una vez que se ha establecido una conexión, los datos de usuario se protegen encapsulándolos en una PDU de SDT o, si se ha seleccionado el modo «sin encabezamiento», encapsulando solamente los datos de usuario NLSP.

E.4.2 Emplazamiento

El NLSP en modo conexión puede emplazarse en diversos lugares dentro de la capa de red. Este protocolo proporciona al usuario NLSP, sea una interfaz de servicio de red OSI (en cuyo caso el usuario corresponde a una entidad de transporte) o, si el usuario es una entidad de protocolo de red adicional (por ejemplo, CLNP de la Rec. UIT-T X.233 | ISO/CEI 8473), el servicio corresponde a una interfaz de subred. La interfaz por debajo del NLSP es virtualmente idéntica al servicio de red OSI, excepto que el usuario del servicio es NLSP en lugar del servicio de transporte y que el servicio puede funcionar en un sistema de extremo o en un sistema intermedio. El protocolo que funciona por debajo del NLSP lo hace como si estuviera funcionando entre dos sistemas de extremo que estuvieran proporcionando el servicio de red OSI aunque, desde una perspectiva general, sólo puede estar funcionando con un sistema intermedio y no interconecta directamente con el servicio de transporte. El funcionamiento del NLSP-CO con un sistema intermedio y de extremo a extremo se ilustra en las Figuras E.4-1, E.4-2, E.4-3 y E.4-4. Son posibles otros emplazamientos del NLSP.



a) NOTA – Incluye una función de convergencia al modo conexión.

Figura E.4-1 – Ilustración de un NLSP en un entorno con múltiples redes

E.4.3 Correspondencia de la interfaz de servicio NLSP/UN

En un sistema de extremo, la interfaz de servicio NLSP corresponde directamente con el servicio de red OSI.

Se soportan dos formas de correspondencia del servicio UN. En una de ellas, la interfaz de servicio UN corresponde con el equivalente al servicio de red OSI, transportándose la PDU de CSC en el campo datos de usuario de la primitiva UN conexión. En la otra forma, corresponde directamente con la Recomendación X.25 como se define en la Rec. X.223 del CCITT | ISO 8878, con la excepción de que la PDU de CSC se transporta en el campo de facilidades de protección de la Recomendación X.25.

E.4.4 Direccionamiento

Las direcciones utilizadas en la interfaz de servicio NLSP son direcciones de punto de acceso al servicio de red (NSAP) del servicio de red OSI si el NLSP está funcionando en la posición superior de la capa de red, o direcciones de punto de acceso a subred (SNPA) si está funcionado por debajo de otro protocolo de capa de red como el CLNP. Si hay ocultación de dirección (es decir, si Param_Prot es FALSE), las direcciones en la interfaz de servicio UN son las mismas que las direcciones en la interfaz de servicio NLSP.

Si se proporciona ocultación de dirección (es decir, si Param_Prot es TRUE), las direcciones utilizadas en la interfaz de servicio UN (direcciones UN) tienen la forma de las direcciones NLSP (por ejemplo, en el caso de que la dirección NLSP sea una dirección NSAP estructurada de acuerdo con la Rec. X.213 del CCITT | ISO 8348/AD2), no obstante lo cual se utilizan para identificar entidades NLSP que pueden estar situadas en un sistema intermedio o en un sistema de extremo. Estas direcciones UN pueden gestionarse de la misma manera que las direcciones NSAP. Se puede utilizar los mismos esquemas de registro para adjudicar direcciones y se puede utilizar los mismos protocolos de encaminamiento para gestionar el encaminamiento. Sin embargo, están en dominios de encaminamiento aislados. El NLSP trata la correspondencia de la dirección NSAP a la dirección UN utilizando el atributo de asociación de seguridad Adr_served (dirección servida) para identificar la dirección NSAP servida por las direcciones UN contenidas en el atributo de asociación de seguridad Peer_Adr (dirección de par).

E.5 NLSP en modo sin conexión

E.5.1 Funcionamiento básico

La protección del protocolo NLSP en modo sin conexión (CL) se obtiene, simplemente, encapsulando los datos de usuario en una PDU de SDT.

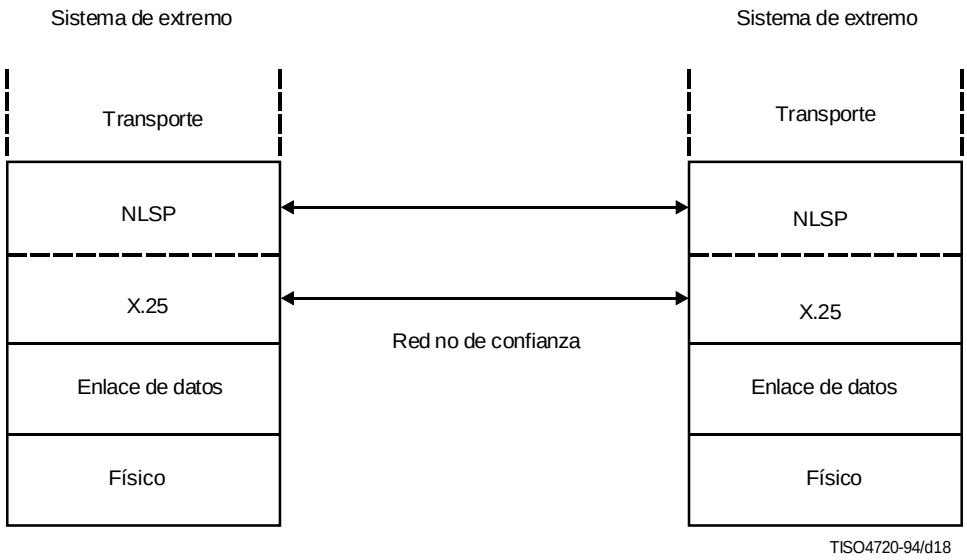


Figura E.4-2 – Ilustración de un NLSP-CO entre sistemas de extremo

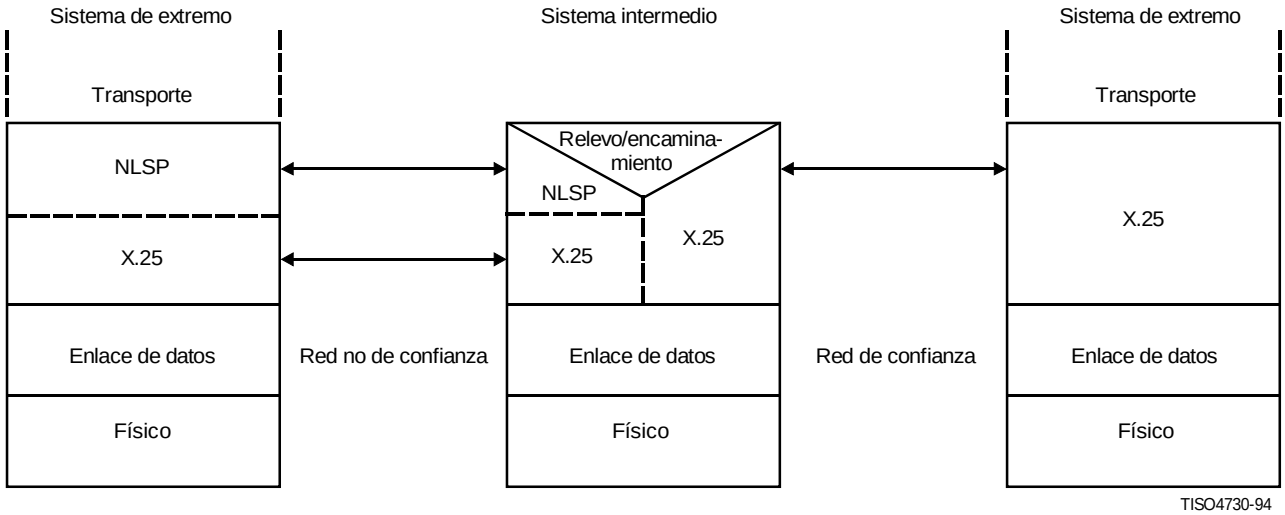


Figura E.4-3 – Ilustración de un NLSP-CO con una red no de confianza

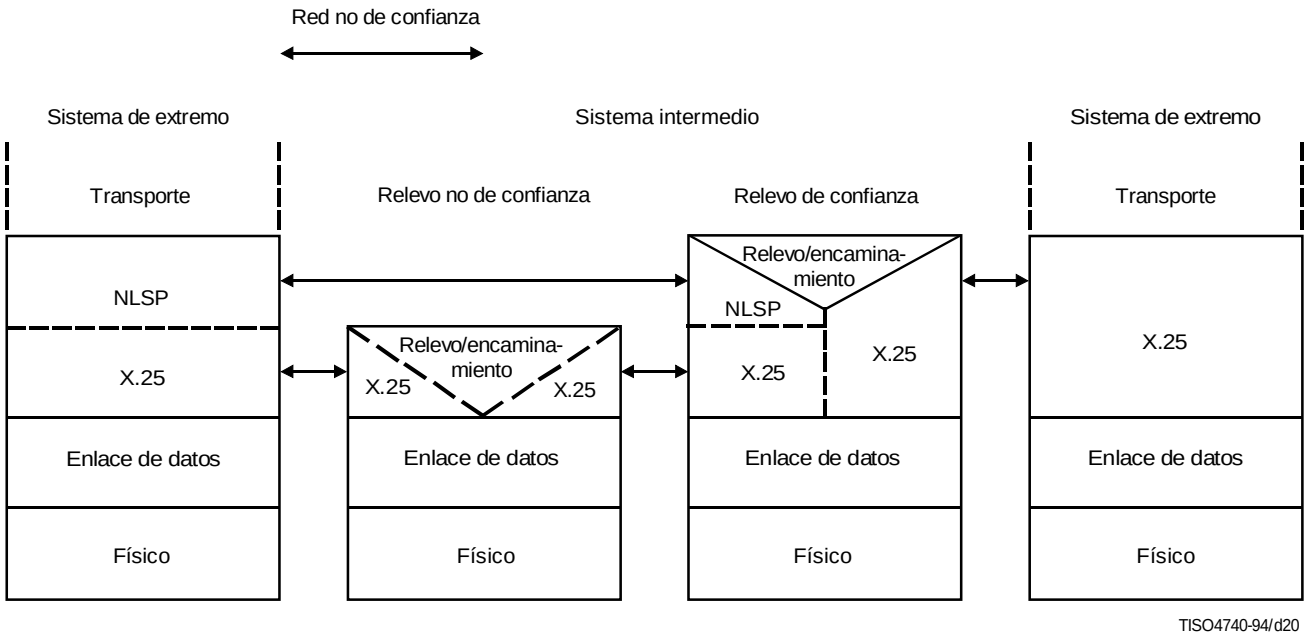


Figura E.4-4 – Ilustración de un NLSP-CO con un sistema de relevo no de confianza

E.5.2 Emplazamiento

El NLSP en modo sin conexión puede funcionar:

a) o bien en la posición superior de la capa de red, encapsulando NSDU en una PDU de SDT antes de que sean tratadas por el protocolo de red en modo sin conexión (CLNP) de la Rec. UIT-T X.233 | ISO/CEI 8473) (véase la Figura E.5-1). Esta pila (de protocolos) sólo puede utilizarse entre dos sistemas de extremo;

b) o bien por debajo del protocolo de red en modo sin conexión, encapsulando PDU del protocolo en modo sin conexión antes de hacerlas corresponder con la subred subyacente (véase la Figura E.5-2). Esta pila (de protocolos) deberá utilizarse conjuntamente con sistemas intermedios con relevador «de confianza», o de extremo a extremo, donde no hay relevos de red entre dos sistemas comunicantes;

c) o bien funcionando bajo una capa de protocolo (CLNP) de la Rec. UIT-T X.233 | ISO/CEI 8473 para el dominio «de confianza»/«rojo» y estableciendo la correspondencia con otra capa de protocolo CLNP para el dominio «no de confianza»/«negro». Esta pila es la más flexible y puede funcionar en cualquier entorno. Los sistemas intermedios «de confianza» relevan el protocolo CLNP superior después de retirar la protección de seguridad proporcionada por el NLSP. Otros sistemas de relevo «no de confianza» relevan el protocolo CLNP inferior pasando a lo largo, transparentemente, datos protegidos NLSP (véase la Figura E.5-3).

NOTAS

1 La representación de dos capas de la Rec. UIT-T X.233 | ISO/CEI 8473 y de una capa NLSP no implica necesariamente máquinas de protocolo distintas. Esto depende de la política local en materia de implementación.

2 La existencia de dos capas de protocolo CLNP no implica necesariamente la existencia de implementaciones distintas.

E.5.3 Correspondencia de las interfaces de servicio NLSP/UN

En el primer caso, que es el de un NLSP que funciona en la posición superior de la capa de red, la interfaz de servicio NLSP es idéntica al servicio de red OSI, y la interfaz de servicio UN es la misma, con la única diferencia de que interconecta con una entidad NLSP y no con el servicio de transporte.

En el segundo caso, que es el de un NLSP que funciona por debajo del CLNP, la interfaz de servicio NLSP es equivalente al servicio proporcionado por una subred que funciona por debajo del CLNP, y el servicio UN es el mismo que el servicio de la subred.

En el último caso, la interfaz por encima del NLSP ve el protocolo CLNP que tiene situado encima como si fuera una subred. La interfaz UN es percibida por el protocolo CLNP situado debajo como si fuera el servicio de red OSI.

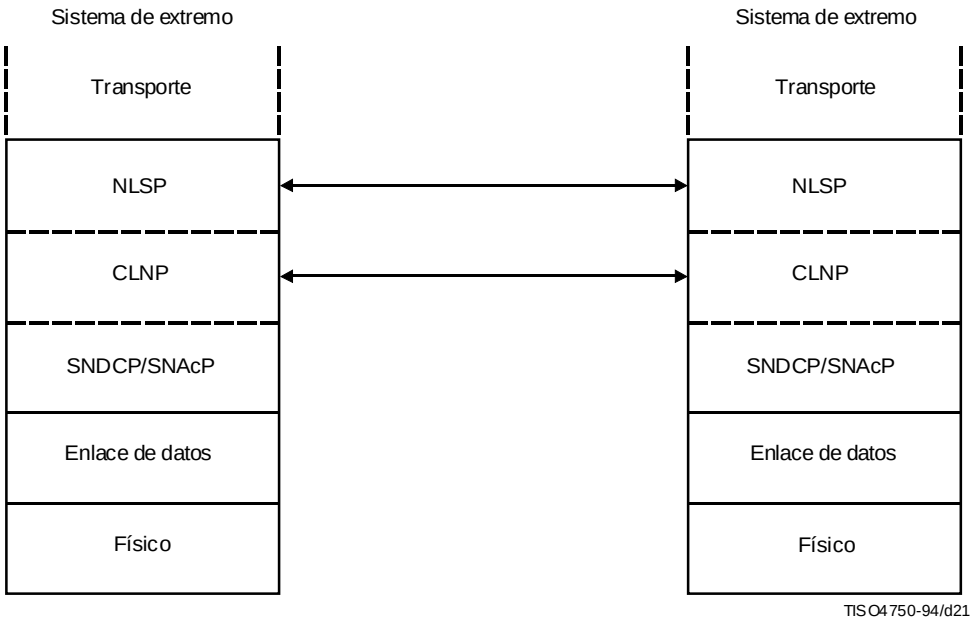


Figura E.5-1 – Ilustración de un NLSP-CL entre sistemas de extremo

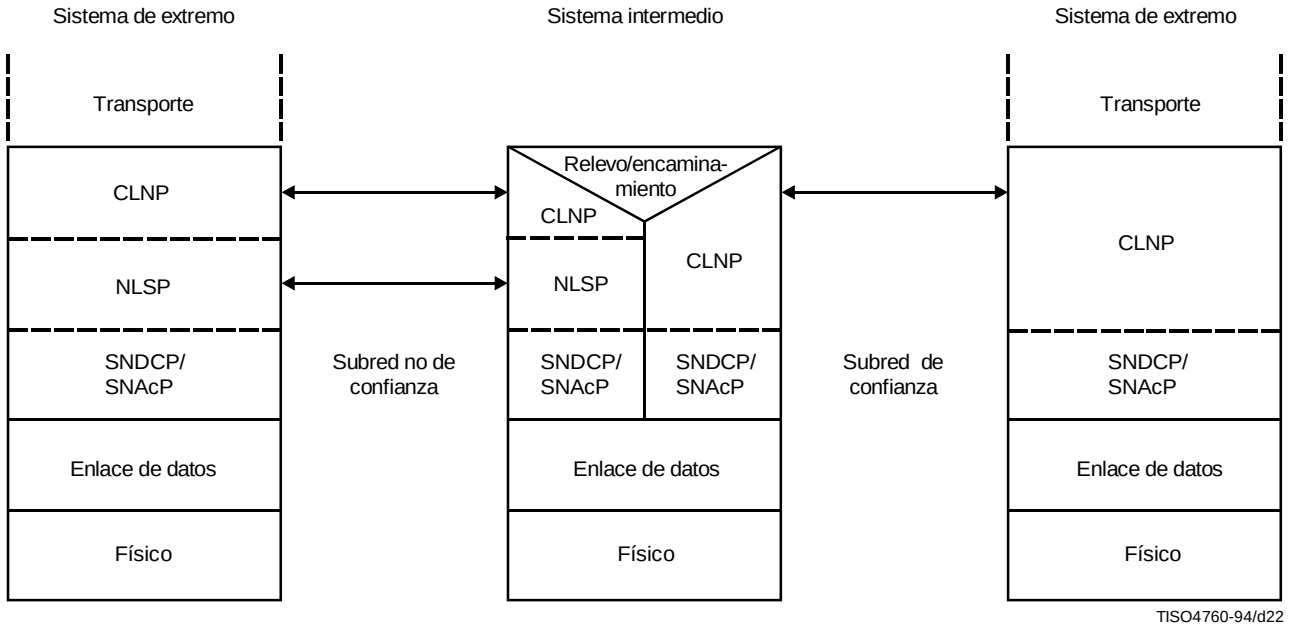


Figura E.5-2 – Ilustración de un NLSP-CL con una red no de confianza

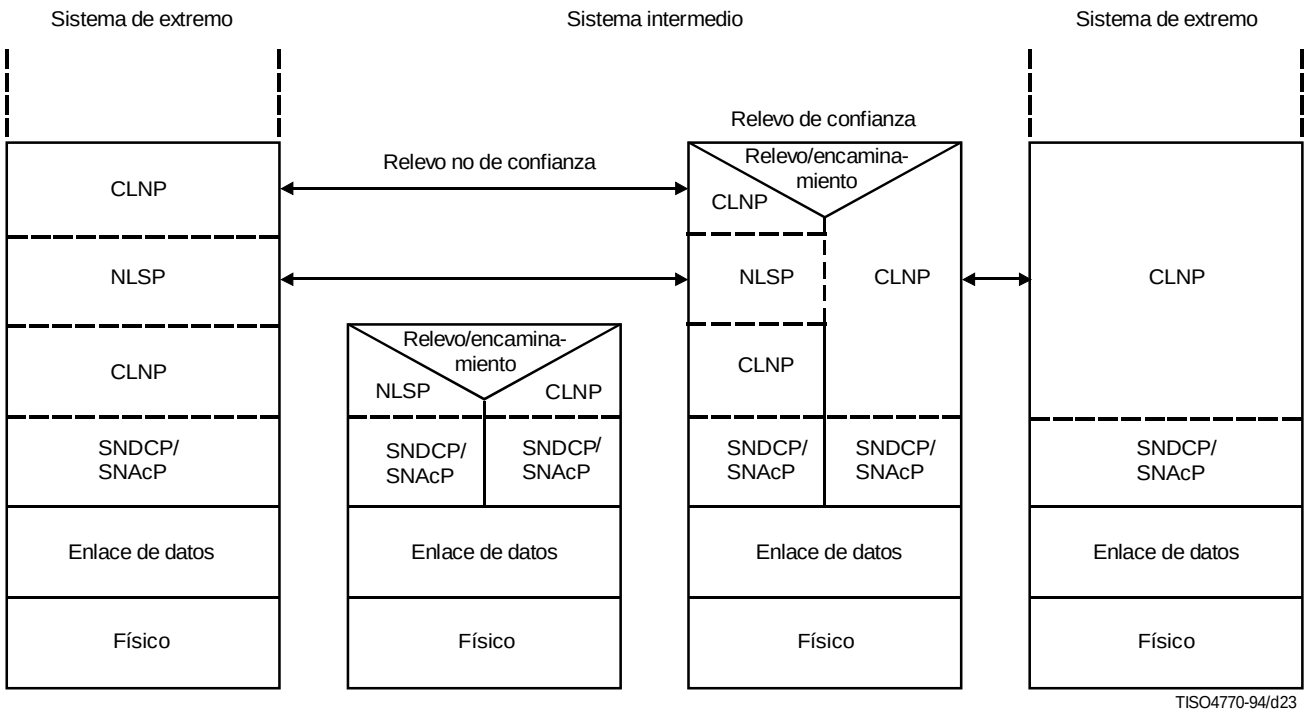


Figura E.5-3 – Ilustración de un NLSP-CL con un sistema de relevo no de confianza

E.5.4 Direccionamiento

En el caso del protocolo NLSP que funciona en la posición superior de la capa de red, la dirección utilizada por el NLSP es una dirección NSAP de red OSI. En el caso de un NLSP que funciona por debajo del protocolo (CLNP) de la Rec. UIT-T X.233 | ISO/CEI 8473 antes de que se le haga corresponder con la subred subyacente, la dirección utilizada en la interfaz por encima y por debajo del NLSP es una dirección de subred (por ejemplo, una dirección MAC de red de área local). En el caso de un NLSP que funciona entre dos capas de CLNP, la dirección que se pasa, hacia abajo, a la entidad NLSP, es una dirección de subred.

Si hay ocultación de dirección (es decir, si Param_Prot es FALSE), las direcciones en la interfaz de servicio UN son las mismas que las direcciones en la interfaz de servicio NLSP.

Si se proporciona ocultación de dirección (es decir, si Param_Prot es TRUE), las direcciones utilizadas en la interfaz de servicio UN (direcciones UN) tienen la misma forma de las direcciones NLSP, no obstante lo cual se utilizan para identificar entidades NLSP que pueden estar situadas en un sistema intermedio o en un sistema de extremo. Estas direcciones UN pueden gestionarse de la misma manera que las direcciones NSAP. Se puede utilizar los mismos esquemas de registro para adjudicar direcciones y se puede utilizar los mismos procedimientos de encaminamiento para gestionar el encaminamiento. Sin embargo, están en dominios de encaminamiento aislados. El NLSP trata la correspondencia de direcciones NSAP a direcciones UN utilizando el atributo de asociación de seguridad Adr_served (dirección servida) para identificar la dirección NSAP servida por las direcciones UN contenidas en el atributo de asociación de seguridad Peer_Adr (dirección de par).

E.5.5 Segmentación

La segmentación y el reensamblado se tratan en la Rec. UIT-T X.233 | ISO/CEI 8473 (protocolo CLNP). La segmentación puede efectuarse antes y después del procesamiento por el protocolo NLSP, lo que depende de las subredes que haya atravesado la PDU. Si la segmentación se efectúa antes del NLSP, cada segmento es encapsulado según el NLSP, enviado al dispositivo de desencapsulación del NLSP, desencapsulado, y seguidamente reensamblado por el CLNP. Si la segmentación se efectúa después del NLSP, el CLNP, primeramente, reensamblará los segmentos. A continuación, el NLSP desencapsulará la PDU completa. El CLNP entregará entonces la PDU desencapsulada a la dirección de destino indicada, mediante procedimientos de comunicación normales.

E.6 Atributos y asociaciones de seguridad

Para que puedan obtenerse comunicaciones seguras, tanto el NLSP-CO como el NLSP-CL tienen que disponer de un conjunto de atributos correspondientes denominados atributos de asociación de seguridad. Estos incluyen:

a) información relativa a la «política» básica, que define o restringe el funcionamiento del NLSP, por ejemplo algoritmo de cifrado, tamaño del bloque de cifrado, número secuencial para la integridad, autoridad definidora de etiquetas;

b) los valores iniciales necesarios para controlar el funcionamiento del NLSP, por ejemplo claves maestras, números secuenciales iniciales para la integridad;

c) los valores actuales necesarios para controlar el funcionamiento del NLSP, por ejemplo la clave de trabajo para una conexión específica, el número secuencial actual para la integridad.

Cuando existe una colección de atributos correspondientes se dice que existe una asociación de seguridad. El conjunto de atributos utilizados para la protección de una PDU en modo sin conexión, o una conexión, es referenciado por un identificador de asociación de seguridad.

El primer conjunto de informaciones relativas a la «política» se denomina un «conjunto convenido de reglas de seguridad», (ASSR, *agreed set of security rules*). Se sugiere que este conjunto se establezca por un procedimiento de registro.

El segundo conjunto de informaciones de control iniciales puede establecerse, o bien «fuera de banda» utilizando sea una interfaz de información local, sea la gestión OSI, o bien «dentro de banda» utilizando un protocolo que funciona conjuntamente con el NLSP y que se llama el «protocolo de establecimiento de asociación de seguridad».

El tercer conjunto de informaciones se actualiza como parte del funcionamiento del protocolo NLSP básico; por ejemplo, en el NLSP-CO pueden establecerse claves de trabajo mediante el intercambio de PDU de control de seguridad de la conexión; los números secuenciales actuales para la integridad se actualizan en cada PDU de transferencia de datos segura.

E.7 Relación funcional dinámica entre el NLSP y el CLNP

E.7.1 Introducción

En la subcláusula E.5.2 de este anexo se describe la relación entre los protocolos NLSP y CLNP en el caso de un ejemplar (dícese una instancia) de comunicación. Esta cláusula tiene por finalidad demostrar la flexibilidad del NLSP cuando se utiliza junto con el CLNP para soportar comunicaciones protegidas y no protegidas independientemente de la arquitectura de las comunicaciones.

La Figura E.7-1 representa el flujo de datos que entra y sale de estos protocolos combinados. El texto que sigue describe el flujo de datos y los parámetros de comunicación requeridos para ello.

E.7.2 Indicación SN-DATO UNIDAD

a) Al entrar una indicación SN-DATO UNIDAD (SN-UNITDATA) (1) [Rec. UIT-T X.233 | ISO/CEI 8473 (CLNP) (véase 5.5)] se comprueba el identificador de protocolo (PID, *protocol identifier*) en el primer octeto (o si se utiliza direccionamiento para identificar el protocolo, la dirección) para determinar si una parte de la PDU contiene un encabezamiento CLNP o NLSP (2).

b) Si el primer encabezamiento identifica un CLNP se toma una decisión en función de la dirección de destino en el encabezamiento CLNP (3). Si la dirección de destino se identifica como una de las direcciones del sistema de extremo del propio sistema, la PDU del CLNP se envía al proceso de reensamblado (4) [CLNP (véase 6.8)]. Si no es una de las direcciones del sistema de extremo, se procesa el encabezamiento CLNP para reenviarlo (8) como se describe en E.6.4.

c) Si el primer encabezamiento identifica un NLSP, el NLSP procesa entonces los parámetros del servicio de subred y los datos de usuario como UN-DATO UNIDAD. Seguidamente se comprueba la indicación de usuario NLSP-DATO UNIDAD resultante para determinar si el primer octeto es un PID de CLNP (8). Si lo es, NLSP-DATO UNIDAD se procesa como ya se ha dicho en b) (3), y en caso contrario la indicación NLSP-DATO UNIDAD se hace corresponder con una indicación N-DATO UNIDAD (7).

d) Después del reensamblado CLNP (si es necesario) (4) hay que tomar otra decisión (5). Si la PDU de CLNP contiene una PDU de NLSP (es decir, si el primer octeto contiene el PID de NLSP), el NLSP procesa los parámetros de servicio y los datos de usuario CLNP como una indicación N-DATO UNIDAD (6), y en caso contrario se hace corresponder directamente con una indicación N-DATO UNIDAD (7). Seguidamente se comprueba la indicación de usuario NLSP-DATO UNIDAD resultante

para determinar si el primer octeto es un PID de CLNP (8) (o, si se utiliza direccionamiento para identificar el protocolo, se comprueba la dirección). Si lo es, NLSP-DATO UNIDAD se procesa como ya se ha dicho en b) (3), y en caso contrario la indicación NLSP-DATO UNIDAD se hace corresponder con una indicación N-DATO UNIDAD (7).

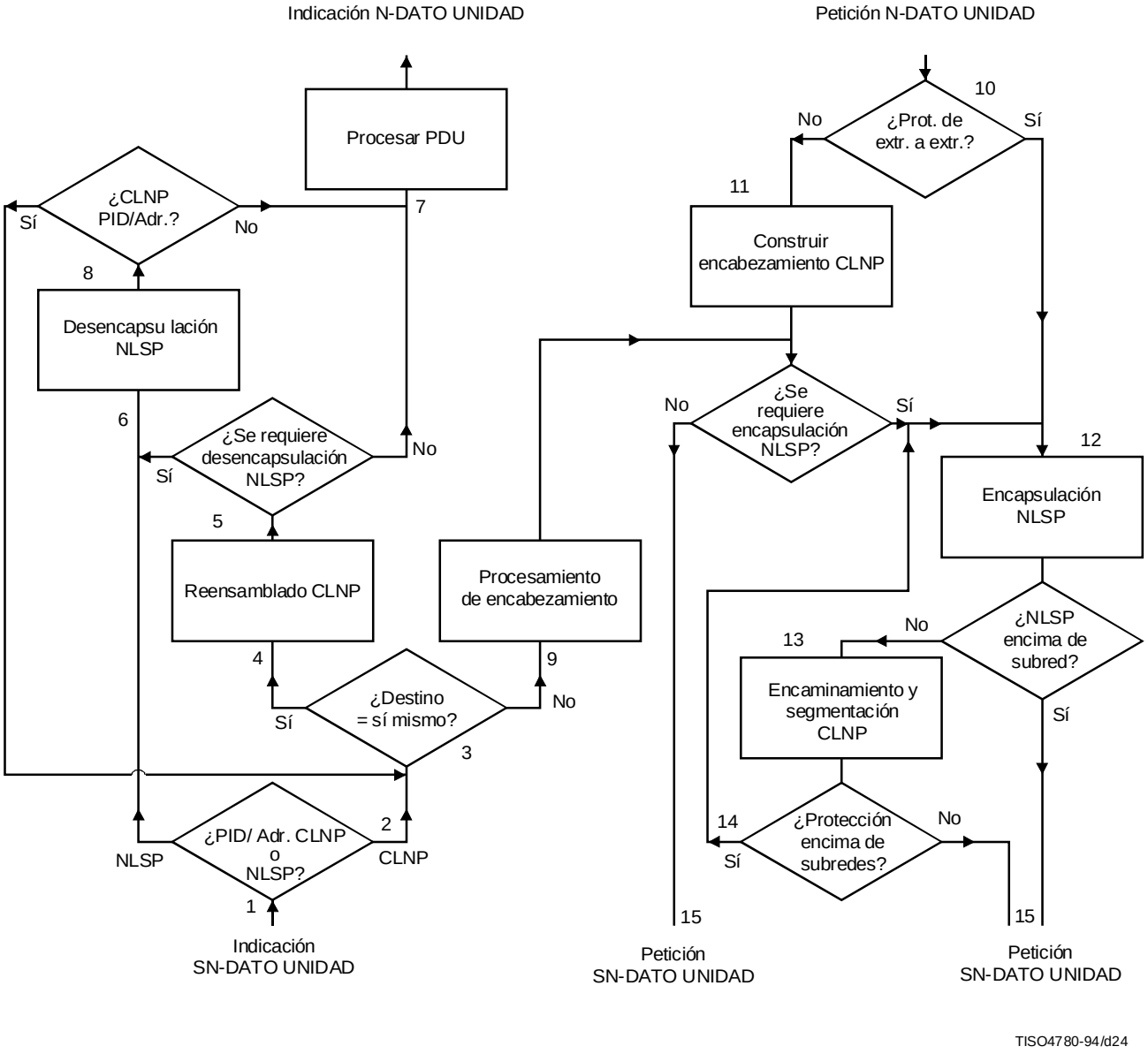


Figura E.7-1 – Diagrama de flujo de NLSP con CLNP

E.7.3 Petición N-DATO UNIDAD

a) Al entrar una petición N-DATO UNIDAD (10), en función de los parámetros de servicio (por ejemplo, dirección de origen o de destino) y de la política de seguridad local, la petición, o bien se hace corresponder directamente con CLNP (véase 5.4) (11), o se hace corresponder con una petición NLSP-DATO UNIDAD y se procesa en consecuencia (12).

b) Si la N-DATO UNIDAD es procesada por CLNP (11), la PDU de CLNP resultante, o bien se hace corresponder directamente con una petición SN-DATO UNIDAD (15), o se hace corresponder con una petición NLSP-DATO UNIDAD (10) para que sea procesada por el NLSP.

c) Si la N-DATO UNIDAD, o una PDU de CLNP, es procesada por NLSP (12), la petición UN-DATO UNIDAD resultante, o bien se hace corresponder directamente con una petición SN-DATO UNIDAD (15), o con el CLNP para procesarla como si fuera una N-DATO UNIDAD (13), lo que dependerá de los parámetros de servicio y de la política de seguridad local. Tras el procesamiento por el protocolo CLNP se puede proporcionar una ulterior protección NLSP si se requiere una protección adicional a través de la subred (14); de lo contrario, la PDU de CLNP se hace corresponder con una SN-DATO UNIDAD.

E.7.4 Reenvío de UPD de CLNP

La decisión de proteger una PDU de CLNP reenviada se basa en la información contenida en el encabezamiento y en los datos de usuario de la PDU de CLNP, así como en las exigencias de la política de seguridad local. Si se requiere protección, la PDU de CLNP se hace corresponder con una petición NLSP-DATO UNIDAD que será procesada por el NLSP (12). En función de los parámetros de servicio y de las exigencias de la política de seguridad local, la UN-DATO UNIDAD resultante se hará corresponder, o bien directamente con una petición SN-DATO UNIDAD [CLNP véase 6.5)] (15) o con el CLNP para procesarla como si fuera una N-DATO UNIDAD (13) de acuerdo con los parámetros de servicio y con las exigencias de la política de seguridad local.

E.7.5 Recapitulación de la interfaz entre el CLNP y el NLSP-CL

Las subcláusulas precedentes muestran la relación funcional entre los protocolos NLSP-CL y CLNP. Para simplificar la exposición, su funcionamiento se muestra como el de dos protocolos distintos, separados por interfaces de servicio. El funcionamiento de estos dos protocolos puede implementarse como un solo protocolo de la capa 3 que combina la funcionalidad de las máquinas de protocolo del CLNP y del NLSP.

E.8 Funcionalidad dinámica relacionada con el modelo estratificado

El método basado en una estructuración en capas para la descripción del NLSP puede relacionarse con la descripción del diagrama de flujo para el ejemplo de configuración ilustrado en la Figura E.7-2, de la manera siguiente:

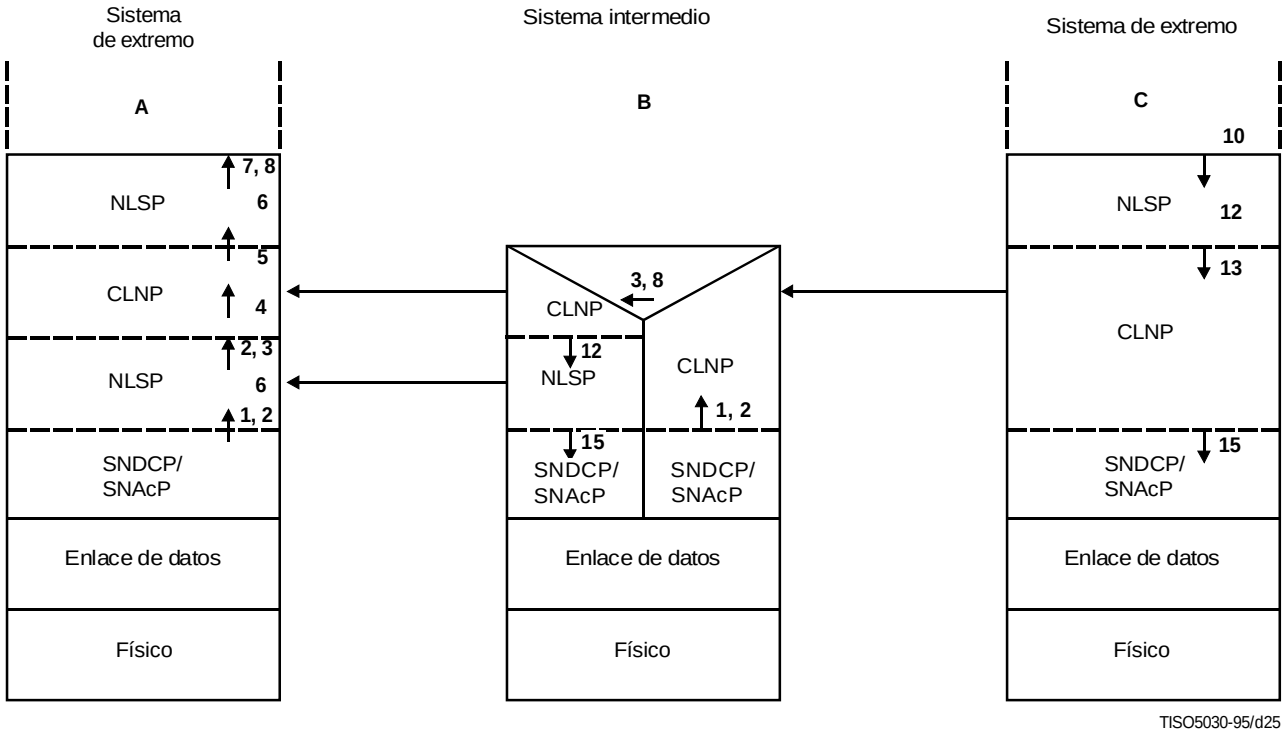


Figura E.7-2 – Modelo estratificado relacionado con el diagrama de flujo

Acción	Referencia al diagrama de flujo
En el sistema de extremo A	
Indicación SN-DATO UNIDAD en el sistema de extremo C	1
Comprobación de la presencia de CLNP o NLSP	2
Comprobación de que el destino es local	3
Reensamblado CLNP	4
Comprobación de la presencia de NLSP	5
Correspondencia con UN-DATO UNIDAD y desencapsulación NLSP	6
Correspondencia con indicación N-DATO UNIDAD	7
Comprobación de la presencia de CLNP	8
En el sistema intermedio B	
Indicación SN-DATO UNIDAD en el sistema intermedio B	1
Comprobación de la presencia de CLNP o NLSP	2
Comprobación de que el destino es local	3
Procesamiento de CLNP para reenvío	8
Correspondencia con NLSP-DATO UNIDAD y encapsulación NLSP	12
Correspondencia de UN-DATO UNIDAD con petición SN-DATO UNIDAD	15
En el sistema de extremo C	
Petición N-DATO UNIDAD en el sistema de extremo A	10
Correspondencia con NLSP-DATO UNIDAD y encapsulación NLSP	12
Correspondencia de UN-DATO UNIDAD con CLNP para su procesamiento como N-DATO UNIDAD	13
Correspondencia de PDU de CLNP con petición SN-DATO UNIDAD	15

Anexo F

Ejemplo de un conjunto convenido de reglas de seguridad

(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 habrán de establecerse, incluidos todos los parámetros necesarios para definir el funcionamiento de los mecanismos para los servicios de seguridad seleccionados. Este anexo presenta un ejemplo de la manera en que pudieran escribirse, en un formulario, los valores de atributos SA que pueden ser establecidos por un ASSR.

ASSR-ID **XYZ(Object identifier)** -- *Da la referencia de objeto utilizada en el SA-P.*

SA-ID_Length **4**

Security services selected Definition Module -- *Indica los servicios de seguridad que podrían ser soportados de acuerdo con las reglas de seguridad y da nombres a los niveles de protección que son soportados utilizando diferentes algoritmos, longitudes de clave, etc.*

PE Auth:	**none,**	**low,**	**high**
AC:	**none,**	**low,**	**high**
Confid:	**none,**	**low,**	**high**
Integ:	**none,**	**low,**	**high**

Security Label Mapping -- *Establece la correspondencia de la etiqueta de seguridad con selecciones de servicios de seguridad.*

Label_Def_Auth **XYZ**

Label->Sensitivity = Unclass
implies:
PE Auth none, AC none, Confid none, Integ none

Label-Sensitivity = Confidential
implies:
PE Auth low, AC low, Confid low, Integ none

Label-Sensitivity = Secret
implies:
PE Auth high, AC high, Confid high, Integ high

Param_Prot **TRUE** -- *Selecciona qué niveles de protección requieren la protección de todos los parámetros de servicio.*

For Security services selected: Integ = high or Conf = high

Mechanism Module – Security labels for Access Control
For Security services selected: AC = high or Conf = high
-- *Indica qué selección de servicios de seguridad requiere etiquetas de seguridad*.

Label_Def_Auth **XYZ**
(Note this must be the same as Auth for protection QOS labels)

Explicit indication **Yes**

Mechanism Module – Integrity Check Value
For security service selection: Integ > none or PE Auth = High or Mechanism Security Labels

ICV_Alg **XYZ**
Rekey after **10 000 PDUs**
Key distrib mechanism **Asymmetric**

Mechanism Module – Integrity Sequence Number

For security services selected: Integ = high or Auth = High

ISN_Len **8 octets total**

Sequence Number **4 octets**

incremented by 1

Timestamp **4 octets**

milliseconds from sync point

Receive ISN Window **Discard previous sequence #.**

Timestamp should be within 2*maximum

variation in network

delay. If outside

window then a replay attack.

Mechanism Module – Encipherment

For security services selected: Conf > low

Enc_Alg_ID **XYZ**

Mode **Chained**

Enc_Blk **8 octets**

key exchange info **(e.g. Prime p, Generator a)**

Rekey after **1 000 PDUs**

Key distrib mechanism **Asymmetric**

Mechanism Module – No Header

For security services selected: Conf = low and Integ = none and not Label mechanism

Mechanism Module – Connection Authentication

For security services selected: AC > Low or PE Auth > Low

Enc_Alg_ID **XYZ**

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

Enc_Alg **RSA**

Anexo G

Asociaciones y atributos de seguridad

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

Para proteger una instancia de comunicación (una SDU en modo sin conexión o una conexión) hay que establecer entre las entidades comunicantes una colección de informaciones (claves y otros atributos necesarios para controlar la operación de seguridad). Esta colección de informaciones se denomina una asociación de seguridad, brevemente, (SA, *security association*).

La información que constituye una SA es, o bien una información estática, que puede ser «personalizada» al establecerse la SA y queda fija durante la existencia de la asociación, o bien una información dinámica, que puede ser actualizada durante la existencia de la asociación de seguridad.

Una SA puede establecerse «fuera de banda» o, en el caso del NLSP-CO, «dentro de banda» mediante el intercambio de PDU de SA. Cuando se utiliza el método dentro de banda, los mecanismos específicos para realizar el SA-P pueden ser los definidos en esta Recomendación UIT-T | Norma Internacional, o mecanismos privados.

Antes de establecer una SA, cada entidad NLSP tiene que haber establecido previamente:

a) Un conjunto común de reglas de seguridad que, en presencia de servicios de seguridad seleccionados, especifica los mecanismos de seguridad que habrán de utilizarse, incluidos todos los parámetros necesarios para definir la operación de los mecanismos (por ejemplo, algoritmo, longitud de las claves, duración de las claves). Estas reglas de seguridad son convenidas de mutuo acuerdo e identificadas inconfundiblemente por las entidades comunicantes. Las reglas de seguridad y sus identificadores pueden ser registrados por terceros. Véase el Anexo F, que presenta un ejemplo de un conjunto convenido de reglas de seguridad.

b) Los servicios de seguridad, y por tanto los mecanismos de seguridad, que pueden utilizarse.

Si se utiliza el método dentro de banda para el establecimiento de una SA, deberá haberse establecido previamente:

c) Los servicios de seguridad iniciales seleccionados, y por tanto los mecanismos de seguridad, que se aplicarán al establecerse una SA.

d) La información básica sobre la aplicación de las claves que se necesite para establecer una SA.

Al establecer una SA, una entidad NLSP establece la siguiente información compartida con su entidad par distante:

e) Los identificadores SA-ID local y distante.

f) Los servicios de seguridad que habrán de utilizarse entre las entidades asociadas para instancias de comunicación.

g) Los mecanismos, y sus parámetros, obtenidos implícitamente según los servicios de seguridad seleccionados.

h) Las claves iniciales compartidas que habrán de utilizarse para la integridad, los mecanismos de cifrado y la autenticación de una instancia de comunicación.

i) El conjunto de etiquetas y direcciones de seguridad que pueden utilizarse en la asociación en cuestión para el control de acceso.

Las referencias SA y las claves compartidas [apartados e) y h) precedentes] deben establecerse para cada asociación. Las otras informaciones pueden estar preestablecidas y ser comunes a varias asociaciones. Además, como parte del establecimiento de una SA personalizada, hay que autenticar la identidad de la entidad par distante. En el anexo C se define un mecanismo que puede utilizarse para la distribución de claves y la autenticación.

Las siguientes informaciones pueden ser actualizadas dinámicamente para una instancia de comunicación:

j) Número(s) secuencial(es) para la integridad, necesario(s) para los datos normales y acelerados en cada sentido de transmisión.

k) Una etiqueta de seguridad.

l) Información de reaplicación de clave para los mecanismos de cifrado/integridad.

Para obtener la autenticación es necesario aplicar mecanismos de autenticación a cada instancia de comunicación.

En la Figura G.1 se muestran diferentes atributos que pueden establecerse en las diferentes etapas de una asociación de seguridad.

<table>
<tr><th>Preestablecidos</th><th>Estáticos</th><th>Dinámicos</th></tr>
<tr><td>Gama de servicios de seguridad seleccionados
Servicios de seguridad iniciales seleccionados
Información básica de claves
Conjunto convenido de reglas de seguridad</td><td>Claves iniciales
SA-ID
Autenticación
Etiqueta de seguridad</td><td>ISN
Autenticación
SA-ID
Información de reaplicación de clave</td></tr>
<tr><td colspan="2">Servicios de seguridad seleccionados
Mecanismos seleccionados
Conjunto de etiquetas/direcciones de seguridad</td><td></td></tr>
</table>

Figura G.1 – Ilustración de los tres aspectos de la asociación de seguridad

Anexo H

Ejemplo de intercambio de testigos de clave – Algoritmo EKE

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

La exposición que sigue es un ejemplo de un algoritmo de intercambio de testigos de clave que puede utilizarse con el protocolo de asociación de seguridad definido en el Anexo C.

Este algoritmo, llamado 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 H.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 C son los siguientes:

- La cadena de bits compartida KTE es (a**XY mod P).
- Key-Token-1 es a, p, (a**X mod P), donde 'a', 'p', y (a**X mod P) se codifican como cadenas de octetos concatenadas.
- Key-Token-2 es (a**Y mod P).
- Key-Token-3 es la información derivada de la cadena de bits KTE compartida (a**XY mod P) al contador de ataques de respuesta.
- Key-Token-4 es la información derivada de la cadena de bits KTE compartida (a**XY mod P) al contador de ataques de respuesta.

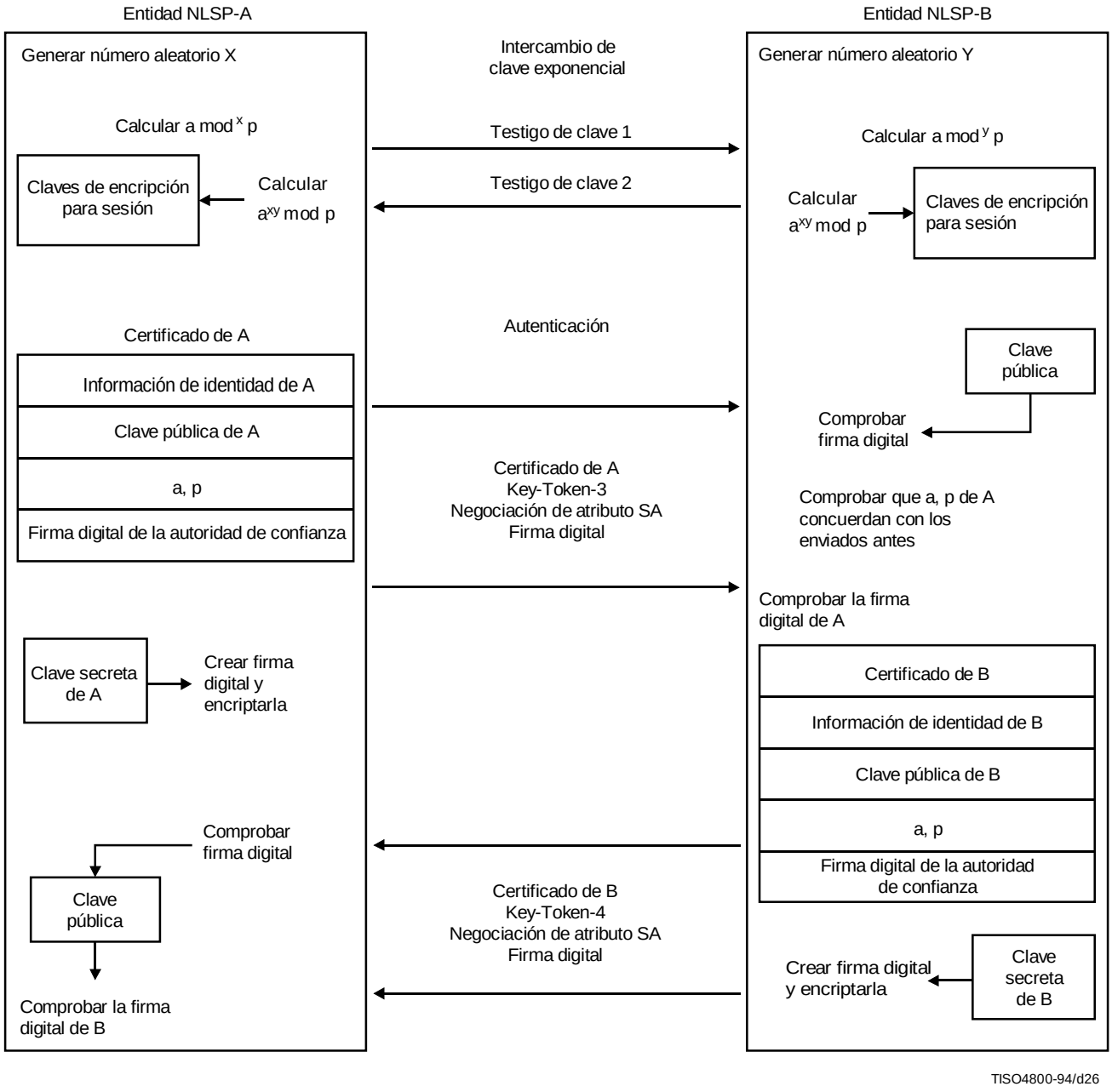


Figura H.1 – Ilustración de la derivación de claves «en línea» y la derivación de claves mediante el algoritmo EKE