UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.803

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(07/94)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MODELO DE SEGURIDAD DE CAPAS SUPERIORES

Recomendación UIT-T X.803

(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.803 se aprobó el 1 de julio de 1994. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10745.

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 UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Introducción y Resumen

La arquitectura de seguridad de la interconexión de sistemas abiertos (Rec. X.800 del CCITT | ISO 7498-2) define los elementos arquitecturales relacionados con la seguridad cuya aplicación es apropiada cuando se requiere protección de seguridad en un entorno de sistemas abiertos.

La presente Recomendación | Norma Internacional describe la selección, colocación y utilización de los servicios y mecanismos de seguridad en las capas superiores (capas de aplicación, presentación y sesión) del modelo de referencia de interconexión de sistemas abiertos.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MODELO DE SEGURIDAD DE CAPAS SUPERIORES

1 Alcance

1.1 Esta Recomendación | Norma Internacional define un modelo arquitectural que sienta las bases para:

a) el desarrollo de servicios y protocolos independientes de la aplicación para seguridad en las capas superiores de OSI; y

b) la utilización de estos servicios y protocolos para satisfacer los requisitos de seguridad de una gran variedad de aplicaciones, minimizando así la necesidad de que los elementos de servicio de aplicación específicos de la aplicación contengan servicios de seguridad internos.

1.2 En particular, esta Recomendación | Norma Internacional especifica:

a) los aspectos de seguridad de la comunicación en las capas superiores de OSI;

b) el soporte en las capas superiores de los servicios de seguridad definidos en la arquitectura de seguridad de OSI y los marcos de seguridad para sistemas abiertos;

c) la posición de los servicios y mecanismos de seguridad, y las relaciones entre ellos en las capas superiores, de acuerdo con las directrices de la Rec. X.800 del CCITT | ISO 7498-2 y de la Rec. UIT-T X.207 | ISO/CEI 9545;

d) las interacciones entre las capas superiores y entre las capas superiores y las inferiores, cuando se prestan y utilizan servicios de seguridad;

e) la necesidad de gestión de información de seguridad en las capas superiores.

1.3 Con respecto al control de acceso, el alcance de esta Recomendación | Norma Internacional incluye servicios y mecanismos de control de acceso a los recursos de OSI y a los recursos accesibles mediante OSI.

1.4 Esta Recomendación | Norma Internacional no incluye:

a) la definición de servicios de OSI o la especificación de protocolos de OSI;

b) la especificación de técnicas y mecanismos de seguridad, su funcionamiento y sus requisitos de protocolo; y

c) aspectos de la provisión de seguridad no relacionados con las comunicaciones OSI.

1.5 Esta Recomendación | Norma Internacional no es una especificación de realización de sistemas ni una base para evaluar la conformidad de las realizaciones.

NOTA – El alcance de esta Recomendación | Norma Internacional incluye la seguridad de aplicaciones sin conexión y aplicaciones distribuidas (tales como aplicaciones de almacenamiento y retransmisión, aplicaciones encadenadas y aplicaciones que actúan en nombre de otras aplicaciones).

2 Referencias normativas

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

la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas Internacionales citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones del UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.207 (1993) | ISO/CEI 9545:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la capa de aplicación.*
- Recomendación UIT-T X.811[1)] | ISO/CEI 10181-2...[1)], *Tecnología de la información – Marcos de seguridad en sistemas abiertos: Marco de autenticación.*
- Recomendación UIT-T X.812[1)] | ISO/CEI 10181-3...[1)], *Tecnología de la información – Marcos de seguridad en sistemas abiertos: Marco de control de acceso.*

2.2 Recomendaciones | Normas Internacionales de contenido técnico equivalente

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

  ISO 7498: 1984/Corr.1:1988, *Information Processing Systems – Open Systems Interconnection – Basic Reference Model.*
- Recomendación X.216 del CCITT (1988), *Definición del servicio de presentación para la interconexión de sistemas abiertos para aplicaciones del CCITT.*

  ISO 8822:1987, *Information Processing Systems – Open Systems Interconnection – Connection Oriented Presentation Service Definition.*
- Recomendación X.217 del CCITT (1988), *Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT.*

  ISO 8649:1987, *Information Processing Systems – Open Systems Interconnection – Service definition for the Association Control Service Element.*
- Recomendación X.700 del CCITT (1992), *Definición del marco de gestión para interconexión de sistemas abiertos para aplicaciones del CCITT.*

  ISO/CEI 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.*
- Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad para interconexión de sistemas abiertos para aplicaciones del CCITT.*

  ISO 7498-2:1988, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security architecture.*

3 Definiciones

3.1 Se utilizan los siguientes términos definidos en la Rec. X.200 del CCITT | ISO 7498:

a) sintaxis abstracta;

b) entidad de aplicación;

c) proceso de aplicación;

d) invocación de proceso de aplicación;

e) información de control de protocolo de aplicación;

f) unidad de datos de protocolo de aplicación;

g) entorno de sistema local;

h) función (N);

---

1) Actualmente en estado de proyecto.

i) retransmisión (N);
j) sistema abierto;
k) contexto de presentación;
l) entidad de presentación;
m) sistema abierto real;
n) gestión de sistemas;
o) sintaxis de transferencia.

3.2 Se utilizan los siguientes términos definidos en la Rec. X.800 del CCITT | ISO 7498-2:

a) control de acceso;
b) autenticación;
c) confidencialidad;
d) integridad de los datos;
e) autenticación de origen de los datos;
f) descifrado;
g) cifrado;
h) clave;
i) no repudio;
j) notarización;
k) autenticación de entidad par;
l) auditoría de seguridad;
m) base de información de gestión de seguridad;
n) política de seguridad;
o) protección selectiva de los campos;
p) firma;
q) confidencialidad del flujo de tráfico;
r) funcionalidad de confianza.

3.3 Se utilizan los siguientes términos definidos en la Rec. X.700 del CCITT | ISO 7498-4:

a) información de gestión;
b) gestión de OSI.

3.4 Se utilizan los siguientes términos definidos en la Rec. UIT-T X.207 | ISO/CEI 9545:

a) asociación de aplicación;
b) contexto de aplicación;
c) invocación de entidad de aplicación (AEI);
d) elemento de servicio de aplicación (ASE);
e) tipo de ASE;
f) objeto de servicio de aplicación (ASO);
g) asociación de ASO;
h) contexto de ASO;
i) invocación de ASO;
j) tipo de ASO;
k) función de control (CF).

3.5 Se utilizan los siguientes términos definidos en la Rec. X.216 del CCITT | ISO 8822:

– valor de datos de presentación.

3.6 Se utilizan los siguientes términos definidos en la Rec. UIT-T X.811 | ISO/CEI 10181-2:

a) intercambio de autenticación;

b) información de autenticación de declaración;

c) declarante;

d) información de autenticación de intercambio;

e) autenticación de entidad;

f) principal;

g) información de autenticación de verificación;

h) verificador.

3.7 Se utilizan los siguientes términos definidos en la Rec. UIT-T X.812 | ISO/CEI 10181-3:

a) certificado de control de acceso;

b) información de control de acceso.

3.8 A los fines de esta Recomendación | Norma Internacional, son aplicables las siguientes definiciones:

estado de seguridad de asociación: Estado de seguridad relacionado con una asociación de seguridad.

contexto de presentación de protección: Contexto de presentación que asocia una sintaxis de transferencia de protección con una sintaxis abstracta.

sintaxis de transferencia de protección: Sintaxis de transferencia basada en procesos de codificación/decodificación que emplea una transformación de seguridad.

sello: Valor de verificación criptográfico que sustenta la integridad pero que no protege contra falsificación por el recibiente (es decir, no admite la facilidad de no repudio).

asociación de seguridad: Relación entre dos o más entidades para la que existen atributos (información y reglas de estado) para regir la prestación de servicios de seguridad que afectan a esas entidades.

función de comunicación de seguridad: Función que admite la transferencia de información relacionada con la seguridad entre sistemas abiertos.

dominio de la seguridad: Conjunto de elementos, política de seguridad, autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad en las que el conjunto de elementos está sujeto a la política de seguridad, administrada por la autoridad de seguridad, para las actividades específicas.

intercambio de seguridad: Transferencia o secuencia de transferencias de información de control de protocolo de aplicación entre sistemas abiertos como parte de la operación de uno o más mecanismos de seguridad.

ítem de intercambio de seguridad: Pieza de información lógicamente distinta que corresponde a una sola transferencia (en una secuencia de transferencias) en un intercambio de seguridad.

función de intercambio de seguridad: Función de comunicación de seguridad, ubicada en la capa de aplicación, que proporciona los medios para comunicar información de seguridad entre invocaciones de entidades de aplicación.

reglas de interacción de seguridad: Aspectos comunes de las reglas necesarias para que se produzcan interacciones entre dominios de seguridad.

estado de seguridad: Información de estado que se mantiene en un sistema abierto y que se requiere para la provisión de servicios de seguridad.

función de seguridad de sistema: Capacidad de un sistema abierto de ejecutar un procesamiento relacionado con la seguridad.

objeto de seguridad de sistema: Objeto que representa un conjunto de funciones de seguridad de sistema conexas.

transformación de seguridad: Conjunto de funciones (funciones de seguridad de sistema y funciones de comunicación de seguridad) que, en combinación, actúan en los ítems de datos de usuario para protegerlos de un modo particular durante la comunicación o el almacenamiento.

NOTA – Las especificaciones de las funciones de seguridad de sistemas y de los objetos de seguridad de sistemas no forman parte de las definiciones de servicios de capa ni de especificaciones de protocolos de OSI.

4 Abreviaturas

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

ACSE Elemento de servicio de control de asociación (*association control service element*)

AE Entidad de aplicación (*application-entity*)

AEI Invocación de entidad de aplicación (*application-entity-invocation*)

ASE Elemento de servicio de aplicación (*application-service-element*)

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

ASO Objeto de servicio de aplicación (*application-service-object*)

CF Función de control (*control function*)

FTAM Transferencia, acceso y gestión de ficheros (*file transfer, access and management*)

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

PE Entidad de presentación (*presentation-entity*)

PEI Invocación de entidad de presentación (*presentation-entity-invocation*)

PDV Valor de datos de presentación (*presentation data value*)

SEI Ítem de intercambio de seguridad (*security exchange item*)

SSO Objeto de seguridad de sistema (*system security object*)

5 Conceptos

El modelo de seguridad trata de la provisión de servicios de seguridad para contrarrestar amenazas relacionadas con las capas superiores de OSI, como las que se describen en el Anexo A a la Rec. X.800 del CCITT | ISO 7498-2. Incluye la protección de la información que pasa a través de sistemas de retransmisión de aplicaciones.

5.1 Política de seguridad

Si dos o más sistemas abiertos reales han de comunicar de manera segura deben estar sujetos a las políticas de seguridad en vigor en sus respectivos dominios de seguridad, y a una política de interacción segura si la comunicación se ha de producir entre dominios de seguridad diferentes. Una política de interacción segura comprende los aspectos comunes de políticas de seguridad en diferentes dominios de seguridad y determina las condiciones en las cuales puede efectuarse la comunicación entre ellos.

Las disposiciones de una política de interacción segura se pueden describir mediante un conjunto de reglas de interacción seguras. Estas reglas rigen, entre otras cosas, la selección de los contextos de ASO (incluidos los contextos de aplicación) que se van a utilizar en casos particulares de comunicación.

5.2 Asociaciones de seguridad

Una asociación de seguridad es una relación entre dos o más entidades para la que existen atributos (información y reglas de estado) que rigen la prestación de servicios de seguridad que afectan a esas entidades. Una asociación de seguridad supone la existencia de reglas de interacción seguras, y el mantenimiento de un estado de seguridad coherente en ambos sistemas.

Desde la perspectiva de las capas superiores de OSI, una asociación de seguridad corresponde con una asociación de ASO. Dos casos especiales son:

– *asociación de seguridad de asociación de aplicación* – Asociación de seguridad entre dos sistemas para sustentar la comunicación protegida a través de una asociación de aplicación;

– *asociación de seguridad con transmisión* – Asociación de seguridad entre dos sistemas para sustentar la comunicación protegida a través de una retransmisión de aplicación (por ejemplo, en aplicaciones con almacenamiento y retransmisión, o con encadenamiento).

Otros ejemplos de tipos diferentes de asociaciones de seguridad son:

- una asociación de seguridad entre dos sistemas que comunican directamente entre sí a través de múltiples asociaciones de aplicación y/o la comunicación de múltiples unidades de datos sin conexión;
- una asociación de seguridad entre una entidad que escribe la información protegida en una memoria de datos (por ejemplo, directorio o memoria de fichero) y entidades que leen esa información;
- una asociación de seguridad entre dos entidades de protocolo de seguridad de capa inferior pares.

Dentro de un proceso de aplicación una asociación de seguridad puede depender del mantenimiento de otra asociación de seguridad con otro sistema, tal como un servidor de autenticación u otro tipo de tercero de confianza.

5.3 Estado de seguridad

Estado de seguridad es la información de estado mantenida en un sistema real abierto y que se necesita para la prestación de servicios de seguridad. La existencia de una asociación de seguridad entre procesos de aplicación implica la existencia de un estado de seguridad compartida.

Es posible que cierta información de estado de seguridad tenga que estar a disposición de uno o más procesos de aplicación antes de intentar el establecimiento de la comunicación, y mantenerla mientras dichas comunicaciones están activas y/o después que finalizan. La naturaleza exacta de esta información de estado depende de los mecanismos y aplicaciones de seguridad particulares.

Dos categorías de estado de seguridad son:

a) *Estado de seguridad de sistema* – Información de estado relacionado con la seguridad que se establece y mantiene en un sistema abierto real, con independencia de la existencia o del estado de cualquier actividad de comunicación;

b) *Estado de seguridad de asociación* – Estado de seguridad relacionado con una asociación de seguridad. En las capas superiores de OSI, el estado de seguridad compartida rige las propiedades de seguridad de los contextos de ASO utilizados entre invocaciones de ASO y/o el estado de seguridad inicial de las asociaciones de aplicación recientemente establecidas. Dos casos especiales son:

   - cuando la asociación de seguridad corresponde con una sola asociación de aplicación. El estado de seguridad se denomina **estado de seguridad de asociación de aplicación.** Pertenece al control de seguridad de las comunicaciones de esa asociación de aplicación;
   - cuando la asociación de seguridad corresponde con una asociación de ASO que conlleva transferencia de información entre dos sistemas de usuario de extremo a través de un sistema de retransmisión de aplicación. El estado de seguridad compartida pertenece a la utilización de mecanismos de seguridad entre los sistemas de usuario de extremo, con independencia de los mecanismos de seguridad relacionados con asociaciones de aplicación individuales establecidas con el sistema de retransmisión de aplicación.

Son ejemplos de estado de seguridad:

a) la información de estado asociada al encadenamiento criptográfico o al restablecimiento de la integridad;

b) el conjunto de etiquetas de seguridad relativas a información que puede ser intercambiada;

c) clave(s) o identificador(es) de clave(s) que se van a emplear en la prestación de los servicios de seguridad en las capas superiores. Entre ellas podrían figurar las claves de autoridades de certificación de confianza conocidas (véase la Rec. X.509 del CCITT | ISO/CEI 9594-8, Marco de la autenticación de directorios) o claves que permiten las comunicaciones con un centro de distribución de claves;

d) identidades autenticadas previamente;

e) números de secuencia y variables de sincronización criptográfica.

El estado de seguridad se puede inicializar de diversas maneras:

a) empleando una función de gestión de seguridad en cuyo caso la información de estado reside en la base de información de gestión de seguridad;

b) como información residual procedente de actividades de comunicación anteriores;

c) por medios externos a OSI.

5.4 Requisitos de la capa de aplicación

Para que los procesos de aplicación participen en comunicaciones seguras han de contar con las disposiciones de seguridad apropiadas del contexto de ASO (o contexto de aplicación) que se utiliza.

La definición de un contexto de ASO puede incluir:

a) los tipos de ASO y/o ASE requeridos para sustentar los protocolos de seguridad;

b) reglas para la negociación y selección de funciones de seguridad relacionadas con las capas de aplicación y presentación;

c) reglas para la selección de servicios de seguridad subyacentes;

d) reglas para la aplicación de servicios de seguridad particulares para determinadas categorías de información que se han de intercambiar;

e) reglas para reautenticar identidades pertinentes durante la vida de una asociación;

f) reglas para el cambio de claves durante la vida de una asociación de ASO (si se utilizan mecanismos criptográficos);

g) reglas que se han de seguir si fallan las comunicaciones o se detectan violaciones de la seguridad.

NOTA – Un contexto de ASO puede definirse por referencia a una definición de tipo de ASO.

Un contexto de aplicación es el caso particular de un contexto de ASO, que describe el comportamiento admisible de comunicaciones colectivas de dos invocaciones de ASO que participan en una asociación de aplicación. Los aspectos de seguridad descritos en 5.4.1 son pertinentes a los contextos de aplicación.

6 Arquitectura

6.1 Modelo global

La prestación de servicios de seguridad OSI conlleva la generación, intercambio y procesamiento de la información de seguridad de acuerdo con los procedimientos de mecanismos de seguridad específicos. Hay dos tipos de función diferentes:

a) *Función de seguridad de sistema* – Capacidad de un sistema de efectuar un procesamiento relacionado con la seguridad, tal como el cifrado/descifrado, firma digital, o la generación o procesamiento de un certificado o testigo de seguridad transmitido en un intercambio de autenticación. La ejecución de dichas funciones no forma parte de la realización de servicios o protocolos de capa de OSI.

b) *Función de comunicación de seguridad* – Función que sustenta la transferencia de la información relacionada con la seguridad entre sistemas abiertos. Estas funciones se realizan en entidades de aplicación o entidades de presentación de OSI. Son ejemplos de funciones de comunicación de seguridad:

   – funciones de intercambio de seguridad, como se describe en 6.3;

   – codificación/decodificación de los elementos de protocolo de la capa de presentación designados para transmitir información cifrada o firmada digitalmente;

   – protocolos para comunicar con un servidor de seguridad, por ejemplo, un servidor de autenticación o un centro de distribución de claves.

La distinción entre funciones de seguridad de sistema y funciones de comunicación de seguridad es importante por dos aspectos. En primer lugar, delinea dos tipos diferentes de normas. Las funciones de seguridad de sistema se especifican en normas de mecanismos de seguridad o de técnicas de seguridad. Estas normas están habitualmente concebidas como normas de uso general y no están necesariamente vinculadas a ningún protocolo o capa de comunicación concreta. Las normas de funciones de seguridad de sistema son posiblemente útiles para otros fines distintos de la seguridad en las comunicaciones. Por otro lado, las funciones de comunicación de seguridad forman parte de las especificaciones de protocolo de comunicaciones concretas (por ejemplo, capas superiores de OSI) y no están necesariamente vinculadas a determinados mecanismos o técnicas de seguridad.

La otra importancia de la distinción es que modela la separación entre la funcionalidad de seguridad y la funcionalidad de las comunicaciones en una realización. Un conjunto de funciones de seguridad de sistema se aplicará típicamente como módulo de seguridad, por ejemplo, como un subsistema de soporte lógico de confianza o un módulo de soporte físico a prueba de falsificación, potencialmente aplicable en una variedad de comunicaciones o de otros entornos. Por tanto, la frontera entre funciones de seguridad de sistema y funciones de comunicaciones de seguridad puede constituir un punto inicial valioso para definir interfaces de realización normalizadas, por ejemplo, una interfaz de programa de aplicación de seguridad.

A efectos arquitecturales se presenta el concepto de **objeto de seguridad de sistema** (SSO). Un SSO es un objeto que representa un conjunto de funciones conexas de seguridad de sistema.

Los SSO pueden interactuar con funciones de comunicación de seguridad a través de una frontera de servicio (interfaz) abstracta, para prestar el servicio o los servicios de seguridad requeridos. Los SSO generan y procesan información de seguridad intercambiada utilizando protocolos de OSI en las capas de aplicación y de presentación. La estructura lógica de la información de seguridad intercambiada puede normalizarse en OSI, de modo que pueda representarse en intercambios de protocolos OSI.

Una invocación de SSO es una instancia de ejecución de un SSO. En un modelo dinámico, una invocación de SSO puede interactuar con una invocación de entidad de OSI, por ejemplo, en una invocación de AE.

El funcionamiento de un SSO puede incluir:

– la aceptación de información de funciones de comunicación de seguridad de OSI, y el suministro de información a las mismas, que pueden enviar y/o recibir información en nombre del SSO;

– el establecimiento de una asociación de aplicación con otro sistema abierto, por ejemplo, un servidor de autenticación de tercero, y la utilización de esa asociación de aplicación para funciones de seguridad de sistema del SSO;

– el establecimiento de una asociación de seguridad que va a utilizarse subsiguientemente para prestar un servicio de seguridad.

NOTA 1 – La especificación de determinadas funciones de seguridad de sistema, objetos de seguridad de sistema o fronteras de servicio abstractas queda fuera del alcance de este modelo de seguridad.

NOTA 2 – Las realizaciones de objetos de seguridad de sistema pueden utilizarse para otros fines que la seguridad de OSI, si bien cualquiera de esas utilizaciones queda fuera del alcance de este modelo de seguridad.

La Figura 1 muestra un modelo básico de funciones de seguridad asociadas a las capas de aplicación y de presentación. Los objetos del modelo son entidades de aplicación (AE), entidades de presentación (PE), SSO y servicios de OSI de soporte (en las capas 1 a 5 de OSI). Los servicios de OSI de soporte facilitan la infraestructura de comunicaciones básica para intercambiar información relacionada con la seguridad (e información no relacionada con la seguridad).

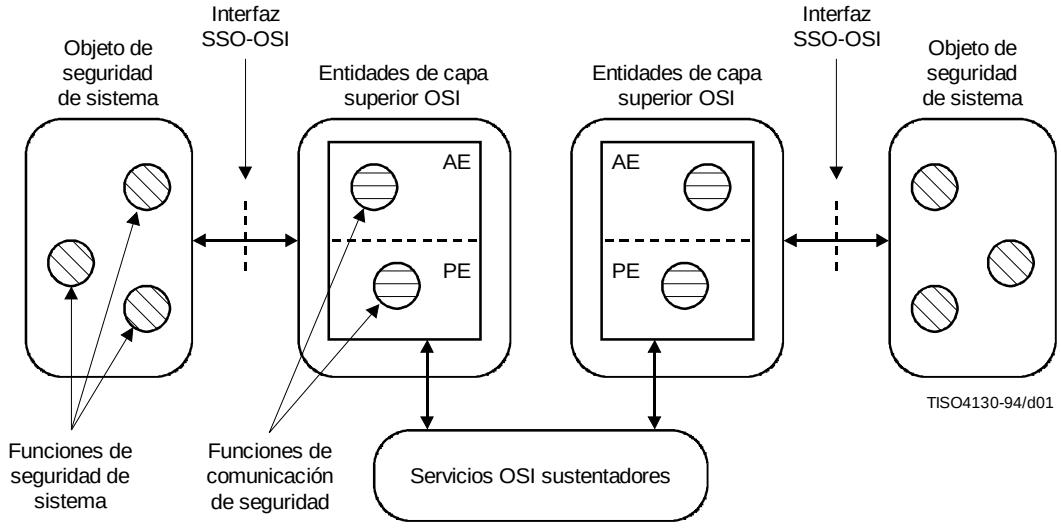

Figura 1 – Funciones de seguridad asociadas con las capas superiores de OSI

Las entidades de capa de OSI en las capas superiores contribuyen a la prestación de servicios de seguridad de la siguiente manera:

- En la capa de aplicación, los AE modelan los aspectos de las comunicaciones de los procesos de aplicación y pueden ser mejorados en términos de ASE, ASO y funciones de control, como se describe en la Rec. X.207 del CCITT | ISO/CEI 9545. Una AE puede contener ASE y/o ASO especializados en la provisión de funciones de comunicación de seguridad. Los ASE y/o los ASO pueden también disponer la información que se ha de proteger utilizando transformaciones de seguridad (véase 6.4) y/o solicitando una calidad de servicio adecuada de las capas subyacentes.
- En la capa de presentación, las funciones de comunicación de seguridad son proporcionadas por la entidad de presentación. Estas funciones pueden trabajar junto con las funciones de seguridad de sistema (por ejemplo, cifrado) utilizadas en la correspondencia de una sintaxis abstracta con una sintaxis de transferencia (véase 6.4).
- En la capa de sesión no se prestan servicios de seguridad. No obstante, en 6.2.1 se señalan algunos aspectos del funcionamiento de la capa de sesión que pueden repercutir en las disposiciones de seguridad dentro del entorno de OSI.

El modelo básico anterior facilita la definición genérica de las fronteras de servicio abstractas entre los componentes de OSI y los SSO y permite acomodar diferentes esquemas de confianza (por ejemplo, los especificados en la Rec. UIT-T X.811 | ISO/CEI 10181-2, Marco de autenticación).

NOTA 3 – Las interacciones entre una AE y una PE, mostradas en la Figura 1, se analizan en 6.4 y 8.1.

6.2 Asociaciones de seguridad

En las capas superiores, una asociación de seguridad corresponde con una asociación de ASO. Este modelo de seguridad no estipula medios específicos para establecer o terminar asociaciones de seguridad. En general, este establecimiento o terminación se puede efectuar junto con los procesos de establecimiento de asociación de ASO normalizados o por otros medios. Se aplican consideraciones arquitecturales especiales a los dos tipos especiales de asociaciones de seguridad identificados en 5.2.

6.2.1 Asociación de seguridad de asociación de aplicación

Una asociación de seguridad de asociación de aplicación corresponde con una asociación de aplicación. Los servicios de seguridad pueden realizarse utilizando:

a) funciones de comunicación de seguridad en la capa de aplicación y funciones de seguridad de sistema asociadas;

b) funciones de comunicación de seguridad en la capa de presentación y funciones de seguridad de sistema asociadas;

c) servicio de seguridad prestados por las capas inferiores.

NOTA 1 – Como se indica en la Rec. X.800 del CCITT | ISO 7498-2, en la capa de sesión no hay mecanismo de seguridad. No obstante, hay dos aspectos del funcionamiento de esa capa que han de tenerse en cuenta al diseñar protocolos de seguridad de capas superiores: el efecto potencial de la utilización de servicios de sesión, que pueden resultar en la no entrega de datos (véase 8.2) y la reutilización en serie de conexiones de transporte para soportar varias conexiones de sesión (véase 8.3).

En algunos casos, se puede requerir una combinación de funciones de comunicación de seguridad en las capas de aplicación y de presentación y funciones de seguridad de sistema asociadas, para prestar un servicio de seguridad.

Los servicios y mecanismos de seguridad que han de utilizarse en una asociación de aplicación vienen especificados por el contexto de aplicación. Dichos servicios de seguridad pueden prestarse utilizando funciones asociadas con uno o más ASE y/o ASO, ya sea separadamente o en combinación.

Los requisitos de seguridad de una asociación de aplicación han de tenerse en cuenta durante el establecimiento de la asociación de una o ambas de las dos maneras siguientes:

a) mediante la utilización de servicios de seguridad para proteger el establecimiento de asociaciones de aplicación;

b) mediante la selección de un contexto de aplicación que incluye servicios de seguridad apropiados.

Los servicios proporcionados por el ACSE se utilizan para establecer una asociación de aplicación y seleccionar un contexto de aplicación adecuado. Las reglas del contexto de aplicación seleccionado pueden incluir reglas seleccionadas con la seguridad. Estas reglas pueden requerir que otros ASE, que (entre otras cosas) pueden prestar servicios de seguridad, funcionen junto con el ACSE durante el establecimiento de la asociación.

NOTA 2 – Las funciones de comunicación de seguridad en la capa de presentación, y las funciones de seguridad de sistema asociadas pueden utilizarse como parte del procedimiento de establecimiento de asociación de aplicación.

El estado de seguridad de asociación inicial lo determina el procedimiento de establecimiento de asociación de aplicación, que puede depender del estado de seguridad del sistema y/o del estado de seguridad de asociación de cualquier asociación de seguridad circundante. Las reglas del contexto de aplicación pueden permitir o requerir otros intercambios de protocolo entre los ASE para cambiar este estado de seguridad de asociación. Tales cambios pueden producirse como parte de los procedimientos de inicialización que siguen al establecimiento de la asociación de aplicación y/o como parte integrante del funcionamiento normal de invocaciones de AE cooperantes.

Durante la vida de una asociación de seguridad puede permitirse la modificación de algunos tipos de información de estado de seguridad (por ejemplo, los números de secuencias de integridad). Puede no permitirse la modificación de otras clases de información de estado de seguridad (por ejemplo, las etiquetas de seguridad).

Los servicios proporcionados por el ACSE se utilizan para terminar una asociación de aplicación. Las reglas del contexto de aplicación de la asociación de aplicación quizá requieran que otros ASE, que (entre otras cosas) pueden prestar servicios de seguridad, funcionen conjuntamente con el ACSE durante la terminación de la asociación de aplicación.

6.2.2 Asociaciones de seguridad con retransmisión

Una asociación de seguridad con retransmisión puede surgir en una aplicación distribuida, tal como una aplicación con almacenamiento y retransmisión o una aplicación con encadenamiento. La asociación de seguridad con retransmisión puede producirse junto con asociaciones de seguridad de asociación de aplicación, como se ilustra en la Figura 2.

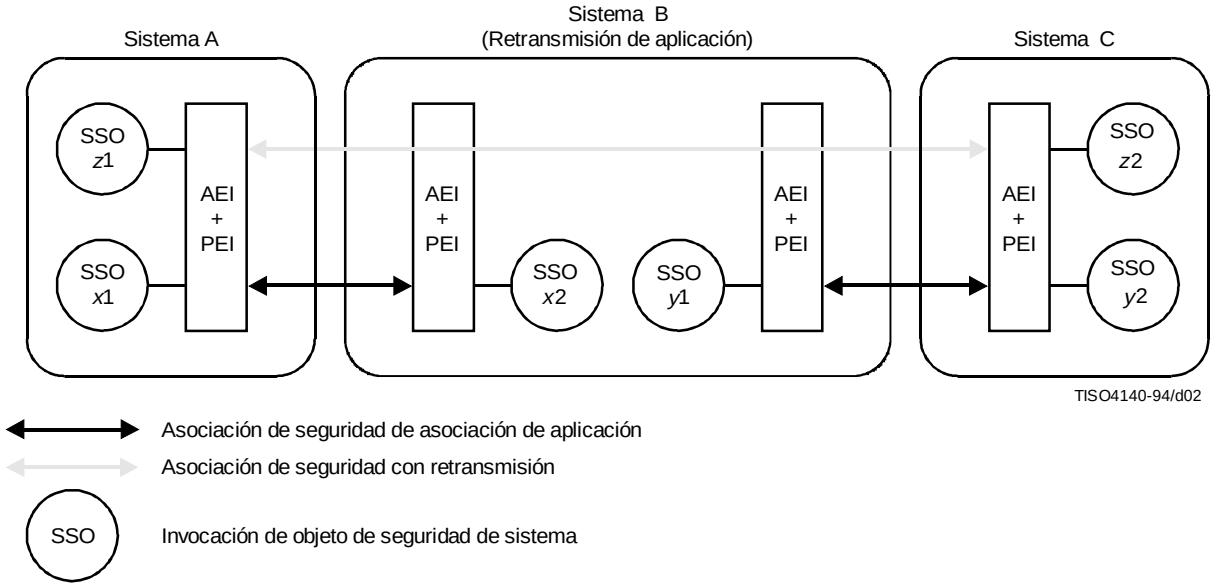

Figura 2 – Escenario de retransmisión de aplicación

La información retransmitida protegida es la información transportada entre las partes de la asociación de seguridad con retransmisión (sistema A y sistema C de la Figura 2). La protección se proporciona utilizando funciones de seguridad de sistema en los SSO *z*1 y *z*2. La información retransmitida protegida está insertada en los PDV transportados en una asociación de aplicación entre sistemas A y B, y también está insertada en los PDV transportados en una asociación de aplicación entre sistemas B y C. Cuando en una asociación de aplicación se transporta información retransmitida protegida, ésta puede estar sujeta a otra protección de seguridad, por ejemplo, la que utiliza funciones de seguridad en los SSO *x*1 y *x*2 cuando es transportada entre los sistemas A y B. Esto es lo que ocurre cuando el PDV que transporta información retransmitida protegida está insertado en otro PDV protegido de acuerdo con la asociación de seguridad de la asociación de aplicación.

El sistema de retransmisión de aplicación puede no poseer los argumentos necesarios (por ejemplo, claves criptográficas) para que la entidad o entidades de presentación de ese sistema abierto puedan decodificar/codificar los valores de datos de presentación que transporta la información retransmitida protegida. En un sistema abierto de este tipo, los valores de los datos de presentación codificados pueden ser retenidos para transmisión posterior. La transmisión posterior está limitada a un contexto de presentación con la misma sintaxis abstracta y de transferencia que aquella en que se recibió el valor de datos de presentación. Por ello, la información que identifica la sintaxis abstracta y la sintaxis de transferencia debe preservarse junto con la codificación dentro del sistema de retransmisión.

Puede plantearse una variante de lo anterior cuando el sistema de retransmisión posee la información necesaria para decodificar la información retransmitida. Por ejemplo, puede poseer una clave pública que utiliza para identificar una firma en esa información (por ejemplo, para sustentar la autenticación de datos de origen). Sin embargo, quizá puede ser necesario retransmitir la información firmada a otro sistema, en cuyo caso hay que preservar la codificación como se describe más arriba.

6.3 Funciones de intercambio de seguridad

Una función de intercambio de seguridad es un tipo de función de comunicación de seguridad, situada en la capa de aplicación, que proporciona los medios para comunicar información de seguridad entre invocaciones de AE. Una función de intercambio de seguridad genera y procesa información de control de protocolo de aplicación, para soportar la comunicación de dicha información.

Estas funciones son proporcionadas por los ASO o ASE.

Un ejemplo de función de intercambio de seguridad es el soporte de comunicaciones para un intercambio de autenticación, como se describe en la Rec. UIT-T X.811 | ISO/CEI 10181-2, en el que un ítem de intercambio de información de autenticación generado en una invocación de AE solicitante, es transportada a una invocación de AE verificador.

6.3.1 Intercambios de seguridad

Un intercambio de seguridad modela la transferencia de información de control de protocolo de aplicación entre sistemas abiertos como parte del funcionamiento de un mecanismo de seguridad.

El intercambio de seguridad puede conllevar:

a) la transferencia de una sola pieza de información entre un sistema abierto y otro; por ejemplo:
   - un certificado de control de acceso;
   - un certificado de clave pública; o
   - un testigo de seguridad.

b) una secuencia de transferencias de información entre sistemas abiertos, con toda la secuencia que forma parte del funcionamiento de un mecanismo de seguridad; por ejemplo:
   - transferencias de información asociadas a un intercambio de autenticación bidireccional o tridireccional; o
   - negociación de clave de sesión bidireccional [por ejemplo, intercambio de clave exponencial de Diffie-Hellman[2)]].

Se asignan identificadores únicos a diferentes tipos de intercambio de seguridad para que su utilización pueda ser indicada en el protocolo.

6.3.2 Información de intercambio de seguridad

Información de intercambio de seguridad es la información comunicada entre sistemas abiertos en un intercambio de seguridad.

La pieza de información de intercambio de seguridad lógicamente distinta, que corresponde a una sola transferencia (posiblemente en una secuencia de transferencias) se llama ítem de intercambio de seguridad (SEI). Para la definición de datos, un SEI se puede descomponer en elementos más pequeños.

---

2) DIFFIE (W.), HELLMAN (M.): New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

Aunque no se ha estipulado ninguna notación de sintaxis abstracta particular para definir la información de intercambio de seguridad, la construcción de una sintaxis abstracta completa que contenga información de intercambio de seguridad se verá facilitada si se utiliza la misma notación para esa información y para el resto de la sintaxis abstracta. La Rec. UIT-T X.830 | ISO/CEI 11586-1 proporciona los medios para utilizar la notación ASN.1.

6.3.3 Provisión de funciones de intercambio de seguridad

Para sustentar un intercambio de seguridad en cualquier contexto ASO dado, es necesario incorporar la función de intercambio de seguridad en algún ASE y/o ASO de ese contexto ASO. Esto supone:

a) la incorporación de las definiciones de tipos de SEI en una sintaxis abstracta;

b) la incorporación de cualesquiera reglas de procedimiento u otras relativas al funcionamiento del intercambio de seguridad en la definición de un tipo de ASE o de ASO, o en otra parte de la definición del contexto ASO;

c) si es necesario, la incorporación de la definición de las reglas de coordinación relativas al intercambio de seguridad en la especificación de una CF.

Por lo general, los intercambios de seguridad pueden incorporarse en cualquier ASE y/o ASO y las definiciones de SEI deberán expresarse de modo que se facilite su incorporación en el mayor número posible de ASE y/o ASO diferentes.

En la Rec. UIT-T X.831 | ISO/CEI 11586-2 y Rec. UIT-T X.832 | ISO/CEI 11586-3 se define un ASE específicamente diseñado para transportar intercambios de seguridad.

6.4 Transformaciones de seguridad

Una transformación de seguridad es un conjunto de funciones (funciones de seguridad de sistema y funciones de comunicación de seguridad) que, en combinación, actúa sobre los ítems de datos de usuario para protegerlos de una manera particular durante la comunicación o el almacenamiento.

Las transformaciones de seguridad conllevan procesamiento relacionado con la seguridad de la información de usuario transportada por protocolos de capas superiores de OSI. Pueden constituir el medio primario para prestar un servicio de confidencialidad, integridad o autenticación de origen de los datos y/o pueden contribuir a la prestación de otros servicios de seguridad, incluidos los de autenticación de entidades, control de acceso y no repudio.

Las transformaciones de seguridad emplean funciones de seguridad de sistema de diversos tipos:

a) funciones de cifrado/descifrado (por ejemplo, para los servicios de confidencialidad);

b) funciones de sellado o firma (por ejemplo, para los servicios de integridad o autenticación de origen de los datos).

Una transformación de seguridad puede emplear una sola función de seguridad de sistema o múltiples funciones de seguridad de sistema de diferentes tipos en combinación. Cuando las funciones de seguridad de sistema se aplican combinadas, no hay restricción arquitectural respecto al tipo que hay que aplicar primero.

Las transformaciones de seguridad emplean también funciones de comunicación situadas dentro de las capas superiores.

NOTA 1 – Los ejemplos a) y b) anteriores no proporcionan una lista exhaustiva de tipos de funciones de seguridad de sistema.

NOTA 2 – Es conveniente limitar el número de tipos de funciones de seguridad de sistema definidos y aplicarlos a una amplia gama de necesidades de seguridad.

NOTA 3 – Las funciones de comunicación de seguridad que forman parte de transformaciones de seguridad se ocupan de representaciones de información, por lo que están asociadas lógicamente con la capa de presentación. No obstante, estas funciones se aplican a una variedad de granularidades diferentes. Algunas veces se aplican para completar los valores de datos de presentación reconocidos por el protocolo de presentación. Algunas veces se aplican a fragmentos seleccionados de información de capa de aplicación. En último caso, desde el punto de vista del realizador, puede ser más conveniente considerar estas funciones de comunicación de seguridad como si estuvieran dentro de la capa de aplicación.

Se asignan identificadores únicos a diferentes tipos de transformación de seguridad para que su utilización se pueda indicar en el protocolo.

Una especificación que indica la utilización de transformaciones de seguridad necesitará incluir:

a) una indicación de la transformación de seguridad particular o los medios por los cuales se determinará la transformación particular;

b) especificación del ítem o ítems de información a los que se ha de aplicar la transformación de seguridad;

c) si el ítem de información que se ha de proteger se especifica en un nivel de sintaxis abstracta, puede ser necesario identificar también las reglas de codificación/decodificación aplicables antes/después de aplicar una transformación de seguridad;

d) la identificación del algoritmo o algoritmos que se deben emplear y las fuentes de cualquier parámetro requerido, por ejemplo, claves.

NOTA 4 – Las reglas de codificación/decodificación utilizadas para generar/verificar valores de comprobación de integridad o firmas digitales deben tener la propiedad de que haya una correspondencia de uno a uno entre el valor de información abstracto y el valor codificado. Las reglas de codificación canónica y distinguida de ASN.1 tienen esta propiedad pero no las reglas de codificación básica de ASN.1.

Hay dos maneras de especificar los ítems de información a los que se aplican las transformaciones de seguridad:

a) los campos seleccionados se indican en una especificación de sintaxis abstracta;

b) se asocia una transformación de seguridad de un determinado tipo con todos los ítems de información transferidos en un contexto de presentación; en este caso, los requisitos de transformación de seguridad se especifican fuera de las especificaciones de sintaxis abstracta.

Estos dos casos se amplían más adelante.

6.4.1 Indicación de campo selectivo en la especificación de sintaxis abstracta

Cuando se ha de proteger campos seleccionados en una sintaxis abstracta, la especificación de sintaxis abstracta debe indicar los ítems que han de ser protegidos utilizando una notación adecuada. Este método es necesario si se ha de aplicar la integridad y/o confidencialidad de campo selectiva con una granularidad más pequeña que la de los valores de datos de presentación completos generados por una sintaxis abstracta.

Ejemplos de notaciones para especificar la utilización selectiva de transformaciones de seguridad en una sintaxis abstracta son las funciones de firma y cifrado definidas en la Rec. UIT-T X.509 | ISO/CEI 9594-8 y la notación PROTECTED definida en la Rec. UIT-T X.830 | ISO/CEI 11586-1.

6.4.2 Contextos de presentación de protección

Cuando una transformación de seguridad se debe aplicar uniformemente a todos los ítems de información de una sintaxis abstracta, esto conlleva el establecimiento y la utilización de un **contexto de presentación de protección**.

El establecimiento de cualquier contexto de presentación conlleva el establecimiento de una sintaxis de transferencia que se ha de utilizar con una sintaxis abstracta dada. Dentro de un contexto de presentación de protección, la sintaxis de transferencia, denominada **sintaxis de transferencia de protección**, se basa en los procesos de codificación/decodificación que emplean una transformación de seguridad. El establecimiento del contexto de presentación de protección incluye la determinación de la transformación de seguridad (y de la función o funciones de seguridad de sistema que intervienen) que formará parte de los procesos de codificación/decodificación entre sintaxis abstracta y sintaxis de transferencia en la transmisión/recepción de todos los valores de datos de presentación de ese contexto de presentación.

Una vez establecido un contexto de presentación protector, es posible que una función de seguridad de sistema que procesa datos de salida necesite transportar información de parámetros a su función de seguridad de sistema correspondiente. Esto podría incluir, por ejemplo:

a) en la primera utilización de un contexto de presentación, parámetros iniciales tales como el vector de inicialización de un proceso criptográfico o el identificador o identificadores de claves;

b) dentro de una secuencia de valores de datos de presentación protegidos, información indicadora de un cambio de parámetro, por ejemplo, el cambio a una nueva clave.

Es posible, por consiguiente, que la definición de una sintaxis de transferencia, necesite acomodar los medios para transportar datos de parámetros de transformación, además de transportar representaciones de información de usuario del servicio de presentación.

La información de parámetros, por ejemplo, claves, requerida por las funciones de seguridad de sistema pueden obtenerse, alternativamente, por medios tales como:

a) el resultado de intercambios previos de protocolos de capa de aplicación, por ejemplo, la clave resultante de un intercambio de seguridad de obtención de claves;

b) un medio local, por ejemplo, la inserción manual de claves.

La Rec. UIT-T X.833 | ISO/CEI 11586-4 especifica una sintaxis de transferencia de protección genérica, capaz de sustentar una variedad de transformaciones de seguridad diferentes.

NOTA – Es posible insertar un valor de datos de presentación dentro de otro y se pueden aplicar transformaciones de seguridad en ambos niveles. En este caso, la codificación del valor de datos de presentación (insertado) interno (para el cual se utiliza una transformación de seguridad en el proceso de codificación) estará también protegida en la transformación de seguridad que se aplica a la codificación del valor de datos de presentación externo. Un ejemplo podría ser cuando los datos (que comprenden un valor de datos de presentación interno) transmitidos entre dos sistemas necesitan estar firmados para probar el origen de los datos, y cuando la protección contra la repetición entre dos sistemas se logra por el sellado aplicado a un valor de datos de presentación externo o a todos los valores de datos de presentación en un contexto de presentación.

7 Servicios y mecanismos

La arquitectura de seguridad de interconexión de sistemas abiertos (Rec. X.800 del CCITT | ISO 7498-2) especifica que:

– la capa de aplicación puede proporcionar uno o más servicios de seguridad del conjunto básico: autenticación, control de acceso, confidencialidad, integridad de datos, y no repudio;

– la capa de presentación no presta servicios de seguridad, pero en dicha capa pueden ubicarse mecanismos de seguridad para soportar la prestación de servicios de seguridad de la capa de aplicación;

– la capa de sesión no presta servicios de seguridad ni contiene mecanismos de seguridad.

7.1 Autenticación

7.1.1 Autenticación de entidad

7.1.1.1 Cometido de las capas superiores en la autenticación de entidad

El objetivo de la autenticación es garantizar la identidad de una entidad. El cometido de la capa de aplicaciones facilitar la autenticación de entidades conocidas a dicha capa. Esta autenticación está disponible en el momento del establecimiento de la asociación ASO y durante su utilización.

La capa de aplicación permite autenticar una amplia gama de principales. Esto depende de la naturaleza de la aplicación y de la política de seguridad en vigor.

NOTA – El concepto de *autenticación de entidad par* definido en la Rec. X.800 del CCITT | ISO 7498-2 es un caso especial de la *autenticación de entidad* definida en la Rec. UIT-T X.811 | ISO/CEI 10181-2.

Las capas inferiores no proporcionan la autenticación de entidades por debajo de la capa de aplicación.

7.1.1.2 Provisión de autenticación de entidad

La autenticación de entidad puede ser proporcionada en la capa de aplicación mediante la comunicación de información de autenticación de intercambio, que puede emplear funciones de intercambio de seguridad de acuerdo con lo indicado en 6.3.

La autenticación de entidad sólo garantiza una entidad en un determinado instante. Para mantener esa garantía mientras dura una asociación de ASO es preciso utilizar un servicio de integridad de conexión (definido en la Rec. X.800 del CCITT | ISO 7498-2). En algunos casos, puede ser necesario obtener una seguridad ulterior de la identidad de una entidad tras un periodo de tiempo, mediante intercambios de autenticación adicionales.

7.1.1.3 Gestión de autenticación de entidad

Cuando se proporciona autenticación de entidad, se puede necesitar la gestión de información de autenticación de declaración y/o la información de autenticación de verificación, por ejemplo, claves criptográficas. Como se describe en la Rec. UIT-T X.811 | ISO/CEI DIS 10181-2, esto puede conllevar alguno de los siguientes procedimientos:

– *instalación*, en el que se definen la información de autenticación de declaración y la información de autenticación de verificación;

– *cambio de información de autenticación*, en el que un principal o un gestor cambian la información de autenticación de declaración y la información de autenticación de verificación;

- *distribución*, en el que cualquier entidad puede adquirir suficiente información de autenticación de verificación con la que verificar información de autenticación de intercambio;
- *inhabilitación*, en el que se establece un estado según el cual, un principal que previamente podía ser autenticado, está inhabilitado temporalmente;
- *rehabilitación*, en el que se termina el estado establecido en un procedimiento de inhabilitación;
- *desinstalación*, en el que se elimina un principal del colectivo de principales autenticables.

Cuando se aplican esos procedimientos utilizando protocolos de OSI, esto puede entrañar funciones de intercambio de seguridad de conformidad con 6.3. Dichos procedimientos pueden emplear también servicios de gestión de seguridad de OSI.

La política de seguridad en vigor puede requerir además que se informe de las tentativas de autenticación fallidas para generar una alarma y/o anotarlas en un registro de auditoría de seguridad.

7.1.2 Autenticación de origen de los datos

7.1.2.1 Cometido de las capas superiores en la autenticación de origen de los datos

La autenticación de origen de los datos se refiere a la autenticación de la entidad a la que se imputa haber originado un determinado conjunto de datos. Esta no es necesariamente la entidad par directa en un caso de comunicación, por lo que la autenticación de origen de los datos tiene una finalidad diferente de la autenticación de entidad.

A cada elemento de datos de un caso de comunicación puede haberse aplicado o no la autenticación de origen de los datos. Para asegurar la oportunidad de los datos recibidos, puede ser que la autenticación de origen de los datos tenga que ser capaz de validar también, la fecha de origen y la fuente.

7.1.2.2 Provisión de la autenticación de origen de los datos

La autenticación de origen de los datos en la capa de aplicación se proporciona mediante el intercambio de información de seguridad, que puede llevar, por ejemplo, una firma digital basada en los datos y en un identificador del origen de los mismos. La autenticación de origen de los datos se puede proporcionar en el momento del establecimiento de la asociación de ASO o en cualquier otro momento durante una asociación de ASO.

Los servicios de autenticación de origen de los datos utilizan transformaciones de seguridad, que emplean normalmente mecanismos de cifrado o de firma digital.

7.1.2.3 Gestión de autenticación de origen de los datos

La gestión de autenticación de origen de los datos es, por lo general, igual que la gestión de la autenticación de entidad (véase 7.1.1.3).

7.2 Control de acceso

7.2.1 Generalidades

El protocolo de capa de aplicación puede proporcionar el intercambio de información de control de acceso, por ejemplo, un certificado de control de acceso, que lleva información relativa a la concesión, aplicación y/o revocación de los derechos de control de acceso.

La información de control de acceso puede ser intercambiada en el momento del establecimiento de la asociación de ASO o en cualquier otro momento durante una asociación de ASO. Los derechos de acceso presentados durante una asociación de ASO pueden modificar (aumentar o disminuir) los derechos válidos durante el resto de la asociación de ASO o ser válidos únicamente para una petición específica.

El control de acceso puede ser aplicado en varios niveles de granularidad. Aquí se distinguen dos niveles, llamados niveles de asociación de ASO y de recurso, pero se admite que determinados protocolos pueden introducir niveles adicionales en la categoría de recurso.

7.2.2 Control de acceso de asociación de ASO

7.2.2.1 Cometido de las capas superiores en el control de acceso de asociación de ASO

El control de acceso de asociación de ASO se aplica al nivel de asociación de aplicación y se refiere al control de acceso a sistemas y procesos (por ejemplo, procesos de aplicación) más bien que a los objetos dentro de los sistemas, y a si la asociación de ASO desde un determinado sistema distante, con el contexto ASO y las características de seguridad solicitados será autorizada a comenzar o a continuar si se utiliza después del establecimiento de la asociación de ASO.

7.2.2.2 Provisión de control de acceso de asociación de ASO

El control de acceso de asociación de ASO puede ser sustentado mediante las funciones de intercambio de seguridad descritas en 6.3. Dichas funciones admiten todas las clases de mecanismos identificados en la Rec. UIT-T X.812 | ISO/CEI 10181-3, Marco de control de acceso.

Esta función de intercambio de seguridad puede ser proporcionada por un ASE utilizado junto con el ACSE, para facilitar el control de acceso en el momento del establecimiento de la asociación de aplicación. Además, un intercambio de seguridad en ese momento permite retener cierta información de control de acceso para utilizarla después al tomar decisiones de control de acceso, durante la vida de la asociación de aplicación.

7.2.2.3 Gestión de control de acceso de asociación de ASO

La política de seguridad en vigor en un sistema puede exigir que se informe de toda tentativa de acceso, y en particular de toda tentativa de acceso fallida, para generar una alarma y/o anotarla como parte de un registro de auditoría de seguridad. Los servicios de gestión de seguridad de OSI proporcionan los medios para mantener la información de control de acceso.

7.2.3 Control de acceso a recursos

7.2.3.1 Cometido de las capas superiores en el control de acceso a recursos

El control de acceso a recursos se relaciona con el control de acceso a un determinado recurso, tal como un objeto u objetos de información de una base de información. Cuando un objeto de información está estructurado en partes, se puede proporcionar otros niveles de control de acceso. Un ejemplo de dicho recurso es un fichero. Se puede utilizar el control de acceso para determinar si el iniciador de acceso tiene derecho a efectuar una determinada operación en el fichero, tal como leer o modificar.

7.2.3.2 Provisión de control de acceso a recursos

El control de acceso a recursos puede ser de la incumbencia de un ASE o ASO particular que proporciona el protocolo para intercambiar peticiones y respuestas de manipulación de un determinado recurso. Por ejemplo, el control de acceso a ficheros corresponde a la transferencia, acceso y gestión de ficheros (FTAM) (ISO 8571).

Los ASE o ASO pueden utilizar una o más clases de mecanismos definidos en la Rec. UIT-T X.812 | ISO/CEI 10181-3, así como la información de acceso de control retenida, resultante de la utilización del control de acceso de asociación de ASO.

7.2.3.3 Gestión de control de acceso a recursos

La política de seguridad en vigor en un sistema puede requerir que se informe de toda tentativa de acceso, y en particular de toda tentativa de acceso fallida, para generar una alarma y/o anotarla como parte de un registro de auditoría de seguridad. La gestión de la información de control de acceso puede conseguirse mediante el protocolo de aplicación específico o mediante un protocolo de gestión de la capa de aplicación de uso general.

7.3 No repudio

7.3.1 Cometido de las capas superiores en el no repudio

El servicio de no repudio es un servicio de capa de aplicación. Comprende los siguientes casos (definidos en la Rec. X.800 del CCITT | ISO 7498-2), pero no está limitado a ellos:

a) no repudio con prueba de origen;

b) no repudio con prueba de la entrega.

En el servicio de no repudio con prueba de origen, se da al recibiente de la información prueba de su origen. Esto lo protegerá contra cualquier tentativa subsiguiente del emisor de negar falsamente el envío de esa información. El cometido de las capas superiores en el no repudio con prueba de origen consiste en proporcionar la prueba de que un ítem de información determinado fue enviado por una entidad de aplicación determinada.

En el no repudio con prueba de entrega, se da al emisor de la información prueba de la entrega de la misma. Esto lo protegerá contra cualquier tentativa subsiguiente del recibiente de negar falsamente la recepción de esa información. El cometido de las capas superiores en el no repudio con prueba de entrega consiste en proporcionar la prueba de que un ítem de información determinado fue recibido por una entidad de aplicación determinada.

7.3.2 Provisión de no repudio

En la provisión de los servicios de no repudio se pueden utilizar mecanismos de firma digital o de cifrado. Esto puede conllevar la utilización de las transformaciones de seguridad descritas en 6.4. Según la política de seguridad en vigor, el servicio de no repudio puede emplear un mecanismo de notarización.

Para el no repudio con prueba de origen puede necesitarse una interacción con un tercero de confianza, y se requiere siempre para el no repudio con prueba de entrega.

Puede que un emisor y/o recibiente necesiten utilizar múltiples asociaciones de ASO para las interacciones, por ejemplo, con un servicio de generación de firma, un servicio de sello de hora y/o un servicio de directorio.

7.3.3 Gestión de no repudio

Si se utilizan mecanismos de firma digital y/o cifrado para prestar un servicio de no repudio, la gestión de tales mecanismos puede incluir:

- la gestión de claves; y
- el establecimiento de parámetros y algoritmos criptográficos.

Si se utiliza un mecanismo de notarización para prestar un servicio de no repudio, la gestión de dicho servicio puede incluir:

- la distribución de información relativa a notarios; y
- la interacción con notarios.

7.4 Integridad

7.4.1 Cometido de las capas superiores en la integridad

La integridad se puede proporcionar como un servicio de la capa de aplicación. En la prestación de este servicio pueden emplearse funciones de comunicación de seguridad en la capa de presentación y funciones de seguridad de sistemas asociadas. Es posible prestar los siguientes servicios:

a) integridad en modo con conexión con recuperación;

b) integridad en modo con conexión sin recuperación;

c) integridad de campos seleccionados en modo con conexión;

d) integridad en modo sin conexión;

e) integridad de campos seleccionados en modo sin conexión.

Todos los tipos de servicios de integridad, excepto los de integridad de campos seleccionados, podrán prestarse en las capas inferiores.

La integridad puede aplicarse con cualquiera de los siguientes grados de granularidad:

a) un valor de datos de presentación individual;

b) una serie de valores de datos de presentación en un contexto de presentación;

c) parte, o un conjunto de partes, de un valor de datos de presentación individual.

7.4.2 Provisión de integridad

Pueden prestarse servicios de integridad utilizando las transformaciones de seguridad descritas en 6.4.

La detección de una violación de la integridad dentro de la capa de presentación se señala como una indicación a la entidad de aplicación receptora. Sin embargo, no es factible analizar los datos recibidos ni ponerlos explícitamente a disposición del usuario del servicio de presentación. De todos modos, los datos sospechosos deben estar disponibles, a efectos de análisis/auditoría, dentro del sistema abierto receptor. Dependiendo de ese análisis pueden invocarse otras acciones conexas en el entorno de OSI.

7.4.3 Gestión de la integridad

La gestión de la integridad puede implicar la comunicación de materias clave. Cuando se produce esta comunicación en una asociación de ASO (posiblemente la misma que aquella en la que se emplea el servicio de integridad), dicha asociación puede emplear funciones de intercambio de seguridad de conformidad con 6.3. La comunicación de algunas materias claves quizá requiera servicios de gestión de seguridad de OSI.

7.5 Confidencialidad

7.5.1 Cometido de las capas superiores en la confidencialidad

La confidencialidad puede proporcionarse como un servicio de capa de aplicación. En la prestación de este servicio pueden emplearse funciones de comunicación de seguridad en la capa de presentación y funciones de seguridad de sistema asociadas. Es posible prestar los siguientes servicios:

a) confidencialidad en modo con conexión;

b) confidencialidad en modo sin conexión;

c) confidencialidad de campos seleccionados;

d) confidencialidad de flujo de tráfico.

Todos los tipos de servicios de confidencialidad, excepto el de confidencialidad de campos seleccionados, podrán prestarse en las capas inferiores.

La confidencialidad puede aplicarse con cualquiera de los siguientes grados de granularidad:

– un valor de datos de presentación individual;

– una serie de valores de datos de presentación en un contexto de presentación;

– parte, o un conjunto de partes, de un valor de datos de presentación individual.

7.5.2 Provisión de confidencialidad

Los servicios de confidencialidad pueden prestarse utilizando las transformaciones de seguridad descritas en 6.4.

7.5.3 Gestión de confidencialidad

La gestión de confidencialidad puede implicar la comunicación de materiales de claves. Cuando se produce esta comunicación en una asociación de ASO (posiblemente la misma que aquella en la que se emplea el servicio de confidencialidad), dicha asociación puede emplear funciones de intercambio de seguridad de conformidad con 6.3. La comunicación de algunos materiales de claves quizá requiera servicios de gestión de seguridad de OSI.

8 Interacciones entre capas

8.1 Interacciones entre las capas de aplicación y de presentación

8.1.1 Invocación de transformaciones de seguridad

En el momento del establecimiento de un contexto de presentación es posible especificar, por medios locales, que se aplique una transformación de seguridad a los valores de datos de presentación transferidos mediante ese contexto de presentación. Para mayores detalles sobre contextos de presentación de protección, véase 6.4.2.

La utilización de transformaciones de seguridad también puede ser indicada por notación en una especificación de sintaxis abstracta. Para detalles, véase 6.4.1.

Cuando un valor de datos de presentación al que se aplica una transformación tiene insertados valores de datos de presentación, la transformación se aplicará también a estos valores.

La detección de una violación de integridad se señala como una indicación a la entidad de aplicación receptora.

8.1.2 Soporte de la información requerida por la capa de presentación

La entidad de presentación iniciadora obtiene la identidad de una transformación de seguridad requerida a partir de la base de información de gestión de seguridad o bien, por implicación, de la sintaxis de transferencia utilizada para un contexto de presentación.

Los parámetros de transformación de seguridad, incluidas las claves de cifrado, se pueden obtener por medios locales a partir de la información mantenida en la base de información de gestión de seguridad o puede ser determinada a través de intercambios de datos insertados en una sintaxis de transferencia de protección. La información de parámetros también puede ser transportada en otros valores de datos de presentación protegidos en la misma asociación de ASO. La determinación de los valores de parámetros puede requerir el empleo de diversos atributos de la conexión, incluidas las entidades de los puntos de acceso al servicio de presentación iniciadores y respondedores.

NOTA – Esta información puede incluir información de estado o dependiente de la secuencia. Puede ser necesario que las funciones de seguridad de sistema modifiquen esta información.

8.1.3 Aspectos relativos a aplicaciones distribuidas

Algunas aplicaciones distribuidas, tales como las aplicaciones con almacenamiento y retransmisión o con encadenamiento, requieren que las unidades de datos de protocolo de aplicación, o partes de las mismas, pasen a través de un sistema abierto que actúa como un retransmisor de aplicación (véase 6.2.3). En un sistema de retransmisión de aplicación de este tipo, pueden retenerse los valores de datos de presentación codificados para transmisión posterior. La transmisión posterior está limitada a un contexto de presentación con las mismas sintaxis abstracta y de transferencia que aquella en la que se recibió el valor de datos de presentación.

8.2 Interacciones entre las capas de presentación y de sesión

Aunque la capa de sesión no contiene servicios o mecanismos de seguridad, las operaciones dentro de dicha capa pueden afectar al funcionamiento de determinados mecanismos de seguridad en la capa de presentación. En particular, el funcionamiento de servicios de sesión destructivos, tales como la resincronización, que descartan datos, afectará al funcionamiento de los mecanismos de cifrado y al soporte de la integridad de datos en la capa de presentación. La capa de presentación puede contener procedimientos que traten estos efectos.

Por ejemplo, cuando se produce una resincronización de sesión, quizá sea necesario resincronizar procesos de encadenamiento criptográficos (por ejemplo, servicios de integridad sustentadores) en la capa de presentación.

8.3 Utilización de servicios de las capas inferiores

Las reglas de interacción segura pueden requerir que las comunicaciones de OSI sean protegidas utilizando prestaciones de seguridad de las capas inferiores. Dichas prestaciones pueden necesitarse además o en lugar de las medidas de seguridad de las capas superiores.

Los servicios de seguridad de capas inferiores pueden proporcionar cierta protección que no puede ofrecerse en las capas superiores. En particular, los servicios de seguridad de las capas inferiores pueden utilizarse para proteger la información de control de protocolo de todas las capas superiores y proporcionar un alto grado de confidencialidad del flujo de tráfico.

La identificación de las necesidades de prestaciones de seguridad proporcionadas por el servicio de transporte está definida en la Rec. X.214 del CCITT | ISO 8072 desde el punto de vista de un parámetro de calidad de servicio de protección, que es parte del servicio utilizado para el establecimiento de la conexión de transporte. Este parámetro permite comunicar las necesidades de servicios de seguridad entre un usuario del servicio de transporte y un proveedor de dicho servicio.

La selección de las prestaciones de seguridad del servicio de transporte (mediante un parámetro de calidad de servicio de protección) puede ser determinada total o parcialmente por la gestión de sistemas locales, en vez de por las máquinas de protocolo de las capas superiores.

NOTA – El concepto de calidad de servicio de protección se está estudiando y puede ser modificado (o posiblemente eliminado) en normas de capas inferiores antes de la próxima revisión de esta norma.

Anexo A

Relación con la gestión de interconexión de sistemas abiertos (OSI)

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

A.1 Gestión de servicios y mecanismos de seguridad

Pueden utilizarse servicios de gestión de seguridad de OSI para gestionar servicios y mecanismos de seguridad. La gestión de servicios de seguridad se refiere a la gestión de servicios de seguridad particulares, tales como la autenticación de entidad y el control de acceso. Los servicios de seguridad se prestan utilizando uno o más mecanismos de seguridad. La gestión de mecanismos de seguridad se refiere a la supervisión y control de estos mecanismos.

Las actividades de gestión de seguridad se relacionan típicamente con:

a) la gestión de políticas de seguridad;

b) las interacciones entre funciones de seguridad y otras funciones de OSI (por ejemplo, gestión de configuración);

c) las interacciones entre funciones de gestión de servicios de seguridad y de gestión de mecanismos de seguridad;

d) el informe de alarmas de seguridad y gestión de pistas de auditoría de seguridad;

e) la gestión de información de control de acceso.

A.2 Objetos, atributos e informes de eventos relacionados con la seguridad

La gestión de OSI proporciona funciones que permiten gestionar objetos y atributos relacionados con la seguridad, y generar informes de eventos relacionados con la seguridad. Estos objetos, atributos e informes de eventos incluyen:

a) informes de eventos relacionados con alarmas de seguridad, definidos en la Rec. X.736 del CCITT | ISO/CEI 10164-7;

b) objetos, atributos e informes de eventos pertenecientes a pistas de auditoría de seguridad, definidos en la Rec. X.740 del CCITT | ISO/CEI 10164-8;

c) objetos y atributos pertenecientes al control de acceso para la gestión OSI, como se define en la Rec. UIT-T X.741 | ISO/CEI 10164-9.

A.3 Funciones de gestión de seguridad específicas

Las entidades de gestión dentro de cada capa de OSI, pueden generar informes después de la detección de ataques a la seguridad, o riesgos de la misma, indicando eventos normales y anormales, incluidas la activación y desactivación del servicio. Los aspectos relativos a la gestión del tratamiento de eventos en OSI comprenden el informe a distancia de intentos aparentes de violar la seguridad del sistema o el informe de eventos. La función de informe de alarmas de seguridad definida en la Rec. X.736 del CCITT | ISO/CEI 10164-7 admite tales requisitos.

La auditoría de seguridad incluye aspectos de registro cronológico y/o recopilación a distancia de información de pistas de auditoría de eventos seleccionados, la recopilación a distancia de registros de auditoría seleccionados, y la preparación de informes de auditoría de seguridad. La función de pista de auditoría de seguridad, definida en la Rec. X.740 del CCITT | ISO/CEI 10164-8 admite estos requisitos.

A.4 Otros aspectos relativos a la gestión

Los objetos relacionados con la seguridad pueden ser creados y suprimidos y los atributos de esos objetos pueden ser manipulados por la función de gestión de objetos especificada en la Rec. 730 del CCITT | ISO/CEI 10164-1. Por ejemplo, se puede crear listas de control de acceso y administrar la información de seguridad especificada en las mismas.

Las relaciones entre objetos que representan aplicaciones de OSI y objetos relacionados con la seguridad pueden ser administrados por la función de gestión de relaciones especificada en la Rec. X.732 del CCITT | ISO/CEI 10164-3.

Anexo B

Bibliografía

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

– Recomendación UIT-T X.509 (1993) | ISO/CEI 9594-8, *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Marco de autenticación.*

– Recomendación X.730 del CCITT (1992) | ISO/CEI 10164-1:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de objetos.*

– Recomendación X.732 del CCITT (1992) | ISO/CEI 10164-3:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Atributos para la representación de relaciones*.

– Recomendación X.736 del CCITT (1992) | ISO/CEI 10164-7:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de informe de alarmas de seguridad.*

– Recomendación X.740 del CCITT (1992) | ISO/CEI 10164-8:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pistas de auditoría de seguridad.*

– Recomendación UIT-T X.741[3)] | ISO/CEI 10164-9...[3)], *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para control de acceso.*

– Recomendación UIT-T X.830[3)] | ISO/CEI 11586-1...[3)], *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas superiores – Descripción general, modelos y notación.*

– Recomendación UIT-T X.831[3)] | ISO/CEI 11586-2...[3)], *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas superiores – Definición de servicio del elemento de servicio de intercambio de seguridad.*

– Recomendación UIT-T X.832[3)] | ISO/CEI 11586-3...[3)], *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas superiores – Especificación de protocolo del elemento de servicio de intercambio de seguridad.*

– Recomendación UIT-T X.833[3)] | ISO/CEI 11586-4...[3)], *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas superiores – Especificación de sintaxis de transferencia de protección.*

3) Actualmente en estado de proyecto.