



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

X.831

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/95)

**REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS
SEGURIDAD**

**TECNOLOGÍA DE LA INFORMACIÓN –
INTERCONEXIÓN DE SISTEMAS ABIERTOS –
SEGURIDAD GENÉRICA DE LAS CAPAS
SUPERIORES: DEFINICIÓN DE SERVICIO DEL
ELEMENTO DE SERVICIO DE INTERCAMBIO
DE SEGURIDAD**

Recomendación UIT-T X.831

(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.º 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.831 se aprobó el 10 de abril de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 11586-2.

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.

© UIT 1996

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

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

	<i>Página</i>
Sumario	ii
Introducción.....	ii
1 Alcance.....	1
2 Referencias normativas	1
2.1 Recomendaciones Normas Internacionales idénticas.....	1
3 Definiciones	1
4 Abreviaturas	2
5 Convenios.....	2
6 Sinopsis del servicio.....	2
6.1 Facilidades de servicio específicas.....	2
6.2 Modelo de procedimiento para la facilidad de servicio SE-TRANSFERENCIA.....	2
7 Definición del servicio	3
7.1 Parámetros de las primitivas del servicio.....	3
7.2 Primitivas del servicio.....	4
8 Información de secuenciación	4

Sumario

Esta Recomendación | Norma Internacional pertenece a una serie de Recomendaciones que presentan un conjunto de facilidades para ayudar a la construcción de protocolos de capas superiores de OSI que soporten la prestación de servicios de seguridad. Esta Recomendación define el servicio proporcionado por el elemento de servicio de seguridad (SESE), que es un elemento de servicio de aplicación (ASE) que facilita la comunicación de información de seguridad para soportar la prestación de servicios de seguridad en la capa de aplicación de OSI.

Introducción

Esta Recomendación | Norma Internacional pertenece a una serie de Recomendaciones | Normas Internacionales multiparte, que presentan colectivamente un conjunto de facilidades para soportar la prestación de servicios de seguridad en los protocolos de la capa de aplicación. Sus partes son las siguientes:

- Parte 1: Sinopsis, modelos y notación
- Parte 2: Definición de servicio del elemento de servicio de intercambio de seguridad
- Parte 3: Especificación del protocolo del elemento de servicio de intercambio de seguridad
- Parte 4: Especificación de la sintaxis de transferencia de protección
- Parte 5: Formulario PICS del elemento de servicio de intercambio de seguridad
- Parte 6: Formulario PICS de la sintaxis de transferencia de protección

Esta Recomendación | Norma Internacional constituye la Parte 2 de esta serie.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

**TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS
ABIERTOS – SEGURIDAD GENÉRICA DE LAS CAPAS SUPERIORES:
DEFINICIÓN DE SERVICIO DEL ELEMENTO DE
SERVICIO DE INTERCAMBIO DE SEGURIDAD**

1 Alcance

1.1 Esta serie de Recomendaciones | Normas Internacionales define un conjunto de facilidades genéricas destinadas a facilitar la prestación de servicios de seguridad en los protocolos de capa de aplicación, que comprenden:

- a) un conjunto de herramientas de notación que permitan la especificación de requisitos de protección selectiva de los campos en una especificación de sintaxis abstracta, y la especificación de intercambios de seguridad y transformaciones de seguridad;
- b) una definición de servicio, especificación de protocolo y formulario PICS para un elemento de servicio de aplicación (ASE) que permita la prestación de servicios de seguridad dentro de la capa de aplicación de OSI;
- c) una especificación y un formulario PICS para una sintaxis de transferencia de seguridad, asociada con soporte de la capa de presentación para servicios de seguridad en la capa de aplicación.

1.2 Esta Recomendación | Norma Internacional define el servicio proporcionado por el elemento de servicio de intercambio de seguridad (SESE, *security exchange service element*). El SESE es un ASE que permite la comunicación de información de seguridad para soportar la prestación de servicios de seguridad dentro de la capa de aplicación.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas 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 citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores.*

3 Definiciones

Se utilizan los siguientes términos definidos en la Rec. UIT-T X.803 | ISO/CEI 10745:

- intercambio de seguridad;
- elemento de intercambio de seguridad.

4 Abreviaturas

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

ASE	Elemento de servicio de aplicación (<i>application service element</i>)
OSI	Interconexión de sistemas abiertos (<i>open systems interconnection</i>)
PICS	Enunciado de conformidad de implementación de protocolo (<i>protocol implementation conformance statement</i>)
SEI	Elemento de intercambio de seguridad (<i>security exchange item</i>)

5 Convenios

La cláusula 7 emplea una presentación tabular de los parámetros de las primitivas del servicio SESE. Cada parámetro se resume mediante la siguiente notación:

M	la presencia del parámetro es obligatoria (<i>mandatory</i>)
O	la presencia del parámetro es una opción de la máquina de protocolo SESE
U	la presencia del parámetro es una opción del usuario del servicio SESE
C	la presencia del parámetro es condicional
(=)	el valor de este parámetro es idéntico al valor del parámetro correspondiente de la primitiva del servicio SESE precedente

6 Sinopsis del servicio

El elemento de servicio de intercambio de seguridad permite la comunicación de información asociada con cualquier intercambio de seguridad, que se describe en la Parte 1. Este servicio suele utilizarse para la transferencia de información de autenticación, de control de acceso, de no repudio o de gestión de seguridad.

6.1 Facilidades de servicio específicas

Se definen las siguientes facilidades de servicio:

- a) SE-TRANSFERENCIA;
- b) SE-U-ABORTO;
- c) SE-P-ABORTO.

La facilidad de servicio SE-TRANSFERENCIA se utiliza para iniciar un intercambio de seguridad de un cierto tipo, transferir el primer elemento de intercambio de seguridad (SEI), así como transferir los otros SEI de un intercambio de seguridad. Es la única facilidad de servicio requerida al efectuar un intercambio de seguridad.

La facilidad de servicio SE-U-ABORTO es utilizada por el usuario del servicio SESE para indicar que se ha producido un error. Este servicio se utiliza para terminar anormalmente un intercambio de seguridad en curso. Opcionalmente, este servicio puede también terminar anormalmente la asociación ASO.

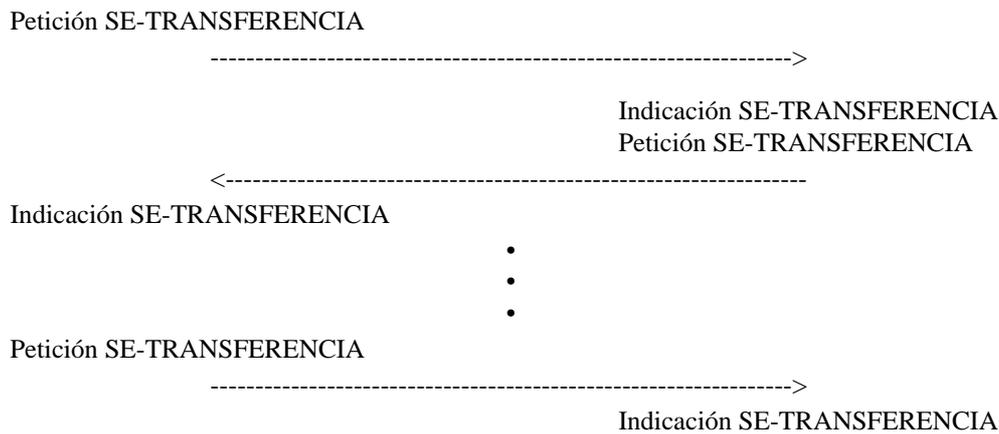
La facilidad de servicio SE-P-ABORTO es utilizada por el proveedor del servicio SESE para indicar que se ha producido un error. Este servicio se utiliza para terminar anormalmente un intercambio de seguridad en curso. Opcionalmente, este servicio puede también terminar anormalmente la asociación ASO.

6.2 Modelo de procedimiento para la facilidad de servicio SE-TRANSFERENCIA

La Parte 1 de esta Recomendación | Norma Internacional define el modelo de procedimiento para intercambios de seguridad:

Un elemento de intercambio de seguridad (SEI) es transferido de A a B. Este va opcionalmente seguido por una o más transferencias de SEI entre A y B, de acuerdo con el intercambio de seguridad específico identificado en la SE-TRANSFERENCIA. La secuencia puede ser terminada al recibo de cualquier SEI, por generación de una indicación de error por el usuario del servicio o por el proveedor del servicio.

El diagrama de secuencia temporal presentado a continuación es un ejemplo que ilustra el caso especial de una secuencia de transferencias de SEI en direcciones alternadas para un intercambio de seguridad n-direccional. (Este es un ejemplo de la clase de intercambio «alternativo» definida en 6.1 de la Rec. UIT-T X.830 | ISO/CEI 11586-1.)



7 Definición del servicio

Las primitivas del servicio SESE son de los siguientes tipos:

SE-TRANSFERENCIA	No confirmada
SE-U-ABORTO	No confirmada
SE-P-ABORTO	Iniciada por el proveedor

7.1 Parámetros de las primitivas del servicio

Siguen a continuación descripciones de los parámetros de las primitivas del servicio.

7.1.1 Identificador de intercambio de seguridad

Este parámetro identifica el tipo concreto de intercambio de seguridad que se inicia. El identificador se establece cuando se define el intercambio de seguridad, utilizando la clase de objeto de información INTERCAMBIO DE SEGURIDAD definida en la Parte 1.

7.1.2 Identificador de invocación

Este parámetro identifica la invocación de un determinado intercambio de seguridad. Se utiliza para referirse posteriormente a esa invocación para fines de correlación, en una primitiva SE-TRANSFERENCIA, SE-U-ABORTO o SE-P-ABORTO.

Los identificadores de invocación son especialmente útiles cuando se tratan múltiples invocaciones de intercambio de seguridad dentro del contexto de, por ejemplo, una asociación de aplicación.

Los identificadores de invocación son proporcionados por los usuarios de servicios que inician intercambios de seguridad, y es responsabilidad de dichos usuarios asegurar que estos identificadores sean inequívocos dentro del ámbito de todas las invocaciones de intercambios de seguridad activas.

7.1.3 Elemento de intercambio de seguridad

El elemento a transmitir implicado por el identificador de intercambio de seguridad.

7.1.4 Identificador de elemento

En una primitiva SE-TRANSFERENCIA, este parámetro indica qué elemento del intercambio de seguridad está transmitiendo esta primitiva. En una primitiva SE-U-ABORTO o SE-P-ABORTO, este parámetro indica el elemento de un intercambio de seguridad en el que se ha detectado una condición de error.

La especificación de un intercambio de seguridad puede imponer constricciones específicas a la utilización del «identificador de elemento». Es responsabilidad del usuario SESE asegurar que se cumplan estas constricciones.

7.1.5 Bandera de comienzo

En una primitiva SE-TRANSFERENCIA, este parámetro se utiliza para indicar la transferencia del primer elemento de intercambio de seguridad de un intercambio de seguridad.

7.1.6 Bandera de fin

En una primitiva SE-TRANSFERENCIA, este parámetro se utiliza para indicar que este intercambio de seguridad corresponde al último intercambio de seguridad requerido para satisfacer el mecanismo de seguridad. Es necesario acomodar los mecanismos que requieren n intercambios, donde n no se conoce *a priori*.

7.1.7 Lista de errores

Este parámetro consiste en una o más listas de códigos de error con parámetros de error opcionales. El código de error indica la causa de que se haya generado una SE-U-ABORTO. Los códigos de error se establecen cuando se define un intercambio de seguridad, utilizando la clase de objeto de información SE-ERROR definida en la Parte 1. Los parámetros de error opcionales proporcionan información que describe la causa de un aborto.

7.1.8 Código de problema

Este parámetro indica la causa de que se genere una SE-P-ABORTO. El conjunto de posibles valores se especifica en la cláusula 6 de la Parte 3.

7.1.9 Indicador de fatalidad

En una primitiva petición SE-U-ABORTO, este parámetro se utiliza para indicar al proveedor del servicio SESE si debe o no terminarse la asociación ASO (por ejemplo, asociación de aplicación).

En las primitivas indicación SE-U-ABORTO y SE-P-ABORTO, este parámetro se utiliza para indicar al usuario del servicio SESE si debe o no terminarse la asociación ASO (por ejemplo, asociación de aplicación).

7.2 Primitivas del servicio

Los parámetros de las primitivas del servicio SESE se indican a continuación. (Véase en 6.1 una definición de los servicios SESE y en 7.1 una descripción de los parámetros específicos.)

7.2.1 Servicio SE-TRANSFERENCIA

Los parámetros del servicio SE-TRANSFERENCIA son los siguientes:

<i>Nombre del parámetro</i>	<i>Petición</i>	<i>Indicación</i>
Identificador de intercambio de seguridad	M	M(=)
Identificador de invocación	U	C(=)
Elemento de intercambio de seguridad	M	M(=)
Identificador de elemento	U	C(=)
Bandera de comienzo	U	C(=)
Bandera de fin	U	C(=)

7.2.2 Servicio SE-U-ABORTO

Los parámetros del servicio SE-U-ABORTO son los siguientes:

<i>Nombre del parámetro</i>	<i>Petición</i>	<i>Indicación</i>
Identificador de invocación	U	C(=)
Identificador de elemento	U	C(=)
Lista de errores	U	C(=)
Indicador de fatalidad	U	C(=)

7.2.3 Servicio SE-P-ABORTO

Los parámetros de servicio SE-P-ABORTO son los siguientes:

<i>Nombre del parámetro</i>	<i>Petición</i>
Identificador de invocación	O
Identificador de elemento	O
Código de problema	M
Indicador de fatalidad	O

8 Información de secuenciación

La única restricción de secuenciación estipulada en esta definición del servicio es que la invocación de las primitivas SE-TRANSFERENCIA con el mismo identificador de invocación debe ser consecuente con 7.1.2.