UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.411

(06/1999)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Sistemas de tratamiento de mensajes

Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos

Recomendación UIT-T X.411

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

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 declaraciones 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 de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	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.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–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	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

NORMA INTERNACIONAL ISO/CEI 10021-4
RECOMENDACIÓN UIT-T X.411

Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos

Resumen

Esta Recomendación | Norma Internacional contiene una versión mejorada de la operación de registro P3 que introduce el soporte del elemento de servicio entrega restringida y añade extensibilidad general a la operación de registro. La ASN.1 ha sido completamente revisada para utilizar las nuevas Recomendaciones X.680 y X.880, a la vez que se mantiene una compatibilidad total con los protocolos P1 y P3 de 1988 y 1992. Esta Recomendación | Norma Internacional incorpora mejoras en la utilización de caracteres ISO/CEI 10646 en direcciones-OR, nuevos valores de códigos de error para seguridad y la resolución de defectos de seguridad utilizando certificados de la Versión 3, extensiones de mensajería de clase comercial, portadas de fax, y la utilización del Directorio de 1997.

Orígenes

La Recomendación UIT-T X.411 fue aprobada el 18 de junio de 1999. Se publica también un texto idéntico como Norma Internacional ISO/CEI 10021-4.

En virtud de la decisión del UIT-T de publicar nuevas ediciones del conjunto de Recomendaciones sobre Sistemas de tratamiento de mensajes, esta edición de la Rec. UIT-T X.411 agrupa la Rec. X.411 (11/1995), el corrigendum técnico 1 a la Recomendación X.411 (08/1997), la enmienda 1 a la Recomendación X.411 (12/1997), el corrigendum técnico 2 a la Recomendación X.411 (12/1997) y el corrigendum técnico 3 a la Recomendación X.411 (09/1998).

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. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Introducción

Esta Definición de servicio forma parte de un conjunto de Recomendaciones | Normas Internacionales que definen el tratamiento de mensajes en un entorno distribuido de sistemas abiertos.

El tratamiento de mensajes facilita el intercambio de mensajes entre usuarios sobre la base de un almacenamiento y retransmisión. Un mensaje remitido por un usuario (el *originador*) se transfiere a través del sistema de transferencia de mensajes (MTS, *message transfer system*) y se entrega a uno o más usuarios (los *destinatarios*).

El MTS consta de un cierto número de agentes-de-transferencia-de-mensajes (MTA, *message transfer agent*), que transfieren mensajes y los entregan a los destinatarios deseados.

Esta Definición de servicio ha sido desarrollada conjuntamente por el UIT-T y la ISO/CEI. Se publica como texto común, Rec. UIT-T X.411 | ISO/CEI 10021-4.

NORMA INTERNACIONAL ISO/CEI 10021-4
RECOMENDACIÓN UIT-T X.411

Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos

SECCIÓN 1 – INTRODUCCIÓN

1 Alcance

Esta Recomendación | Norma Internacional define el servicio abstracto proporcionado por el MTS (servicio abstracto de MTS), y especifica los procedimientos que deben realizar los MTA para garantizar un funcionamiento distribuido correcto del MTS.

La Rec. UIT-T X.402 | ISO/CEI 10021-2 identifican otras Recomendaciones | Normas Internacionales que definen otros aspectos de los sistemas de tratamiento de mensajes.

El acceso al servicio abstracto de MTS definido en esta Recomendación | Norma Internacional puede ser facilitado por el protocolo de acceso (P3) del MTS, definido en la Rec. UIT-T X.419 | ISO/CEI 10021-6. El funcionamiento distribuido del MTS definido en esta Recomendación | Norma Internacional puede garantizarse mediante la utilización del protocolo de transferencia del MTS (P1) también definido en la Rec. UIT-T X.419 | ISO/CEI 10021-6. Los medios de encaminamiento de mensajes en el MTS se especifican en ISO/CEI 10021-10.

La sección 2 de esta Recomendación | Norma Internacional define el servicio abstracto del MTS. La cláusula 6 describe el modelo de sistema de transferencia de mensajes. La cláusula 7 proporciona una visión de conjunto del servicio abstracto del MTS. La cláusula 8 define la semántica de los parámetros del servicio abstracto del MTS. La cláusula 9 define la sintaxis-abstracta del servicio abstracto del MTS.

La sección 3 de esta Recomendación | Norma Internacional define el servicio abstracto del MTA. La cláusula 10 perfecciona el modelo de MTS, presentado inicialmente en la cláusula 6, para mostrar que el MTS incluye un cierto número de MTA que interfuncionan entre sí para prestar el servicio abstracto del MTS. La cláusula 11 proporciona una visión de conjunto del servicio abstracto de MTA. La cláusula 12 define la semántica de los parámetros del servicio abstracto de MTA. La cláusula 13 define la sintaxis-abstracta del servicio abstracto de MTA.

La sección 4 de esta Recomendación | Norma Internacional especifica los procedimientos realizados por los MTA para garantizar el funcionamiento distribuido correcto del MTS.

El anexo A proporciona una definición de referencia de los identificadores de objetos del MTS citados en los módulos ASN.1 del texto de esta Recomendación | Norma Internacional.

El anexo B proporciona una definición de referencia de los límites superiores de las limitaciones de tamaño impuestas sobre los tipos de datos de longitud variable definidos para los módulos ASN.1 en la Rec. UIT-T X.411.

El anexo C proporciona la definición del servicio abstracto del sistema de transferencia de mensajes de 1988.

El anexo D identifica las diferencias técnicas entre las versiones ISO/CEI y del UIT-T de la Rec. UIT-T X.411 y de la publicación ISO/CEI 10021-4.

El anexo E es un índice de esta Recomendación | Norma Internacional, clasificado por: definiciones de los parámetros del MTS, abreviaturas, términos, módulos ASN.1, clases de objetos de información ASN.1, tipos ASN.1 y valores ASN.1.

2 Referencias normativas

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

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

2.1 Interconexión de sistemas abiertos

En esta Definición de servicio se citan las siguientes especificaciones de la ISO:

- Recomendación UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.
- Recomendación UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información*.
- Recomendación UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones*.
- Recomendación UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de las especificaciones de la notación de sintaxis abstracta uno*.
- Recomendación UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Tecnología de la información – Operaciones a distancia: Conceptos, modelo y notación*.

2.2 Sistemas de tratamiento de mensajes

En esta Definición de servicio se citan las siguientes especificaciones de sistemas de tratamiento de mensajes:

- Recomendación UIT-T F.400/X.400 (1999): *Servicios de tratamiento de mensajes: Visión de conjunto del sistema y del servicio de tratamiento de mensajes*.

  ISO/CEI 10021-1:1990, *Information technology – Message Handling Systems (MHS) – Part 1: System and service overview*.
- Recomendación UIT-T X.402 (1999) | ISO/CEI 10021-2:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Arquitectura global*.
- Recomendación UIT-T X.413 (1999) | ISO/CEI 10021-5:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Memoria de mensajes: Definición del servicio abstracto*.
- Recomendación UIT-T X.419 (1999) | ISO/CEI 10021-6:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Especificaciones de protocolo*.
- Recomendación UIT-T X.420 (1999) | ISO/CEI 10021-7:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería interpersonal*.
- Recomendación UIT-T X.412 (1999) | ISO/CEI 10021-10:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Encaminamiento por el sistema de tratamiento de mensajes*.
- Recomendación CCITT X.408 (1988), *Sistemas de tratamiento de mensajes: Reglas de conversión de tipos de información codificada*.

2.3 Sistemas de directorio

En esta Definición de servicio se citan las siguientes especificaciones de sistemas de directorio:

- Recomendación UIT-T X.500 (1997) | ISO/CEI 9594-1:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios*.
- Recomendación UIT-T X.501 (1997) | ISO/CEI 9594-2:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*.
- Recomendación UIT-T X.509 (1997) | ISO/CEI 9594-8:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco de autenticación*.
- Recomendación UIT-T X.511 (1997) | ISO/CEI 9594-3:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto*.
- Recomendación UIT-T X.518 (1997) | ISO/CEI 9594-4:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Procedimientos para operación distribuida*.
- Recomendación UIT-T X.519 (1997) | ISO/CEI 9594-5:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo*.

- Recomendación UIT-T X.520 (1997) | ISO/CEI 9594-6:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados*.
- Recomendación UIT-T X.521 (1997) | ISO/CEI 9594-7:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Clases de objeto seleccionadas*.
- Recomendación UIT-T X.525 (1997) | ISO/CEI 9594-9:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Replicación*.
- Recomendación UIT-T X.530 (1997) | ISO/CEI 9594-10:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Utilización de la gestión de sistemas para la administración del directorio*.

2.4 Indicativos de país

En esta Definición de servicio se cita la siguiente especificación de indicativo de país:

- ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.
- Recomendación X.121 del UIT-T (1996), *Plan de numeración internacional para redes públicas de datos.*

2.5 Servicios telemáticos

Esta Definición de servicio cita las siguientes especificaciones de servicio telemático:

- Recomendación CCITT F.170 (1992), *Disposiciones operacionales para el servicio facsímil público internacional entre oficinas públicas (burofax)*.
- Recomendación UIT-T T.30 (1993), *Procedimientos de transmisión de documentos por facsímil por la red telefónica general conmutada*.

3 Definiciones

A los efectos de esta Definición de servicio se aplican las definiciones de la Rec. UIT-T X.402 | ISO/CEI 10021-2.

4 Abreviaturas

A los efectos de esta Definición de servicio se aplican las siglas que se encuentran en la Rec. UIT-T X.402 | ISO/CEI 10021-2.

5 Convenios

Esta Definición de servicio utiliza los convenios descriptivos descritos a continuación.

5.1 Términos

A lo largo de esta Definición de servicio, la redacción de los términos definidos y los nombres y valores de los parámetros del servicio abstracto de MTS y del servicio abstracto de MTA, a menos que sean nombres propios, comienzan con una letra minúscula y se unen con un guión de la siguiente forma: término-definido. Los nombres propios comienzan con una letra mayúscula (en el texto inglés) y no se unen mediante guión. Los nombres y los valores de los parámetros del servicio abstracto de MTS y del servicio abstracto de MTA (incluidos los componentes de dirección OR definidos en ISO/CEI 10021-2) se escriben en **negrita**.

5.2 Presencia de parámetros

En los cuadros de los parámetros de las cláusulas 8 y 12, la presencia de cada parámetro se califica de la siguiente forma:

Obligatorio (M): Parámetro obligatorio que debe existir siempre.

Opcional (O): Argumento opcional que debe existir a discreción del invocador de la operación-abstracta; un resultado opcional existirá a discreción del ejecutor de la operación-abstracta.

Condicional (C): Debe existir un parámetro condicional según se define en esta Definición de servicio.

Cuando existe un parámetro condicional, debido a una cierta acción del MTS sobre el mensaje, sonda o informe, éste se define explícitamente. La presencia de otros parámetros condicionales depende de la presencia de estos parámetros en otras operaciones-abstractas (por ejemplo, la presencia de un argumento condicional de la operación-abstracta de transferencia-mensaje depende de la presencia del mismo argumento facultativo en la correspondiente operación-abstracta de remisión-mensaje).

5.3 Definiciones de sintaxis abstracta

Esta Definición de servicio define la sintaxis-abstracta del servicio abstracto de MTS y del servicio abstracto de MTA utilizando la notación de sintaxis abstracta (ASN.1) definida en la Rec. UIT-T X.680 | ISO/CEI 8824-1, la Rec. UIT-T X.681 | ISO/CEI 8824-2, la Rec. UIT-T X.682 | ISO/CEI 8824-3 y la Rec. UIT-T X.683 | ISO/CEI 8824-4, y los convenios de Definición de servicio abstracto descritos en la Rec. UIT-T X.402 | ISO/CEI 10021-2, que utiliza la notación de operaciones a distancia definida en la Rec. UIT-T X.880 | ISO/CEI 13712-1.

Cuando se introducen cambios en los protocolos definidos en la Recomendación X.411 del CCITT (1984), éstos se señalan en las definiciones de sintaxis abstracta subrayándolos.

Si bien la sintaxis abstracta en esta Definición de servicio contiene marcas de ampliación, no se ha verificado que éstas aparezcan en todos los ejemplares en que sería necesario para poder usar sin riesgos las reglas de codificación compactadas.

5.4 Interpretación de los valores de tiempo UTC

Las fechas y las horas en los protocolos MHS se representan utilizando el tipo tiempo UTC (*UTCTime*) ASN.1 que utiliza sólo dos cifras decimales para representar el año y no especifica el siglo. Como los sistemas MHS deben admitir fechas tanto del pasado (por ejemplo, momento de presentación de mensajes antiguos que pueden quedar retenidos en almacenamiento local o ser retransmitidos) como del futuro (momento de expiración, momento de entrega aplazada), es importante observar un convenio normalizado para evitar le presentación inexacta o el funcionamiento defectuoso del MHS cuando se comparan las fechas de siglos distintos.

Las dos cifras decimales permiten expresar 100 años distintos; hace falta una implementación que asocie cada uno de esos valores a un siglo determinado. El convenio elegido es que las fechas hasta 10 años antes del momento actual y hasta 40 años después del momento actual se asociarán con el siglo correspondiente y la interpretación de los 49 valores restantes dependerá de la implementación. Por ejemplo, con un sistema que funcione en 1996, los valores "86" a "99" se interpretan como 1986 a 1999, los valores "00" a "36" se interpretan como 2000 a 2036 y los valores "37" a "85" dependen de la implementación.

NOTA – Este convenio permite dos posibles estrategias de implementación. Se puede elegir por ejemplo una interpretación fija de todos los valores del año de modo que el convenio sea válido durante la existencia prevista del producto o se pueden interpretar las fechas dinámicamente, basándose en la fecha efectiva, de modo que la implementación siga siendo válida indefinidamente. Por ejemplo, en la implementación se puede elegir la gama fija 1970 a 2069 para los valores disponibles, lo que significa que la implementación habrá de ser revisada si se la sigue utilizando en el año 2029.

SECCIÓN 2 – SERVICIO ABSTRACTO DEL SISTEMA DE TRANSFERENCIA DE MENSAJES

6 Modelo del sistema de transferencia de mensajes

El tratamiento de mensajes facilita el intercambio de mensajes entre usuarios, sobre la base de un almacenamiento y retransmisión. A través de un sistema de transferencia de mensajes se transfiere un mensaje remitido por un usuario (el *originador*) y se entrega a uno o más usuarios (los *destinatarios*).

Se describe el MTS utilizando un modelo abstracto –el servicio abstracto de MTS– para definir los servicios prestados por el MTS en su conjunto.

El MTS se modela como un *objeto*, cuyo comportamiento global puede describirse sin hacer referencia a su estructura interna. Los servicios prestados por el objeto del MTS se encuentran disponibles en los *puertos*. Un tipo de puerto representa una visión particular de los servicios proporcionados por el objeto del MTS.

También se modela un usuario del MTS como un objeto que contiene los servicios prestados por el MTS a través de un puerto emparejado con un puerto del MTS del mismo tipo.

Un tipo de puerto corresponde a un conjunto de *operaciones-abstractas* que pueden tener lugar en un puerto; aquellas que puede realizar el objeto del MTS (invocado por el objeto del usuario-MTS), y aquellas que puede invocar el objeto de MTS (realizados por el objeto del usuario-MTS).

Un puerto puede ser simétrico, en cuyo caso el objeto del MTS puede invocar igualmente el conjunto de operaciones realizadas por el objeto del MTS, y viceversa. Por el contrario, el puerto puede ser asimétrico en cuyo caso el objeto se denomina *suministrador* o *consumidor* en relación con el tipo de puerto. Los términos *suministrador* y *consumidor* se utilizan únicamente para distinguir entre los papeles de un par de puertos que invocan o realizan operaciones. La asignación de los términos es generalmente intuitiva cuando un objeto proporciona un servicio utilizado por otro objeto; el objeto del servicio (por ejemplo, MTS) se considera generalmente como el *suministrador*, y el objeto del usuario (por ejemplo, un objeto del usuario-MTS) se considera generalmente como *consumidor*.

Antes de que los objetos puedan invocar operaciones sobre otros, deben ligarse a una *asociación* abstracta. La vinculación de una asociación entre objetos establece una relación entre los objetos que dura hasta que se libera la asociación. El iniciador de la asociación es quien libera siempre la asociación. La vinculación de una asociación establece las *credenciales* de los objetos que interaccionan, el *contexto-aplicación* y el *contexto-seguridad* de la asociación. El *contexto-aplicación* de una asociación puede ser uno o más tipos del puerto emparejado entre los dos objetos.

El modelo presentado es abstracto. Es decir, un observador exterior no siempre puede identificar las fronteras entre los objetos, o decidir el momento o los medios para la realización de las operaciones. Sin embargo, en ciertos casos el modelo abstracto puede ser *realizado*. Por ejemplo, una pareja de objetos que comunican a través de puertos emparejados puede colocarse en diferentes sistemas abiertos. En este caso, la frontera entre los objetos resulta visible, se exponen los puertos, y las operaciones pueden proporcionarse como casos de comunicación OSI.

El objeto del MTS soporta puertos de tres tipos diferentes: un *puerto-remisión*, un *puerto-entrega* y un *puerto-administración*.

Un puerto-remisión permite a un usuario-MTS remitir mensajes al MTS para su transferencia y entrega a uno o más usuarios-MTS destinatarios, y sondear la aptitud del MTS para entregar un mensaje-asunto.

Un puerto-entrega permite a un usuario-MTS aceptar la entrega de mensajes del MTS, y aceptar informes sobre la entrega o no entrega de mensajes y de sondas.

Un puerto-administración permite a un usuario-MTS modificar los parámetros a largo plazo contenidos en el MTS asociados con la entrega de mensajes, y permite al MTS o al usuario-MTS cambiar las *credenciales* con otro.

Un mensaje remitido por un usuario-MTS a través de un puerto-remisión se entregará normalmente a uno o más usuarios-MTS destinatarios a través de puertos-entrega. Los usuarios-MTS originadores pueden elegir la posibilidad de recibir notificación de la entrega o no entrega de un mensaje a través de su puerto-entrega.

La figura 1 presenta un modelo del sistema de transferencia de mensajes (MTS, *message transfer system*).

La cláusula 7 da una visión de conjunto del servicio abstracto de MTS.

Figura 1 – Modelo del sistema de transferencia de mensajes

7 Visión de conjunto del servicio abstracto del sistema de transferencia de mensajes

Esta Definición de servicio define los servicios siguientes que componen el servicio abstracto de MTS:

Vinculación y desvinculación MTS

a) vinculación-MTS;

b) desvinculación-MTS.

Operaciones abstractas en el puerto de remisión

c) remisión-mensajes;

d) remisión-sonda;

e) cancelación-entrega-diferida;

f) control-remisión.

Operaciones abstractas en el puerto de entrega

g) entrega-mensajes;

h) entrega-informes;

i) control-entrega.

Operaciones abstractas en el puerto de administración

j) registro;

k) cambio-credenciales.

7.1 Vinculación y desvinculación al MTS

La **vinculación-MTS** permite al usuario-MTS establecer una asociación con el MTS, o al MTS establecer una asociación con el usuario-MTS. Otras operaciones-abstractas distintas de las de vinculación-MTS pueden invocarse únicamente en el contexto de una asociación establecida.

La **desvinculación-MTS** permite la liberación de una asociación establecida por el iniciador de la asociación.

7.2 Puerto de remisión

La operación-abstracta **remisión-mensaje** permite a un usuario-MTS remitir un mensaje al MTS para su transferencia y entrega a uno o más usuarios-MTS destinatarios.

La operación-abstracta **remisión-sonda** permite a un usuario-MTS remitir una sonda para determinar si podría transferirse y entregarse un mensaje a uno o más usuarios-MTS, si éste fuera presentado.

La operación-abstracta **cancelación-entrega-diferida** permite a un usuario-MTS solicitar la cancelación de un mensaje previamente remitido (para entrega-diferida) mediante la invocación de la operación abstracta remisión-mensaje.

La operación-abstracta **control-remisión** permite al MTS limitar la utilización por parte del usuario de las operaciones-abstractas puerto-remisión.

Las operaciones-abstractas **remisión-mensaje** y **remisión-sonda** pueden provocar la invocación subsiguiente de la operación-abstracta entrega-informe por parte del MTS.

7.3 Puerto de entrega

La operación-abstracta **entrega-mensaje** permite al MTS entregar un mensaje al usuario-MTS.

La operación-abstracta **entrega-informe** permite al MTS acusar recibo al usuario-MTS en relación con el resultado de la invocación previa de las operaciones-abstractas remisión-mensaje o remisión-sonda. Para la operación abstracta remisión-mensaje, la operación abstracta entrega-informe indica la entrega o no entrega del mensaje presentado. Para la operación-abstracta remisión-sonda, la operación-abstracta entrega-informe indica si podría entregarse o no un mensaje en el caso de que éste se presentara. La operación-abstracta entrega-informe puede también transportar una notificación entrega-física por un PDS.

La operación-abstracta **control-entrega** permite a un usuario-MTS limitar la utilización de las operaciones-abstractas puerto-entrega por parte del MTS.

7.4 Puerto de administración

La operación-abstracta **registro** permite a un usuario-MTS cambiar los parámetros a largo plazo del usuario-MTS contenidos en el MTS, asociados a la entrega de un mensaje.

La operación abstracta **cambio-credenciales** permite a un usuario-MTS cambiar sus **credenciales** con el MTS o al MTS cambiar sus **credenciales** con el usuario-MTS.

8 Definición del servicio abstracto del sistema de transferencia de mensajes

En esta cláusula, se define la semántica de los parámetros del servicio abstracto del MTS.

La cláusula 8.1 define la vinculación-MTS y la desvinculación-MTS. La cláusula 8.2 define el puerto-remisión. La cláusula 8.3 define el puerto-entrega. La cláusula 8.4 define el puerto-administración. La cláusula 8.5 define algunos tipos de parámetros comunes.

La sintaxis-abstracta del servicio abstracto del MTS se define en la cláusula 9.

8.1 Vinculación-MTS y desvinculación-MTS

En esta cláusula se definen las operaciones vinculación-MTS y desvinculación-MTS utilizadas para establecer y liberar asociaciones entre un usuario-MTS y el MTS.

8.1.1 Vinculación-abstracta y desvinculación-abstracta

En esta cláusula se definen las operaciones siguientes: vinculación-abstracta y desvinculación-abstracta;

a) vinculación-MTS;

b) desvinculación-MTS.

8.1.1.1 Vinculación-MTS

La vinculación-MTS permite a un usuario-MTS establecer una asociación con el MTS, o al MTS establecer una asociación con un usuario-MTS.

La vinculación-MTS establece las **credenciales** de un usuario-MTS y permite al usuario-MTS interaccionar, y establece el **contexto-aplicación** y el contexto-seguridad de la asociación. Únicamente el iniciador puede liberar esta asociación (utilizando la desvinculación-MTS).

Sólo pueden invocarse otras operaciones-abstractas diferentes de la vinculación-MTS en el contexto de una asociación establecida.

La consecución con éxito de vinculación-MTS significa el establecimiento de una asociación.

La interrupción de vinculación-MTS debido a un error-vinculación indica que no se ha establecido una asociación.

8.1.1.1.1 Argumentos

El cuadro 1 enumera los argumentos de vinculación-MTS, y para cada argumento califica su presencia e indica la cláusula donde se define el argumento.

Cuadro 1 – Argumentos de vinculación-MTS

Argumento	Presencia	Cláusula
Argumentos de vinculación		
Nombre-iniciador	M	8.1.1.1.1
Credenciales-iniciador	M	8.1.1.1.2
Contexto-seguridad	O	8.1.1.1.3
Mensajes-esperando	O	8.1.1.1.4

8.1.1.1.1.1 Nombre-iniciador

Este argumento contiene un nombre para el iniciador de la asociación. Debe ser generado por el iniciador de la asociación.

Si el iniciador es un usuario-MTS, el nombre es el **nombre-OR** del usuario-MTS, que está inscrito en el MTS (véase 8.4.1.1.1.1). El **nombre-iniciador** contiene la **dirección-OR** y puede contener también opcionalmente el **nombre-directorio**, del usuario-MTS, (**dirección-OR-y-nombre-directorio-facultativo**). El **nombre-iniciador** también indica si el iniciado es un UA o una MS.

Si el iniciador es el MTS (o un MTA – véase la cláusula 11), el nombre es un **nombre-MTA**, que conoce el usuario-MTS.

8.1.1.1.1.2 Credenciales-iniciador

Este argumento contiene las **credenciales** del iniciador de la asociación. Debe ser generado por el iniciador de la asociación.

Las **credenciales-iniciador** pueden utilizarse por el respondedor para autenticar la identidad del iniciador (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si se utiliza únicamente una autenticación-simple, las **credenciales-iniciador** consisten en una **contraseña** simple asociada al **nombre-iniciador**.

Si se utiliza la autenticación-protegida, las **credenciales-iniciador** consisten en una **contraseña** protegida, como se describe en la cláusula 6 de la Rec. UIT-T X.509 | ISO/CEI 9594-8 (Protected1 o Protected2) y opcionalmente argumentos para dicho proceso de protección (time1, time2, random1 y random2) cuyo significado se acuerda de forma bilateral. La descripción de la autenticación protegida en el anexo H de la Rec. UIT-T X.402 | ISO/CEI 10021-2 se aplica también a la vinculación MTS (aparte del mecanismo protegido para cambiar la contraseña).

Si se utiliza una autenticación-fuerte, las **credenciales-iniciador** comprenden un **testigo-vinculación-iniciador** y de forma opcional un **certificado-iniciador** o un **selector-certificado**.

El **testigo-vinculación-iniciador** es un **testigo** generado por el iniciador de la asociación. Si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**, los **datos-firmados** incluyen un **número-aleatorio**. Los **datos-criptados** de un **testigo-asimétrico** pueden utilizarse para transportar información-sobre-seguridad secreta (por ejemplo, una o más claves-criptación-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-iniciador**.

En el citado **testigo-asimétrico** (véase 8.5.8) pueden emplearse algoritmos simétricos.

El **certificado-iniciador** es un **certificado** del iniciador de la asociación, generado por una fuente de confianza (por ejemplo, autoridad-certificación) y, opcionalmente, certificados adicionales que proporcionan un trayecto-certificación para el certificado del iniciador. Puede suministrarse por el iniciador de la asociación, si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**. Si el iniciador es un usuario-MTS, el **certificado-iniciador** contendrá la **dirección-OR** del iniciador en el componente *Dirección x400*, dentro de su campo de nombre alternativo de sujeto (véase 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), a menos que la política-de-seguridad proporcione una vinculación alternativa del certificado al usuario-MTS. Si el iniciador es el MTS, el **certificado-iniciador** contendrá el **nombre-MTA** del iniciador en un *nombre-mta* (véase A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) en el componente *otroNombre* de su campo de nombre alternativo de sujeto, a menos que la política de seguridad proporcione una vinculación alternativa del certificado al MTA iniciador. El **certificado-iniciador** puede utilizarse para transportar una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del iniciador de la asociación. La clave-criptación-pública-asimétrica puede utilizarse por el respondedor para validar el **testigo-vinculación-iniciador** y calcular **datos-criptados** en el **testigo-vinculación-respondedor**. Si se sabe que el respondedor dispone o tiene acceso al **certificado** del iniciador (por ejemplo, a través del directorio), puede omitirse el **certificado-iniciador** cuando el iniciador tiene más de un certificado, puede proporcionarse un **selector-certificado** para identificar el certificado aplicando cualquier criterio de selección de certificado especificado para la concordancia de certificados (véase 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

8.1.1.1.1.3 Contexto-seguridad

Este argumento identifica el **contexto-seguridad** con el que el iniciador de la asociación propone funcionar. Puede generarse por el iniciador de la asociación.

El **contexto-seguridad** incluye una o más **etiquetas-seguridad** que definen la sensibilidad de las interacciones que pueden producirse entre el usuario-MTS y el MTS a lo largo de la duración de la asociación, en línea con la política-seguridad en vigor. El **contexto-seguridad** debe ser uno entre los autorizados por las **etiquetas-seguridad-usuario** registradas del usuario-MTS y por las **etiquetas-seguridad** asociadas al MTA del MTS.

Una vez establecido, el **contexto-seguridad** del puerto-remisión y del puerto-entrega puede restringirse transitoriamente utilizando las operaciones-abstractas de control-remisión (véase 8.2.1.4.5) y de control-entrega (véase 8.3.1.3.1.7), respectivamente.

Si no se establecen los **contextos-seguridad** entre el usuario-MTS y el MTS, la sensibilidad de las interacciones que pueden producirse entre el usuario-MTS y el MTS pueden dejarse a la discreción del invocador de una operación-abstracta.

8.1.1.1.1.4 Mensajes-esperando

Este argumento indica el número de mensajes y el número total de octetos que esperan para ser entregados por el MTS al usuario-MTS, para cada **prioridad**. Puede generarse por el iniciador de la asociación.

Este argumento estará únicamente presente cuando el MTS inicie una asociación con un usuario-MTS, y cuando un usuario-MTS se abone al elemento-de-servicio retención de entrega (definido en la Recomendación UIT-T X.400 | ISO/CEI 10021-1).

8.1.1.1.2 Resultados

El cuadro 2 enumera los resultados de vinculación-MTS, y para cada resultado califica su presencia e indica la cláusula donde se define el resultado.

Cuadro 2 – Resultados de vinculación-MTS

Resultado	Presencia	Cláusula
Resultado de vinculación		
Nombre-respondedor	M	8.1.1.1.2.1
Credenciales-respondedor	M	8.1.1.1.2.2
Mensajes-esperando	O	8.1.1.1.2.3

8.1.1.1.2.1 Nombre-respondedor

Este argumento contiene un nombre para el respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

Si el respondedor es un usuario-MTS, el nombre es el **nombre-OR** del usuario-MTS, que se inscribe con el MTS (véase 8.4.1.1.1.1). El **nombre-respondedor** contendrá la **dirección-OR** y puede contener también de forma opcional el **nombre-directorio**, del usuario-MTS (**dirección-OR-y-nombre-opcional-directorio**). El **nombre-respondedor** también indica si el respondedor es un UA o una MS.

Si el respondedor es el MTS (o un MTA – véase la cláusula 11), el nombre es un **nombre MTA**, que conoce el usuario-MTS.

8.1.1.1.2.2 Credenciales-respondedor

Este argumento contiene las **credenciales** del respondedor de la asociación. Debe ser generado por el respondedor de la asociación.

Las **credenciales-respondedor** pueden utilizarse por el iniciador para autenticar la identidad del respondedor (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si se utiliza únicamente la autenticación-simple, las **credenciales-respondedor** incluyen una **contraseña** simple asociada al **nombre-respondedor**.

Si se utiliza una autenticación-protegida, las **credenciales-respondedor** consisten en una **contraseña** protegida, como se describe en la cláusula 6 de la Rec. UIT-T X.509 | ISO/CEI 9594-8 (Protected1 o Protected2) y opcionalmente argumentos para dicho proceso de protección (time1, time2, random1 y random2) cuyo significado se acuerda de forma bilateral.

Si se utiliza una autenticación-fuerte, las **credenciales-respondedor** constan de un **testigo-vinculación-respondedor** y, opcionalmente, un **certificado-respondedor** o **selector-certificado**. El **testigo-vinculación-respondedor** es un testigo generado por el respondedor de la asociación. El **testigo-vinculación-respondedor** debe ser del mismo tipo que el **testigo-vinculación-iniciador**. Si el **testigo-vinculación-respondedor** es un **testigo-asimétrico**, los **datos-firmados** constan de un **número-aleatorio** (que puede estar relacionado con el **número-aleatorio** suministrado en el **testigo-vinculación-iniciador**). Los **datos-criptados** de un **testigo asimétrico** pueden utilizarse para transportar información-sobre-seguridad secreta (por ejemplo, una o más claves-criptación-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-respondedor**.

En el citado **testigo-asimétrico** (véase 8.5.8) pueden emplearse algoritmos simétricos.

El **certificado-respondedor** es un **certificado** del respondedor de la asociación, generado por una fuente de confianza (por ejemplo, una autoridad-certificación) y, opcionalmente, certificados adicionales que proporcionan un trayecto-certificación para el certificado del respondedor. Puede proporcionarlo el respondedor de la asociación, siempre que el **testigo-vinculación-respondedor** sea un **testigo-asimétrico**. Si el respondedor es un usuario-MTS, el **certificado-respondedor** contendrá la **dirección OR** del respondedor en el componente *Dirección x400* de su campo de nombre alternativo de sujeto (véase 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), a menos que la política de seguridad proporcione una vinculación alternativa del certificado al usuario-MTS. Si el respondedor es el MTS, el **certificado-respondedor** contendrá el **nombre-MTA** del respondedor en un *nombre-mta* (véase A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) en el componente *otroNombre* de su campo de nombre alternativo de sujeto, a menos que la política de seguridad proporcione una vinculación alternativa del certificado al MTA respondedor. El **certificado-respondedor** puede utilizarse para transportar una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del respondedor de la asociación. El iniciador puede utilizar la clave-criptación-pública-asimétrica del respondedor para validar el **testigo-vinculación-respondedor**. Si se sabe que el iniciador dispone o tiene acceso al **certificado** del respondedor (por ejemplo, a través del directorio), puede omitirse el **certificado-respondedor** y, cuando el respondedor tiene más de un certificado, puede proporcionarse un **selector-certificado** para identificar el certificado aplicando cualquier criterio de selección de certificado especificado para la concordancia de certificados (véase 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

8.1.1.1.2.3 Mensajes esperando

Este argumento indica el número de mensajes y el número total de octetos que esperan para ser entregados por el MTS al usuario-MTS, para cada **prioridad**. Puede generarse por el respondedor de la asociación.

Este argumento debe estar únicamente presente cuando el MTS conteste a una asociación iniciada por un usuario-MTS, y cuando un usuario-MTS se abone al elemento-de-servicio retención de entrega (véase la Rec. UIT-T X.400 | ISO/CEI 10021-1).

8.1.1.1.3 Errores-vinculación

Los errores-vinculación que pueden interrumpir la vinculación-MTS se definen en 8.1.2.

8.1.1.2 Desvinculación-MTS

La desvinculación-MTS permite liberar una asociación establecida por el iniciador de la asociación.

8.1.1.2.1 Argumentos

La desvinculación-MTS no tiene argumentos.

8.1.1.2.2 Resultados

La desvinculación-MTS devuelve un resultado vacío como indicación de la liberación de la asociación.

8.1.1.2.3 Errores-desvinculación

No existen errores-desvinculación que puedan interrumpir la desvinculación-MTS.

8.1.2 Errores-vinculación

En esta cláusula se definen los siguientes errores-vinculación:

a) error-autenticación;
b) ocupado;
c) modo-diálogo-inaceptable;
d) contexto-seguridad-inaceptable;
e) confidencialidad-asociación-inadecuada.

8.1.2.1 Error-autenticación

El error-vinculación de error-autenticación notifica que no puede establecerse una asociación debido a un error de autenticación; las **credenciales** del iniciador no son aceptables o están indebidamente especificadas.

El error-vinculación de error-autenticación no tiene parámetros.

8.1.2.2 Ocupado

El error-vinculación ocupado notifica que una asociación no puede establecerse porque el respondedor está ocupado.

El error-vinculación-ocupado no tiene parámetros.

8.1.2.3 Modo-diálogo-inaceptable

Un error-vinculación de modo-diálogo-inaceptable notifica que el modo-diálogo propuesto por el iniciador de la asociación es inaceptable para el respondedor (véase la Rec. UIT-T X.419 | ISO/CEI 10021-6).

El error-vinculación de diálogo-inaceptable no tiene parámetros.

8.1.2.4 Contexto-seguridad-inaceptable

Un error-vinculación de contexto-seguridad-inaceptable notifica que el **contexto-seguridad** propuesto por el iniciador de la asociación resulta inaceptable para el respondedor.

El error-vinculación de contexto-seguridad-inaceptable no tiene parámetros.

8.1.2.5 Confidencialidad-asociación-inadecuada

El error-vinculación de confidencialidad-asociación-inadecuada indica que no se puede establecer una asociación porque la conexión subyacente no proporciona la confidencialidad necesaria.

8.2 Puerto de remisión

En esta cláusula se definen las operaciones-abstractas y los errores-abstractos que se producen en el puerto de remisión.

8.2.1 Operación-abstracta

En esta cláusula se definen las siguientes operaciones-abstractas en el puerto-de-depósito:

a) remisión-mensaje;

b) remisión-sonda;

c) cancelación-entrega-diferida;

d) control-remisión.

8.2.1.1 Remisión-mensaje

La operación abstracta remisión-mensaje permite al usuario-MTS remitir un mensaje al MTS para su transferencia y entrega a uno o más usuarios-MTS destinatarios.

La ejecución satisfactoria de la operación-abstracta significa que el MTS ha aceptado la responsabilidad del mensaje (pero no que se haya entregado ya a los destinatarios deseados).

La interrupción de la operación-abstracta por un error-abstracto indica que el MTS no puede asumir la responsabilidad del mensaje.

8.2.1.1.1 Argumentos

El cuadro 3 enumera los argumentos de la operación-abstracta remisión-mensaje, y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

8.2.1.1.1.1 Nombre-originador

Este argumento contiene el **nombre-OR** del originador del mensaje. Se debe generar por el usuario-MTS originador. Si en el momento de la remisión la **dirección-OR** no está incluida en el **nombre-originador**, la insertará el MTA originador. El **nombre-originador** no cambia durante la progresión del mensaje a través del MTS. Cuando el argumento de seguridad utiliza el **nombre-originador**, su **dirección-OR** la generará el usuario-MTS originador.

El **nombre-originador** contiene el **nombre-OR** de un originador individual, es decir, no debe contener el **nombre-OR** de una DL.

8.2.1.1.1.2 Nombre-destinatario

Este argumento contiene el **nombre-OR** de un destinatario del mensaje, que lo generará el originador del mensaje. Se debe especificar un valor de este argumento para cada destinatario del mensaje.

El **nombre-destinatario** contiene el **nombre-OR** de un destinatario individual o de una DL.

8.2.1.1.1.3 Destinatario-alternativo-autorizado

Este argumento indica si puede entregarse el mensaje a un destinatario-alternativo asignado por el MD-destinatario, si el **nombre-destinatario** no identifica un usuario-MTS. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **destinatario-alternativo-autorizado** o **destinatario-alternativo-prohibido**.

Si este argumento tiene el valor **destinatario-alternativo-autorizado** y el **nombre-destinatario** (especificado por el originador del mensaje, o añadido por una ampliación-DL, o sustituido mediante una nueva dirección por el **destinatario-alternativo-asignado-destinatario** o por el **destinatario-alternativo-solicitado-originador**, o presente mediante una combinación de una nueva dirección y una ampliación) no identifica a un usuario-MTS, el mensaje puede redirigirse hacia un destinatario-alternativo asignado por el MD-destinatario para recibir dichos mensajes. Si el MD-destinatario no ha asignado ninguno de estos destinatarios-alternativos, o si este argumento tiene el valor **destinatario-alternativo-prohibido**, se generará un informe de no-entrega.

En ausencia de este argumento, se supondrá por defecto **destinatario-alternativo-prohibido**.

Cuadro 3 – Argumentos de remisión-mensaje

Argumento	Presencia	Cláusula
Argumento del originador		
Nombre-originador	M	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	M	8.2.1.1.1.2
Destinatario-alternativo-autorizado	O	8.2.1.1.1.3
Reasignación-destinatario-prohibida	O	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	O	8.2.1.1.1.5
Ampliación-DL-prohibida	O	8.2.1.1.1.6
Revelación-de-otros-destinatarios	O	8.2.1.1.1.7
Destinatarios-exentos-DL	O	8.2.1.1.1.40
Argumento de prioridad		
Prioridad	O	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	O	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	O	8.2.1.1.1.10
Conversión-explícita	O	8.2.1.1.1.11
Argumentos de tiempo de entrega		
Tiempo-entrega-diferida	O	8.2.1.1.1.12
Último-tiempo-entrega	O	8.2.1.1.1.13
Argumento de método de entrega		
Método-entrega-solicitado	O	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	O	8.2.1.1.1.15
Petición-dirección-envío-físico	O	8.2.1.1.1.16
Modos-entrega-física	O	8.2.1.1.1.17
Tipo-correo-certificado	O	8.2.1.1.1.18
Número-destinatario-para-aviso	O	8.2.1.1.1.19
Atributos-reproducción-física	O	8.2.1.1.1.20
Dirección-devolución-originador	O	8.2.1.1.1.21
Argumentos de petición de informes		
Petición-informe-originado	M	8.2.1.1.1.22
Petición-devolución-contenido	O	8.2.1.1.1.23
Petición-informe-entrega-física	O	8.2.1.1.1.24

Cuadro 3 – Argumentos de remisión-mensaje

Argumento	Presencia	Cláusula
Argumentos de seguridad		
Certificado-originador	O	8.2.1.1.1.25
Testigo-mensaje	O	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	O	8.2.1.1.1.27
Verificación-integridad-contenido	O	8.2.1.1.1.28
Verificación-autenticación-mensaje-origen	O	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	O	8.2.1.1.1.30
Petición-prueba-de-remisión	O	8.2.1.1.1.31
Petición-prueba-de-entrega	O	8.2.1.1.1.32
Múmtiples-certificado-originador	O	8.2.1.1.1.41
Certificados-destinatario	O	8.2.1.1.1.42
Selectores-certificado	O	8.2.1.1.1.43
Contraorden-selectores-certificado	O	8.2.1.1.1.44
Argumentos de contenido		
Tipos-información-codificada-originales	O	8.2.1.1.1.33
Tipo-contendio	M	8.2.1.1.1.34
Identificador-contenido	O	8.2.1.1.1.35
Correlador-contenido	O	8.2.1.1.1.36
Contenido	M	8.2.1.1.1.37
Tipo-notificación	O	8.2.1.1.1.38
Mensaje-servicio	O	8.2.1.1.1.39

8.2.1.1.1.4 Reasignación-de-destinatario-prohibida

Este argumento indica si el mensaje puede reasignarse a otro usuario-MTS registrado como un **destinatario-alternativo-asignado-destinatario** por el destinatario-deseado. Puede ser generado por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **reasignación-de-destinatario-prohibida** o **reasignación-de-destinatario-autorizada**.

Si este argumento tiene el valor **reasignación-de-destinatario-autorizada** y el destinatario-deseado ha registrado un **destinatario-alternativo-asignado-destinatario** aplicable, el mensaje se redireccionará a ese **destinatario-alternativo-asignado-destinatario**.

Si este argumento tiene el valor **reasignación-destinatario-prohibida** y el destinatario-deseado ha registrado un **destinatario-alternativo-asignado-destinatario** aplicable, si el originador del mensaje ha especificado **destinatario-alternativo-solicitado-originador** se redirecciona el mensaje al **destinatario-alternativo-solicitado-originador**, o si el originador del mensaje no ha especificado ningún **destinatario-alternativo-solicitado-originador**, se generará un informe-de-no-entrega.

En ausencia de este argumento, se supondrá por defecto **reasignación-de-destinatario-autorizada**.

8.2.1.1.1.5 Destinatario-alternativo-solicitado-originador

Este argumento contiene el **nombre-OR** del destinatario alternativo solicitado por el originador del mensaje. Puede generarse por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

El **destinatario-alternativo-solicitado-originador** contiene el **nombre-OR** de un destinatario-alternativo individual o DL.

Si este argumento está presente y no resulta posible la entrega del mensaje al **nombre-destinatario** (especificado por el originador del mensaje, o añadido por una ampliación-DL, o sustituido mediante una nueva dirección por el **destinatario-alternativo-asignado-destinatario**), el mensaje se debe redirigir al **destinatario-alternativo-solicitado-originador** especificado por este argumento.

Si el originador del mensaje ha especificado un **destinatario-alternativo-solicitado-originador**, el mensaje será redirigido a ese destinatario alternativo con preferencia a uno asignado por el MD-destinatario.

8.2.1.1.1.6 Ampliación-DL-prohibida

Este argumento indica si se producirá una ampliación-DL dentro del MTS para cualquier **nombre-destinatario** que designe una DL. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **ampliación-DL-prohibida** o **ampliación-DL-autorizada**.

En ausencia de este argumento, se supondrá por defecto **ampliación-DL-autorizada**.

8.2.1.1.1.7 Revelación-de-otros-destinatarios

Este argumento indica si debe indicarse el **nombre-destinatario** de todos los destinatarios a cada usuario-MTS destinatario al entregar el mensaje. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **revelación-de-otros-destinatarios-solicitada** o **revelación-de-otros-destinatarios-prohibida**.

En ausencia de este argumento, se supondrá por defecto **revelación-de-otros-destinatarios-prohibida**.

8.2.1.1.1.8 Prioridad

Este argumento especifica la prioridad relativa del mensaje: **normal**, **no-urgente** o **urgente**. Puede generarse por el originador del mensaje.

En ausencia de este argumento, se supondrá por defecto una **prioridad normal**.

8.2.1.1.1.9 Conversión-implícita-prohibida

Este argumento indica si puede realizarse una conversión implícita del **contenido** del mensaje. Puede generarse por el originador del mensaje.

Este argumento puede tener los siguientes valores: **conversión-implícita-prohibida** o **conversión-implícita-autorizada**.

En ausencia de este argumento, se supondrá por defecto **conversión-implícita-autorizada**.

Véase igualmente 8.2.1.1.1.10.

8.2.1.1.1.10 Conversión-con-pérdida-prohibida

Este argumento indica si puede realizarse una conversión o conversiones del **tipo-información-codificada** del **contenido** del mensaje, en el caso de que dicha conversión o conversiones pueden dar lugar a una pérdida de información. La pérdida de información se define en la Rec. X.408 del CCITT. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **conversión-con-pérdida-prohibida** o **conversión-con-pérdida-autorizada**.

En ausencia de este argumento, se supondrá por defecto **conversión-con-pérdida-autorizada**.

El efecto combinado de los argumentos de **conversión-implícita-prohibida** y de **conversión-con-pérdida-prohibida** se refiere únicamente a las conversiones-implícitas y se define en el cuadro 4.

Cuadro 4 – Efecto combinado de los argumentos de conversión

Conversión implícita	Conversión con pérdida	Efecto combinado
autorizada	con-pérdida-autorizada	autorizado
autorizada	con-pérdida-prohibida	con-pérdida-prohibida
prohibida	con-pérdida-autorizada	prohibido
prohibida	con-pérdida-prohibida	prohibido

8.2.1.1.1.11 Conversión explícita

Este argumento indica el tipo de conversión del **contenido** del mensaje solicitado explícitamente por el originador para el destinatario. Puede generarse por el originador del mensaje. Puede especificarse un valor diferente de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **ia5-texto-a-teletex**, **texto-ia5-a-facsímil-g3**, **texto-ia5-a-g4-clase-1**, **texto-ia5-a-videotex**, **teletex-a-texto-ia5**, **teletex-a-facsímil-g3**, **teletex-a-g4-clase-1**, **teletex-a-videotex**, **videotex-a-texto-ia5** o **videotex-a-télex**. Pueden definirse otros tipos de **conversión-explícita** en adiciones o en versiones futuras de esta Rec. | Norma Internacional. La **conversión-explícita** se debe realizar conforme a lo especificado en la Recomendación X.408 del CCITT.

En ausencia de este argumento, no se efectuará ninguna conversión explícita.

NOTA – Cuando se especifica la **conversión-explícita** para una DL de destinatarios, ésta se aplica a todos los miembros de la DL.

8.2.1.1.1.12 Tiempo-entrega-diferida

Este argumento especifica el **tiempo** antes del cual no debería entregarse el mensaje al destinatario o destinatarios. Puede generarse por el originador del mensaje.

8.2.1.1.1.13 Último-tiempo-entrega

Este argumento contiene el **tiempo** después del cual no debería entregarse el mensaje al destinatario o destinatarios. Puede generarse por el originador del mensaje.

El tratamiento de la no entrega debido al **último-tiempo-entrega** se describe en 14.3.2.4.

8.2.1.1.1.14 Método-entrega-solicitado

Este argumento indica el método preferido de entrega del mensaje al destinatario. Puede generarse por el originador del mensaje. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno o más de los siguientes valores: **cualquier-método-entrega**, **entrega-mhs**, **entrega-física**, **entrega-télex**, **entrega-teletex**, **entrega-facsímil-g3**, **entrega-facsímil-g4**, **entrega-terminal-ia5**, **entrega-videotex**, o **entrega telefónica**.

Si se especifica más de un valor de este argumento para un destinatario, se supondrá que la secuencia de valores implica un orden de preferencia del originador respecto de los métodos-entrega.

En ausencia de este argumento, se supondrá por defecto **cualquier-método-entrega**.

Si el **nombre-destinatario** generado por el originador del mensaje contiene un **nombre-directorio** pero omite una **dirección-OR**, el MTS puede utilizar el **método-entrega-solicitado** como una indicación de la forma de **dirección-OR** en que el MTS debería transformar **el nombre-directorio** (por ejemplo utilizando el directorio). Si no puede encontrarse una **dirección-OR**, se debe devolver al originador del mensaje un error-abstracto **destinatario-impropiamente-especificado** o un informe de no-entrega.

Si el **método-entrega-solicitado** suministrado-originador entra en conflicto con el método-entrega preferido del destinatario (por ejemplo registrado en el directorio en el atributo método-entrega-preferido), el **método-entrega-solicitado** del originador tiene preferencia. Si el **método-entrega-solicitado** entra en conflicto con los requisitos de conversión del originador (véanse 8.2.1.1.1.9 a 8.2.1.1.1.11), se debe devolver un informe de no-entrega al originador del mensaje.

8.2.1.1.1.15 Envío-físico-prohibido

Este argumento indica si está prohibido el envío-físico de un mensaje. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los siguientes valores: **envío-físico-autorizado**, o **envío-físico-prohibido**.

En ausencia de este argumento, se supondrá por defecto **envío-físico-autorizado**.

8.2.1.1.1.16 Petición-dirección-envío-físico

Este argumento indica si debe devolverse en un informe la dirección-envío-físico del destinatario. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los siguientes valores: **dirección-envío-físico-solicitada**, o **dirección-envío-físico-no-solicitada**.

En ausencia de este argumento, se supondrá por defecto dirección-envío-físico-no-solicitada.

Se puede solicitar una dirección-de-envío-físico cuando el envío físico esté prohibido o permitido (véase 8.2.1.1.1.15).

8.2.1.1.1.17 Modos-entrega-física

Este argumento indica el modo de entrega-física al destinatario que ha de utilizarse. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

El valor de este argumento es la combinación de dos componentes independientes. Si está presente, el primer componente tendrá uno de los valores siguientes: **correo-ordinario**, **urgente**, **entrega-inmediata**, **retirada-ventanilla**, **retirada-ventanilla-con-aviso-telefónico**, **retirada-ventanilla-con-aviso-télex** o **retirada-ventanilla-con-aviso-teletex**. Si está presente, el segundo componente puede tener el valor **entrega-burofax**. Cuando se solicita **entrega-burofax** y el primer componente también está presente, el servicio burofax activa el primer componente.

La **entrega-burofax** comprende todos los modos de entrega del A al H definidos en la Rec. F.170 del CCITT, es decir: A – Entrega regular, B – Urgente, C – Entrega inmediata, D – Retirada en ventanilla, E – Retirada en ventanilla con aviso telefónico, F – Telefax, G – Retirada en ventanilla con aviso télex y H – Retirada en ventanilla con aviso teletex.

En ausencia de este argumento, se supondrá por defecto **correo-ordinario**.

8.2.1.1.1.18 Tipo-correo-certificado

Este argumento indica el tipo de correo certificado que ha de utilizarse para entregar físicamente el mensaje al destinatario. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **correo-no-certificado**, **correo-certificado**, o **correo-certificado-a-dirección-en-persona**.

En ausencia de este argumento, se supondrá por defecto **correo-no-certificado**.

8.2.1.1.1.19 Número-destinatario-para-aviso

Este argumento contiene el número de teléfono, télex o teletex del destinatario, para utilizarlo en combinación con los modos **modo-entrega-física**, **modo-recogida-oficina-postal-con-aviso** y **modo-entrega-burofax**. Pueden generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario y el argumento de los **modos-entrega-física** especifica un **modo-entrega-física**, un **modo-recogida-oficina-postal-con-aviso** o un **modo-entrega-burofax**. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

8.2.1.1.1.20 Atributos-reproducción-física

Este argumento indica los **atributos-reproducción-física** que se han de aplicar cuando el mensaje es reproducido en forma física. Puede ser generado por el originador del mensaje si es probable que el mensaje requiera reproducción, por ejemplo, si la dirección del destinatario designa una unidad de acceso, o si el **método-entrega-solicitado** especifica un método de entrega en el que participa una unidad de acceso. Se puede especificar un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento se especifica como un identificador de objeto. Los siguientes valores se definen en esta especificación:

básico No se requiere ninguna reproducción especial, se debe aplicar la reproducción normal ofrecida por al AU.

ninguna portada El mensaje debe ser reproducido sin la adición de una portada suministrada por el AU. Este valor es particularmente apropiado para unidades de acceso facsímil.

Otros valores de este argumento pueden ser registrados privadamente y utilizados mediante acuerdo. En adiciones a la presente Recomendación | Norma Internacional o en futuras versiones de la misma se pueden definir otros valores normalizados.

En ausencia de este argumento, se supone el valor **básico**.

8.2.1.1.1.21 Dirección-devolución-originador

Este argumento contiene la **dirección-OR-postal** del originador del mensaje. Puede generarlo el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física a uno o más destinatarios, o si el originador del mensaje proporcionó una o más **direcciones-postales-OR** de los destinatarios. Puede generarse igualmente por el originador del mensaje si una DL de destinatarios contiene o es probable que contenga uno o más miembros para los cuales se solicita la entrega-física.

La **dirección-devolución-originador** contendrá la **dirección-postal-OR** de cada originador (**dirección-OR**), es decir no contendrá ni el **nombre-directorio** de un originador ni el **nombre-directorio** de una DL.

8.2.1.1.1.22 Petición-informe-originador

Este argumento indica la categoría de informe solicitada por el originador del mensaje. Se debe generar por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes:

no-informe: el originador del mensaje solicita la supresión de los informes de no-entrega;

informe-no-entrega: se devuelve un informe únicamente en el caso de no-entrega;

informe: se devuelve un informe en el caso de entrega o de no-entrega.

El valor de este argumento puede cambiarse en un punto-ampliación de DL de acuerdo con la política-de-información de la DL. Dicho cambio puede afectar al número y tipo de informe que el originador del mensaje puede recibir sobre la entrega a una DL.

8.2.1.1.1.23 Petición-devolución-contenido

Este argumento indica si el **contenido** del mensaje debe devolverse con cualquier informe-no-entrega. Se puede generar por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **devolución-contenido-solicitada** o **devolución-contenido-no-solicitada**.

En ausencia de este argumento, se supondrá por defecto **devolución-contenido-no-solicitada**.

La supresión de los informes-no-entrega por el originador del mensaje (véase 8.2.1.1.1.22) tiene preferencia sobre una petición de devolución del **contenido**.

En el caso de informes-no-entrega entregados al propietario de una DL (véase 8.3.1.2.1.4), el **contenido** del mensaje no estará presente.

8.2.1.1.1.24 Petición-informe-entrega-física

Este argumento indica el tipo de informe-entrega-física solicitado por el originador del mensaje. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-OR** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **devolución-de-correo-inentregable-por-PDS, devolución-de-notificación-por-PDS, devolución-de-notificación-por-MHS** o **devolución-de-notificación-por-MHS-y-PDS**.

En ausencia de este argumento, se supondrá por defecto **devolución-de-correo-inentregable-por-PDS**.

8.2.1.1.1.25 Certificado originador

Este argumento contiene un **certificado** de originador del mensaje. Será generado por una fuente de confianza (por ejemplo, una autoridad de certificación), y puede ser suministrador por el originador del mensaje.

El **certificado de originador** se puede utilizar para transportar una copia verificada de la clave de criptación pública asimétrica (**clave-pública-sujeto**) del originador del mensajes.

NOTA – Si hay que transmitir más de un certificado de originador a todos los destinatarios, el certificado para **verificación-autenticación-origen-mensaje** es transportado en este argumento y los demás certificados son transportados en el argumento **múltiples-certificados-originador**. Si se requieren certificados especializados para cada destinatario, los certificados especializados son indicados en el argumento **contraorden-selectores-certificados** (véase 8.2.1.1.1.44).

Cuando el mismo algoritmo y la misma clave secreta han sido utilizados para calcular firmas digitales transportadas en uno o más de los siguientes argumentos: **verificación-autenticación-origen-mensaje**, **verificación-integridad-contenido** o **testigo-mensaje**, la correspondiente clave-criptación-pública-asimétrica del originador puede ser utilizada

por los destinatarios del mensaje para validar firmas digitales transportadas en el argumento **verificación-integridad-contenido** y en el argumento **testigo-mensaje**, si se utiliza un testigo asimétrico con un algoritmo asimétrico (véase 8.5.8). Puede ser utilizada también por los destinatarios del mensaje y cualquier MTA a través del cual se transfiere el mensaje, para validar la **verificación-autenticación-origen-mensaje**.

8.2.1.1.1.26 Testigo-mensaje

Este argumento contiene el **testigo** asociado al mensaje. Puede generarse por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

Si el **testigo-mensaje** es un **testigo-asimétrico**, los **datos-firmados** pueden incluir:

cualquiera de los siguientes argumentos: el **identificador-algoritmo-confidencialidad-contenido**, la **verificación-integridad-contenido**, la **etiqueta-seguridad-mensaje**, y la **prueba-de-petición-entrega**; y

un **número-secuencia-mensaje**, que identifique la posición del mensaje en una secuencia de mensajes del originador al destinatario al que se refiere el **testigo-mensaje** (para proporcionar el elemento-de-servicio de integridad de secuencia de mensajes, definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). La primera ocurrencia de un número secuencia puede ser un número aleatorio.

Si el **testigo-mensaje** es un **testigo-asimétrico**, los **datos-criptados** pueden incluir:

una **clave-confidencialidad-contenido**: clave-criptación-simétrica utilizada con el **identificador-algoritmo-confidencialidad-contenido** por el originador del mensaje para criptar el contenido del mensaje y por el destinatario del mensaje para descriptar el **contenido** del mensaje; y/o

la **verificación-integridad-contenido**: puede incluirse en los **datos-criptados**, si se requiere confidencialidad de la **verificación-integridad-contenido** y/o si la **etiqueta-seguridad-mensaje** se incluye en los **datos-criptados** (para confidencialidad de la etiqueta-seguridad-mensaje) y debe mantenerse la asociación entre la verificación-integridad-contenido y la etiqueta-seguridad-mensaje;

la **etiqueta-seguridad-mensaje**: puede incluirse en los **datos-criptados**, si se requiere confidencialidad de la **etiqueta-seguridad-mensaje**;

una **clave-integridad-contenido**: clave-criptación-simétrica utilizada con el **identificador-algoritmo-integridad-contenido**, por el originador del mensaje para calcular la **verificación-integridad-contenido**; y por el destinatario para validar la **verificación-integridad-contenido**;

un **número-secuencia-mensaje**: definido para los **datos-firmados** anteriormente, pero que puede incluirse en los **datos-criptados** si se requiere confidencialidad de la secuencia. La primera ocurrencia de un número secuencia puede ser un número aleatorio.

Si el **testigo-mensaje** es un **testigo-asimétrico** y los **datos-firmados** del **testigo-mensaje** incluyen la **verificación-integridad-contenido**, el **testigo-mensaje** podría proporcionar el no-repudio-del-origen del **contenido** del mensaje, sujeto a la disponibilidad de una infraestructura de claves públicas adecuada (elemento-de-servicio de no repudio del origen, definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Si los **datos-firmados** del **testigo-mensaje** incluyen tanto la **verificación-integridad-contenido** como la **etiqueta-seguridad-mensaje**, el **testigo-mensaje** proporciona una prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el **contenido** del mensaje.

En el citado **testigo-asimétrico** (véase 8.5.8) pueden emplearse algoritmos simétricos. Si para el **testigo-mensaje** y la **verificación-integridad-contenido** se emplean algoritmos simétricos, el **testigo-mensaje** sólo soporta elementos-de-servicio de no repudio del origen si la política de seguridad vigente prevé la intervención de una tercera parte que haga de notario.

NOTA 1 – Si hay que intercambiar múltiples certificados para procesar el **testigo-mensaje**, los certificados pueden ser transportados en el argumento **múltiples-certificados-originador**, en el argumento **certificados-por-cada-destinatario**, o en ambos.

NOTA 2 – Un certificado necesario para implementar un acuerdo de claves para los datos criptados del testigo puede utilizar un certificado de originador en el argumento **múltiples-certificados-originador**, junto con el certificado del destinatario en el argumento **certificado-por-cada-destinatario**. El certificado apropiado puede ser identificado utilizando certificados de la Versión 3, que contienen ampliaciones de certificado para este fin; la identificación puede transportarse en los argumentos **selectores-certificado** y **contraorden-selectores-certificado**. (Por ejemplo, la **utilización de claves** puede ser empleada para indicar el certificado que se ha de utilizar para fines de acuerdo de claves y **políticas de certificados** se puede utilizar para indicar la política en virtud de la cual ha de funcionar el acuerdo de claves.)

8.2.1.1.1.27 Identificador-algoritmo-confidencialidad-contenido

Este argumento contiene un **identificador-algoritmo**, que identifica el algoritmo utilizado por el originador del mensaje para criptar el **contenido** del mensaje (para proporcionar el elemento-de-servicio confidencialidad de contenido definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Puede generarse por el originador del mensaje.

El algoritmo puede utilizarse por el destinatario o destinatarios del mensaje para descifrar el **contenido** del mensaje.

El algoritmo de confidencialidad-contenido puede ser un algoritmo-criptación-simétrico o asimétrico.

Si se utiliza un algoritmo-criptación-simétrico, la **clave-confidencialidad-contenido** utilizada para criptar el **contenido** del mensaje, y que el destinatario puede utilizar para descriptar el **contenido** del mensaje, puede deducirse del **testigo-mensaje** enviado con el mensaje. Como alternativa, puede distribuirse por algún otro medio la **clave-confidencialidad-contenido**.

Si se utiliza un algoritmo-criptación-asimétrico, la clave-criptación-pública-asimétrica del destinatario deseado puede ser utilizada por el originador del mensaje para criptar el **contenido** del mensaje. El destinatario puede utilizar la clave-criptación-asimétrica-secreta del destinatario para descriptar el **contenido** del mensaje. Si se utiliza un algoritmo-criptación-asimétrico, el mensaje puede dirigirse únicamente a un único destinatario, o a un conjunto de destinatarios que compartan la misma pareja de claves-criptación-asimétricas.

8.2.1.1.1.28 Verificación-integridad-contenido

Este argumento proporciona al destinatario del mensaje los medios para validar que no se ha modificado el **contenido** del mensaje (para proporcionar el elemento de servicio integridad de contenido definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Puede ser generado por el originador del mensaje. Se puede especificar un valor diferente del argumento para cada destinatario del mensaje.

Si el valor de este argumento es específico de un destinatario, porque se ha utilizado un algoritmo o clave específicos para generar este valor (es decir, cuando se especifican diferentes valores del argumento para cada destinatario del mensaje), los certificados apropiados pueden ser transportados por el argumento **múltiples-certificados-originador** e identificados por el argumento **contraorden-selectores-certificado**.

Si el mismo algoritmo y la misma clave han sido utilizados para generar este argumento para todos los destinatarios (es decir, se especifica el mismo valor del argumento para cada destinatario del mensaje), el certificado apropiado puede ser transportado por el argumento **certificados-originador**, o si se ha de transmitir más de un certificado de originador, se utilizará el argumento **múltiples-certificados-originador** y el certificado apropiado será identificado por los argumentos **contraorden-selectores-certificado**.

Este argumento permite al destinatario del mensaje validar la integridad del contenido del mensaje recibido y la autenticación del originador del mensaje.

La **verificación-integridad-contenido** permite validar la integridad del contenido destinatario por destinatario, utilizando un algoritmo-criptación-simétrico o asimétrico.

NOTA 1 – La **verificación-autenticación-origen-mensaje** proporciona los medios para validar la integridad-contenido mensaje por mensaje, utilizando un algoritmo-criptación-asimétrico.

La **verificación-integridad-contenido** puede incluirse también en los **datos-firmados** o en los **datos-criptados** del **testigo-mensaje** para proporcionar el no-repudio-del-origen del **contenido** del mensaje, sujeto a la disponibilidad de una infraestructura de claves públicas adecuada, y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el **contenido** del mensaje.

NOTA 2 – De este modo, hay tres argumentos distintos de **verificación-integridad-contenido**, un argumento por destinatario y dos en el **testigo-mensaje**.

La **verificación-integridad-contenido** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-integridad-contenido** (un **identificador-algoritmo**).

NOTA 3 – Los diversos argumentos **VERIFICACIÓN-INTEGRIDAD-CONTENIDO** pueden ser calculados utilizando diferentes algoritmos. En particular, cuando la **VERIFICACIÓN-INTEGRIDAD-CONTENIDO** se incluye en los **DATOS-FIRMADOS** o en los **DATOS-CRIPTADOS** del **TESTIGO-MENSAJE**, se puede calcular utilizando un algoritmo diferente del argumento **verificación-integridad-contenido** por destinatario.

La **verificación-integridad-contenido** contiene el **identificador-algoritmo-de-integridad-de-contenido** y una firma digital que se genera utilizando una o más funciones cifradas (por ejemplo, versión comprimida, desmenuzada o doble desmenuzada) del **contenido** del mensaje, y condicionalmente el **identificador-algoritmo-integridad-contenido**.

NOTA 4 – La **verificación-integridad-contenido** podrá ser calculada utilizando el contenido claro (es decir no criptado) o el contenido criptado. Esta elección se puede hacer independientemente para cada ocurrencia de la verificación de integridad de contenido en el mensaje. Esta elección es dictada por la política de seguridad en vigor y puede ser indicada también por el **identificador-algoritmo-integridad-contenido**.

El **identificador-algoritmo-integridad-contenido** especificará:

1) si la **verificación-integridad-contenido** se calcula utilizando el **contenido** claro (es decir, no criptado) o criptado, si esta elección no viene dictada por la política de seguridad;
2) la presencia o ausencia del **identificador-algoritmo-integridad-contenido** dentro de la secuencia ASN.1 en la que se calcula la firma;

3) la regla de codificación ASN.1 (CER o DER) a aplicar a la secuencia ASN.1 antes del troceado;
4) la función troceado;
5) si el valor troceado ha de ser o no codificado dentro de la cadena de bits ASN.1 antes del cifrado;
6) el algoritmo utilizado para proteger el valor hash (por ejemplo, un algoritmo de la criptación asimétrico); y
7) cualesquiera parámetros del algoritmo tales como claves necesarias, valores de inicialización e instrucciones de relleno.

El algoritmo integridad-contenido puede ser un algoritmo-criptación-simétrico o asimétrico.

Si se utiliza un algoritmo-criptación-simétrico, la **clave-integridad-contenido** utilizada para calcular la **verificación-integridad-contenido**, y que puede utilizar el destinatario para validar la **verificación-integridad-contenido**, puede deducirse del **testigo-mensaje** enviado con el mensaje. Como alternativa, la **clave-integridad-contenido** puede distribuirse por varios otros procedimientos.

NOTA 5 – La utilización de un algoritmo-criptación-simétrico puede permitir la compresión y criptación simultáneos del **contenido** del mensaje para crear la **verificación-integridad-contenido**.

Si se utiliza un algoritmo-criptación-asimétrico, la clave-criptación-asimétrico-secreta del originador puede ser utilizada por el originador del mensaje para calcular la **verificación-integridad-contenido**. El destinatario puede utilizar la clave-criptación-público asimétrica del originador (**clave-pública-sujeto**) deducida del **certificado-originador**, o **múltiples-certificados-originador** para validar el valor apropiado de **verificación-integridad-contenido**.

NOTA 6 – Cuando se requieren múltiples certificados, el certificado apropiado puede ser identificado por los argumentos **selectores-certificado** y **contraorden-selectores-certificado**, o mediante la utilización de la ampliación **utilización clave** o la ampliación **políticas certificado** definidas en la Rec. UIT-T X.509 | ISO/CEI 9594-8, o por una combinación de ambas. Por ejemplo, el certificado requerido para validar una firma digital por destinatario (el valor de una **verificación-integridad-contenido** por destinatario) puede ser identificada por el argumento **contraorden-selectores-certificado** entregados al destinatario. Si se entrega más de un certificado a este usuario, el certificado apropiado puede ser determinado por la **utilización-clave** y la ampliación **políticas-certificado** (es decir, **utilización-clave** será la **firma-digital**, el identificador de objeto en la extensión **políticas-certificado** puede indicar la política en virtud de la cual la firma fue generada y ha de ser utilizada, y esta política a su vez puede definir en qué dominios la firma es válida).

8.2.1.1.1.29 Verificación-autenticación-origen-mensaje

Este argumento proporciona al destinatario o destinatarios del mensaje, y a cualquier MTA a través del cual se transfiera un mensaje, los medios para autenticar el origen del mensaje (para proporcionar el elemento-de-servicio autenticación de origen de mensaje definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Puede generarse por el identificador del mensaje.

La **verificación-autenticación-origen-mensaje** proporciona la prueba del origen del mensaje (autenticación del origen del mensaje), garantía de que el **contenido** del mensaje no ha sido modificado (el elemento-de-servicio integridad de contenido definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1) y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el mensaje.

La **verificación-autenticación-origen-mensaje** se calcula utilizando el algoritmo (algoritmo-criptación-asimétrico y función-trocear) identificada por el **identificador-algoritmo-autenticación-origen-mensaje** (un **identificador-algoritmo**).

La **verificación-autenticación-origen-mensaje** contiene el **identificador-algoritmo-autenticación-origen-mensaje**, y una versión criptada asimétricamente, troceada del **identificador-algoritmo-autenticación-origen-mensaje**, el **contenido** del mensaje, el **identificador-contenido** y la **etiqueta-seguridad-mensaje**. Se incluyen componentes facultativos en la **verificación-autenticación-origen-mensaje** si están presentes en el mensaje.

Si se utiliza igualmente la confidencialidad-contenido (véase 8.2.1.1.1.27), se calcula **verificación-autenticación-origen-mensaje** utilizando la versión criptada del **contenido** del mensaje [para permitir que la **verificación-autenticación-origen-mensaje** sea validada por otro que no sea el destinatario-deseado (por ejemplo, por un MTA) sin comprometer la confidencialidad del **contenido** del mensaje]. Si la versión clara (es decir sin criptar) del **contenido** del mensaje se utiliza para calcular la **verificación-autenticación-origen-mensaje**, ésta facilita la autenticación del origen del mensaje y el no repudio del origen del **contenido** del mensaje (firma), definidos en la Rec. UIT-T X.400 | ISO/CEI 10021-1. Sin embargo, si se utiliza la versión criptada del **contenido** del mensaje, la **verificación-autenticación-origen-mensaje** facilita la autenticación del origen del mensaje, pero no el no repudio del origen del **contenido** del mensaje.

El originador del mensaje puede calcular **verificación-autentificación-origen-mensaje** utilizando la clave-criptación-secreta-asimétrica del originador. La **verificación-autenticación-origen-mensaje** puede validarse por el destinatario o destinatarios del mensaje, y por cualquier MTA a través del cual se transfiere el mensaje, utilizando la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del originador del mensaje deducida a partir del **certificado-originador**.

Adiciones o futuras versiones de esta Recomendación | Norma Internacional pueden definir otras formas de **verificación-autenticación-origen-mensaje** (por ejemplo, basadas en técnicas-criptación-simétricas) que pueden ser utilizadas por los MTA a través de los cuales se transfiere el mensaje para autenticar el origen del mensaje.

8.2.1.1.1.30 Etiqueta-seguridad-mensaje

Este argumento asocia una **etiqueta-seguridad** al mensaje (o sonda). Puede ser generado por el originador del mensaje (o sonda), en línea con la política-seguridad en vigor.

La **etiqueta-seguridad-mensaje** de un informe será la misma que la **etiqueta-seguridad-mensaje** del mensaje sujeto (o sonda).

Si se asignan **etiquetas-seguridad** a los usuarios-MTS, a los MTA y a otros objetos del MHS, el tratamiento, por estos objetos, de mensajes, sondas e informes que transportan **etiquetas-seguridad-mensaje** puede determinarse por la política-seguridad en vigor. Si no se asignan etiquetas-seguridad a los usuarios-MTS, a los MTA y a otros objetos del MHS, el tratamiento, por estos objetos, de los mensajes, sondas e informes que transportan **etiquetas-seguridad-mensaje** puede ser discrecional.

Si establecen contextos-seguridad entre el originador y un MTA (el MTA-originador) del MTS (véanse las cláusulas 8.1.1.1.1.3 y 8.2.1.4.1.5), la **etiqueta-seguridad-mensaje** que puede asignar el originador a un mensaje (o sonda) puede determinarse por el **contexto-seguridad** (contexto-seguridad-remisión), en línea con la política-seguridad en vigor. Si no se establecen **contextos-seguridad** entre el originador y el MTA-originador, la asignación de una **etiqueta-seguridad-mensaje** a un mensaje (o sonda) puede quedar a la discreción del originador.

Si se establecen **contextos-seguridad** entre dos MTA (véase 12.1.1.1.1.3), la transferencia de mensajes, sondas o informes entre los MTA puede determinarse por las **etiquetas-seguridad-mensaje** de los mensajes, sondas o informes, y el **contexto-seguridad**, en línea con la política-seguridad en vigor. Si no se establecen **contextos-seguridad** entre los MTA, la transferencia de mensajes, sondas e informes puede quedar a la discreción del emisor.

Si se establecen **contextos-seguridad** entre un usuario-MTS y un MTA (MTA-que-entrega) del MTS (véanse las cláusulas 8.1.1.1.1.3 y 8.3.1.3.1.7), la entrega de mensajes e informes puede determinarse por las **etiquetas-seguridad-mensaje** de los mensajes e informes y el **contexto-seguridad** (contexto-seguridad-entrega), en línea con la política-seguridad en vigor. Si las **etiquetas-seguridad-usuario** registradas del destinatario autorizan la **etiqueta-seguridad-mensaje** de un mensaje o informe, pero el **contexto-seguridad** corriente del destinatario (contexto-seguridad-entrega) no la autoriza, entonces al MTA-que-entrega puede retener-para-entrega. Si no se establecen los **contextos-seguridad** entre los usuarios-MTS y el MTA-que-entrega, la entrega de mensajes e informes puede realizarse a discreción del MTA-que-entrega.

8.2.1.1.1.31 Petición-prueba-de-remisión

Este argumento indica si el originador del mensaje solicita la **prueba-de-remisión** (para proporcionar el elemento-de-servicio prueba de remisión definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1) del mensaje al MTS. Puede ser generado por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **prueba-de-remisión-solicitada** o **prueba-de-remisión-no-solicitada**.

En ausencia de este argumento se supondrá que el valor por defecto es **prueba-de-remisión-no-solicitada**.

8.2.1.1.1.32 Petición-prueba-de-entrega

Este argumento indica si el originador del mensaje solicita **prueba-de-entrega** (para proporcionar el elemento-de-servicio prueba de entrega definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1) del mensaje al destinatario. Puede ser generado por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno de los siguientes valores: **prueba-de-entrega-solicitada** o **prueba-de-entrega-no-solicitada**.

En ausencia de este argumento, se supondrá que el valor por defecto es **prueba-de-entrega-no-solicitada**.

8.2.1.1.1.33 Tipos-información-codificada-originales

Este argumento identifica los **tipos-información-codificada** originales del **contenido** del mensaje. Puede generarse por el originador del mensaje.

La ausencia de este argumento indica que los **tipos-de-información-codificada-originales** del **contenido** del mensaje están **sin especificar**.

8.2.1.1.1.34 Tipo-contenido

Este argumento identifica el tipo de **contenido** del mensaje. Identifica la sintaxis abstracta y las reglas de codificación utilizadas. Será generado por el originador del mensaje. El **tipo contenido** será o incorporado o ampliado.

Un **tipo-contenido** incorporado puede tener uno de los siguientes valores:

sin identificar: designa un **tipo-contenido** sin identificar y sin limitación; la utilización de este **tipo-contenido** sin identificar constituye un acuerdo bilateral entre usuarios-MTS;

externo: designa un **tipo-contenido** que se reserva para el interfuncionamiento entre sistemas 1988 y sistemas 1984; sólo se utilizará con el **protocolo-transferencia-mts-1984** (véase la Rec. UIT-T X.419 | ISO/CEI 10021-6).

NOTA 1 – Las reglas de interfuncionamiento garantizan que nunca se utilice el **tipo-contenido externo** junto con la **transferencia-mts** o el **protocolo-transferencia-mts**. Aunque el **tipo-contenido externo** está previsto para permitir el interfuncionamiento entre todos los sistemas desde los intermedios de 1984 hasta los de 1988, un sistema de 1984 puede entregar (o remitir) un **contenido** del **tipo-contenido externo**, siempre y cuando el usuario-MTS (o el propio MTA) realice una operación equivalente a las adaptaciones indicadas en la Rec. UIT-T X.419 | ISO/CEI 10021-6.

mensajería-interpersonal-1984: identifica el definido en la Rec. UIT-T X.420 | ISO/CEI 10021-7;

mensajería-interpersonal-1988: identifica el definido en la Rec. UIT-T X.420 | ISO/CEI 10021-7;

mensajería-edi: identifica el **tipo-contenido edim** definido en la Rec. UIT T X.435 | ISO/CEI 10021-9;

mensajería-voz: identifica el **tipo-contenido vm** definido en la Rec. UIT T X.440.

Un **tipo-contenido** ampliado se especifica empleando un identificador de objeto.

Un valor específico de un **tipo-contenido** ampliado definido en esta Definición de servicio es:

sobre-interior: **tipo-contenido** ampliado que es un mensaje en sí (sobre y contenido). Cuando es entregado al destinatario indicado en el sobre-exterior se suprime este sobre y se descifra el contenido si es necesario, lo que da lugar a un sobre-exterior y a su contenido. La información contenida en el sobre interior se utiliza para transferir el contenido del sobre interior a los destinatarios indicados en el sobre interior. El tipo del **contenido** OCTET STRING es una **APDU-MTS** (véase la figura 6 de la Rec. UIT-T X.419 | ISO/CEI 10021-6) codificada utilizando las reglas de codificación básicas de la ASN.1. [Obsérvese que el sobre-interior y el contenido pueden protegerse introduciendo seguridad en el **contenido** del sobre-exterior utilizando los argumentos de seguridad (véanse las cláusulas 8.2.1.1.1.25 a 8.2.1.1.1.32).]

Pueden definirse otros **tipos-contenido** ampliado normalizados en otras especificaciones de MHS o en otras Recomendaciones | Normas Internacionales. Pueden utilizarse otros valores de este argumento mediante acuerdos bilaterales entre usuarios-MTS.

NOTA 2 – Si se utiliza el servicio de confidencialidad de contenido, la sintaxis y la codificación identificadas por el **tipo-contenido** son la sintaxis y la codificación del contenido antes de la criptación.

8.2.1.1.1.35 Identificador-contenido

Este argumento contiene un identificador del **contenido** del mensaje. Puede generarse por el originador del mensaje.

El **identificador-contenido** puede ser entregado al destinatario o destinatarios del mensaje, y devuelto al originador con algún informe o informes. Este argumento no es alterado por el MTS.

8.2.1.1.1.36 Correlador-contenido

Este argumento contiene información que permite al originador del mensaje efectuar la correlación del **contenido** del mensaje. Puede generarse por el originador del mensaje.

El **correlador-contenido** no es entregado al destinatario o destinatarios del mensaje, pero se devuelve al originador con algún informe o informes. Este argumento no es alterado por el MTS.

8.2.1.1.1.37 Contenido

Este argumento contiene la información del mensaje que se pretende transportar al destinatario o destinatarios. Será generado por el originador del mensaje.

Excepto cuando se realiza una conversión, el MTS no modifica el **contenido** del mensaje; al contrario éste pasa de forma transparente a través de él.

El **contenido** puede ser criptado para asegurar su confidencialidad (véase 8.2.1.1.1.27).

NOTA – El valor de la cadena de octetos que contiene el contenido **codificado** no cambia cuando el mensaje pasa por el MTS.

8.2.1.1.1.38 Tipo-notificación

Este argumento indica que el **contenido** es una notificación, e indica que es uno de los tres tipos de notificación (tipo-1, tipo-2 o tipo-3); la utilización de dichos valores se define en la especificación de **contenido** correspondiente. Puede ser generado por el originador del mensaje, pero solamente si el **contenido** es una notificación definida en la especificación de **contenido** correspondiente.

La indicación **tipo-notificación** no es entregada al destinatario o destinatarios del mensaje ni es devuelta al originador con ningún informe. Según la política aplicada, este argumento puede ser verificado por el MTS.

8.2.1.1.1.39 Mensaje-servicio

Este argumento indica que el mensaje es de servicio. Puede ser generado por el originador del mensaje, pero sólo se utiliza previo acuerdo bilateral.

La indicación **mensaje-servicio** no es entregada al destinatario o destinatarios del mensaje ni es devuelta al originador con ningún informe. Según la política aplicada, este argumento puede ser verificado por el MTS.

8.2.1.1.1.40 Destinatarios-exentos-DL

Este argumento contiene los **nombres-OR** de los posibles destinatarios que se solicita no sean añadidos al conjunto de destinatarios deseados como resultados de la expansión-DL. Puede ser generado por el originador del mensaje.

Este argumento no es modificado durante el procesamiento de MTA y se incluye en operaciones de transferencia subsiguientes con independencia de si se ha efectuado la expansión-DL.

El argumento **destinatarios-exentos-DL** es entregado al destinatario o destinatarios, pero no es devuelto al originador con ningún informe.

8.2.1.1.1.41 Múltiples-certificados-originador

Este argumento contiene un **certificado** del originador del mensaje, o el **nombre-directorio** de una inserción en el directorio que contiene un certificado del originador, o múltiples certificados (o nombre-de-directorio) cuando los certificados contienen diferentes trayectos de certificación o son emitidos por diferentes autoridades de certificación o tienen fines diferentes. Cada **certificado** será generado por una fuente de confianza (por ejemplo, una autoridad de certificación), y puede ser suministrado por el originador del mensaje.

El argumento **múltiples-certificados-originador** se puede utilizar para transmitir las copias verificadas de información pública del originador necesarias para verificar firmas digitales o utilizarse para fines de acuerdo de claves. Puede transportar la clave de criptación pública asimétrica (**clave-pública-sujeto**) del originador del mensaje, u otra información pública necesaria para el procesamiento de acuerdo de claves.

Se pueden producir múltiples **certificados** o **nombres-directorio** cuando se ha de transportar más de un tipo de información verificada del originador del mensaje:

NOTA 1 – Si se requieren certificados especializados para cada destinatario, éstos se indican en el argumento **contraorden-selector-certificado**.

NOTA 2 – Para aplicar un acuerdo de claves puede ser necesario tener certificados en ambos argumentos **múltiples-certificados-originador** y **certificado-destinatario**.

Cuando se ha de utilizar un certificado dentro de **múltiples-certificados-originador** para una finalidad determinada, se utilizarán certificados de la Versión 3 (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8) para indicar la finalidad de la información contenida en el certificado. Las ampliaciones de **utilización-clave** y **políticas-certificado** de los certificados de la Versión 3 pueden ser utilizadas individualmente o en combinación, para indicar la finalidad de un certificado transportado en el elemento **múltiples-certificados-originador**. La ampliación de **utilización-clave** y **políticas-certificado** puede indicar cuándo se necesita la clave de criptación pública asimétrica del originador para validar una firma digital en cualquiera de los siguientes argumentos: **verificación-autenticación-origen-mensaje, verificación-integridad-contenido** o **testigo-mensaje**. Asimismo, si se transporta más de un valor de la firma digital utilizando los diversos argumentos verificación-integridad-contenido, el certificado apropiado puede ser indicado por la combinación de las ampliaciones de certificado **utilización-clave** y **políticas-certificado**. Estas ampliaciones pueden indicar cuándo es necesaria la información pública del originador para fines de acuerdos de clave en el procesamiento del argumento **testigo-mensaje**.

Varias firmas digitales pueden ser generadas por el originador de un mensaje, que son transportadas en los argumentos **verificación-autenticación-origen-mensaje**, **verificación-integridad-contenido** y/o **testigo-mensaje**. Si el mismo algoritmo y la clave pública asimétrica del originador se necesitan para validar todas las firmas digitales, esto puede ser indicado por la combinación de las ampliaciones de certificado **utilización-clave** y **políticas-certificado**.

NOTA 3 – Si se necesitan algoritmo especializados y claves públicas asimétricas del originador para verificar firmas digitales para cada destinatario, se requieren también certificados especializados para cada destinatario. En este caso, el certificado especializado se identifica en el argumento **contraorden-selectores-certificado**.

8.2.1.1.1.42 Certificados-destinatario

Este argumento contiene un **certificado** del destinatario del mensaje y opcionalmente su trayecto de certificación. El **certificado** será generado por una fuente de confianza (por ejemplo, una autoridad de certificación) y puede ser suministrado por el originador del mensaje. Se puede especificar un valor diferente de este argumento para cada destinatario del mensaje.

El **certificado-destinatario** puede ser utilizado para transportar una copia verificada de información pública que se utilizará para acordar las claves. Identifica la clave-de-criptación-pública-asimétrica (**clave-pública-sujeto**) del destinatario del mensaje que utilizó el originador. Esta identificación puede alternativamente transportarse en el argumento **contraorden-selectores-certificado**. Esta identificación sólo es necesaria si el destinatario tiene más de un certificado para el algoritmo identificado.

El certificado transportado en **certificado-destinatario** puede ser utilizado para fines de acuerdo de claves, tales como generación de claves necesarias para procesar los **datos-criptados** en el **testigo-mensaje**.

Si el mensaje es ampliado por una o más DL seguras en el trayecto de mensaje, los **certificados por destinatario** pueden ser generados por la DL.

8.2.1.1.1.43 Selectores-certificado

Este argumento contiene información suficiente para identificar un **certificado** cuando un usuario tiene más de un **certificado** con el mismo **identificador-algoritmo**. Permite identificar un **certificado** del originador para validar determinadas firmas digitales en los argumentos **verificación-autenticación-origen-mensaje**, **verificación-integridad-contenido**, o **testigo-mensaje**, o puede utilizarse para acordar las claves de criptación; también permite identificar un certificado de cada destinatario para acordar las claves o para la criptación asimétrica. Puede ser generado por el originador del mensaje.

Cada componente de **selectores-certificado** permite especificar cualquiera de los criterios de selección de certificado para concordancia de certificados indicados en 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8, que es aplicable a un certificado de usuario. El destinatario añade el identificador-algoritmo adecuado (en **subjectPublicKeyAlgID**, identificador de algoritmo de clave pública del sujeto) y el tiempo de remisión del mensaje (o creación del testigo) en el que fueron válidos el certificado y la clave privada (en **certificateValid** y **privateKeyValid**) según los criterios de selección especificados por el originador antes de seleccionar un certificado. Los criterios especificados, combinados con estos valores, deberán ser suficientes para seleccionar un certificado. Por ejemplo, esto permite la identificación inequívoca de un solo certificado por **expedidor** y **número-serie**, o la identificación genérica de una clase de certificado con **objetivo-clave** o **política-certificados** (la cual, junto con el identificador-algoritmo adecuado y la fecha de validez, dará un único certificado para cada usuario). El valor de cada componente se aplica a todos los destinatarios a menos que haya un valor correspondiente en ese componente de **contraorden-selectores-certificado** para ese destinatario. Los argumentos **certificado-originador** o **certificados-originador-múltiple** puede contener, aunque no es obligatorio, los certificados identificados.

El argumento **selectores-certificado** contiene los siguientes componentes:

destinatario-criptación;
originador-criptación;
verificación-integridad-contiendo;
firma-testigo;
autenticación-origen-mensaje.

El *destinatario-criptación* identifica uno de los certificados de destinatario, y cada uno de los otros identifica uno de los certificados del originador. Los dos primeros se aplican a criptación-testigo si algoritmo-confidencialidad-contenido es simétrico, y a criptación-contenido si es asimétrico.

8.2.1.1.1.44 Contraorden-selectores-certificado

Este argumento contiene información suficiente para identificar un **certificado** cuando un usuario tiene más de un **certificado** con el mismo **identificador-algoritmo**. Permite identificar un **certificado** del originador para validar firmas digitales específicas en los argumentos **verificación-integridad-contiendo** o **testigo-mensaje**, o puede utilizarse para acordar las claves de criptación; también permite identificar un certificado de cada destinatario para acordar las claves o para la criptación asimétrica. Puede ser generado por el originador del mensaje. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento es idéntico al argumento **selectores-certificado**, pero no contiene el componente *autenticación-origen-mensaje*.

Si este argumento está presente, el valor en cada componente que está presente sustituye al valor del componente correspondiente del argumento **selectores-certificado**.

8.2.1.1.2 Resultados

El cuadro 5 enumera los resultados de la operación-abstracta remisión-mensaje, y para cada resultado califica su presencia e identifica la cláusula en el que se define el resultado.

Cuadro 5 – Resultados de la operación-abstracta remisión-mensaje

Resultado	Presencia	Cláusula
Identificador-remisión-mensaje	M	8.2.1.1.2.1
Tiempo-remisión-mensaje	M	8.2.1.1.2.2
Certificado-MTA-originador	O	8.2.1.1.2.3
Prueba-de-remisión	C	8.2.1.1.2.4
Identificador-contenido	C	8.2.1.1.1.35

8.2.1.1.2.1 Identificador-remisión-mensaje

Este resultado contiene un **identificador-MTS** que identifica unívoca e inequívocamente la remisión-mensaje. Debe ser generado por el MTS.

El MTS proporciona el **identificador-remisión-mensaje** al notificar, al usuario-MTS, la entrega o la no-entrega del mensaje, a través de la operación abstracta entrega-informe.

El usuario-MTS proporciona el **identificador-remisión-mensaje** al cancelar un mensaje cuya entrega estaba diferida, a través de la operación-abstracta cancelación-entrega-diferida.

8.2.1.1.2.2 Tiempo-remisión-mensaje

Este resultado indica el **tiempo** en que el MTS acepta la responsabilidad del mensaje. Debe ser generado por el MTS.

8.2.1.1.2.3 Certificado-MTA-originador

Este resultado contiene el **certificado** del MTA en el que se ha depositado el mensaje (MTA-originador). Debe ser generado por una fuente de confianza (por ejemplo, una autoridad-certificación), y puede suministrarse por el MTA-originador, si el originador del mensaje solicitó una **prueba-de-remisión** (véase 8.2.1.1.1.31) y se utiliza un algoritmo-criptación-asimétrico para calcular la **prueba-de-remisión**.

Puede utilizarse el **certificado-MTA-originador** para enviar al originador del mensaje una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del MTA-originador.

El originador del mensaje puede utilizar la clave-criptación-pública-asimétrica de los MTA-originadores para validar la **prueba-de-remisión**.

8.2.1.1.2.4 Prueba-de-remisión

Este resultado proporciona al originador del mensaje la prueba de remisión del mensaje al MTS (para proporcionar el elemento-de-servicio prueba de remisión definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). En función del algoritmo-criptación utilizado y de la política de seguridad en vigor, este argumento puede proporcionar igualmente el elemento-de-servicio no repudio de remisión (definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Debe ser generado por el MTA-originador del MTS, si el originador del mensaje solicitó la **prueba-de-remisión** (véase 8.2.1.1.1.31).

Se calcula la **prueba-de-remisión** utilizando el algoritmo identificado por el **identificador-algoritmo-prueba-de-remisión** (un **algoritmo-identificador**).

La **prueba-de-remisión** contiene el **identificador-algoritmo-prueba-de-remisión**, y una función criptada (por ejemplo, una versión comprimida o troceada) del **identificador-algoritmo-prueba-de-remisión**, los argumentos de remisión-mensaje (véase 8.2.1.1.1) del mensaje sujeto, y el **identificador-remisión-mensaje** y el **tiempo-remisión-mensaje**.

La recepción de este resultado proporciona al originador del mensaje la prueba de remisión del mensaje. La no-recepción de este resultado no proporciona ni la prueba de remisión ni la prueba de no-remisión (a menos que se utilicen un enlace seguro y una funcionalidad de confianza).

Si se utiliza un algoritmo-criptación-asimétrico, el MTA-originador puede calcular la **prueba-de-remisión**, utilizando la clave-criptación-asimétrica-secreta del MTA-originador. El originador del mensaje puede validar la **prueba-de-remisión** utilizando la clave-criptación-pública-asimétrica del MTA-originador (**clave-pública-sujeto**) deducida del **certificado-MTA-originador**. Puede proporcionarse igualmente una **prueba-de-remisión** para el no repudio de remisión sujeto a la disponibilidad de una infraestructura de claves públicas adecuada.

Si se utiliza un algoritmo-criptación-simétrico, la clave-criptación-simétrica que el MTA-originador utilizó para calcular la **prueba-de-remisión**, y que el originador puede utilizar para validar la **prueba-de-remisión**, puede deducirse a partir de los **testigos-vinculación** (véanse las cláusulas 8.1.1.1.1.3 y 8.1.1.1.2.2) intercambiados al iniciar la asociación. Como alternativa, la clave-criptación-simétrica utilizada para la **prueba-de-remisión** puede intercambiarse por algún otro procedimiento. Si se utiliza un algoritmo-criptación-simétrico, la **prueba-de-remisión** únicamente puede proporcionar el no repudio de la remisión si la política-seguridad en vigor proporciona la intervención de una tercera parte que actúe como notario.

8.2.1.1.3 Errores-abstractos

El cuadro 6 enumera los errores abstractos que pueden interrumpir la operación-abstracta remisión-mensaje, y para cada error abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 6 – Errores-abstractos de remisión-mensaje

Error-abstracto	Cláusula
Control-remisión-violado	8.2.2.1
Elemento-de-servicio-no-abonado	8.2.2.2
Originador-no-válido	8.2.2.4
Destinatario-indebidamente-especificado	8.2.2.5
Petición-incoherente	8.2.2.7
Error-seguridad	8.2.2.8
Función-crítica-no-soportada	8.2.2.9
Error-vinculación-distante	8.2.2.10

8.2.1.2 Remisión-sonda

La operación-abstracta remisión-sonda permite a un usuario-MTS remitir una sonda para determinar si podría transferirse y entregarse un mensaje (mensaje-sujeto) a uno o más usuarios-MTS destinatarios, si éste se presentara.

El éxito de una sonda no garantiza que un mensaje remitido posteriormente pueda ser realmente entregado, sino más bien que en el momento actual el destinatario es válido y el mensaje no tropezará con obstáculos importantes para la entrega.

Para cualesquiera **nombres-destinatarios** que designen una DL, la operación-abstracta remisión-sonda determina si se produciría una ampliación de la DL especificada (pero no DL anidadas).

Para cualesquiera **nombres-destinatarios** para los cuales se produciría un redireccionamiento, la operación-abstracta remisión-sonda determina si podría transferirse y entregarse el mensaje al destinatario sustitutivo.

El usuario-MTS suministra la mayoría de los argumentos utilizados para la remisión-mensaje y la longitud del contenido del mensaje-sujeto. La operación-abstracta remisión-sonda no culmina con la entrega a los destinatarios deseados del mensaje-sujeto, sino que establece si probablemente lo haría la operación-abstracta remisión-mensaje.

La ejecución satisfactoria de la operación-abstracta significa que el MTS ha aceptado hacerse cargo de la sonda (pero no que la haya llevado a cabo todavía).

La interrupción de la operación-abstracta por un error-abstracto indica que el MTS no puede hacerse cargo de la sonda.

8.2.1.2.1 Argumentos

El cuadro 7 enumera los argumentos de la operación-abstracta remisión-sonda, y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

Cuadro 7 – Argumentos de remisión-sonda

Argumento	Presencia	Cláusula
Argumento del originador		
Nombre-originador	M	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	M	8.2.1.1.1.2
Destinatario-alternativo-autorizado	O	8.2.1.1.1.3
Reasignación-destinatario-prohibida	O	8.2.1.1.1.4
Destinatario-alternativo-solicitado	O	8.2.1.1.1.5
Ampliación-DL-prohibida	O	8.2.1.1.1.6
Argumentos de conversión		
Conversión-implícita-prohibida	O	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	O	8.2.1.1.1.10
Conversión-explícita	O	8.2.1.1.1.11
Argumento de método de entrega		
Método-entrega-solicitado	O	8.2.1.1.1.14
Argumento de entrega física		
Atributos-reproducción-física	O	8.2.1.1.1.20
Argumento de petición de informes		
Petición-informe-originador	M	8.2.1.1.1.22
Argumentos de seguridad		
Certificado-originador	O	8.2.1.1.1.25
Comprobación-autenticación-origen-sonda	O	8.2.1.2.1.1
Etiqueta-seguridad-mensaje	O	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-original	O	8.2.1.1.1.33
Tipo-contenido	M	8.2.1.1.1.34
Identificador-contenido	O	8.2.1.1.1.35
Correlador-contenido	O	8.2.1.1.1.36
Longitud-contenido	O	8.2.1.2.1.2
Tipo-notificación	O	8.2.1.1.1.38
Mensaje-servicio	O	8.2.1.1.1.39

8.2.1.2.1.1 Verificación-autenticación-origen-sonda

Este argumento proporciona a cualquier MTA a través del cual se transfiere la sonda, los medios para autenticar el origen de la sonda (proporcionar el elemento-de-servicio autenticación del origen de la sonda definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Puede generarse por el originador de la sonda.

La **verificación-autenticación-origen-sonda** proporciona la prueba del origen de la sonda (autenticación del origen de la sonda), y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el **identificador-contenido** del mensaje-sujeto.

La **verificación-autenticación-origen-sonda** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-autenticación-origen-sonda** (un **identificador-algoritmo**).

La **verificación-autenticación-origen-sonda** contiene el **identificador-algoritmo-autenticación-origen-sonda**, y una versión criptada asimétricamente, troceada del **identificador-algoritmo-autenticación-origen-sonda**, el **identificador-contenido** y la **etiqueta-seguridad-mensaje** del mensaje-sujeto. En la **verificación-autenticación-origen-sonda** se incluyen componentes facultativos si éstos están presentes en la sonda.

El originador de la sonda puede calcular la **verificación-autenticación-origen-sonda** utilizando la clave-criptación-secreta-asimétrica del originador. La **verificación-autenticación-origen-sonda** puede validarse por cualquier MTA a través del cual se transfiere el mensaje, utilizando la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del originador del mensaje deducida a partir del **certificado-originador**.

Adiciones o futuras versiones de esta Recomendación | Norma Internacional pueden definir otras formas de **verificación-autenticación-origen-sonda** (por ejemplo, basadas en técnicas-criptación-simétricas) que pueden ser utilizadas por los MTA a través de los cuales se transfiere el mensaje para autenticar el origen de la sonda.

8.2.1.2.1.2 Longitud-contenido

Este argumento especifica la longitud, en octetos, del **contenido** del mensaje-sujeto. Puede generarse por el originador de la sonda.

8.2.1.2.2 Resultados

El cuadro 8 enumera los resultados de la operación-abstracta remisión-sonda, y para cada resultado califica su presencia e identifica la cláusula donde se define el resultado.

Cuadro 8 – Resultados de remisión-sonda

Resultado	Presencia	Cláusula
Identificador-remisión-sonda	M	8.2.1.2.2.1
Tiempo-remisión-sonda	M	8.2.1.2.2.2
Identificador-contenido	C	8.2.1.1.1.35

8.2.1.2.2.1 Identificador-remisión-sonda

Este resultado contiene un **identificador-MTS** que identifica de forma inequívoca la remisión-sonda. Debe ser generado por el MTS.

El MTS proporciona el **identificador-remisión-sonda**, al notificar al usuario-MTS, de su capacidad o incapacidad para entregar el mensaje-sujeto, a través de la operación-abstracta de entrega-informe.

8.2.1.2.2.2 Tiempo-remisión-sonda

Este resultado indica el **tiempo** en que el MTS acepta la responsabilidad de la sonda. Debe ser generado por el MTS.

8.2.1.2.3 Errores abstractos

El cuadro 9 enumera los errores abstractos que pueden interrumpir la operación-abstracta remisión-sonda, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 9 – Errores-abstractos de remisión-sonda

Error-abstracto	Cláusula
Control-remisión-violado	8.2.2.1
Elemento-de-servicio-no-abonado	8.2.2.2
Originador-no-válido	8.2.2.4
Destinatario-indebidamente-especificado	8.2.2.5
Petición-incoherente	8.2.2.7
Error-seguridad	8.2.2.8
Función-crítica-no-soportada	8.2.2.9
Error-vinculación-distante	8.2.2.10

8.2.1.3 Cancelación-entrega-diferida

La operación-abstracta cancelación-entrega-diferida permite a un usuario-MTS abortar la entrega-diferida de un mensaje previamente remitido por dicho usuario a través de la operación-abstracta remisión-mensaje.

El usuario-MTS identifica el mensaje cuya entrega debe cancelarse mediante el **identificador-remisión-mensaje** devuelto por el MTS como resultado de una invocación previa de la operación-abstracta remisión-mensaje.

La ejecución satisfactoria de la operación-abstracta significa que el MTS ha cancelado la entrega-diferida del mensaje.

La interrupción de la operación-abstracta por un error-abstracto indica que la entrega-diferida del mensaje no puede cancelarse. La entrega-diferida de un mensaje no puede cancelarse si el mensaje ya ha progresado para su entrega y/o transferencia dentro del MTS. El MTS puede rehusar cancelar la entrega-diferida de un mensaje, si el MTS proporcionó al originador del mensaje la **prueba-de-remisión**.

8.2.1.3.1 Argumentos

El cuadro 10 enumera los argumentos de la operación-abstracta cancelación-entrega-diferida y, para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 10 – Argumentos de cancelación entrega-diferida

Argumento	Presencia	Cláusula
Argumento de remisión		
Identificador-remisión-mensaje	M	8.2.1.3.1.1

8.2.1.3.1.1 Identificador-remisión-mensaje

Este argumento contiene el **identificador-remisión-mensaje** del mensaje cuya entrega diferida debe ser cancelada. Debe ser suministrado por el usuario-MTS.

El MTS devuelve el **identificador-remisión-mensaje** (un **identificador-MTS**) como resultado de una invocación previa de la operación-abstracta remisión-mensaje (véase 8.2.1.1.2.1), cuando se presentó el mensaje para entrega-diferida.

8.2.1.3.2 Resultados

La operación-abstracta cancelación-entrega-diferida devuelve un resultado vacío como indicación de éxito.

8.2.1.3.3 Errores-abstractos

El cuadro 11 enumera los errores-abstractos que pueden interrumpir la operación-abstracta cancelación-entrega-diferida, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 11 – Errores-abstractos de cancelación-entrega-diferida

Error-abstracto	Cláusula
Cancelación-entrega-diferida-rechazada	8.2.2.3
Identificador-remisión-mensaje-no-válido	8.2.2.6
Error-vinculación-distante	8.2.2.10

8.2.1.4 Control-remisión

La operación-abstracta control-remisión permite al MTS limitar transitoriamente las operaciones-abstractas puerto-remisión que puede invocar el usuario-MTS, y los mensajes que el usuario-MTS puede remitir al MTS a través de la operación-abstracta remisión-mensaje.

El usuario-MTS debe retener hasta un tiempo posterior, en vez de abandonar, las operaciones-abstractas y los mensajes prohibidos actualmente.

La ejecución satisfactoria de la operación-abstracta significa que los controles especificados están actualmente en vigor. Estos controles sobreseen cualquier otro en vigor, y permanecen vigentes hasta que se libera la asociación o el MTS reinvoca la operación-abstracta control-remisión.

La operación-abstracta devuelve una indicación de cualquier operación-abstracta que pudiera invocar el usuario-MTS, o cualquier tipo de mensaje que el usuario-MTS pudiera remitir, a no ser por los controles que prevalecen.

8.2.1.4.1 Argumentos

El cuadro 12 enumera los argumentos de la operación-abstracta control-remisión, y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

Cuadro 12 – Argumentos de control-remisión

Argumento	Presencia	Cláusula
Argumentos de control-remisión		
Limitación	O	8.2.1.4.1.1
Operaciones-admisibles	O	8.2.1.4.1.2
Prioridad-inferior-admisible	O	8.2.1.4.1.3
Longitud-contenido-máxima-admisible	O	8.2.1.4.1.4
Contexto-seguridad-admisible	O	8.2.1.4.1.5

8.2.1.4.1.1 Limitación

Este argumento indica si los controles sobre las operaciones-abstractas de puerto-remisión deben actualizarse o suprimirse. Puede generarse por el MTS.

Este argumento puede tener uno de los siguientes valores:

actualización: los otros argumentos actualizan los controles que prevalecen;

supresión: todos los controles deben suprimirse; los otros argumentos deben ignorarse.

En ausencia de este argumento, se supondrá el valor por defecto de **actualización**.

8.2.1.4.1.2 Operaciones-admisibles

Este argumento indica las operaciones-abstractas que el usuario-MTS puede invocar sobre el MTS. Puede generarse por el MTS.

Este argumento puede tener el valor **autorizado** o **prohibido** para cada uno de los siguientes:

remisión-mensaje: el usuario-MTS puede/no puede invocar la operación-abstracta remisión-mensaje; y

remisión-sonda: el usuario-MTS puede/no puede invocar la operación-abstracta remisión-sonda.

Otras operaciones-abstractas de puerto-remisión no están sujetas a controles, y pueden invocarse en cualquier momento.

En ausencia de este argumento, las operaciones-abstractas que puede invocar el usuario-MTS permanecen sin cambios. Si no estaba en vigor ningún control previo, el usuario-MTS puede invocar tanto la operación-abstracta remisión-mensaje como la operación-abstracta remisión-sonda.

8.2.1.4.1.3 Prioridad-inferior-admisible

Este argumento contiene la **prioridad** del mensaje de prioridad más baja que el usuario-MTS debe remitir al MTS a través de la operación-abstracta remisión-mensaje. Puede generarse por el MTS.

Este argumento puede tener uno de los siguientes valores del argumento de **prioridad** de la operación-abstracta de remisión-mensaje: **normal**, **no urgente** o **urgente**.

En ausencia de este argumento, la **prioridad** del mensaje de prioridad más baja que debe remitir el usuario-MTS al MTS permanece sin modificar. Si no está ningún control previo en vigor, el usuario-MTS puede presentar mensajes de cualquier prioridad.

8.2.1.4.1.4 Longitud-contenido-máxima-admisible

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el usuario-MTS debe remitir al MTS a través de la operación-abstracta remisión-mensaje. Puede generarse por el MTS.

En ausencia de este argumento, la **longitud-contenido-máxima-admisible** de un mensaje que el usuario-MTS puede remitir al MTS permanece sin modificar. Si no está en vigor ningún control previo, la longitud del contenido no está explícitamente limitada.

8.2.1.4.1.5 Contexto-seguridad-admisible

Este argumento limita de forma transitoria la sensibilidad de las operaciones-abstractas de puerto-remisión (contexto-seguridad-remisión) que el usuario-MTS puede invocar en el MTS. Es una limitación transitoria del **contexto-seguridad** establecido al iniciarse la asociación (véase 8.1.1.1.1.3). Puede generarse por el MTS.

El **contexto-seguridad-admisible** consta de una o más **etiquetas-seguridad** del conjunto de **etiquetas-seguridad** establecidas como **contexto-seguridad** al establecerse la asociación.

En ausencia de este argumento, el **contexto-seguridad** de las operaciones-abstractas de puerto-remisión permanece sin modificar.

8.2.1.4.2 Resultados

El cuadro 13 enumera los resultados de la operación-abstracta control-remisión, y para cada resultado califica su presencia e identifica la cláusula donde se define el resultado.

Cuadro 13 – Resultados de control-remisión

Resultado	Presencia	Cláusula
Resultados "esperando"		
Operaciones-esperando	O	8.2.1.4.2.1
Mensajes-esperando	O	8.2.1.4.2.2
Tipos-información-codificados-esperando	O	8.2.1.4.2.3
Tipos-contenido-esperando	O	8.2.1.4.2.4

8.2.1.4.2.1 Operaciones-esperando

Este resultado indica las operaciones-abstractas que retiene el usuario-MTS y que el usuario-MTS invocaría en el MTS si no fuera por los controles que prevalecen. Puede generarse por el usuario-MTS.

Este resultado puede tener el valor **reteniendo** o **no-reteniendo** para cada uno de los siguientes:

remisión-mensaje: el usuario-MTS está/no está reteniendo mensajes, e invocaría la operación-abstracta remisión-mensaje en el MTS si no fuera por los controles que prevalecen; y

remisión-sonda: el usuario-MTS está/no está reteniendo sondas, e invocaría la operación-abstracta remisión-sonda en el MTS si no fuera por los controles que prevalecen.

En ausencia de este resultado, puede suponerse que el usuario-MTS no está reteniendo ningún mensaje ni ninguna sonda para su remisión al MTS debido a los controles que prevalecen.

8.2.1.4.2.2 Mensajes-esperando

Este resultado indica la categoría de los mensajes que el usuario-MTS está reteniendo para su remisión al MTS, y que remitiría a través de la operación-abstracta remisión-mensaje, si no fuera por los controles que prevalecen. Puede generarse por el usuario MTS.

Este resultado puede adoptar uno de los siguientes valores:

contenido-largo: el usuario-MTS ha retenido mensajes para su remisión al MTS que exceden el control de **longitud-contenido-máxima-admisible** actualmente en vigor;

baja prioridad: el usuario-MTS ha retenido mensajes para su remisión al MTS de una **prioridad** inferior al control de **prioridad-inferior-admisible** actualmente en vigor;

otras-etiquetas-seguridad: el usuario-MTS ha retenido mensajes para su remisión al MTS, que transportan **etiquetas-seguridad-mensaje** diferentes de las permitidas por el contexto-seguridad actual.

En ausencia de este resultado, puede suponerse que el usuario-MTS no está reteniendo ningún mensaje ni ninguna sonda para su remisión al MTS debido a los controles de **longitud-contenido-máxima-admisible**, **prioridad-inferior-admisible** o **contexto-seguridad-admisible** actualmente en vigor.

8.2.1.4.2.3 Tipos-información-codificada-esperando

Este resultado indica los **tipos-información-codificada** del **contenido** de cualquier mensaje retenido por el usuario-MTS para su remisión al MTS debido a los controles que prevalecen. Puede generarse por el usuario-MTS.

En ausencia de este resultado, los **tipos-información-codificada** de cualquier mensaje retenido por el usuario-MTS para su remisión al MTS están **sin-especificar**.

8.2.1.4.2.4 Tipos-contenido-esperando

Este resultado indica los **tipos-contenido** de cualquier mensaje retenido por el usuario-MTS para su remisión al MTS debido a los controles que prevalecen. Puede generarse por el usuario-MTS.

En ausencia de este resultado, los **tipos-contenido** de cualquier mensaje retenido por el usuario-MTS para su remisión al MTS están **sin-especificar**.

8.2.1.4.3 Errores-abstractos

El cuadro 14 enumera los errores-abstractos que pueden interrumpir la operación-abstracta control-remisión, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 14 – Errores-abstractos de control-remisión

Error-abstracto	Cláusula
Error-seguridad	8.2.2.8
Error-vinculación-distante	8.2.2.10

8.2.2 Errores-abstractos

En esta cláusula se definen los siguientes errores-abstractos de puerto-remisión:

a) control-remisión-violado;
b) elemento-de-servicio-no-abonado;
c) cancelación-entrega-diferida-rechazada;
d) originador-no-válido;
e) destinatario-indebidamente-especificado;
f) identificador-remisión-mensaje-no-válido;
g) petición-incoherente;
h) error-seguridad;
i) función-crítica-no-soportada;
j) error-vinculación-distante.

8.2.2.1 Control-remisión-violado

El error-abstracto de control-remisión-violado informa de la violación, por el usuario-MTS, de un control sobre los servicios de puerto-remisión impuestos por el MTS a través del servicio de control-remisión.

El error-abstracto de control-remisión-violado no tiene parámetros.

8.2.2.2 Elemento-de-servicio-no-abonado

El servicio de elemento-de-servicio-no-abonado informa que la operación-abstracta solicitada no puede ser proporcionada por el MTS porque el usuario-MTS no está abonado a uno de los elementos-de-servicio que la petición requiere.

El error-abstracto de elemento-de-servicio-no-abonado no tiene parámetros.

8.2.2.3 Cancelación-entrega-diferida-rechazada

El error-abstracto de cancelación-entrega-diferida-rechazada informa que el MTS no puede cancelar la entrega-diferida de un mensaje, porque el mensaje ya ha progresado para su transferencia y/o entrega o porque el MTS ha proporcionado al originador una **prueba-de-remisión**.

El error-abstracto de cancelación-entrega-diferida-rechazada no tiene parámetros.

8.2.2.4 Originador-no-válido

El error-abstracto originador-no-válido informa que no puede remitirse el mensaje o la sonda porque el originador está incorrectamente identificado.

El error-abstracto originador-no-válido no tiene parámetros.

8.2.2.5 Destinatario-indebidamente-especificado

El error-abstracto destinatario-indebidamente-especificado informa que no puede remitirse el mensaje o la sonda porque el destinatario o destinatarios están indebidamente especificados.

El error-abstracto destinatario-indebidamente-especificado tiene el siguiente parámetro generado por el MTS:

destinatarios-indebidamente-especificados: **nombres-destinatarios** indebidamente especificados.

8.2.2.6 Identificador-remisión-mensaje-no-válido

El error-abstracto identificador-remisión-mensaje-no-válido informa que no puede cancelarse una entrega-diferida de un mensaje porque el **identificador-remisión-mensaje** es inválido, o identifica un mensaje remitido por otro usuario-MTS.

El error-abstracto identificador-remisión-mensaje-no-válido no tiene parámetros.

8.2.2.7 Petición-incoherente

El error-abstracto petición-incoherente informa que la operación-abstracta solicitada no puede ser proporcionada por el MTS porque el usuario-MTS ha realizado una petición-incoherente.

El error-abstracto petición-incoherente no tiene parámetros.

8.2.2.8 Error-seguridad

El error-abstracto error-seguridad informa que la operación-abstracta solicitada no puede ser proporcionada por el MTS o por el usuario-MTS porque se violaría la política-seguridad en vigor.

El error-abstracto error-seguridad tiene el siguiente parámetro, generado por el MTS:

problema-seguridad: identificador de la causa de violación de la política-seguridad.

La utilización de códigos de error-seguridad depende de la política-seguridad y de la implementación de funciones de seguridad. En particular, estos códigos de error-seguridad pueden ser utilizados para una función de supervisión de seguridad penetrante, que supervisa el funcionamiento de rutina de un UA, una MS, o un MTA y asegura que la política-seguridad no es violada por el funcionamiento normal del componente del MHS.

El parámetro **problema-seguridad** puede tener uno de los siguientes valores para las operaciones-abstractas remisión-mensaje o remisión-sonda.

a) Los siguientes valores indican una violación de seguridad por el usuario:

   violación-política-seguridad: la política-seguridad es violada;

   rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados;

   nombre-DL-no autorizado: el nombre-OR del usuario-MTS destinatario identifica una DL cuya utilización no está autorizada por motivos de seguridad;

   NOTA – Si el MTA no puede determinar que el nombre-OR identifica una DL, se puede utilizar en su lugar el valor nombre-destinatario-no autorizado.

   nombre-originador-no autorizado: el nombre-OR del usuario-MTS originador no está autorizado por motivos de seguridad;

   nombre-destinatario-no autorizado: el nombre-OR del usuario-MTS destinatario no está autorizado por motivos de seguridad;

   etiqueta-seguridad-desconocida: el identificador de política de seguridad en la etiqueta de seguridad de mensaje no es reconocido por el MTA. Esta política no es soportada por el MTA.

b) Los siguientes valores indican un error dentro del sistema de seguridad:

   etiqueta-seguridad-no-válida: el identificador de política de seguridad en la etiqueta de seguridad del mensaje identifica una política que es conocida por el MTA, pero que no es aceptable para ese sistema;

   ausencia-parámetro-obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

   fallo-seguridad-operación: la operación remisión fracasó por motivos de seguridad;

   fallo-contexto-seguridad: la etiqueta de seguridad del mensaje es incompatible con la contexto seguridad en vigor.

El parámetro problema-seguridad puede tener uno de los siguientes valores para la operación-abstracta control-remisión:

a) Los siguientes valores indican una violación de seguridad por el usuario:

   violación-política-seguridad: la política-seguridad es violada;

   rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados.

b) Los siguientes valores indican un error dentro del sistema de seguridad:

   cambio-incompatible-con-contexto-seguridad-original: el contexto-seguridad-admisible propuesto no es un subconjunto del contexto-seguridad original;

ausencia-parámetro-obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

fallo-seguridad-operación: la operación control-remisión fracasó por motivos de seguridad.

8.2.2.9 Función-crítica-no-soportada

El error-abstracto función-crítica-no-soportada informa que un argumento de la operación-abstracta ha sido marcado como **crítico-para-remisión** (véase 9.2) pero que no está soportado por el MTS.

El error-abstracto función-crítica-no-soportado no tiene parámetros.

8.2.2.10 Error-vinculación-distante

El error-abstracto error-vinculación-distante informa que la operación-abstracta solicitada no puede ser proporcionada por la MS debido a que ésta no puede vincularse al MTS, o porque no existe asociación entre la MS y la UA. Este error-abstracto sólo se produce en casos de remisión indirecta al MTS a través de una MS o al invocar el MTS una operación-abstracta de control-remisión a través de una MS.

El error-abstracto error-vinculación-distante no tiene parámetros.

8.3 Puerto de entrega

En esta cláusula se definen las operaciones-abstractas y los errores-abstractos que ocurren en un puerto-entrega.

8.3.1 Operaciones-abstractas

En esta cláusula se definen las siguientes operaciones-abstractas de puerto-entrega:

a) entrega-mensaje;

b) entrega-informe;

c) control-entrega.

8.3.1.1 Entrega-mensaje

La operación-abstracta entrega-mensaje permite que el MTS entregue un mensaje a un usuario-MTS.

El usuario-MTS no debe rehusar la entrega de un mensaje a menos que la entrega viole las limitaciones de control-entrega entonces en vigor.

8.3.1.1.1 Argumentos

El cuadro 15 enumera los argumentos de la operación-abstracta entrega-mensaje y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 15 – Argumentos de entrega-mensaje

Argumento	Presencia	Cláusula
Argumentos de entrega		
Identificador-entrega-mensaje	M	8.3.1.1.1.1
Tiempo-entrega-mensaje	M	8.3.1.1.1.2
Tiempo-presentación-mensaje	M	8.2.1.1.2.2
Información-rastreo	O	12.2.1.1.1.3
Información-rastreo-interna	O	12.2.1.1.1.4
Argumento del originador		
Nombre-originador	M	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-este-destinatario	M	8.3.1.1.1.3
Nombre-destinatario-deseado-originalmente	C	8.3.1.1.1.4
Historia-redireccionamiento	C	8.3.1.1.1.5
Otros-nombres-destinatarios	C	8.3.1.1.1.6
Historia-ampliación-DL	C	8.3.1.1.1.7
Destinatarios-exentos-DL	O	8.2.1.1.1.40

Cuadro 15 – Argumentos de entrega-mensaje

Argumento	Presencia	Cláusula
Argumento de prioridad		
Prioridad	C	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Tipos-información-codificada-convertidos	C	8.3.1.1.1.8
Argumento de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	C*	8.2.1.1.1.15
Petición-dirección-envío-físico	C*	8.2.1.1.1.16
Modos-entrega-física	C*	8.2.1.1.1.17
Tipo-correo-certificado	C*	8.2.1.1.1.18
Número-destinatario-para-aviso	C*	8.2.1.1.1.19
Atributos-reproducción-física	C*	8.2.1.1.1.20
Dirección-devolución-originador	C*	8.2.1.1.1.21
Petición-informe-entrega-física	C*	8.2.1.1.1.24
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Testigo-mensaje	C	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	C	8.2.1.1.1.27
Verificación-integridad-contenido	C	8.2.1.1.1.28
Verificación-autenticación-origen-mensaje	C	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Petición-prueba-de-entrega	C	8.2.1.1.1.32
Múltiples-certificados-originador	O	8.2.1.1.1.41
Certificados-destinatario	O	8.2.1.1.1.42
Selectores-certificado	O	8.2.1.1.1.43
Contraorden-selectores-certificado	O	8.2.1.1.1.44
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	M	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Contenido	M	8.2.1.1.1.37

NOTA – C* indica que estos argumentos están ausentes normalmente para destinatarios-no-PD, pero pueden aparecer en casos especiales (por ejemplo, redireccionamiento).

8.3.1.1.1.1 Identificador-entrega-mensaje

Este argumento contiene un **identificador-MTS** que distingue el mensaje de todos los demás mensajes en el puerto de entrega. Debe ser generado por el MTS y debe tener el mismo valor que el **identificador-remisión-mensaje** suministrado por el originador del mensaje al remitirse el mensaje.

8.3.1.1.1.2 Tiempo-entrega-mensaje

Este argumento contiene el **tiempo** en que se produce la entrega y en que el MTS renuncia a su responsabilidad sobre el mensaje. Debe ser generado por el MTS.

En el caso de entrega física, este argumento indica el **tiempo** en que la PDAU ha tomado la responsabilidad de imprimir y entregar posteriormente el mensaje.

El valor de este argumento debe ser el mismo que el valor del **tiempo-entrega-mensaje** indicado al originador del mensaje (véase 8.3.1.2.1.9) en el informe-entrega.

8.3.1.1.1.3 Nombre-este-destinatario

Este argumento contiene el **nombre-OR** del destinatario al que se entrega el mensaje. Debe ser generado por el MTS.

El valor de este argumento debe ser el mismo que el valor del argumento **nombre-destinatario** (es decir, el que hizo que el mensaje se entregara a este destinatario) que estaba presente en el mensaje inmediatamente anterior a la entrega.

El **nombre-este-destinatario** contiene el **nombre-OR** del destinatario individual, es decir no debe contener el **nombre-OR** de una DL.

El **nombre-OR** del destinatario-deseado (si es diferente, y el mensaje ha sido redirigido o ampliado-DL) está contenido en el argumento **nombre destinatario deseado-originalmente**.

8.3.1.1.1.4 Nombre-destinatario-deseado-originalmente

Este argumento contiene el **nombre-OR** del destinatario especificado por el originador en el momento de la remisión, tal como lo modifica el procedimiento remisión-mensaje (véase 14.6.1). Deberá ser generado por el MTS (por el MTA que realice la entrega-mensaje o la generación-informe) si el **nombre-OR** del destinatario especificado-originalmente ha sido sustituido como consecuencia de una ampliación o de un redireccionamiento-DL.

8.3.1.1.1.5 Historia-redireccionamiento

Este argumento documenta los eventos de redireccionamiento que han ocurrido durante el paso del mensaje por el MTS. Si ha habido direccionamiento deberá ser generado por el MTS. Para cada evento de redireccionamiento, el argumento contiene el **nombre-OR** del destinatario deseado previo a la redirección, el **tiempo** en que ocurre la redirección, y los motivos de la misma.

El **motivo-redireccionamiento** tiene uno de los valores siguientes:

destinatario-alternativo-asignado-destinatario: el destinatario-deseado del mensaje solicitó que se redirigiera el mensaje a un **destinatario-alternativo-asignado-destinatario**; el originador del mensaje no prohibió una reasignación-destinatario (véase 8.2.1.1.1.4); el MTS redirige el mensaje al **destinatario-alternativo-asignado-destinatario**;

destinatario-alternativo-solicitado-originador: el mensaje no pudo entregarse al destinatario-deseado o al **destinatario-alternativo-asignado-destinatario** (si está inscrito); el argumento **destinatario-alternativo-solicitado-originador** identificó un destinatario-alternativo solicitado por el originador del mensaje; el MTS redirigió el mensaje al **destinatario-alternativo-solicitado-originador**;

destinatario-alternativo-asignado-destinatario-MD: el argumento **nombre-destinatario** no identificó un usuario-MTS destinatario; el argumento **destinatario-alternativo-autorizado** generado por el originador del mensaje autorizó la entrega a un destinatario-alternativo; el MTS redirigió el mensaje a un destinatario-alternativo asignado por el destinatario-MD para recibir dichos mensajes;

sustitución-directorio: la **dirección-OR** del destinatario-deseado no identificó un usuario-MTS destinatario; el **nombre-OR** de ese destinatario-deseado también contenía un **nombre-directorio** que se utilizaba para obtener del directorio una **dirección-OR** diferente para ese destinatario-deseado; el MTS redirigió el mensaje hacia la **dirección-OR** de sustitución para ese destinatario-deseado;

alias: el argumento **nombre-destinatario** no contenía una dirección preferida del usuario-MTS especificado; el MTS redirigió el mensaje a una dirección preferida de dicho usuario-MTS.

NOTA 1 – La diferencia entre dirección preferida y no preferida se establece mediante configuración local.

Algunos sistemas conformes a las versiones anteriores de esta especificación podrían no soportar los valores **alias** y/o **consulta de directorio**. Estos valores no serán transmitidos a sistemas que no los soporten, salvo por acuerdo bilateral.

NOTA 2 – Para lograr esto, se recomienda que las implementaciones MTA que se prevé utilizar en la frontera entre sistemas antiguos y nuevos (por ejemplo, en fronteras de dominio) se proporcionen con la facilidad configurable para modificar la **historia de redireccionamiento**. Esta facilidad podría reemplazar al valor **alias** por **destinatario-alternativo-asignado-por-destinatario** y/o reemplazar el valor **consulta-de-directorio** por **originador-alternativo-asignado-por-destinatario** como se requiere cuando se transfiere a MTA adyacentes específicos.

8.3.1.1.1.6 Otros-nombres-destinatarios

Si el originador del mensaje solicitó la revelación de los otros destinatarios, este argumento contiene los **nombres-OR** de los destinatarios especificados-originalmente que no sean el destinatario (si lo hay) identificado por el argumento **nombre-destinatario-deseado-originalmente**, si está presente, o por el argumento **nombre-este-destinatario**. Este argumento sólo es generado por el MTS si la operación-abstracta de remisión-mensaje tiene el argumento **revelación-de-otros-destinatarios** puesto a **revelación-de-otros-destinatarios-solicitada** y si hay por lo menos uno de esos destinatarios.

Cada **nombre-otro-destinatario** contiene el **nombre-OR** de un destinatario individual o de una DL.

NOTA – Si se ha efectuado la ampliación de DL no se revelan los **nombres-OR** de los miembros de DL. El **nombre-OR** de DL sólo se revela si es el de un destinatario especificado-originalmente.

8.3.1.1.1.7 Historia-ampliación-DL

Este argumento contiene la secuencia de **nombres-OR** de cualesquiera DL que hayan sido ampliadas para añadir destinatarios a la copia del mensaje entregado al destinatario, y el tiempo de cada ampliación. Debe ser generado por el MTS si se produjo cualquier ampliación-DL.

8.3.1.1.1.8 Tipos-información-codificada-convertida

Este argumento identifica los **tipos-información-codificada** del **contenido** del mensaje después de la conversión, si ésta tuvo lugar. Puede generarse por el MTS.

8.3.1.1.2 Resultados

El cuadro 16 enumera los resultados de la operación-abstracta entrega-mensaje, y para cada resultado, califica su presencia e identifica la cláusula donde se define el resultado.

Cuadro 16 – Resultado de entrega-mensaje

Resultado	Presencia	Cláusula
Resultados de prueba de entrega		
Certificado-destinatario	O	8.3.1.1.2.1
Prueba-de-entrega	C	8.3.1.1.2.2

8.3.1.1.2.1 Certificado-destinatario

Este argumento contiene el **certificado** del destinatario del mensaje. Debe ser generado por una fuente de confianza (por ejemplo, una autoridad-certificación), y puede ser suministrado por el destinatario del mensaje, si el originador del mensaje solicitó una **prueba-de-entrega** (véase 8.2.1.1.1.32) y se utiliza un algoritmo-criptación-asimétrico para calcular la **prueba-de-entrega**.

Puede utilizarse el **certificado-destinatario** para transportar una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del destinatario del mensaje.

El originador del mensaje puede utilizar la clave-criptación-pública-asimétrica del destinatario para validar la **prueba-de-entrega**.

8.3.1.1.2.2 Prueba-de-entrega

Este argumento proporciona al originador del mensaje una prueba de que se ha entregado el mensaje al destinatario (para proporcionar el elemento-de-servicio prueba de entrega definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1) en función del algoritmo-criptación utilizado y de la política-seguridad en vigor. Este argumento puede proporcionar igualmente el elemento-de-servicio no-repudio de entrega (definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Debe ser generado por el destinatario del mensaje, si el originador del mensaje solicitó una **prueba-de-entrega** (véase 8.2.1.1.1.32).

La **prueba-de-entrega** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-prueba-de-entrega** (un **identificador-algoritmo**).

La **prueba-de-entrega** contiene el **identificador-algoritmo-prueba-de-entrega** y una función criptada (por ejemplo, una versión comprimida o troceada) del **identificador-algoritmo-prueba-de-entrega**, el **tiempo-entrega** y el **nombre-este-destinatario**, el **nombre-destinatario-deseado-originalmente**, el **contenido** del mensaje, el **identificador-contenido**, y la **etiqueta-seguridad-mensaje** del mensaje entregado. Se incluyen componentes facultativos en la **prueba-de-entrega** si están presentes en el mensaje entregado. Obsérvese que la **prueba-de-entrega** se calcula utilizando el **contenido** del mensaje entregado (es decir, cifrado o sin criptar).

La recepción de este argumento proporciona al originador del mensaje una prueba de entrega del mensaje al destinatario. La no-recepción de este argumento no proporciona ni la prueba de entrega ni la prueba de no entrega (a menos que se utilice una ruta segura y una funcionalidad de confianza).

Si se utiliza un algoritmo-criptación-asimétrico, el destinatario del mensaje puede calcular la **prueba-de-entrega** mediante la clave-criptación-secreta-asimétrica del destinatario. El originador del mensaje puede validar la **prueba-de-entrega** utilizando la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) deducida del **certificado-destinatario**. Una **prueba-de-entrega** asimétrica puede igualmente proporcionar un no repudio de entrega sujeto a la disponibilidad de una infraestructura de claves públicas adecuada.

Si se utiliza un algoritmo-simétrico, el destinatario utiliza una clave-criptación-simétrica para calcular la **prueba-de-entrega**, y el originador para validar la **prueba-de-entrega**. Si se utiliza un algoritmo-criptación-simétrico, entonces la **prueba-de-entrega** puede proporcionar únicamente un no repudio de entrega si la política-seguridad en vigor proporciona la intervención de una tercera parte que actúe como notario. Los procedimientos mediante los cuales se distribuye la clave-criptación-simétrica no se definen en esta Definición de servicio.

8.3.1.1.3 Errores-abstractos

El cuadro 17 enumera los errores-abstractos que pueden interrumpir la operación-abstracta entrega-mensaje, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 17 – Errores-abstractos de entrega-mensaje

Error-abstracto	Cláusula
Control-entrega-violado	8.3.2.1
Error-seguridad	8.3.2.3
Función-crítica-no-soportada	8.3.2.4

8.3.1.2 Entrega-informe

La operación-abstracta **entrega-informe** permite que el MTS proporcione el acuse de recibo al usuario-MTS de uno o más resultados de una invocación previa de las operaciones-abstractas remisión-mensaje o remisión-sonda.

Para la operación-abstracta remisión-mensaje, la operación-abstracta entrega-informe indica la entrega o no-entrega del mensaje remitido a uno o más destinatarios.

Para la operación-abstracta remisión-sonda, la operación-abstracta entrega-informe indica si podría entregarse un mensaje o producirse una ampliación-DL, si se remitiera el mensaje.

Una invocación sencilla de la operación-abstracta remisión-mensaje o remisión-sonda puede provocar varias apariciones de la operación abstracta entrega-informe, cubriendo cada una de ellas uno o más destinatarios deseados. Una aparición sencilla de la operación-abstracta entrega-informe puede informar tanto sobre la entrega como la no-entrega a diferentes destinatarios.

Una invocación de la operación-abstracta remisión-mensaje o remisión-sonda por un usuario-MTS puede provocar apariciones de la operación-abstracta entrega-informe a otro usuario-MTS, es decir, informes entregados al propietario de una DL.

El usuario-MTS no debe rehusar aceptar la entrega de un informe a menos que la entrega del informe viole las restricciones del control-entrega entonces en vigor.

8.3.1.2.1 Argumentos

El cuadro 18 enumera los argumentos de la operación-abstracta entrega-informe y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 18 – Argumentos de entrega-informe

Argumento	Presencia	Cláusula
Argumento de remisión de sujeto		
Identificador-remisión-sujeto	M	8.3.1.2.1.1
Argumentos de destinatario		
Nombre-destinatario-real	M	8.3.1.2.1.2
Nombre-destinatario-deseado-originalmente	C	8.3.1.1.1.4
Historia-redireccionamiento	C	8.3.1.1.1.5
Originador-e-historia-ampliación-DL	C	8.3.1.2.1.3
Nombre-DL-informador	C	8.3.1.2.1.4
Argumentos del sobre del informe		
Historia-redireccionamiento	C	8.3.1.2.1.5
Información-rastreo	O	12.2.1.1.1.3
Información-rastreo-interno	O	12.2.1.1.1.4
Nombre-MTA-informador	C	8.3.1.2.1.17
Argumento de conversión		
Tipos-información-codificada-convertidos	C	8.3.1.2.1.6
Argumentos de información suplementaria		
Información-suplementaria	C	8.3.1.2.1.7
Dirección-envío-físico	C	8.3.1.2.1.8
Argumentos de entrega		
Tiempo-entrega-mensaje	C	8.3.1.2.1.9
Tipo-de-usuario-MTS	C	8.3.1.2.1.10
Argumentos de no-entrega		
Código-motivo-no-entrega	C	8.3.1.2.1.11
Código-diagnóstico-no-entrega	C	8.3.1.2.1.12
Argumentos de seguridad		
Certificado-destinatario	C	8.3.1.1.2.1
Prueba-de-entrega	C	8.3.1.1.2.2
Certificado-MTA-informador	C	8.3.1.2.1.13
Comprobación-autenticación-origen-informe	C	8.3.1.2.1.14
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	C	8.3.1.2.1.15
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido-devuelto	C	8.3.1.2.1.16

8.3.1.2.1.1 Identificador-remisión-sujeto

Este argumento contiene el **identificador-remisión-mensaje** o el **identificador-remisión-sonda** del sujeto del informe. Debe ser suministrado por el MTS.

8.3.1.2.1.2 Nombre-destinatario-real

Este argumento contiene el **nombre-OR** de un destinatario del mensaje. Debe ser generado por el originador del mensaje, o por el MTS si el mensaje ha sido redirigido o ampliado-DL. Debe especificarse un valor diferente de este argumento para cada destinatario del sujeto al que se refiere el informe.

En el caso de un informe de entrega, el **nombre-destinatario-real** es el nombre del destinatario real del mensaje y tiene el mismo valor que el argumento de **nombre-este-destinatario** del mensaje entregado. En el caso de un informe-no-entrega, el **nombre-destinatario-real** es el **nombre-OR** del destinatario al que iba dirigido el mensaje cuando se encontró la razón para no-entrega.

El **nombre-destinatario-real** puede ser un **nombre-destinatario** especificado-originalmente, o el **nombre-OR** de un destinatario sustitutivo al que se ha redirigido el mensaje, o el nombre de un miembro-DL si el mensaje ha sido ampliado-DL. Si el mensaje ha sido redirigido o ampliado-DL, el **nombre-OR** del destinatario-especificado originalmente está contenido en el argumento de **nombre-destinatario-deseado-originalmente**.

El **nombre-destinatario-real** contiene el **nombre-OR** de un destinatario individual o de una DL.

8.3.1.2.1.3 Originador-e-historia-ampliación-DL

Este argumento contiene una secuencia de **nombres-OR** e instantes asociados que documentan la historia del origen del mensaje-sujeto. El primer **nombre-OR** de la secuencia es el **nombre-OR** del originador del sujeto, y el resto de la secuencia es una secuencia de **nombres-OR** de las DL que han sido ampliadas al dirigir el sujeto hacia el destinatario (la última es la misma que la **historia-ampliación-DL**). Debe ser generado por el MTA-originador del informe si se ha producido cualquier ampliación-DL en el sujeto.

El **originador-e-historia-ampliación-DL** contiene el **nombre-OR** del originador del sujeto y de cada una de las DL, y el instante en que se ha producido el suceso asociado.

8.3.1.2.1.4 Nombre-DL-informador

Este argumento contiene el **nombre-OR** de la DL que envió el informe al propietario de la DL. Debe ser generado por un punto-ampliación-DL (un MTA) al enviar un informe al propietario de la DL, en línea con la política-informadora de la DL.

El **nombre-DL-informador** contiene el **nombre-OR** de la DL que envía el informe.

8.3.1.2.1.5 Historia-redireccionamiento

Este argumento documenta los eventos de redireccionamiento que han ocurrido durante el paso del informe por el MTS. Deberá ser generado por el MTS si el informe ha sido redirigido. Para cada evento de redireccionamiento que ocurra, contiene el **nombre-destino-informe** previo a la redirección, el **tiempo** en que ésta ocurre y los motivos de la misma. Los valores de **motivo-redireccionamiento** se definen en 8.3.1.1.1.5, excepto en que el **destinatario-alternativo-solicitado-originador** no se aplica a los informes.

NOTA – En el cuadro 18 la historia-redireccionamiento del argumento de destinatario contiene la historia-redireccionamiento del sujeto del informe, mientras que la historia-redireccionamiento de los argumentos del sobre del informe contiene la historia-redireccionamiento del propio informe.

8.3.1.2.1.6 Tipos-información-codificada-convertidos

Este argumento identifica los **tipos-información-codificada** del **contenido** del mensaje-sujeto después de la conversión, si ésta tuvo lugar. Para un informe sobre un mensaje, este argumento indica los **tipos-información-codificada** reales del **contenido** del mensaje convertido. Para un informe sobre una sonda, este argumento indica los **tipos-información-codificada** que el **contenido** del mensaje-sujeto habría contenido después de la conversión, si se hubiera remitido el mensaje-sujeto. Puede generarse por el MTS. Puede especificarse un valor diferente de este parámetro para cada destinatario del sujeto al que se refiere el informe.

8.3.1.2.1.7 Información-suplementaria

Este argumento puede contener información suministrada por el originador del informe, como una cadena imprimible. Puede generarse por el MTA-originador del informe o una unidad-acceso asociada. Puede especificarse un valor diferente para cada destinatario deseado del sujeto al que se refiere el informe.

Una unidad-acceso-teletex o una facilidad de conversión teletex-télex pueden utilizar la **información-suplementaria**. Ésta puede contener un acuse de recibo recibido, una duración de transmisión télex, o una nota y mensaje registrado recibido como una cadena imprimible.

Otras unidades-acceso o el MTA-originador del propio informe pueden utilizar igualmente la **información-suplementaria**, para transportar información imprimible al originador del mensaje.

8.3.1.2.1.8 Dirección-envío-físico

Este argumento contiene la nueva **dirección-OR-postal** del destinatario-físico del mensaje. Puede generarse por la PDAU asociada al MTA-originador del informe, si el originador del mensaje solicitó la dirección-envío-físico del destinatario (véase 8.2.1.1.1.16). Puede especificarse un valor diferente de este argumento para cada destinatario deseado del mensaje-sujeto a que se refiere el informe.

8.3.1.2.1.9 Tiempo-entrega-mensaje

Este argumento contiene el **tiempo** en que se entregó (o se podría haber entregado) el mensaje-sujeto al usuario-MTS destinatario. Debe ser generado por el MTS si el mensaje fue (o se podría haber) entregado satisfactoriamente. Puede especificarse un valor diferente de este argumento para cada destinatario deseado del sujeto a que se refiere el informe.

En el caso de una entrega física, este argumento indica el **tiempo** en que la PDAU ha asumido la responsabilidad de imprimir y posteriormente entregar el mensaje.

Si se entregó el mensaje-sujeto, el valor de este argumento debe ser el mismo que el valor del argumento del **tiempo-entrega-mensaje** del mensaje entregado (véase 8.3.1.1.1.2).

8.3.1.2.1.10 Tipo-de-usuario-MTS

Este argumento indica el tipo del usuario-MTS destinatario a quien se entregó (o se podría haber entregado) el mensaje. Debe ser generado por el MTS si el mensaje se entregó (o se podría haber entregado) satisfactoriamente. Puede especificarse un valor diferente para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tener uno de los siguientes valores:

público: UA que pertenece a una Administración;

privado: UA que pertenece a alguien distinto de una Administración;

ms: memoria de mensaje (message-store);

DL: lista-distribución (distribution-list);

PDAU: unidad-acceso-entrega-física (physical-delivery-access-unit);

destinatario-físico: destinatario físico de un PDS;

otra: unidad-acceso de otra categoría.

8.3.1.2.1.11 Código-motivo-no-entrega

Este argumento contiene un código que indica el motivo de la entrega fallida de un mensaje-sujeto (o, que en el caso de una sonda, habría fallado). Debe ser generado por el MTS, si el mensaje se entregó (o se hubiera entregado) sin éxito. Puede especificarse un valor diferente de este argumento para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tener uno de los siguientes valores:

fallo-transferencia: indica que, mientras que el MTS intentaba entregar o sondear la entrega del mensaje-sujeto, algún fallo de comunicación le impidió hacerlo;

incapaz-de-transferir: indica que, debido a algún problema con el propio sujeto, el MTS no pudo entregar o sondear la entrega del mensaje-sujeto;

conversión-no-realizada: indica que una conversión necesaria para la entrega del mensaje-sujeto no pudo (o no podría) realizarse;

reproducción-física-no-realizada: indica que el PDAU no pudo reproducir físicamente el mensaje-sujeto;

entrega-física-no-realizada: indica que el PDS no pudo entregar físicamente el mensaje-sujeto;

entrega-limitada: indica que el destinatario está abonado al elemento-de-servicio de entrega-limitada (definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1) que impidió (o impediría) la entrega del mensaje-sujeto;

operación-directorio-infructuosa: indica que el resultado de una operación de directorio solicitada no tuvo éxito;

entrega-aplazada-no-realizada: indica que no se ha podido realizar una petición de entrega aplazada del mensaje-sujeto.

fallo-transferencia-por-motivos-seguridad: indica que aunque el MTS trató de entregar o sondear la entrega del mensaje-sujeto, no pudo hacerlo por un fallo de seguridad.

Pueden especificarse otros **códigos-motivo-no-entrega** en adiciones o futuras versiones de esta Recomendación | Norma Internacional.

En el argumento **código-diagnóstico-no-entrega** está contenida otra información adicional sobre la naturaleza del problema que impide la entrega.

8.3.1.2.1.12 Código-diagnóstico-no-entrega

Este argumento contiene un código que indica la naturaleza del problema que hizo fracasar la entrega o la sonda de entrega del mensaje-sujeto. Puede generarse por el MTS si se entregó (o se hubiera entregado) el mensaje sin éxito. Puede especificarse un valor diferente de este argumento para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tomar uno de los siguientes valores:

nombre-OR-no-reconocido: el argumento del **nombre-destinatario** del sujeto no contiene un **nombre-OR** reconocido por el MTS;

nombre-OR-ambiguo: el argumento del **nombre-destinatario** del sujeto identifica más de un posible destinatario (es decir, es ambiguo);

congestión-MTS: el sujeto no pudo progresar, debido a una congestión en el MTS;

bucle-detectado: se detectó que el sujeto estaba haciendo un bucle dentro del MTS;

destinatario-indisponible: el usuario-MTS destinatario estaba (o estaría) indisponible para recibir la entrega del mensaje-sujeto;

tiempo-máximo-expirado: el tiempo máximo para entregar el mensaje-sujeto, o para realizar la sonda-sujeto, ha expirado;

tipos-información-codificada-no-soportados: el usuario-MTS destinatario no soporta los tipos-información-codificada del mensaje-sujeto;

contenido-demasiado-largo: la **longitud-contenido** del mensaje-sujeto es demasiado larga para que el usuario-MTS acepte la entrega (excede la longitud-contenido-máxima-entregable);

conversión-no-práctica: la conversión requerida para entregar el mensaje-sujeto no resulta práctica;

conversión-implícita-prohibida: la conversión requerida para entregar el mensaje-sujeto ha sido prohibida por el originador del sujeto (véase 8.2.1.1.1.9);

conversión-implícita-no-abonada: el destinatario no se ha abonado a la conversión requerida para entregar el mensaje-sujeto;

argumentos-no-válidos: se ha detectado que uno o más argumentos del sujeto son no válidos;

error-sintaxis-contenido: se ha detectado un error de sintaxis en el contenido del mensaje-sujeto (no aplicable a las sondas-sujeto);

violación-limitación-tamaño: indica que el valor de uno o más parámetros del sujeto violaron las limitaciones de tamaño definidas en esta Definición de servicio, y que el MTS no estaba preparado para manejar el valor o valores especificados;

violación-protocolo: indica que faltan uno o más argumentos obligatorios en el sujeto;

tipo-contenido-no-soportado: indica que era (o sería) necesario el procesamiento de un **tipo-contenido** no soportado por el MTS para entregar el mensaje-sujeto;

demasiados-destinatarios: indica que el MTS fue (o sería) incapaz de entregar el mensaje-sujeto debido al número de destinatarios especificados del mensaje-sujeto (véase 8.2.1.1.1.2);

no-acuerdo-bilateral: indica que la entrega del mensaje-sujeto exigía (o exigiría) un acuerdo bilateral inexistente;

función-crítica-no-soportada: indica que una función crítica requerida para la transferencia o entrega del mensaje-sujeto no estaba soportada por el MTA-originador del informe;

conversión-con-pérdida-prohibida: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información; la conversión con pérdida de información fue prohibida por el originador del sujeto (véase 8.2.1.1.1.10);

línea-demasiado-larga: la conversión requerida para la entrega del mensaje-sujeto provocaría una pérdida de información porque la longitud de la línea era demasiado larga;

página-partida: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información porque se partiría una página original;

pérdida-símbolo-pictórico: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más símbolos pictóricos;

pérdida-símbolo-puntuación: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más símbolos de puntuación;

pérdida-carácter-alfabético: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más caracteres alfabéticos;

pérdida-información-múltiple: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida múltiple de información;

reasignación-destinatario-prohibida: indica que el MTS no pudo (o no podría) entregar el mensaje-sujeto porque el originador del sujeto prohibió el redireccionamiento a un **destinatario-alternativo-asignado-destinatario** (véase 8.2.1.1.1.4);

bucle-redireccionamiento-detectado: no pudo redirigirse el mensaje-sujeto a un destinatario sustitutivo porque el destinatario había redirigido previamente el mensaje (bucle-redireccionamiento);

ampliación-DL-prohibida: indica que el MTS no pudo (o no podría) entregar el mensaje-sujeto porque el originador del sujeto prohibió la ampliación de las DL (véase 8.2.1.1.1.6);

no-autorización-remisión-DL: el originador del sujeto (o de la DL de la que esta DL es miembro, en el caso de DL anidadas) no tiene autorización para remitir mensajes a esta DL;

fallo-ampliación-DL: indica que el MTS no pudo completar la ampliación de esta DL;

atributos-reproducción-física-no-soportados: el PDAU no soporta los atributos-reproducción-física requeridos (véase 8.2.1.1.1.20);

entrega-física-correo-imposible-dirección-incorrecta: fue imposible entregar el mensaje-sujeto porque la **dirección-OR-postal** especificada del destinatario era incorrecta;

entrega-física-correo-imposible-oficina-incorrecta-o-no-válida: fue imposible entregar el mensaje-sujeto porque la oficina-entrega física identificada por la **dirección-OR-postal** especificada del destinatario era incorrecta o no válida (no existe);

entrega-física-correo-imposible-dirección-incompleta: fue imposible entregar el mensaje-sujeto porque la **dirección-OR-postal** especificada del destinatario estaba incompletamente especificada;

correo-imposible-entregar-destinatario-desconocido: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** no era conocido en esa dirección;

correo-imposible-entregar-destinatario-fallecido: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** había fallecido;

correo-imposible-entregar-organización-desaparecida: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** había desaparecido;

correo-imposible-entregar-destinatario-rehusó-aceptar: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** rehusó aceptarlo;

correo-imposible-entregar-destinatario-no-recogió: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** no recogió el correo;

correo-imposible-entregar-destinatario-cambió-dirección-permanente: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** ha cambiado la dirección permanente ("se trasladó"), y el reenvío no resultó procedente;

correo-imposible-entregar-destinatario-cambió-dirección-temporalmente: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** ha cambiado la dirección temporalmente ("está de viaje"), y el reenvío no resultó procedente;

correo-imposible-entregar-destinatario-cambió-dirección-temporal: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-OR-postal** había cambiado la dirección temporal ("partido"), y el reenvío no resultó procedente;

correo-imposible-entregar-nueva-dirección-desconocida: fue imposible entregar el mensaje-sujeto porque el destinatario se había trasladado y la nueva dirección del destinatario era desconocida;

correo-imposible-entregar-destinatario-no-deseó-reenvío: fue imposible entregar el mensaje-sujeto porque la entrega requeriría un envío-físico que el destinatario no deseó;

correo-imposible-entregar-originador-prohibió-envío: el envío-físico necesario para la entrega del mensaje ha sido prohibido por el originador del mensaje-sujeto (véase 8.2.1.1.1.15);

error-mensajería-segura: el sujeto no pudo progresar porque la etiqueta de seguridad del mensaje violaría la política-seguridad en vigor, lo cual va en contra del contexto de seguridad;

incapaz-de-subgradar: el sujeto no puede ser transferido porque no puede ser degradado (véase el anexo B a la Rec. UIT-T X.419 | ISO/CEI 10021-6);

imposible-completar-transferencia: el sistema receptor ha indicado que es permanentemente incapaz de completar la transferencia del sujeto; por ejemplo, cuando la transferencia es de un tamaño tal que nunca sería aceptada;

límite-alcanzado-intentos-transferencia: se ha alcanzado el número máximo o la duración de la repetición de intentos de transferir el sujeto;

tipo-notificación-incorrecta: el mensaje-sujeto contenía un argumento de **tipo-notificación** que no se correspondía con su **contenido**.

Para errores de seguridad, este argumento puede tener uno de los valores siguientes:

a) Los siguientes valores indican una violación de seguridad por el usuario:

ampliación-DL-prohibida-por-política-seguridad: el mensaje fue dirigido a una DL, pero la política de seguridad prohibió la ampliación de esa DL;

destinatario-alternativo-prohibido: el mensaje-sujeto habría sido redireccionado, pero el nuevo destinatario es inaceptable por motivos de seguridad;

violación-política-seguridad: la política-seguridad es violada;

rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados;

miembro-DL-no-autorizado: la expansión-DL no se efectuó porque el MTA descubrió que la política de seguridad había prohibido que uno de los miembros de la DL recibiese este mensaje;

nombre-DL-no-autorizado: el MTA ha detectado que el nombre-OR del destinatario identifica una DL, pero la política de seguridad local no permite la transferencia hacia adelante al punto de ampliación-DL;

nombre-destinatario-deseado-originalmente-no-autorizado: el nombre-OR del destinatario deseado originalmente del mensaje redireccionado o DL-ampliado no está autorizado por motivos de seguridad;

nombre-originador-no-autorizado: el nombre-OR del usuario-MTS originador no está autorizado por motivos de seguridad;

nombre-destinatario-no-autorizado: el nombre-OR del usuario-MTS destinatario no está autorizado por motivos de seguridad;

sistema-no-fiable: la entrega del mensaje-sujeto requeriría que el mensaje-sujeto se transfiriese a un sistema inseguro, lo cual es incompatible con la etiqueta de seguridad del mensaje.

b) Los siguientes valores indican un error dentro del sistema de seguridad:

fallo-autenticación-en-mensaje-sujeto: la validación del argumento verificación-autenticación-origen-mensaje, o testigo-mensaje (es decir, firma, o cualquier otro dato de testigo) del mensaje-sujeto fracasó, por lo que el contenido del mensaje no pudo ser autenticado ni validado;

fallo-descriptación: el contenido-mensaje-sujeto no pudo ser descriptado;

clave-descriptación-no-obtenible: la clave requerida no pudo ser obtenida para descriptar los datos criptados del testigo-mensaje o para confidencialidad del contenido;

fallo-creación-doble-sobre: la política de seguridad requirió la creación de un sobre exterior para proteger el mensaje-sujeto. Sin embargo, el MTA no pudo crear el sobre exterior;

fallo-restablecimiento-mensaje-con-doble-sobre: el mensaje-sujeto contenía un sobre interior, pero el fallo de los servicios de seguridad en el sobre exterior impidió que el MTA extrajese el mensaje interior para el procesamiento subsiguiente;

fallo-de-prueba-de-mensaje: se detectó un fallo en los argumentos prueba de seguridad del mensaje-sujeto;

fallo-integridad-en-mensaje-sujeto: fracasó la validación del argumento verificación-integridad-contenido del mensaje-sujeto, por lo que el contenido del mensaje no pudo ser validado;

etiqueta-seguridad-no-válida: el identificador de política de seguridad en la etiqueta de seguridad del mensaje identifica una política que es conocida por el UA o MTA destinatario, pero que no es aceptable para ese sistema;

fallo-clave: no se pudieron obtener las claves requeridas:

ausencia-parámetro-obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

fallo-seguridad-operación: la operación transferencia o entrega fracasó por motivos de seguridad;

fallo-repudio-de-mensaje: la política de seguridad requería la utilización de una firma con propiedades de no-repudio, pero el mensaje-sujeto no estaba firmado con una firma no-repudiable en el origen;

fallo-contexto-seguridad-mensaje: la etiqueta de seguridad del mensaje es incompatible con el contexto-seguridad en vigor;

fallo-descriptación-testigo: el testigo del mensaje no pudo ser descriptado;

error-testigo: se ha detectado un error con el argumento testigo-mensaje del mensaje-sujeto;

etiqueta-seguridad-desconocida: el identificador de política de seguridad en la etiqueta de seguridad del mensaje no es reconocido por el UA o el MTA destinatario. Esta política no es soportada por dicho sistema;

identificador-algoritmo-no-soportado: el destinatario no soporta los identificadores de algoritmo utilizados por el argumento de seguridad del mensaje-sujeto;

política-seguridad-no-soportada: el destinatario no soporta la política-seguridad requerida, identificada en el argumento etiqueta-seguridad-mensaje del mensaje-sujeto.

Pueden especificarse otros **códigos-diagnóstico-no-entrega** en futuras versiones o adiciones de esta Recomendación | Norma Internacional.

8.3.1.2.1.13 Certificado-MTA-informador

Este argumento contiene el **certificado** del MTA que ha generado el informe. Debe ser generado por una fuente de confianza (por ejemplo, autoridad de certificación), y puede ser suministrado por el MTA-informador si se suministra una **comprobación-autenticación-origen-informe**.

Puede utilizarse un **certificado-MTA-informador** para transportar una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del MTA-informador.

El originador del mensaje y cualquier MTA a través del cual se transfiere el informe pueden utilizar la clave-criptación-pública-asimétrica del MTA-informador, para validar la **verificación-autenticación-origen-informe**.

8.3.1.2.1.14 Verificación-autenticación-origen-informe

Este argumento proporciona al originador del mensaje-sujeto (o-sonda), y a cualquier otro MTA a través del cual se transfiere el informe, los medios para autenticar el origen del informe (para proporcionar el elemento-de-servicio autenticación del origen del informe definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1). Puede ser generado por el MTA-informador si existe una **verificación-autenticación-origen-mensaje** (o **sonda**).

La **verificación-autenticación-origen-informe** proporciona la prueba del origen del informe (autenticación del origen del informe), y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el informe.

La **verificación-autenticación-origen-informe** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-autenticación-origen-informe** (un **identificador-algoritmo**).

La **verificación-autenticación-origen-informe** contiene el **identificador-algoritmo-autenticación-origen-informe**, y una versión cifrada asimétricamente, troceada:

del **identificador-algoritmo-autenticación-origen-informe**;

el **identificador-contenido** del sujeto;

la **etiqueta-seguridad-mensaje** del sujeto;

y todos los valores de los argumentos siguientes (por-destinatario):

el **nombre-destinatario-real**;

el **nombre-destinatario-deseado-originalmente**; y:

para un informe-entrega:

el **tiempo-entrega-mensaje**;

el **tipo-de-usuario-MTS**;

el **certificado-destinatario** si el originador del mensaje lo solicita para los destinatarios a los que se refiere el informe;

la **prueba-de-entrega** si el originador del mensaje lo solicita para los destinatarios a los que se refiere el informe y si el informe está en un mensaje; o

para un informe-no-entrega:

el **código-motivo-no-entrega**; y

el **código-diagnóstico-no-entrega**.

Si están presentes en el informe, se incluyen componentes facultativos en la **verificación-autenticación-origen-informe**.

El MTA-informador puede calcular la **verificación-autenticación-origen-informe** utilizando la clave-criptación-asimétrico-secreta del MTA-informador. El originador del sujeto y cualquier MTA a través del cual se transfiera el informe puede validar la **verificación-autenticación-origen-informe** utilizando la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) deducida a partir del **certificado-MTA-informador**.

Adiciones o futuras versiones de esta Recomendación | Norma Internacional pueden definir otras formas de **verificación-autenticación-origen-informe** (por ejemplo, basadas en técnicas-criptación-simétricas) que pueden utilizar los MTA a través de los cuales se transfieren informes para autenticar el origen del informe.

8.3.1.2.1.15 Tipo-contenido

Este argumento identifica el tipo de **contenido** del mensaje (véase 8.2.1.1.1.34). Deberá generarlo el MTA-informador. Este argumento puede estar ausente en la recepción sólo si el informe ha tenido su origen o ha pasado por un sistema de 1984.

8.3.1.2.1.16 Contenido-devuelto

Este argumento contiene el **contenido** del mensaje-sujeto si el originador del mensaje-sujeto indicó que debe devolverse el **contenido** (véase 8.2.1.1.1.23). Debe ser generado por el originador del mensaje, y el MTS puede devolverlo (si el MTA-informador o el MTA-originador soporta el elemento-de-servicio devolución de contenido).

Este argumento puede estar presente únicamente si existe al menos un informe de no-entrega en la entrega-informe, y si el destinatario del informe es el originador del mensaje-sujeto [y no, por ejemplo, el propietario de una DL (véase 8.3.1.2.1.4)].

Este argumento no estará presente si se ha realizado cualquier conversión de **tipo-información-codificada** sobre el **contenido** del mensaje-sujeto.

8.3.1.2.1.17 Nombre MTA informador

Este argumento identifica al MTA que creó el informe. Comprende un nombre-MTA, un identificador-dominio global y facultativamente un nombre-directorio de un **agente de transferencia de mensajes MHS** (véase A.1.3 de la Rec. UIT-T X.402 | ISO/CEI 10021-2). Puede ser generado por el MTA-informador, pero será generado si es requerido por la política de seguridad en vigor.

NOTA 1 – Con independencia de cualquier utilización para fines de seguridad, este argumento puede ser usado con fines de diagnóstico para indicar el MTA que generó el informe.

NOTA 2 – La información-rastreo-interna contiene también el nombre del MTA-informador. En los entornos donde la información-rastreo-interna no es suprimida en cualquier punto entre el originador y el destinatario, esta información puede ser usada como una alternativa a este argumento.

NOTA 3 – Cuando es utilizada con servicios tales como autenticación-origen-informe o prueba-de-entrega, una política de seguridad típica requeriría que este parámetro sea generado siempre que se invoquen estos servicios.

8.3.1.2.2 Resultados

La operación-abstracta de entrega-informe devuelve un resultado vacío como indicación de éxito.

8.3.1.2.3 Errores-abstractos

El cuadro 19 enumera los errores-abstractos que pueden interrumpir la operación-abstracta entrega-informe, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 19 – Errores-abstractos de entrega-informe

Error-abstracto	Cláusula
Control-entrega-violado	8.3.2.1
Error-seguridad	8.3.2.3
Función-crítica-no-soportada	8.3.2.4

8.3.1.3 Control-entrega

La operación-abstracta control-entrega permite al usuario-MTS limitar de forma transitoria las operaciones-abstractas de puerto-entrega que puede invocar el MTS, y los mensajes que puede entregar el usuario-MTS a través de la operación-abstracta entrega-mensaje.

El MTS debe retener hasta un tiempo posterior, en vez de abandonar, las operaciones-abstractas y los mensajes prohibidos.

La ejecución satisfactoria de la operación-abstracta significa que los controles especificados están actualmente en vigor. Estos controles sobreseen cualquier otro previamente en vigor, y permanecen vigentes hasta que se libera la asociación, el usuario-MTS reinvoca la operación-abstracta control-entrega o el usuario-MTS invoca la operación-abstracta de registro en el puerto-administración para imponer limitaciones más rigurosas que los controles especificados.

La operación-abstracta devuelve una indicación de cualquier operación-abstracta que invocara el MTS, o cualquier tipo de mensaje que entregaría o sobre el que informaría el MTS, a no ser por los controles que prevalecen.

8.3.1.3.1 Argumentos

El cuadro 20 enumera los argumentos de la operación-abstracta control-entrega y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 20 – Argumentos de control-entrega

Argumentos	Presencia	Cláusula
Argumentos de control de entrega		
Limitación	O	8.3.1.3.1.1
Operaciones-admisibles	O	8.3.1.3.1.2
Prioridad-inferior-admisible	O	8.3.1.3.1.3
Tipos-información-codificada-admisible	O	8.3.1.3.1.4
Tipos-contenido-admisibles	O	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	O	8.3.1.3.1.6
Contexto-seguridad-admisible	O	8.3.1.3.1.7

8.3.1.3.1.1 Limitación

Este argumento indica si los controles sobre las operaciones-abstractas de puerto-entrega deben actualizarse o suprimirse. Puede generarse por el usuario-MTS.

Este argumento puede tener uno de los siguientes valores:

actualización: los demás argumentos actualizan los controles que prevalecen;

supresión: todos los controles deben suprimirse (se aplicarán los controles por defecto registrados con el MTS mediante la operación-abstracta de registro del puerto-administración); los demás argumentos deben ignorarse.

En ausencia de este argumento, se supondrá por defecto el valor **actualización**.

8.3.1.3.1.2 Operaciones-admisibles

Este argumento indica las operaciones-abstractas que el MTS puede invocar sobre el usuario-MTS. Puede generarse por el usuario-MTS.

Este argumento puede tener el valor **autorizado** o **prohibido** para cada uno de los siguientes:

entrega-mensaje: el MTS puede/no puede invocar la operación-abstracta de entrega-mensaje; y

entrega-informe: el MTS puede/no puede invocar la operación-abstracta de entrega-informe.

Otras operaciones-abstractas de puerto-entrega no están sujetas a controles, y pueden invocarse en cualquier momento.

En ausencia de este argumento, las operaciones-abstractas que puede invocar el MTS permanecen sin modificaciones. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará el control por defecto registrado con el MTS mediante la operación-abstracta de registro en el puerto-administración.

8.3.1.3.1.3 Prioridad-inferior-admisible

Este argumento contiene la **prioridad** del mensaje de prioridad más baja que el MTS debe remitir al usuario-MTS a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-MTS.

Este argumento puede tener uno de los siguientes valores del argumento de **prioridad** de la operación-abstracta de entrega-mensaje: normal, no-urgente o urgente.

En ausencia de este argumento, la **prioridad** del mensaje de inferior prioridad que debe entregar el MTS al usuario-MTS permanece sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se debe aplicar el control por defecto registrado con el MTS mediante la operación-abstracta registro del puerto-administración.

8.3.1.3.1.4 Tipos-información-codificada-admisibles

Este argumento indica los **tipos-información-codificada**, que deben aparecer en los mensajes que el MTS entregará al usuario-MTS a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-MTS.

El argumento incluye **tipos-de-información-codificada-aceptable**, **tipos-de-información-codificada-no-aceptable** y **tipos-de-información-codificada-exclusivamente-aceptable**. Cada uno de ellos identifica una lista de **tipos-de-información-codificada** específica; véase 8.4.1.1.1.3.1.

En ausencia de este argumento, los **tipos-información-codificada-admisibles** de un mensaje que el MTS puede entregar al usuario-MTS permanecen sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se debe aplicar el control por defecto registrado con el MTS mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.5 Tipos-contenido-admisibles

Este argumento contiene los tipos-contenido, que deben aparecer en el mensaje que el MTS debe entregar al usuario-MTS a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-MTS.

Los **tipos-contenido-admisibles** especificados deben estar entre los autorizados a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**tipos-contenido-entregables**).

En ausencia de este argumento, los **tipos-contenido-admisibles** de un mensaje que el MTS puede entregar al usuario-MTS permanecen sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará por defecto el control registrado con el MTS mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.6 Longitud-contenido-máxima-admisible

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el MTS debe remitir al usuario-MTS a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-MTS.

La **longitud-contenido-máxima-admisible** no debe exceder la autorizada a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**longitud-contenido-máxima-entregable**).

En ausencia de este argumento, la **longitud-contenido-máxima-admisible** de un mensaje que el MTS puede entregar al usuario-MTS permanece sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará por defecto el control registrado con el MTS mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.7 Contexto-seguridad-admisible

Este argumento limita de forma transitoria la sensibilidad de las operaciones-abstractas de puerto-entrega (contexto-seguridad-entrega) que el MTS puede invocar en el usuario-MTS. Es una limitación temporal del **contexto-seguridad** establecido al iniciarse la asociación (véase 8.1.1.1.1.4). Puede generarse por el usuario-MTS.

El **contexto-seguridad-admisible** consta de una o más **etiquetas-seguridad** del conjunto de **etiquetas-seguridad** establecidas como **contexto-seguridad** al establecerse la asociación.

En ausencia de este argumento, el **contexto-seguridad** de las operaciones-abstractas de puerto-entrega permanece sin modificar.

8.3.1.3.2 Resultados

El cuadro 21 enumera los resultados de la operación-abstracta control-entrega, y para cada resultado califica su presencia e identifica la cláusula donde se define el resultado.

Cuadro 21– Resultados de control-entrega

Resultado	Presencia	Cláusula
Resultados "esperando"		
Operaciones-esperando	O	8.3.1.3.2.1
Mensaje-esperando	O	8.3.1.3.2.2
Tipos-información-codificada-esperando	O	8.3.1.3.2.3
Tipos-contenido-esperando	O	8.3.1.3.2.4

8.3.1.3.2.1 Operaciones-esperando

Este resultado indica las operaciones-abstractas que retiene el MTS y que el MTS invocaría en el usuario-MTS si no fuera por los controles que prevalecen. Puede generarse por el MTS.

Este resultado puede tener el valor **reteniendo** o **no-reteniendo** para cada uno de los siguientes:

entrega-mensaje: el MTS está/no está reteniendo mensajes, e invocaría la operación abstracta de entrega-mensaje en el usuario-MTS si no fuera por los controles que prevalecen; y

entrega-informe: el MTS está/no está reteniendo informes, e invocaría la operación-abstracta de entrega-informe en el usuario-MTS si no fuera por los controles que prevalecen.

En ausencia de este resultado, puede suponerse que el MTS no está reteniendo ningún mensaje ni ninguna sonda para su entrega al usuario-MTS debido a los controles que prevalecen.

8.3.1.3.2.2 Mensajes-esperando

Este resultado indica la categoría de los mensajes que el MTS está reteniendo para su remisión al usuario-MTS, y que remitiría a través de la operación-abstracta entrega-mensaje, si no fuera por los controles que prevalecen. Puede generarse por el MTS.

Este resultado puede adoptar uno de los siguientes valores:

contenido-largo: el MTS ha retenido mensajes para su entrega al usuario-MTS que exceden el control **longitud-contenido-máxima-admisible** actualmente en vigor;

baja-prioridad: el MTS ha retenido mensajes para su entrega al usuario-MTS de una prioridad inferior al control de **prioridad-inferior-admisible** actualmente en vigor;

otras-etiquetas-seguridad: el MTS ha retenido mensajes para su entrega al usuario-MTS que transportan **etiquetas-seguridad-mensaje** diferentes de las permitidas por el contexto-seguridad actual.

En ausencia de este resultado, puede suponerse que el MTS no está reteniendo ningún mensaje ni ninguna sonda para su entrega al usuario-MTS debido a los controles de **longitud-contenido-máxima-admisible**, **prioridad-inferior-admisible** o **contexto-seguridad-admisible** actualmente en vigor.

8.3.1.3.2.3 Tipos-información-codificada-esperando

Este resultado indica los **tipos-información-codificada** del **contenido** de cualquier mensaje retenido por el MTS para su entrega al usuario-MTS debido a los controles que prevalecen. Puede generarse por el MTS.

En ausencia de este resultado, los **tipos-información-codificada** de cualquier mensaje retenido por el MTS para su entrega al usuario-MTS estarán **sin-especificar**.

8.3.1.3.2.4 Tipos-contenido-esperando

Este resultado indica los **tipos-contenido** de cualquier mensaje retenido por el MTS para su entrega al usuario-MTS debido a los controles que prevalecen. Puede generarse por el MTS.

En ausencia de este resultado, los **tipos-contenido** de cualquier mensaje retenido por el MTS para su entrega al usuario-MTS estarán **sin-especificar**.

8.3.1.3.3 Errores-abstractos

El cuadro 22 enumera los errores-abstractos que pueden interrumpir la operación-abstracta control-entrega, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 22 – Errores-abstractos de control-entrega

Error-abstracto	Cláusula
Control-viola-registro	8.3.2.2
Error-seguridad	8.3.2.3
Operación-rehusada	8.3.2.5

8.3.2 Errores-abstractos

En esta cláusula se definen los siguientes errores-abstractos de puerto-entrega:

a) control-entrega-violado;

b) control-viola-registro;

c) error-seguridad;

d) función-crítica-no-soportada;

e) operación-rehusada.

8.3.2.1 Control-entrega-violado

El error-abstracto de control-entrega-violado informa de la violación por el MTS de un control sobre las operaciones-abstractas de puerto-entrega impuestas por el usuario-MTS a través de la operación-abstracta de control-entrega.

El error-abstracto de control-entrega-violado no tiene parámetros.

8.3.2.2 Control-viola-registro

El error-abstracto control-viola-registro informa que el MTS no puede aceptar el control que el usuario-MTS intenta imponer sobre las operaciones-abstractas porque violan los parámetros de registro existentes.

El error-abstracto control-viola-registro no tiene parámetros.

8.3.2.3 Error-seguridad

El error-abstracto error-seguridad informa que la operación-abstracta pedida no puede ser proporcionada por el usuario-MTS porque se violaría la política-seguridad en vigor.

El error-abstracto error-seguridad tiene el siguiente parámetro, generado por el usuario-MTS:

problema-seguridad: Identificador relativo a la causa de violación de la política-seguridad.

El parámetro problema-seguridad puede tener uno de los siguientes valores para las operaciones-abstractas entrega-mensaje o entrega-informe:

a) Los siguientes valores indican una violación de seguridad por el usuario:

violación-política-seguridad: la política-seguridad es violada;

rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados;

nombre-destinatario-deseado-originalmente-no-autorizado: el nombre-OR del destinatario deseado originalmente del mensaje redireccionado o DL-ampliado no está autorizado por motivos de seguridad;

nombre-originador-no-autorizado: el nombre-OR del usuario-MTS originador no está autorizado por motivos de seguridad;

nombre-destinatario-no-autorizado: el nombre-OR del usuario-MTS destinatario no está autorizado por motivos de seguridad.

b) Los siguientes valores indican un error dentro del sistema de seguridad:

fallo-autenticación-en-mensaje-sujeto: la validación del argumento verificación-integridad-contenido, verificación-autenticación-origen-mensaje, o testigo-mensaje (es decir, firma, o cualquier otro dato de testigo) del mensaje fracasó, por lo que el contenido del mensaje no pudo ser autenticado ni validado;

fallo-descriptación: el contenido del mensaje no pudo ser descriptado;

clave-descriptación-no-obtenible: la clave requerida no pudo ser obtenida para descriptat los datos-criptados del testigo-mensaje o para confidencialidad del contenido;

fallo-de-prueba-de-mensaje: se detectó un fallo en los argumentos prueba-de-seguridad del mensaje;

fallo-integridad en el mensaje-sujeto: fracasó la validación del argumento verificación-integridad-contenido del mensaje, por lo que el contenido del mensaje no pudo ser validado;

etiqueta-seguridad-no-válida: el identificador de política de seguridad en la etiqueta de seguridad del mensaje identifica una política que es conocida por el UA pero que no es aceptable para ese UA;

fallo-clave: no se pudieron obtener las claves requeridas;

ausencia-parámetro-obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

fallo-seguridad-operación: la operación entrega fracasó por motivos de seguridad;

fallo-repudio-de-mensaje: la política de seguridad requería la utilización de una firma con propiedades de no-repudio, pero el mensaje no estaba firmado con una firma no-repudiable en el origen;

fallo-contexto-seguridad: la etiqueta de seguridad del mensaje es incompatible con el contexto-seguridad en vigor;

fallo-descriptación-testigo: el testigo del mensaje no pudo ser descriptado;

error-testigo: se ha detectado un error con el argumento testigo-mensaje del mensaje;

etiqueta-seguridad-desconocida: el identificador de política de seguridad en la etiqueta de seguridad del mensaje no es reconocido por el UA. Esta política no es soportada por dicho UA;

identificador-algoritmo-no-soportado: el destinatario no soporta los identificadores de algoritmo utilizados por el argumento seguridad del mensaje;

política-seguridad-no-soportada: el destinatario no soporta la política-seguridad requerida, identificada en el argumento etiqueta-seguridad-mensaje;

El parámetro problema-seguridad puede tener uno de los siguientes valores para la operación-abstracta control-entrega:

a) Los siguientes valores indican una violación de seguridad por el usuario:

violación-política-seguridad: la política-seguridad es violada;

rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados.

b) Los siguientes valores indican un error dentro del sistema de seguridad:

cambio-incompatible-con-contexto-seguridad-original: el contexto-seguridad-admisible propuesto no es un subconjunto del contexto-seguridad original;

ausencia parámetro obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

fallo-seguridad-operación: la operación control-entrega fracasó por motivos de seguridad.

8.3.2.4 Función-crítica-no-soportada

El error-abstracto función-crítica-no-soportada informa que un argumento de la operación-abstracta ha sido marcado como **crítico-para-entrega** (véase 9.2) pero que no está soportado por el usuario-MTS.

El error-abstracto función-crítica-no-soportada no tiene parámetros.

8.3.2.5 Operación-rehusada

El error-abstracto operación-rehusada indica que el MTS ha rehusado realizar una operación por motivos de política local. El error operación-rehusada tiene dos parámetros que genera el MTS, a saber, **argumento-rehusado** y **motivo-rehusado**.

El parámetro **argumento-rehusado** indica cual es el argumento que ha motivado el rechazo de la operación. Para la operación control-entrega informará de uno de los argumentos enumerados en el cuadro 20 o uno de los argumentos que componen la clase-entregable o un argumento de ampliación. Para la operación de registro indicará uno de los argumentos enumerados en el cuadro 23, o un requisito de ampliación.

El parámetro **motivo-rechazo** tendrá uno de los valores siguientes:

facilidad-no-disponible: el usuario ha intentado utilizar una facilidad que el MTS no tiene disponible para sus usuarios;

facilidad-no-abonada: el usuario ha intentado utilizar una facilidad sujeta a abono, no estando abonado a la misma;

parámetro inaceptable: el usuario ha especificado un valor de parámetro que el MTA no puede aceptar.

8.4 Puerto de administración

En esta cláusula se definen las operaciones-abstractas y los errores-abstractos que ocurren en un puerto-administración.

8.4.1 Operaciones-abstractas

En esta cláusula se definen las siguientes operaciones-abstractas de puerto-administración:

a) registro;

b) cambio-credenciales.

8.4.1.1 Registro

La operación-abstracta registro permite a un usuario-MTS realizar cambios a largo plazo en varios parámetros del usuario-MTS retenido por el MTS afectado por la entrega de mensajes al usuario-MTS, y recuperar los valores de estos parámetros.

Dichos cambios permanecen vigentes hasta ser superados por la nueva invocación de la operación-abstracta de registro. Sin embargo, algunos parámetros pueden ser transitoriamente reemplazados mediante la invocación de la operación-abstracta control-entrega.

NOTA 1 – Esta operación-abstracta debe ser invocada antes de que pueda utilizarse cualquier otro puerto-remisión, puerto-entrega u operación-abstracta de puerto-administración o habrá tenido lugar un registro equivalente localmente.

NOTA 2 – Esta operación-abstracta no incluye los parámetros existentes involucrados por el elemento-de-servicio destinatario alternativo autorizado definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1. La forma en que se suministran y modifican dichos parámetros es asunto local.

NOTA 3 – Pueden utilizarse otros mecanismos distintos del registro para asignar valores a cualquiera de los parámetros de registro.

NOTA 4 – La definición de la operación-abstracta registro para utilización en un contexto de aplicación de 1988 figura en el anexo C.

8.4.1.1.1 Argumentos

El cuadro 23 enumera los argumentos de la operación-abstracta registro y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 23 – Argumentos de registro

Argumento	Presencia	Cláusula
Argumentos de registro		
Nombre-usuario	O	8.4.1.1.1.1
Dirección-usuario	O	8.4.1.1.1.2
Clases-entregables	O	8.4.1.1.1.3
Redireccionamientos-asignados-destinatario	O	8.4.1.1.1.4
Entrega-limitada	O	8.4.1.1.1.5
Extracción-registros	O	8.4.1.1.1.6
Argumentos de control de entrega por defecto		8.4.1.1.1.7
Operaciones-admisibles	O	8.3.1.3.1.2
Prioridad-inferior-admisible	O	8.3.1.3.1.3
Tipos-información-codificada-admisibles	O	8.3.1.3.1.4
Tipos-contenido-admisibles	O	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	O	8.3.1.3.1.6

8.4.1.1.1.1 Nombre-usuario

Este argumento contiene el **nombre-OR** del usuario-MTS, si ha de cambiarse el **nombre-usuario**. Puede ser generado por el usuario-MTS.

Un MD no está obligado a proporcionar a los usuarios-MTS la posibilidad de modificar sus propios **nombres-OR**. Si así lo hace, el MD puede limitar esa posibilidad. Puede prohibir a ciertos usuarios-MTS cambiar sus **nombres-OR**, o puede limitar el ámbito del cambio a un subconjunto definido localmente de los componentes de sus **nombres-OR**. Un nuevo **nombre-OR** propuesto será rechazado si su dirección OR ya está asignada a otro usuario-MTS o DL.

En ausencia de este argumento, el **nombre-usuario** del usuario-MTS permanece sin modificar.

8.4.1.1.1.2 Dirección-usuario

Este argumento contiene la **dirección-usuario** del usuario-MTS, si éste la solicita o si se ha de modificar. Puede ser generado por el usuario-MTS.

La **dirección-usuario** puede contener una de las siguientes formas de dirección del usuario-MTS:

la **dirección-X.121** y/o el **ID-TSAP** (*transport service access point identifier* – identificador del punto de acceso del servicio de transporte); o

la **dirección-PSAP** (*presentation service access point address* – dirección del punto de acceso del servicio de presentación).

En adiciones o futuras versiones de esta Recomendación | Norma Internacional pueden definirse otras formas de **dirección-usuario**.

En ausencia de este argumento, la **dirección-usuario** del usuario-MTS (si existe) permanece sin modificar.

8.4.1.1.1.3 Clases-entregables

Este argumento contiene todos los conjuntos de criterios que determinan qué mensajes serán entregados al usuario-MTS, si cualquiera de estos criterios han de ser cambiados. Si está presente, este argumento sustituye a las **clases-entregable** registradas previamente. Puede ser generado por el usuario-MTS.

Cada conjunto de criterios forma una **clase-entregable**. La **clase-entregable** contiene facultativamente **constricciones-de-tipos-de-información-codificada**, **tipos-de-contenido-entregable**, **longitud-de-contenido-máxima-entregable** y **etiquetas-seguridad-entregables**. La ausencia de valores para un componente determinado indica que no existe restricción en los valores de este componente en esta **clase-entregable**.

El MTS entregará un mensaje al usuario-MTS solamente si el mensaje satisface todos los criterios por lo menos en una de las **clases-entregables** en el conjunto registrado.

En ausencia de este argumento, las **clases-entregables** permanecerán inalteradas.

8.4.1.1.1.3.1 Constricciones-de-tipos-de-información-codificada

Este componente indica los **tipos-de-información-codificada** que el MTS permitirá que aparezcan en los mensajes entregados al usuario-MTS, si éstos han de ser constreñidos dentro de una **clase-entregable**.

El componente contiene **tipos-de-información-codificada-aceptable**, **tipos-de-información-codificada-no-aceptable** y **tipos-de-información-codificada-exclusivamente-aceptable**. Cada uno de ellos identifica una lista de **tipos-de-información-codificada** específica.

Si un mensaje no tiene **tipos-de-información-codificada**, siempre satisfará cualquier **constricción-de-tipos-de-información-codificada**.

Si los **tipos-de-información-codificada** del mensaje que se ha de entregar son incompatibles con las **constricciones-de-tipos-de-información-codificada**, el mensaje no satisface las constricciones de esta **clase-entregable**, y no es necesario considerar ningún otro criterio de la **clase-entregable**.

El MTS determina si un mensaje satisface las **constricciones-de-tipo-de-información-codificada** de una **clase-entregable** conforme al procedimiento definido en 14.3.4.4, ítem 7 c).

Se considera que los **tipos-de-información-codificada** en un mensaje que se ha de entregar son los que estarían presentes en el mensaje después de todas las conversiones, (si hubiere alguna).

Según los requisitos locales o las capacidades proporcionadas por el entorno informático de un usuario, éste puede elegir uno de los siguientes registros que:

a) Permite la entrega de todos los mensajes con independencia de los **tipos-de-información-codificada** que contienen. En este caso, no es necesario que se registren las **restricciones-tipos-de-información-codificada**.

b) Permite la entrega de todos los mensajes salvo aquellos que contienen al menos un **tipo-de-información-codificada** en el conjunto de **tipos-de-información-codificada-no-aceptable** registrado. En este caso no es necesario registrar **tipos-de-información-codificada-aceptable** o **tipos-de-información-codificada-exclusivamente-aceptable**.

NOTA 1 – Por ejemplo, este registro puede ser apropiado para un usuario-MS que no soporta la parte de cuerpo vocal, para evitar que los mensajes que contienen grandes partes de cuerpo vocales consuman el espacio de almacenamiento disponible para los mensajes entregados.

c) Permite la entrega del mensaje si éste contiene por lo menos uno de los **tipos-de-información-codificada-aceptable** registrados. En este caso no es necesario registrar **tipos-de-información-codificada-no-aceptable** o **tipos-de-información-codificada-exclusivamente-aceptable** registrados.

NOTA 2 – Por ejemplo, un usuario-IPMS puede requerir que se entreguen todos los mensajes que contienen la parte de cuerpo de texto IA5. Tras leer las partes de cuerpo IA5, el usuario puede evaluar la importancia de la información contenida en las otras partes del cuerpo, y decidir si ha de buscar otros medios para procesar estas partes de cuerpo.

d) Requiere que todos los **tipos-de-información-codificada** en el mensaje se registren como **tipos-de-información-codificada-exclusivamente-aceptable**, y lo rechaza si no es así. En este caso, es necesario registrar los **tipos-de-información-codificada-aceptable** o los **tipos-de-información-codificada-no-aceptable**.

NOTA 3 – Esto puede ser apropiado si el UA de usuario soporta un conjunto relativamente pequeño de tipos-de-información-codificada. Esto es idéntico al servicio soportado por la operación abstracta Register-88.

e) Permite la entrega del mensaje si éste no contiene ninguno de los **tipos-de-información-codificada-no-aceptable-registrada**, y contiene por lo menos un **tipo-de-información-codificada** registrada en **tipos-de-información-codificada-aceptable**, o bien sólo contiene **tipos-de-información-codificada** registradas como **tipos-de-información-codificada-exclusivamente-aceptable**. En este caso, pueden ser registrados todos los **tipos-de-información-codificada-no-aceptable**, **tipos-de-información-codificada-aceptables**, y **tipos-de-información-codificada-exclusivamente-aceptable**.

NOTA 4 – Esto satisface los requisitos indicados en b), c) y d). Por ejemplo, un usuario-IPMS puede utilizar esta combinación para asegurar que las partes de cuerpo vocal no se entregan nunca, que las partes de cuerpo transferencia de ficheros se entregan siempre (sujeto a la ausencia de partes de cuerpo vocal), y que cuando ninguno de estos tipos de parte de cuerpo está presente, sólo se entregan los mensajes que contienen un conjunto prescrito de partes de cuerpo.

El MTS devolverá un error si el usuario-MTS intenta registrar un **tipo-de-información-codificada** ya sea en **tipos-de-información-codificada-no-aceptable** o en **tipos-de-información-codificada-aceptable** o bien **tipos-de-información-codificada-exclusivamente-aceptable**.

Los **tipos-de-información-codificada-aceptable** y los **tipos-de-información-codificada-exclusivamente-aceptable** indican también los **tipos-de-información-codificada** posibles que la conversión implícita puede producir útilmente.

En ausencia de este componente, las **constricciones-de-tipos-de-información-codificada** no tendrán constricciones.

8.4.1.1.1.3.2 Tipos-de-contenido-entregable

Este componente indica los **tipos-de-contenido** que el MTS debe permitir que aparezcan en los mensajes entregados al usuario-MTS, si han de ser constreñidos dentro de una **clase-entregable**.

Si la **longitud-de-contenido** del mensaje que se ha de entregar rebasa el valor especificado por la **longitud-de-contenido-máxima-entregable**, el mensaje no satisface las constricciones de esta **clase-entregable** y no es necesario considerar otros criterios de **clase-entregable**. El usuario-MTS se puede registrar para recibir el **tipo-de-contenido-no-identificado**.

En ausencia de este componente, los **tipos-de-contenido-entregable** no tendrán constricciones.

8.4.1.1.1.3.3 Longitud-de-contenido-máximo-entregable

Este componente contiene la **longitud-de-contenido**, en octetos, del mensaje de contenido más largo que el MTS debe permitir que aparezca en los mensajes entregados al usuario-MTS, si han de ser constreñidos dentro de una **clase-entregable**.

Si la **longitud-de-contenido** del mensaje que se ha de entregar rebasa el valor especificado por la **longitud-de-contenido-máxima-entregable**, el mensaje no satisface las constricciones de esta **clase-entregable** y no es necesario considerar otros criterios de la **clase-entregable**.

En ausencia de este componente, la **longitud-de-contenido-máximo-entregable** de mensajes no tendrá constricciones.

8.4.1.1.1.3.4 Etiquetas-de-seguridad-entregables

Este componente contiene las **etiquetas-de-seguridad** del usuario-MTS, si han de ser constreñidas dentro de una **clase-entregable**.

Si las **etiquetas-de-seguridad** del mensaje que se ha de entregar no concuerdan con las especificadas en las **etiquetas-de-seguridad-entregables**, el mensaje no satisface las constricciones de esta **clase-entregable** y no es necesario considerar otros criterios de la **clase-entregable**.

Algunas políticas-de-seguridad pueden permitir únicamente modificar las **etiquetas-de-seguridad-entregables** si se utiliza un enlace seguro. Se puede proporcionar otros medios locales de modificar las **etiquetas-de-seguridad-entregables** de manera segura.

En ausencia de este componente, las **etiquetas-de-seguridad-entregables** no tendrán constricciones.

8.4.1.1.1.4 Redireccionamientos-asignados-por-destinatario

En caso que deba modificarse la asignación de destinatarios-alternativos, este argumento contiene una lista ordenada de los **nombres-OR** de los **destinatarios-alternativos-asignados-por-destinatario** y, opcionalmente, una o más **clases-redireccionamiento** asociadas con cada destinatario-alternativo. Si este argumento está presente, su valor sustituye en su totalidad cualquier asignación previa de destinatarios-alternativos. Puede ser generado por el usuario-MTS.

Si se especifican uno o más **destinatarios-alternativo-asignado-destinatario**, todos los mensajes (o informes) para el usuario-MTS serán redireccionados al primer destinatario-alternativo para el cual el mensaje (o informe) cumple los criterios en una de las **clases-redireccionamiento** asociadas al destinatario-alternativo. Aquellos mensajes (o informes) que no cumplan ningún criterio de **clase-redireccionamiento** para ningún **destinatario-alternativo-asignado-destinatario**, serán entregados al usuario-MTS. El usuario-MTS especifica el orden de los destinatarios-alternativos. La ausencia de cualquier **clase-redireccionamiento** indica un destinatario-alternativo al que se redirigirán todos los mensajes (o informes), excepto aquellos que cumplan las **clases-redireccionamiento** específicas asociadas a destinatarios-alternativos anteriores. La ausencia de un **destinatario-alternativo-asignado-por-destinatario** indica la entrega al usuario-MTS.

NOTA – Si hay una lista de **redireccionamientos-asignados-por-destinatario**, la **clase-de-redireccionamiento** ausente debe ser la última en la lista ya que no se utilizarán elementos posteriores.

La **clase-de-redireccionamiento** contiene facultativamente una **longitud-de-contenido** máxima y facultativamente conjuntos de valores para cada uno de los **tipos-de-información-codificada**, **tipo-de-contenido**, **etiquetas-de-seguridad-entregables**, **restricción** y **prioridad**. La ausencia de valores para un tipo determinado indica que no existen restricciones sobre los valores de ese tipo en esta **clase-de-redireccionamiento**. La **clase-de-redireccionamiento** indica también los tipos de objeto de información MHS al cual se aplica la **clase-de-redireccionamiento**: mensaje solamente, informes solamente o mensajes e informes.

El **destinatario-alternativo-asignado-por-destinatario** contendrá el **nombre-OR** del destinatario-alternativo.

Si el argumento de **redireccionamientos-asignados-por-destinatario** contiene un solo elemento con el **destinatario-alternativo-asignado-por-destinatario** y la **clase-de-redireccionamiento** ausente, no se registra ningún **destinatario-asignado-por-destinatario**.

Cuando se registran **redireccionamientos-asignados-por-destinatario** y **clases-entregables**, el redireccionamiento tiene precedencia con respecto a las restricciones de entrega.

En ausencia de este argumento, los **redireccionamientos-asignados-por-destinatario**, si hubiere alguno, permanecen inalterados.

8.4.1.1.1.5 Entrega-restringida

Este argumento indica el **nombre-OR** de otros usuarios-MTS de los cuales el usuario-MTS desea (o no desea) recibir mensajes, si la **entrega-restringida** ha de ser modificada. Comprende una lista ordenada de **restricciones**. Si el argumento **entrega-restringida** está presente, su valor sustituye completamente cualquier valor previo. Puede ser generado por el usuario-MTS.

El MTS rechazará como no entregable cualquier mensaje para el usuario-MTS que es originado o ampliado-dl por otro usuario-MTS del cual el usuario-MTS no consiente en aceptar la entrega. Cada restricción puede especificar la fuente que está desautorizada, sea como **nombre-OR** completo o como un modelo de **nombre-OR** completo.

Si una o más **restricciones** están registradas, las fuentes (**nombre-originador**, **historia-de-redireccionamiento**, **historia-de-DL-ampliación**) de cada mensaje se comparan con la lista autorizada de **restricciones** hasta que se encuentre una concordancia. La comparación se detiene inmediatamente que aparece una concordancia con una **restricción** y el mensaje es entregado si está permitido o se rechaza como no entregable si no está permitido. Si no hay **restricciones** de concordancia, el mensaje es entregado.

La Rec. UIT-T X.402 | ISO/CEI 10021-2 especifica los procedimientos para determinar las concordancias de los **nombres-OR**, ya sean exactas o según un modelo.

El usuario-MTS puede registrar para recibir todos los mensajes, que es el estado antes de cualquier registro de **entrega-restringida**, especificando una sola **restricción** en la cual todos los tipos de fuente están permitidos y se omite el nombre de fuente.

Cuando **entrega-restringida** y **redireccionamientos-asignados-por-destinatario** están registrados, el redireccionamiento tiene precedencia con respecto a la **entrega-restringida**.

En ausencia de este argumento, la **entrega-restringida** permanecerá inalterada.

8.4.1.1.1.6 Extracción-de-registros

Este argumento indica los registros individuales que el usuario-MTS pide sean devueltos en el resultado de la operación-abstracta de registro. Puede ser generado por el usuario-MTS.

El resultado devuelto refleja el estado de la información registrada después que se han procesado todos los otros argumentos de registro.

El argumento contiene varios elementos, cada uno de los cuales, si está fijado, pide el valor registrado de la clase de información correspondiente.

En ausencia de este argumento, no se solicita ninguna información de registro.

8.4.1.1.1.7 Argumentos-control-entrega-por-defecto

Los argumentos de control por defecto son los mismos que los argumentos de la operación-abstracta control-entrega, definidos en 8.3.1.3.1. Excepto para **contexto-seguridad-admisible** y **restricta**, estos argumentos pueden ser generados por el usuario-MTS.

Se registran los controles por defecto como argumentos de la operación-abstracta de registro. Estos controles por defecto entran en vigor al comienzo de una asociación, y permanecen vigentes hasta que son suspendidos por una invocación de la operación-abstracta de control-entrega.

Los argumentos de control por defecto no deben admitir mensajes cuya entrega esté prohibida por los valores registrados prevalecientes del argumento **tipos-información-codificada-entregables**, del argumento **tipos-contenido-entregables** o del argumento **longitud-máxima-contenido-entregable**.

8.4.1.1.2 Resultados

La operación-abstracta de registro devuelve un resultado vacío a menos que esté presente un resultado de extensión, o esté presente el argumento **extracción-de-registro** en la invocación. En el segundo caso, se devuelven los registros identificados en el argumento **extracción-de-registro**.

Los resultados son idénticos a los argumentos de la operación abstracta de registro enumerados en el cuadro 23 (salvo que **extracción-de-registros** está ausente).

8.4.1.1.3 Errores-abstractos

El cuadro 24 enumera los errores-abstractos que pueden interrumpir la operación-abstracta de registro y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 24 – Errores-abstractos de registro

Error-abstracto	Cláusula
Registro-rechazado	8.4.2.1
Error-de-vinculación-distante	8.2.2.10
Operación-rehusada	8.3.2.5
Error-seguridad	8.4.2.4

8.4.1.2 Cambio-credenciales

La operación-abstracta cambio-credenciales permite al usuario-MTS modificar las **credenciales** de autenticación-simple del usuario-MTS en poder del MTS, o permite al MTS modificar las **credenciales** de autenticación-simple del MTS en poder del usuario-MTS.

Durante el establecimiento de una asociación se intercambian las **credenciales** para la autenticación mutua de la identidad del usuario-MTS y del MTS.

La finalización con éxito de la operación-abstracta significa que se han cambiado las **credenciales**.

La interrupción de la operación-abstracta por un error-abstracto indica que no se han cambiado las **credenciales**, bien porque las antiguas **credenciales** estaban incorrectamente especificadas o porque las nuevas **credenciales** resultan inaceptables.

8.4.1.2.1 Argumentos

El cuadro 25 enumera los argumentos de la operación-abstracta cambio-credenciales y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro 25 – Argumentos de cambio-credenciales

Argumento	Presencia	Cláusula
Argumentos de credenciales		
Credenciales-antiguas	M	8.4.1.2.1.1
Credenciales-nuevas	M	8.4.1.2.1.2

8.4.1.2.1.1 Credenciales-antiguas

Este argumento contiene las **credenciales** vigentes (antiguas) del invocador de la operación-abstracta en poder del ejecutor de la operación-abstracta. Debe ser generado por el invocador de la operación-abstracta.

Si se utiliza únicamente una autenticación-simple, las **credenciales** incluyen una **contraseña** simple asociada al **nombre-usuario**, o al **nombre-MTA** del invocador.

8.4.1.2.1.2 Credenciales-nuevas

Este argumento contiene las nuevas **credenciales** propuestas del invocador de la operación-abstracta que debe poseer el ejecutor de la operación-abstracta. Debe ser generado por el invocador de la operación-abstracta.

La política de seguridad en rigor puede limitar el tipo de **nuevas-credenciales**.

8.4.1.2.2 Resultados

La operación-abstracta cambio-credenciales devuelve un resultado vacío como indicación del éxito.

8.4.1.2.3 Errores-abstractos

El cuadro 26 enumera los errores-abstractos que pueden interrumpir la operación-abstracta de cambio-credenciales y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro 26 – Errores-abstractos de cambio de credenciales

Error-abstracto	Cláusula
Credenciales-nuevas-inaceptables	8.4.2.2
Credenciales-antiguas-incorrectamente-especificadas	8.4.2.3
Error-de-vinculación-distante	8.2.2.10
Error-seguridad	8.4.2.4

8.4.2 Errores-abstractos

En esta cláusula, se definen los siguientes errores-abstractos del puerto-administración:

a) registro-rechazado;

b) credenciales-nuevas-inaceptables;

c) credenciales-antiguas-incorrectamente-especificadas;

d) error-seguridad.

8.4.2.1 Registro-rechazado

El error-abstracto registro-rechazado notifica que no pueden registrarse los parámetros pedidos porque uno o más están indebidamente especificados.

El error-abstracto registro-rechazado no tiene parámetros.

8.4.2.2 Credenciales-nuevas-inaceptables

El error-abstracto credenciales-nuevas-inaceptables notifica que no pueden cambiarse las **credenciales** porque las **credenciales-nuevas** son inaceptables.

El error-abstracto credenciales-nuevas-inaceptables no tiene parámetros.

8.4.2.3 Credenciales-antiguas-incorrectamente-especificadas

El error-abstracto credenciales-antiguas-incorrectamente-especificadas notifica que no pueden cambiarse las **credenciales** porque las **credenciales** (**antiguas**) vigentes están incorrectamente especificadas.

El error-abstracto-credenciales-antiguas-incorrectamente-especificadas no tiene parámetros.

8.4.2.4 Error-seguridad

El error-abstracto error-seguridad informa que la operación-abstracta solicitada no puede ser proporcionada por el MTS o el usuario-MTS porque se violaría la política-seguridad en vigor.

El error-abstracto error seguridad tiene los siguientes parámetros:

problema-seguridad: un identificador para la causa de la violación de la política-seguridad.

El parámetro problema-seguridad puede tener uno de los siguientes valores para la operación-abstracta registro:

registro-etiqueta-seguridad-usuario-prohibido: no se permite al usuario utilizar la operación registro para cambiar etiquetas de seguridad;

actualización-etiqueta-seguridad-no-válida: el valor propuesto de la etiqueta-seguridad-entregable no es aceptable para la política-seguridad;

ausencia-parámetro-obligatorio: está ausente un elemento de seguridad obligatorio para cumplir la política-seguridad en vigor;

fallo-seguridad-operación: la operación registro fracasó por motivos de seguridad;

redireccionamiento prohibido: la política-seguridad prohíbe el registro de redireccionamientos-asignados-al-destinatario;

nombre-destinatario-alternativo-rechazado: el destinatario alternativo solicitado es inaceptable por motivos de seguridad;

violación-política-seguridad: la política-seguridad es violada;

rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados;

actualización-etiqueta-seguridad-no-autorizada: el usuario no es autorizado por la política-seguridad a actualizar la etiqueta-seguridad-entregable;

nombre-usuario-no-autorizado: el nuevo valor propuesto de nombre-usuario es inadmisible, por motivos de seguridad.

El parámetro problema-seguridad puede tener uno de los siguientes valores para la operación cambio-credenciales:

fallo-seguridad-operación: la operación cambio-credenciales fracasó por motivos de seguridad;

violación-política-seguridad: la política-seguridad es violada;

rechazo-servicios-seguridad: los servicios de seguridad solicitados no pueden ser soportados.

8.5 Tipos comunes de parámetros

En esta cláusula se define un cierto número de tipos comunes de parámetros del servicio abstracto MTS.

8.5.1 Identificador-MTS

El MTS asigna **identificadores-MTS** para distinguir entre los mensajes y sondas del servicio abstracto MTS y entre los mensajes, sondas e informes dentro del MTS.

El **identificador-MTS** asignado a un mensaje en un puerto-remisión (**identificador-remisión-mensaje**) es idéntico al **identificador-mensaje** correspondiente en un puerto-transferencia y al correspondiente **identificador-entrega-mensaje** en un puerto-de-entrega. De forma similar, el **identificador-MTS** asignado a una sonda en un puerto-remisión (**identificador-remisión-sonda**) es idéntico al **identificador-sonda** correspondiente en un puerto-transferencia. Se asignan igualmente **identificadores-MTS** a los informes en los puertos-transferencias (**identificador-informe**).

Un **identificador-MTS** consta de:

un **identificador-local** asignado por el MTA, que identifica sin ambigüedad el suceso en cuestión dentro del MD;

el **identificador-dominio-global** del MD, que garantiza que el **identificador-MTS** es inequívoco a lo largo del MTS.

8.5.2 Identificador-dominio-global

Un **identificador-dominio-global** identifica inequívocamente un MD en el interior del MHS.

Se utiliza un **identificador-dominio-global** para garantizar que un **identificador-MTS** no resulta ambiguo a lo largo del MTS y para identificar la fuente de un **elemento-información-rastreo**.

En el caso de un ADMD, un **identificador-dominio-global** consta del **nombre-país** y del **nombre-dominio-administración** del MD.

En el caso de un PRMD, un **identificador-dominio-global** consta del **nombre-país** y, opcionalmente, del **nombre-dominio-administración** del ADMD asociado, más un **identificador-dominio-privado**. El **identificador-dominio-privado** es una identificación única del PRMD y puede ser idéntico al **nombre-dominio-privado** del PRMD. Como un asunto nacional, esta identificación puede ser relativa al país designado por el **nombre-país** o relativa al ADMD asociado. Si la identificación es relativa a la ADMD, estará entonces presente ese **nombre-dominio-administración.** Cuando el **nombre-dominio-administración** es opcional en el servicio abstracto, pero obligatorio en la sintaxis abstracta y no se especifica valor alguno, se codificará como un espacio (véase 18.3.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2).

NOTA – La distinción entre el **identificador-dominio-privado** y el **nombre-dominio-privado** se ha conservado para asegurar la compatibilidad con la Recomendación X.411 del CCITT (1984). A menudo serán idénticos.

8.5.3 Nombre-MTA

Un **nombre-MTA** es un identificador para un MTA que identifica unívocamente al MTA dentro del MD al que pertenece.

8.5.4 Tiempo

Se especifica un parámetro **tiempo** en términos del tiempo universal coordinado (UTC, *coordinated universal time*) y puede contener igualmente de forma opcional una desviación respecto del UTC para incorporar el tiempo local. La precisión de la hora del día es de un segundo o de un minuto según determine el generador del parámetro.

8.5.5 Nombre-OR

Un **nombre-OR** identifica al originador o destinatario de un mensaje según los principios de denominación y direccionamiento descritos en la Rec. UIT-T X.402 | ISO/CEI 10021-2.

En un puerto-remisión, un **nombre-OR** consta de una **dirección-OR**, o un **nombre-directorio** o ambos (**dirección-OR-y-o-nombre-directorio**). En todos los tipos de puerto restantes, un **nombre-OR** consta de una **dirección-OR** y, opcionalmente, un **nombre-directorio** (**dirección-OR-y-nombre-directorio-facultativo**). Un **nombre-directorio** y una **dirección-OR** pueden denominar cada uno un originador o un destinatario individual o una DL.

En la Rec. UIT-T X.501 | ISO/CEI 9594-2 se define un **nombre-directorio**. El MTS utiliza el **nombre-directorio** únicamente cuando está ausente o es no válida la **dirección-OR**.

Una **dirección-OR** consta de un cierto número de **atributos-normales** seleccionados a partir de los definidos en la Rec. UIT-T X.402 | ISO/CEI 10021-2, y opcionalmente de un cierto número de atributos definidos por el MD al cual está suscrito el originador/destinatario (**atributos-definidos-dominio**).

En la cláusula 9 de la definición de la sintaxis abstracta, los atributos normales están representados por **atributos-normales-incorporados** y por **atributos-normales-ampliación**, y los atributos definidos-dominio están representados por **atributos-definidos-dominio-incorporado** y por **atributos-definidos-dominio-ampliación**.

En la cláusula 18.5 de la Rec. UIT-T X.402 | ISO/CEI 10021-2 se especifican varias formas de **dirección-OR**. Estas formas indican qué atributos normales y definidos-dominio pueden utilizarse conjuntamente para constituir una **dirección-OR** válida.

En la cláusula 18.3 de la Rec. UIT-T X.402 | ISO/CEI 10021-2 se especifican reglas que indican los juegos de caracteres – numéricos, imprimibles y teletex de los cuales puede extraerse el valor de un determinado atributo normal, y por lo tanto se definen las combinaciones válidas de las distintas variantes de ese atributo normal en la sintaxis abstracta.

8.5.6 Tipos-información-codificada

Los **tipos-información-codificada** de un mensaje representan el tipo o tipos de información que aparecen en su **contenido**. Pueden especificarse tanto los **tipos-información-codificada** básicos como los **tipos-información-codificada** definidos externamente, en caso contrario los **tipos-información-codificada** de un mensaje están **sin-especificar**.

Los **tipos-información-codificada** básicos son aquellos definidos originalmente en la Recomendación X.411 del CCITT (1984). El tipo **desconocido** es utilizado para indicar un **tipo-información-codificada** que en este caso no está indicado por un **tipo-información-codificada** definido externamente y diferente de los tipos siguientes. El tipo **texto-ia5** (teleimpresor) se define en la Recomendación T.50 del CCITT. El tipo **facsímil-g3** se define en las Recomendaciones T.4 y T.30 del CCITT. El tipo **clase-1-g4** se define en las Recomendaciones T.5, T.6, T.400 y T.503 del CCITT. El tipo **teletex** se define en las Recomendaciones F.200, T.61 y T.60 del CCITT. El tipo **videotex** se define en las Recomendaciones T.100 y T.101 del CCITT. El tipo **documento-formatable-simple (sfd)** y el tipo **télex** se

definían en la Recomendación X.420 (1984) del CCITT (las partes de cuerpo SFD y TLX ya no se definen en ninguna Recomendación del CCITT). El tipo **modo mixto** se define en las Recomendaciones T.400 y T.501 del CCITT.

NOTA 1 – El tipo de información codificada **desconocida** se proporciona para representar **tipos-información-codificada** en subadaptaciones para sistemas de 1984 (permaneciendo presente en la ulterior elevación del nivel), así como para su utilización en casos en los que no se ha definido **tipo-información-codificada** definido externamente para un tipo de información particular.

Los **tipos-información-codificada** definidos-externamente son aquellos que no son **tipos-información-codificada** básicos.

En la cláusula 9 de la definición de la sintaxis abstracta, los **tipos-información-codificada** son la unión lógica de los **tipos-información-codificada-incorporados** y los **tipos-información-codificada-ampliados**. Estos últimos son aquellos a los cuales identificadores-objeto han sido atribuidos por una autoridad competente. Comprenden los **tipos-información-codificada** normales y definidos-privadamente.

Un **tipo-información-codificada** básico puede estar representado de manera equivalente por un bit en los **tipos-información-codificada-incorporados** o por un **tipo-información-codificada-ampliado.** El anexo A actúa de autoridad de registración para que los identificadores-objeto se empleen como registraciones de **tipo-información-codificada-ampliado** de los **tipos-información-codificada** básicos.

Un **tipo-información-codificada** definido-externamente siempre está representado por un **tipo-información-codificada-ampliado**. Otras normas definen identificadores-objeto que pueden utilizarse como **tipo-información-codificada-ampliado**.

Se definen **parámetros-no-básicos** para los **tipos-información-codificada** básicos **facsímil-g3** y **teletex**, para compatibilidad regresiva con la Recomendación X.411 (1984) del CCITT únicamente. Se recomienda que para cada combinación requerida de un **tipo-información-codificada** básica y un conjunto específico de **parámetros-no-básicos**, se defina y utilice de preferencia un **tipo-información-codificada** definida-externamente.

NOTA 2 – Es probable que se supriman los **parámetros-no-básicos** en una futura versión de esta Recomendación | Norma Internacional.

Los **parámetros-no-básicos** para **facsímil-g3** corresponden a los campos de información facsímil (FIF, *facsimile information field*) de tres – o cuatro – octetos transportados por la señal de instrucción digital (DCS, *digital command signal*) definidos en la Recomendación T.30 del CCITT. Los parámetros son **bi-dimensional**, **resolución-fina**, **longitud-ilimitada**, **longitud-b4**, **anchura-a3**, **anchura-b4** y **sin-comprensión**.

Los **parámetros-no-básicos** para **teletex** corresponden a la capacidad terminal no-básica transportada por la instrucción de comienzo de documento (CDS, *command document start*) definida en la Recomendación T.62 del CCITT. Los parámetros son: **conjuntos-caracteres-gráficos** opcionales, **conjuntos-caracteres-control**, **formatos-páginas** opcionales, **capacidades-terminal-misceláneas** facultativas, y un parámetro de **uso-privado**.

Cuando se indican **parámetros-no-básicos**, estos parámetros representan el "O" lógico de los **parámetros-no-básicos** de cada ejemplar de **tipo-información-codificada** en un **contenido** de mensaje. Así, este parámetro sirve únicamente para indicar si existe compatibilidad de **tipo-información-codificada**, o si se requiere conversión. Si se requiere conversión, se inspeccionará el **contenido** del mensaje para determinar que **parámetros-no-básicos** se aplican a cualquier ejemplo de **tipo-información-codificada**.

8.5.7 Certificado

Puede utilizarse un **certificado** para transportar una copia verificada de la clave-criptación-pública-asimétrica del sujeto del **certificado**.

Un **certificado** contiene uno o más elementos de información de certificación. Cada caso de información de certificación contiene los siguientes parámetros:

identificador-algoritmo-firma: **identificador-algoritmo** para el algoritmo utilizado por la autoridad de certificación que expidió el **certificado** para calcular la **firma**;

expedidor: **nombre-directorio** de la autoridad-certificación que expidió el certificado;

validez: fecha y hora del día antes de las cuales no deberá utilizarse el **certificado**, y una fecha y hora del día después de la cual no se debe confiar en el **certificado**;

sujeto: **nombre-directorio** del sujeto del **certificado**;

clave-pública-sujeto: las claves-criptación-públicas-asimétricas del sujeto;

algoritmo: los **identificadores-algoritmo**, asociados con una **clave-pública-sujeto**;

firma: versión asimétricamente criptada, troceada de los anteriores parámetros calculados por la autoridad de certificación que expidió el **certificado** utilizando el algoritmo identificado por el **identificador-algoritmo-firma** y la clave-criptación-secreta-asimétrica de la autoridad-certificación.

Se utilizarán certificados de la Versión 3 cuando el originador o los destinatarios tienen que certificar más de un conjunto de información pública.

Los certificados de la Versión 3 soportan una capacidad de ampliación de la información que ha de ser firmada como parte del certificado. Las ampliaciones de certificados normalizadas se definen en la Rec. UIT-T X.509 | ISO/CEI 9594-8. Las diversas ampliaciones normalizadas se pueden utilizar para indicar la finalidad de la información contenida en el certificado. Las extensiones normalizadas se resumen como sigue:

Información de clave y política: Estas ampliaciones de certificado y de CRL transportan información adicional sobre las claves, que incluye identificadores de clave para claves de sujeto y de expedidor, indicadores de la utilización deseada o restringida de la clave e indicadores de política de certificado.

Atributos de sujeto y de expedidor: Estas ampliaciones de certificado y de CRL soportan nombres alternativos, de diversas formas de nombre, para un sujeto de certificado, un expedidor de certificado o un expedidor de CRL. Estas ampliaciones pueden transportar también información de atributos adicional sobre el sujeto del certificado, para facilitar la confianza del usuario de certificado en que el sujeto de certificado es una determinada persona o entidad.

Constricciones de trayecto de certificación: Estas ampliaciones de certificado permiten que se incluyan especificaciones de constricciones en certificados-CA, es decir, certificados para CA expedidos por otros CA, con el fin de facilitar el procesamiento automatizado de trayectos de certificación cuando hay múltiples políticas de certificado. Se producen múltiples políticas de certificado cuando las políticas varían para diferentes aplicaciones en un entorno o cuando se interfunciona con entornos externos. Las constricciones pueden limitar los tipos de certificados que pueden ser emitidos por el CA del sujeto o que pueden producirse subsiguientemente en un trayecto de certificación.

Ampliaciones de CRL básica: Estas ampliaciones de CRL permiten que una CRL incluya indicaciones de motivo de revocación, prevea la suspensión temporal de un certificado e incluya números de secuencia de emisión-de-CRL para que los usuarios del certificado puedan detectar las CRL que faltan en una secuencia de un expedidor de CRL.

Puntos de distribución de CRL y CRL-delta: Estas ampliaciones de certificado y de CRL permiten dividir el conjunto completo de información de revocación de un CA en CRL distintas y combinar la información de revocación de múltiples CA en una CRL. Estas extensiones soportan también la utilización de CRL parciales que indican solamente los cambios que se han producido desde la emisión de la CRL anterior.

Las ampliaciones de **información de clave y política** pueden ser utilizadas para indicar qué certificado está asociado con qué firma digital que acompaña el mensaje, incluida la **verificación-autenticación-origen-mensaje** y la **verificación-integridad-contenido** y el **testigo-mensaje** de los distintos destinatarios.

Si el originador y un destinatario de un **certificado** son servidos por la misma autoridad-certificación, el destinatario puede utilizar la clave de criptación-pública-asimétrica de la autoridad-certificación para validar el **certificado,** y derivar la clave-criptación-pública-asimétrica del originador (**clave-pública-sujeto**).

Si el originador y un destinatario de un **certificado** son servidos por autoridades-certificación diferentes, el destinatario puede requerir un trayecto-certificación-retorno para autenticar el **certificado** del originador. Por consiguiente, el **certificado** puede incluir un **trayecto-certificación** asociado.

El **trayecto-certificación** puede comprender un **trayecto-certificación-hacia adelante** que incluye el **certificado** de la autoridad de certificación que expidió el **certificado**, junto con los certificados de todas sus autoridades-certificación superiores. El **trayecto-certificación-hacia adelante** puede incluir también los certificados de otras autoridades-certificación, certificados recíprocamente por la autoridad-certificación que expidió el **certificado**, o cualquiera de sus autoridades-certificación superiores.

Un destinatario del **certificado** puede completar el trayecto-certificación-retorno requerido entre el destinatario y el originador del **certificado** añadiendo el trayecto-certificación-inversa propio del destinatario al **trayecto-certificación-hacia adelante** suministrado por el originador, en un punto-de-confianza-común. El trayecto-certificación-inversa incluye el certificado-inverso de la autoridad-certificación del destinatario del **certificado**, junto con los certificados inversos de todas sus autoridades-certificación superiores. El trayecto-certificación-inversa puede incluir también los certificados-inversos de otras autoridades-certificación, certificados recíprocamente por la autoridad-certificación del destinatario del **certificado**, o cualquiera de sus autoridades de certificación superiores.

El trayecto-certificación-retorno así formado permite al destinatario del **certificado** validar cada certificado en el trayecto-certificación-retorno a su vez, para derivar la clave-criptación-pública-asimétrica de la autoridad-certificación que emitió el **certificado**. El destinatario puede utilizar entonces la clave-criptación-pública-asimétrica de la autoridad-certificación que expidió el **certificado** para validar el **certificado** y derivar la clave-criptación-pública-asimétrica del originador (**clave-pública-sujeto**).

La ampliación del certificado **constricciones de trayecto de certificación** permite incluir especificaciones de constricciones en certificados-CA, por lo que puede utilizarse para indicar cualesquiera restricciones o controles a la utilización del **trayecto-certificación**.

La forma de un **certificado** es definida en la Rec. UIT-T X.509 | ISO/CEI 9594-8 como el tipo de datos **certificados**.

NOTA – El término **certificado** utilizado en esta especificación difiere de la utilización del mismo término en la Rec. UIT-T X.509 | ISO/CEI 9594-8. La primera puede contener facultativamente un trayecto de certificación, mientras que la segunda no lo puede contener. El término equivalente en la Rec. UIT-T X.509 | ISO/CEI 9594-8 de **certificado** en esta especificación es **certificados** con la "s".

Cuando se ha de utilizar un **certificado** para una finalidad determinada, se utilizarán certificados de la Versión 3 (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8) para indicar la finalidad de la información contenida en el certificado.

Cuando se necesita un **certificado** para validar una firma digital específica en **verificación-integridad-contenido** o **mensaje-testigo**, se utilizarán siempre certificados de la Versión 3. La ampliación de certificado denominada **campo políticas de certificación** del certificado del originador indicará que el certificado (y el trayecto-certificación) ha de ser usado por el destinatario del mensaje para validar la firma digital específica contenida en el argumento **verificación-integridad-contenido** o **testigo-mensaje** (véase 8.2.1.1.1.28). Si todas las firmas emplean el mismo algoritmo y clave pública, sólo será necesario identificar una política dentro del **campo políticas certificación**, y en los demás casos se necesitarán identificadores de objeto distintos para cada tipo de firma.

8.5.8 Testigo

Puede utilizarse un **testigo** para transportar al destinatario del **testigo**, información relativa-seguridad protegida. El **testigo** proporciona la autenticación de la información relativa-seguridad pública, y la confidencialidad y autenticación de la información relativa-seguridad secreta.

El tipo de **testigo** se identifica mediante un **identificador-tipo-distintivo**. Esta Definición de servicio define un tipo de **testigo**: el **testigo-asimétrico**. Adiciones o futuras versiones de esta Recomendación | Norma Internacional pueden definir otros tipos de **testigo**; por ejemplo, **testigos** basados en las técnicas de criptación-simétrica.

Un **testigo-asimétrico** contiene los siguientes parámetros:

identificador-algoritmo-firma: **algoritmo-identificador** para el algoritmo utilizado por el originador del **testigo** para calcular la **firma**;

nombre-destinatario: la **dirección-OR-y/o-nombre-directorio** del destinatario-deseado del **testigo**; o, para la autenticación fuerte en una vinculación-MTA, el **nombre-MTA** y opcionalmente el **identificador-dominio-global** del MTA par (es decir, el destinatario del testigo-vinculación); o, para la autenticación fuerte en una vinculación-MTS el **nombre-MTA** y opcionalmente el **identificador-dominio-global** del MTA cuando el testigo es generado por un usuario-MTS, o la **dirección-OR-y-nombre-directorio-opcional** del usuario-MTS cuando el testigo es generado por el MTS; o, para autenticación fuerte en una vinculación-MS, la **dirección-OR-y-nombre-director-opcional** del usuario-MS (tanto si el testigo es generado por el MS como por el usuario-MS);

tiempo: fecha y hora del día en que se generó el **testigo**;

datos-firmados: información relativa-seguridad pública;

identificador-algoritmo-criptación: **identificador-algoritmo** para el algoritmo utilizado por el originador del testigo para calcular los **datos-criptados**;

datos-criptados: información relativa-seguridad secreta criptada por el originador del **testigo** utilizando el algoritmo identificado por el **identificador-algoritmo-criptada** y la clave-criptación-pública-asimétrica del destinatario-pretendido del **testigo**;

firma: versión **criptada** asimétricamente troceada de los parámetros anteriores calculada por el originador del **testigo** utilizando el algoritmo identificado por el **identificador-algoritmo-firma** y la clave-criptación-asimétrica-secreta del originador.

La forma de un **testigo** se define con más precisión en la Rec. UIT-T X.509 | ISO/CEI 9594-8.

En la definición de **testigo-asimétrico** pueden emplearse algoritmos simétricos siempre y cuando:

el algoritmo (ya sea en el **identificador-algoritmo-firma** o el **identificador-algoritmo-criptación)** se emplea para identificar un algoritmo criptográfico simétrico registrado;

la gestión de las claves simétricas (por ejemplo, distribución clave) es efectuada externamente por el MTS.

NOTA 1 – Cuando se utilizan algoritmos simétricos para los **datos-firmados**, el testigo no proporciona la comprobación de autenticación de origen del mensaje definida en la Rec. UIT-T X.402 | ISO/CEI 10021-2. El testigo sólo demuestra que el mensaje ha sido firmado por un titular de la clave simétrica (es decir, un miembro de un grupo cerrado de usuarios).

NOTA 2 – El **identificador-algoritmo-firma** y el **identificador-algoritmo-criptación** pueden definirse individualmente y, por lo tanto, puede emplearse una combinación de algoritmos simétricos y asimétricos con el testigo.

8.5.9 Etiqueta-seguridad

Pueden utilizarse las **etiquetas-seguridad** para asociar la información seguridad-pertinente con los objetos dentro del MTS.

Pueden asignarse **etiquetas-seguridad** a un objeto en línea con la política-seguridad en vigor para dicho objeto. La política-seguridad puede definir igualmente como deben utilizarse las **etiquetas-seguridad** para reforzar la política-seguridad.

Dentro del campo de aplicación de esta Definición de servicio, pueden asociarse **etiquetas-seguridad** a los mensajes, las sondas y los informes (véase 8.2.1.1.1.30), los usuarios-MTS (véase 8.4.1.1.1.3.4), los MD, los MTA y asociaciones entre un usuario-MTS y un MD (o MTA) (véase 8.1.1.1.1.4) o entre MD (o MTA) (véase 12.1.1.1.1.3). Más allá del campo de aplicación de esta Definición de servicio, una política-seguridad puede, como asunto local o mediante un acuerdo bilateral, asignar adicionalmente **etiquetas-seguridad** a otros objetos dentro del MTS (por ejemplo, rutas seguras).

Una **etiqueta-seguridad** comprende un conjunto de **atributos-seguridad**. Los **atributos- seguridad** pueden incluir un **identificador-política-seguridad**, una **clasificación-seguridad**, una **marca de privacidad**, y un conjunto de **categorías-seguridad**.

Puede utilizarse un **identificador-política-seguridad** para identificar la política-seguridad en vigor a que se refiere la **etiqueta-seguridad**.

Si está presente, una **clasificación-seguridad** puede tener una lista jerárquica de valores. La jerarquía básica de **clasificación-seguridad** se define en esta Definición de servicio pero la utilización de estos valores se define mediante la política-seguridad en vigor. Una política-seguridad puede definir igualmente valores adicionales de **clasificación-seguridad** y su posición en la jerarquía como asunto local o mediante un acuerdo bilateral. La jerarquía básica de **clasificación-seguridad** es, por orden ascendente: **sin-marcar**, **sin-clasificar**, **restringido**, **confidencial**, **secreto**, **alto secreto**.

Si existe, una **marca-privacidad** es una cadena imprimible. El contenido de la cadena imprimible puede definirse mediante una política-seguridad, que puede definir una lista de valores a utilizar o permitir la determinación por el originador de la **etiqueta-seguridad** de dicho valor. Ejemplos de marcas-privacidad son "**CONFIDENCIAL**" y "**MUY ESTRICTAMENTE CONFIDENCIAL**".

Si existe, el conjunto de **categorías-seguridad** proporciona otras restricciones dentro del contexto de una **clasificación-seguridad** y/o **marca-privacidad** típicamente sobre la base de un "necesita-saber". Las **categorías-seguridad** y sus valores pueden definirse por una política-seguridad como asunto local o mediante un acuerdo bilateral. Los ejemplos de posibles **categorías-seguridad** incluyen escritos sobre la **clasificación-seguridad** y/o la **marca-privacidad** (por ejemplo, "**PERSONAL-**", "**PLANTILLA-**", "**COMERCIAL-**", etc.), grupos-cerrados-usuarios, palabras de código, etc.

8.5.10 Identificador-algoritmo

Un **identificador-algoritmo** identifica un **algoritmo** y cualesquiera **parámetros-algoritmo** requeridos por el **algoritmo**. También deberá definir las normas de codificación ASN.1 utilizadas.

Un **identificador-algoritmo** puede extraerse del registro internacional de algoritmos o definirse mediante un acuerdo bilateral.

8.5.11 Contraseña

Una contraseña contiene una cadena IA5 o una cadena de octetos.

Cuando los octetos de un valor de cadena de octetos son la codificación, en un entorno de 8 bits, de los caracteres de un valor de cadena IA5, se considerará que no tiene importancia la elección de las representaciones de la cadena IA5 o de la cadena de octetos.

NOTA 1 – Esta regla de equivalencia no impide que una contraseña sea un valor de cadena de octetos que no sea la codificación de ningún valor de cadena IA5.

NOTA 2 – "Codificación en un entorno de 8 bits" significa que el bit más significativo de cada octeto es cero y no un bit de paridad; ésta es la codificación de los caracteres de cadena IA5 empleados en las reglas de codificación básicas de la ASN.1. Una contraseña de cadena IA5 debe tener el bit superior de cada octeto puesto a cero antes de escribirlo como el valor de un atributo de contraseña de usuario, definido en el directorio de la Rec. UIT-T X.520 | ISO/CEI 9594-6. La regla de equivalencia está concebida para facilitar la utilización de este atributo de directorio.

NOTA 3 – Cuando se emplean las reglas de codificación básicas (BER, *basic encoding rules*) de la ASN.1, dos contraseñas pueden compararse como sigue: los octetos de cada valor de contraseña se extraen de su codificación BER (que puede ser primitiva o construida); la técnica de extracción es la misma para la cadena IA5 y la cadena de octetos. Si los valores extraídos son iguales octeto por octeto, las dos contraseñas se corresponden.

9 Definición de la sintaxis abstracta del sistema de transferencia de mensajes

La sintaxis-abstracta del servicio abstracto del MTS se define en la figura 2. En el anexo C se definen aquellos aspectos de la versión de 1988 del servicio abstracto del MTS que difieren de la de 1994.

La sintaxis-abstracta del servicio abstracto del MTS se define utilizando la notación de sintaxis abstracta (ASN.1) definida en la Rec. UIT-T X.680 | ISO/CEI 8824-1, Rec. UIT-T X.681 | ISO/CEI 8824-2, Rec. UIT-T X.682 | ISO/CEI 8824-3 y Rec. UIT-T X.683 | ISO/CEI 8824-4, y los convenios de definiciones del servicio abstracto descritos en la Rec. UIT-T X.402 | ISO/CEI 10021-2, que utilizan la notación de operaciones distantes definidas en la Rec. UIT-T X.880 | ISO/CEI 13712-1.

La definición de la sintaxis-abstracta del servicio abstracto MTS tiene las siguientes partes principales:

Prólogo: declaraciones de las exportaciones desde el módulo de servicio abstracto del MTS, y de las importaciones a éste (figura 2, partes 1 y 2).

Objetos y puertos: definiciones de los objetos del MTS y del usuario-MTS, y de sus puertos-remisión, -entrega, -administración (figura 2, partes 2 y 3).

Vinculación-MTS, y desvinculación-MTS: definiciones de las operaciones vinculación-MTS y desvinculación-MTS utilizadas para establecer y liberar asociaciones entre un usuario-MTS y el MTS (figura 2, partes 3 y 4).

Puerto de remisión: definiciones de las operaciones-abstractas de puerto-remisión: remisión-mensaje, remisión-sonda, cancelación-entrega-diferida y control-remisión; y sus errores-abstractos (figura 2, partes 4 a 7).

Puerto de entrega: definiciones de las operaciones-abstractas de puerto-entrega: entrega-mensaje, entrega-informe y control-entrega; y sus errores-abstractos (figura 2, partes 7 a 9).

Puerto de administración: definiciones de las operaciones-abstractas de puerto-administración: registro y cambio-credenciales; y sus errores abstractos (figura 2, partes 9 a 11).

Sobre de remisión de mensaje: definición del sobre-remisión-mensaje (figura 2, parte 11).

Sobre de remisión de sonda: definición del sobre-remisión-sonda (figura 2, parte 12).

Sobre de entrega de mensaje: definición del sobre-entrega-mensaje (figura 2, partes 12 y 13).

Sobre de entrega de informe: definición del sobre-entrega-informe (figura 2, partes 13 y 14).

Campos de sobre: definiciones de los campos de sobre (figura 2, partes 14 a 16).

Campos de ampliación: definiciones de los campos-ampliación (figura 2, partes 17 a 22).

Tipos de parámetros comunes: definiciones de los tipos de parámetros comunes (figura 2, partes 23 a 29).

NOTA – El módulo implica ciertos cambios en el protocolo P3 definido en la Rec. X.411 (1984) del CCITT. Estos cambios se señalan en la versión inglesa mediante subrayado. Para las operaciones de control-entrega y registro, los cambios se muestran exclusivamente en el anexo C.

[NOTA – El módulo aplica limitaciones de tamaño a los tipos de datos de longitud-variable utilizando la ampliación de subtipificación SIZE de ASN.1. La violación de una restricción de tamaño constituye una violación de protocolo.]

9.1 Mecanismo de ampliación

En la figura 2 (parte 17) se indica un mecanismo para definir las ampliaciones. Cuando puedan existir ampliaciones, un conjunto de objetos de información parametrizada indica cuales son las ampliaciones definidas en esta Definición de servicio que pueden estar presentes, pero también pueden incluirse ampliaciones adicionales no definidas aquí (por ejemplo, de forma privada o mediante adiciones o versiones futuras de esta Recomendación | Norma Internacional).

NOTA 1 – La ampliación – ExtensionType (tipo de ampliación) normalizada puede identificar exclusivamente ampliaciones definidas en la Rec. UIT-T X.411 | ISO/CEI 10021-4) y en adiciones o versiones futuras de la misma.

Cada tipo de ampliación se producirá a lo sumo una vez en un conjunto de campo de ampliación (ExtensionField). El mismo tipo de ampliación puede aparecer en diferentes lugares del protocolo. Ello se aplica a la vez a las ampliaciones normalizadas y a las ampliaciones privadas.

NOTA 2 – Las ampliaciones por mensaje y por destinatario se refunden en la entrega. Ello debe tenerse en cuenta cuando se defina una ampliación privada.

9.2 Mecanismo de criticidad

Cada **campo-ampliación** definido en la figura 2 (partes 13 a 18) transporta consigo una indicación de su **criticidad** para remisión, transferencia y entrega. Los valores de **criticidad** pueden establecerse cuando se genera el **campo-ampliación**.

Se concibe el mecanismo de criticidad para permitir la transparencia controlada de funciones ampliadas. Una función no-crítica puede ignorarse, pero no será descartada salvo cuando entregue o degrade (véase el anexo B a la Rec. UIT-T X.419 | ISO/CEI 10021-6) un mensaje, mientras que una función crítica debe conocerse y realizarse correctamente para que prosigan los procedimientos normales.

NOTA – Los mensajes con funciones críticas o no-críticas pueden ser rechazados en la remisión con el error de remisión elemento-de-servicio-no-abonado cuando la función corresponde a un elemento de servicio al cual el usuario no se ha abonado, o que no está disponible para suscripción.

En general, un argumento de una operación-abstracta marcado como crítico para el tipo de puerto en cuestión debe tratarse correctamente por quién ejecuta la operación-abstracta o se debe informar del error en la forma adecuada. El invocador de la operación-abstracta debe tratar correctamente todas las funciones marcadas como críticas para este tipo de puerto.

Si la operación-abstracta es de las que informan de un resultado infructuoso, se notifica un fallo en la correcta ejecución de una función crítica mediante la devolución de un error-abstracto de función-soportada-no-soportada. Si la operación-abstracta no es de las que notifican un resultado infructuoso, debe invocarse una operación-abstracta (por ejemplo, un informe) para transportar el resultado infructuoso de la operación anterior (por ejemplo, utilizando el **código-diagnóstico-no-entrega de función-crítica-no-soportada** de un informe).

La ampliación que aparece en el resultado de una operación-abstracta no debe marcarse como crítica para el tipo de puerto en cuestión.

En el caso de **crítica-para-remisión**, el MTS deberá ejecutar correctamente los procedimientos definidos para una función marcada como **crítica-para-remisión** en una operación-abstracta de remisión-mensaje o remisión-sonda o devolverá un error-abstracto de función-crítica-no-soportada.

En el caso de **crítica-para-transferencia**, un MTA receptor deberá ejecutar correctamente los procedimientos definidos para una función en un mensaje o sonda marcado como **crítica-para-transferencia**, o deberá devolver un informe-no-entrega con el **código-diagnóstico-no-entrega** puesto en **función-crítica-no-soportada**. Un MTA incapaz de proporcionar una función marcada como **crítica-para-transferencia** en un informe debe descartar el informe (una política o acuerdo local puede exigir que esta acción sea auditada). Una ampliación marcada como **crítica-para-transferencia** que aparece como un argumento de una operación de remisión-mensaje o remisión-sonda deberá aparecer sin modificación en una operación resultante de transferencia-mensaje o transferencia-sonda en un puerto-transferencia.

En el caso de **crítica-para-entrega**, un MTA-que-entrega ejecutará correctamente los procedimientos definidos para una función marcada como **crítica-para-entrega**, o no entregará el mensaje o sonda y devolverá un informe-no-entrega con el **código-diagnóstico-no-entrega** puesto en **función-crítica-no-soportada**. Un usuario-MTS receptor ejecutará correctamente los procedimientos definidos para una función marcada como **crítica-para-entrega** o devolverá un error-abstracto de función-crítica-no-soportada. Una ampliación marcada como **crítica-para-entrega** que aparece como argumento de una operación de remisión-mensaje o remisión-sonda debe aparecer sin modificación en una operación de transferencia-mensaje o transferencia-sonda en un puerto-transferencia. Una ampliación marcada como **crítica-para-entrega** que aparece como argumento de una operación de transferencia-mensaje o transferencia-sonda debe aparecer sin modificación en cualquier operación de transferencia-mensaje o transferencia-sonda en un puerto-transferencia.

Un MTA que genera un informe no deberá copiar las funciones críticas no soportadas procedentes del sujeto en el informe. Al generar el informe un MTA deberá indicar la **criticidad** (para transferencia y/o entrega) de cualquier función soportada copiada del sujeto en el informe; la **criticidad** de una función en un informe puede ser diferente de su **criticidad** en el sujeto.

Si el MTA o usuario-MTS no puede realizar correctamente los procedimientos definidos para una función marcada como "**crítica-para-entrega**", el informe es descartado.

Los procedimientos relativos a los **campos-ampliación** y a sus indicaciones sobre la **criticidad** se definen posteriormente en la cláusula 14.

Esta Definición de servicio define mediante la notación de clase de objeto de información de ASN.1 el establecimiento recomendado de la indicación de **criticidad** de los **campos-ampliación** que debe suministrar el originador de un mensaje. El originador de un mensaje o sonda puede escoger, mensaje por mensaje, o de acuerdo con una política local (por ejemplo, una política-seguridad) fijar una indicación de **criticidad** de un campo-ampliación diferente de la definida en esta Definición de servicio, relajar o restringir aún más dicha **criticidad**.

En el cuadro 27 se identifican las posibles alternativas que se ofrecen a un MTA para todas la combinaciones de **criticidad**.

Cuadro 27 – Acciones del MTA sobre la criticidad

Crítico para			Remisión* Cláusula 14.6	Sección entrada* Cláusula 14.3.2	Entrega mensaje* Cláusula 14.7	Reduc-ción calidad +
Remisión	Transfe-rencia	Entrega				
			A, R, E	A, R	A, R, D	A, D
		x	A, R, E	A, R	A, N	A, N
	x		A, R, E	A, N	A, R, D	A, N
	x	x	A, R, E	A, N	A, N	A, N
x			A, E	A, R	A, R, D	A, D
X		x	A, E	A, R	A, N	A, N
X	x		A, E	A, N	A, R, D	A, N
X	x	x	A, E	A, N	A, N	A, N

* = Véanse las figuras 6 y 7 para esas etiquetas

\+ = Véase el anexo B a la Rec. UIT-T X.419 | ISO/CEI 10021-6

x = Bit de criticidad puesto a *crítico*

A = Actúa sobre las semánticas

D = Descarta ampliación y entrega o reduce calidad según proceda

E = Error-remisión (elemento-de-servicio-no-abonado)

N = Mensajes o sondas de no-entrega, descarta informes (función-crítica-no-soportada)

R = Retransmisión o entrega, según proceda, conservando intacta la ampliación, pero sin medidas sobre las semánticas

Figura 2 – Definición de sintaxis abstracta del servicio abstracto del MTS (Comienzo)

```
--      Figura 2 – Parte 1 de 29

MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
                     version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONNECTION-PACKAGE, CONTRACT, ERROR, OPERATION, OPERATION-PACKAGE, ROS-OBJECT-CLASS
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
        remote-operations(4)
                        informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions { joint-iso-itu-t remote-operations(4)
                        useful-definitions(7) version1(0) }

        -- MTA Abstract Service

        internal-trace-information, trace-information
                ----
                FROM MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mta-abstract-service(2) version-1999(1) }

        -- MS Abstract Service Extension

        forwarding-request
                ----
                FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
                        abstract-service(1) version-1999(1) }

        -- IPM Information Objects

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                        information-objects(2) version-1999(1) }

        -- Object Identifiers

        id-att-physicalRendition-basic, id-cp-mts-connect, id-ct-mts-access,
        id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user, id-pt-administration,
        id-pt-delivery, id-pt-submission, id-tok-asymmetricToken
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }

        -- Operation and Error Codes

        err-control-violates-registration, err-deferred-delivery-cancellation-rejected,
        err-delivery-control-violated, err-element-of-service-not-subscribed,
        err-inconsistent-request, err-message-submission-identifier-invalid,
        err-new-credentials-unacceptable, err-old-credentials-incorrectly-specified,
        err-operation-refused, err-originator-invalid, err-recipient-improperly-specified,
        err-register-rejected, err-remote-bind-error, err-security-error,
        err-submission-control-violated, err-unsupported-critical-function,
        op-cancel-deferred-delivery, op-change-credentials, op-delivery-control,
        op-message-delivery, op-message-submission, op-probe-submission, op-register,
        op-report-delivery, op-submission-control
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                        mts-access-protocol(1) version-1999(1) }
```

```
--      Figura 2 - Parte 2 de 29
```

-- Directory Definitions

```
        Name
                ----
                FROM InformationFramework { joint-iso-itu-t ds(5) module(1)
                        informationFramework(1) 3 }

        PresentationAddress
                ----
                FROM SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
                        selectedAttributeTypes(5) 3 }

        ALGORITHM, AlgorithmIdentifier, Certificates, ENCRYPTED { }, SIGNATURE { }, SIGNED { }
                ----
                FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
                        authenticationFramework(7) 3 }
```

-- Certificate Extensions

```
        CertificateAssertion
                ----
                FROM CertificateExtensions {joint-iso-itu-t ds(5) module(1)
                        certificateExtensions(26) 0 }
```

-- Upper Bounds

```
        ub-bit-options, ub-built-in-content-type, ub-built-in-encoded-information-types,
        ub-certificates, ub-common-name-length, ub-content-id-length, ub-content-length,
        ub-content-types, ub-country-name-alpha-length, ub-country-name-numeric-length,
        ub-deliverable-class, ub-diagnostic-codes, ub-dl-expansions,
        ub-domain-defined-attributes, ub-domain-defined-attribute-type-length,
        ub-domain-defined-attribute-value-length, ub-domain-name-length,
        ub-encoded-information-types, ub-extension-attributes, ub-extension-types,
        ub-e163-4-number-length, ub-e163-4-sub-address-length, ub-generation-qualifier-length,
        ub-given-name-length, ub-initials-length, ub-integer-options, ub-local-id-length,
        ub-mta-name-length, ub-mts-user-types, ub-numeric-user-id-length,
        ub-organization-name-length, ub-organizational-units,
        ub-organizational-unit-name-length, ub-orig-and-dl-expansions, ub-password-length,
        ub-pds-name-length, ub-pds-parameter-length, ub-pds-physical-address-lines,
        ub-postal-code-length, ub-privacy-mark-length, ub-queue-size, ub-reason-codes,
        ub-recipients, ub-recipient-number-for-advice-length, ub-redirections,
        ub-redirection-classes, ub-restrictions, ub-security-categories, ub-security-labels,
        ub-security-problems, ub-supplementary-info-length, ub-surname-length,
        ub-terminal-id-length, ub-tsap-id-length, ub-unformatted-address-length,
        ub-universal-generation-qualifier-length, ub-universal-given-name-length,
        ub-universal-initials-length, ub-universal-surname-length, ub-x121-address-length
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        upper-bounds(3) version-1999(1) };

        operationObject1 OPERATION ::= {LINKED  {operationObject2}}
        operationObject2 OPERATION ::= {LINKED  {operationObject3}}
        operationObject3 OPERATION ::= {LINKED  {operationObject4}}
        operationObject4 OPERATION ::= {LINKED  {...}}
```

-- Objects

```
MHS-OBJECT ::= ROS-OBJECT-CLASS

mts MHS-OBJECT ::= {
        INITIATES   { mts-forced-access-contract }
        RESPONDS    { mts-access-contract }
        ID          id-ot-mts }

mts-user MHS-OBJECT ::= {
        INITIATES   { mts-access-contract }
        RESPONDS    { mts-forced-access-contract }
        ID          id-ot-mts-user }
```

-- Contracts

```
mts-access-contract CONTRACT ::= {
        CONNECTION              mts-connect
        INITIATOR CONSUMER OF   { submission | delivery | administration }
        ID                      id-ct-mts-access }
```

```
--      Figura 2 - Parte 2 de 29

mts-forced-access-contract CONTRACT ::= {
       CONNECTION              mts-connect
       RESPONDER CONSUMER OF   { submission | delivery | administration }
       ID                      id-ct-mts-forced-access }
```

-- Figura 2 – Parte 3 de 29

-- Connection package

```
mts-connect CONNECTION-PACKAGE ::= {
       BIND        mts-bind
       UNBIND      mts-unbind
       ID          id-cp-mts-connect }
```

-- Ports

```
PORT ::= OPERATION-PACKAGE

submission PORT ::= {
       OPERATIONS      {operationObject1,...}  /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES  {message-submission | probe-submission | cancel-deferred-
delivery,...} /* This information object set has to be extensible because it is used by
Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES  {submission-control,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID                id-pt-submission}

delivery PORT ::= {
       OPERATIONS {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {delivery-control,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES {message-delivery | report-delivery,...} /* This information object
set has to be extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID id-pt-delivery }

administration PORT ::= {
       OPERATIONS {change-credentials,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {register,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES {operationObject1,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID id-pt-administration
```

-- MTS-bind and MTS-unbind

```
ABSTRACT-OPERATION ::= OPERATION

ABSTRACT-ERROR ::= ERROR

mts-bind ABSTRACT-OPERATION ::= {
       ARGUMENT    MTSBindArgument
       RESULT      MTSBindResult
       ERRORS      { mts-bind-error } }

MTSBindArgument ::=  SET {
       initiator-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       initiator-credentials [2] InitiatorCredentials,
       security-context      [3] SecurityContext OPTIONAL,
       ... ,
       extensions            [5] SET OF ExtensionField {{ MTSBindExtensions }} DEFAULT { } }

MTSBindExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

MTSBindResult ::= SET {
       responder-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       responder-credentials [2] ResponderCredentials,
       ... ,
       extensions            [3] SET OF ExtensionField {{ MTSBindResultExtensions }}
                                                                    DEFAULT { } }

MTSBindResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions
```

```
--      Figura 2 - Parte 3 de 29

mts-bind-error ABSTRACT-ERROR ::= {
       PARAMETER  INTEGER {
              busy                                    (0),
              authentication-error                    (2),
              unacceptable-dialogue-mode              (3),
              unacceptable-security-context           (4),
              inadequate-association-confidentiality (5) } (0..ub-integer-options) }

mts-unbind ABSTRACT-OPERATION ::= emptyUnbind
```

```
--      Figura 2 - Parte 4 de 29

--      Association Control Parameters

ObjectName ::= CHOICE {
       user-agent ORAddressAndOptionalDirectoryName,
       mTA [0] MTAName,
       message-store [4] ORAddressAndOptionalDirectoryName}

MessagesWaiting ::= SET {
       urgent [0] DeliveryQueue,
       normal [1] DeliveryQueue,
       non-urgent [2] DeliveryQueue }

DeliveryQueue ::= SET {
       messages [0] INTEGER (0..ub-queue-size),
       octets [1] INTEGER (0..ub-content-length) OPTIONAL }

InitiatorCredentials ::= Credentials

ResponderCredentials ::= Credentials

Credentials ::= CHOICE {
       simple Password,
       strong [0] StrongCredentials,
       ... ,
       protected [1] ProtectedPassword }

Password ::= CHOICE {
       ia5-string IA5String (SIZE (0..ub-password-length)),
       octet-string OCTET STRING (SIZE (0..ub-password-length)) }

StrongCredentials ::= SET {
       bind-token [0] Token OPTIONAL,
       certificate [1] Certificates OPTIONAL,
       ... ,
       certificate-selector [2] CertificateAssertion OPTIONAL }

ProtectedPassword ::= SET {
       signature SIGNATURE { SET {
              password Password,
              time1 [0] UTCTime OPTIONAL,
              time2 [1] UTCTime OPTIONAL,
              random1 [2] BIT STRING OPTIONAL,
              random2 [3] BIT STRING OPTIONAL } },
       time1 [0] UTCTime OPTIONAL,
       time2 [1] UTCTime OPTIONAL,
       random1 [2] BIT STRING OPTIONAL,
       random2 [3] BIT STRING OPTIONAL }

SecurityContext ::= SET SIZE (1..ub-security-labels) OF SecurityLabel

--      Submission Port

message-submission ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageSubmissionArgument
       RESULT            MessageSubmissionResult
       ERRORS            { submission-control-violated |
                           element-of-service-not-subscribed |
                           originator-invalid |
                           recipient-improperly-specified |
                           inconsistent-request |
                           security-error |
                           unsupported-critical-function |
                           remote-bind-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-submission }
```

```
--      Figura 2 – Parte 5 de 29

MessageSubmissionArgument ::= SEQUENCE {
       envelope MessageSubmissionEnvelope,
       content Content }

MessageSubmissionResult ::= SET {
       message-submission-identifier MessageSubmissionIdentifier,
       message-submission-time [0] MessageSubmissionTime,
       content-identifier ContentIdentifier OPTIONAL,
       extensions [1] SET OF ExtensionField {{ MessageSubmissionResultExtensions }}
                                                                    DEFAULT { } }

MessageSubmissionResultExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       originating-MTA-certificate |
       proof-of-submission |
       PrivateExtensions, ... }

probe-submission ABSTRACT-OPERATION ::= {
       ARGUMENT          ProbeSubmissionArgument
       RESULT            ProbeSubmissionResult
       ERRORS            { submission-control-violated |
                           element-of-service-not-subscribed |
                           originator-invalid |
                           recipient-improperly-specified |
                           inconsistent-request |
                           security-error |
                           unsupported-critical-function |
                           remote-bind-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-probe-submission }

ProbeSubmissionArgument ::= ProbeSubmissionEnvelope

ProbeSubmissionResult ::= SET {
       probe-submission-identifier ProbeSubmissionIdentifier,
       probe-submission-time [0] ProbeSubmissionTime,
       content-identifier ContentIdentifier OPTIONAL,
       extensions [1] SET OF ExtensionField {{ ProbeResultExtensions }} DEFAULT { } }

ProbeResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions,
       -- at most one instance of each extension type

cancel-deferred-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          CancelDeferredDeliveryArgument
       RESULT            CancelDeferredDeliveryResult
       ERRORS            { deferred-delivery-cancellation-rejected |
                           message-submission-identifier-invalid |
                           remote-bind-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-cancel-deferred-delivery }

CancelDeferredDeliveryArgument ::= MessageSubmissionIdentifier

CancelDeferredDeliveryResult ::= NULL

submission-control ABSTRACT-OPERATION ::= {
       ARGUMENT          SubmissionControlArgument
       RESULT            SubmissionControlResult
       ERRORS            { security-error | remote-bind-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-submission-control }

SubmissionControlArgument ::= SubmissionControls

SubmissionControlResult ::= Waiting
```

```
--      Figura 2 – Parte 6 de 29

submission-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-submission-control-violated }

element-of-service-not-subscribed ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-element-of-service-not-subscribed }

deferred-delivery-cancellation-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-deferred-delivery-cancellation-rejected }

originator-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-originator-invalid }

recipient-improperly-specified ABSTRACT-ERROR ::= {
       PARAMETER   ImproperlySpecifiedRecipients
       CODE        err-recipient-improperly-specified }

ImproperlySpecifiedRecipients ::= SEQUENCE SIZE (1..ub-recipients) OF RecipientName

message-submission-identifier-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-message-submission-identifier-invalid }

inconsistent-request ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-inconsistent-request }

security-error ABSTRACT-ERROR ::= {
       PARAMETER   SecurityProblem
       CODE        err-security-error }

SecurityProblem ::= INTEGER {
       assemby-instructions-conflict-with-security-services (0),
       authentication-problem (1),
       authentication-failure-on-subject-message (2),
       confidentiality-association-problem (3),
       decryption-failed (4),
       decryption-key-unobtainable (5),
       failure-of-proof-of-message (6),
       forbidden-user-security-label-register (7),
       incompatible-change-with-original-security-context (8),
       integrity-failure-on-subject-message (9),
       invalid-security-label (10),
       invalid-security-label-update (11),
       key-failure (12),
       mandatory-parameter-absence (13),
       operation-security-failure (14),
       redirection-prohibited (15),
       refused-alternate-recipient-name (16),
       repudiation-failure-of-message (17),
       responder-credentials-checking-problem (18),
       security-context-failure (19),
       security-context-problem (20),
       security-policy-violation (21),
       security-services-refusal (22),
       token-decryption-failed (23),
       token-error (24),
       unable-to-aggregate-security-labels (25),
       unauthorised-dl-name (26),
       unauthorised-entry-class (27),
       unauthorised-originally-intended-recipient-name (28),
       unauthorised-originator-name (29),
       unauthorised-recipient-name (30),
       unauthorised-security-label-update (31),
       unauthorised-user-name (32),
       unknown-security-label (33),
       unsupported-algorithm-identifier (34),
       unsupported-security-policy (35) } (0..ub-security-problems)

unsupported-critical-function ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-unsupported-critical-function }
```

```
--      Figura 2 - Parte 6 de 29

remote-bind-error ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-remote-bind-error }

--      Submission Port Parameters

MessageSubmissionIdentifier ::= MTSIdentifier

MessageSubmissionTime ::= Time

ProbeSubmissionIdentifier ::= MTSIdentifier

ProbeSubmissionTime ::= Time

SubmissionControls ::= Controls (WITH COMPONENTS {
       ...,
       permissible-content-types ABSENT,
       permissible-encoded-information-types ABSENT })

Waiting ::= SET {
       waiting-operations [0] Operations DEFAULT { },
       waiting-messages [1] WaitingMessages DEFAULT { },
       waiting-content-types [2] SET SIZE (0..ub-content-types) OF ContentType DEFAULT { },
       waiting-encoded-information-types EncodedInformationTypes OPTIONAL }
```

```
--      Figura 2 - Parte 7 de 29

Operations ::= BIT STRING {
       probe-submission-or-report-delivery (0),
       message-submission-or-message-delivery (1) } (SIZE (0..ub-bit-options))
       -- holding 'one', not-holding 'zero'

WaitingMessages ::= BIT STRING {
       long-content (0),
       low-priority (1),
       other-security-labels (2) } (SIZE (0..ub-bit-options))

--      Delivery Port

message-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageDeliveryArgument
       RESULT            MessageDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-delivery }

MessageDeliveryArgument ::= SEQUENCE {
       COMPONENTS OF MessageDeliveryEnvelope,
       content Content }

MessageDeliveryResult ::=  SET {
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] IMPLICIT ProofOfDelivery OPTIONAL,
       ... ,
       extensions [2] SET OF ExtensionField {{ MessageDeliveryResultExtensions }} DEFAULT { }}

MessageDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

report-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          ReportDeliveryArgument
       RESULT            ReportDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-report-delivery }

ReportDeliveryArgument ::= SET {
       COMPONENTS OF ReportDeliveryEnvelope,
       returned-content [0] Content OPTIONAL }

ReportDeliveryResult ::= CHOICE {
       empty-result NULL,
       ... ,
       extensions SET SIZE (1..MAX) OF ExtensionField {{ ReportDeliveryResultExtensions }} }

ReportDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

delivery-control ABSTRACT-OPERATION ::= {
       ARGUMENT          DeliveryControlArgument
       RESULT            DeliveryControlResult
       ERRORS            { control-violates-registration | security-error | operation-refused}
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-delivery-control }

DeliveryControlArgument ::= SET {
       COMPONENTS OF DeliveryControls,
       extensions [6] SET OF ExtensionField {{ DeliveryControlExtensions }} DEFAULT { } }

DeliveryControlExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions
```

```
--      Figura 2 – Parte 8 de 29


DeliveryControlResult ::= SET {
       COMPONENTS OF Waiting,
       extensions [6] SET OF ExtensionField {{ DeliveryControlResultExtensions }} DEFAULT { }}

DeliveryControlResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

delivery-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-delivery-control-violated }

control-violates-registration ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-control-violates-registration }

operation-refused ABSTRACT-ERROR ::= {
       PARAMETER   RefusedOperation
       CODE        err-operation-refused }

RefusedOperation ::= SET {
       refused-argument CHOICE {
              built-in-argument [1] RefusedArgument,
              refused-extension EXTENSION.&id },
       refusal-reason [2] RefusalReason }

RefusedArgument ::= INTEGER {
       user-name (0),
       user-address (1),
       deliverable-content-types (2),
       deliverable-maximum-content-length (3),
       deliverable-encoded-information-types-constraints (4),
       deliverable-security-labels (5),
       recipient-assigned-redirections (6),
       restricted-delivery (7),
       retrieve-registrations (8), -- value 9 reserved for possible future extension to Register arguments
       restrict (10),
       permissible-operations (11),
       permissible-lowest-priority (12),
       permissible-encoded-information-types (13),
       permissible-content-types (14),
       permissible-maximum-content-length (15),
       permissible-security-context (16) } (0..ub-integer-options)

RefusalReason ::= INTEGER {
       facility-unavailable (0),
       facility-not-subscribed (1),
       parameter-unacceptable (2) } (0..ub-integer-options)

--      Delivery Port Parameters

RecipientCertificate ::= Certificates

ProofOfDelivery ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfDeliveryAlgorithmIdentifier,
       delivery-time MessageDeliveryTime,
       this-recipient-name ThisRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProofOfDeliveryAlgorithmIdentifier ::= AlgorithmIdentifier

DeliveryControls ::= Controls
```

```
--      Figura 2 – Parte 9 de 29


Controls ::= SET {
       restrict [0] BOOLEAN DEFAULT TRUE,
       -- update 'TRUE', remove 'FALSE'
       permissible-operations [1] Operations OPTIONAL,
       permissible-maximum-content-length [2] ContentLength OPTIONAL,
       permissible-lowest-priority Priority OPTIONAL,
       permissible-content-types [4] ContentTypes OPTIONAL,
       permissible-encoded-information-types PermissibleEncodedInformationTypes OPTIONAL,
       permissible-security-context [5] SecurityContext OPTIONAL }

--      Note – The Tags [0], [1] and [2] are altered for the Register operation only.

PermissibleEncodedInformationTypes ::= EncodedInformationTypesConstraints

--      Administration Port

register ABSTRACT-OPERATION ::= {
       ARGUMENT          RegisterArgument
       RESULT            RegisterResult
       ERRORS            { register-rejected | remote-bind-error | operation-refused |
                           security-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }

RegisterArgument ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-class SET SIZE (1..ub-deliverable-class) OF DeliverableClass OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       redirections [3] Redirections OPTIONAL,
       restricted-delivery [4] RestrictedDelivery OPTIONAL,
       retrieve-registrations [5] RegistrationTypes OPTIONAL,
       extensions [6] SET OF ExtensionField {{ RegisterExtensions }} DEFAULT { } }

RegisterExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

RegisterResult ::= CHOICE {
       empty-result NULL,
       non-empty-result SET {
              registered-information [0] RegisterArgument (WITH COMPONENTS {
                     ... ,
                     retrieve-registrations ABSENT} ) OPTIONAL,
              extensions [1] SET OF ExtensionField {{ RegisterResultExtensions }} DEFAULT {}}}

RegisterResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

change-credentials ABSTRACT-OPERATION ::= {
       ARGUMENT          ChangeCredentialsArgument
       RESULT            NULL
       ERRORS            { new-credentials-unacceptable |
old-credentials-incorrectly-specified |
                           remote-bind-error | security-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-change-credentials }

ChangeCredentialsArgument ::= SET {
       old-credentials [0] Credentials (WITH COMPONENTS { simple }),
       new-credentials [1] Credentials (WITH COMPONENTS { simple }) }

register-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-register-rejected }

new-credentials-unacceptable ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-new-credentials-unacceptable }
```

```
--      Figura 2 - Parte 10 de 29

old-credentials-incorrectly-specified ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-old-credentials-incorrectly-specified }

--      Administration Port Parameters

UserName ::= ORAddressAndOptionalDirectoryName

UserAddress ::= CHOICE {
       x121 [0] SEQUENCE {
              x121-address NumericString (SIZE (1..ub-x121-address-length)) OPTIONAL,
              tsap-id PrintableString (SIZE (1..ub-tsap-id-length)) OPTIONAL },
       presentation [1] PSAPAddress }

PSAPAddress ::= PresentationAddress

DeliverableClass ::= MessageClass (WITH COMPONENTS  {
       ... ,
       priority ABSENT,
       objects ABSENT,
       applies-only-to ABSENT })

DefaultDeliveryControls ::= Controls (WITH COMPONENTS {
       ... ,
       restrict ABSENT,
       permissible-security-context ABSENT })

Redirections ::= SEQUENCE SIZE (1..ub-redirections) OF RecipientRedirection

RecipientRedirection ::= SET {
       redirection-classes [0] SET SIZE (1..ub-redirection-classes) OF RedirectionClass
                                                                              OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                              OPTIONAL }

RedirectionClass ::=  MessageClass

MessageClass ::= SET {
       content-types [0] ContentTypes OPTIONAL,
       maximum-content-length [1] ContentLength OPTIONAL,
       encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,
       security-labels [3] SecurityContext OPTIONAL,
       priority [4] SET OF Priority OPTIONAL,
       objects [5] ENUMERATED { messages (0), reports (1), both (2), ... } DEFAULT both,
       applies-only-to [6] SEQUENCE OF Restriction OPTIONAL, -- Not considered in the case of Reports --
       extensions [7] SET OF ExtensionField {{ MessageClassExtensions }} DEFAULT { } }

EncodedInformationTypesConstraints ::= SEQUENCE {
       unacceptable-eits           [0] ExtendedEncodedInformationTypes OPTIONAL,
       acceptable-eits             [1] ExtendedEncodedInformationTypes OPTIONAL,
       exclusively-acceptable-eits [2] ExtendedEncodedInformationTypes OPTIONAL }

MessageClassExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

RecipientAssignedAlternateRecipient ::= ORAddressAndOrDirectoryName

RestrictedDelivery ::=  SEQUENCE SIZE (1..ub-restrictions) OF Restriction

Restriction ::= SET {
       permitted BOOLEAN DEFAULT TRUE,
       source-type BIT STRING {
              originated-by (0),
              redirected-by (1),
              dl-expanded-by (2) } DEFAULT { originated-by, redirected-by, dl-expanded-by },
       source-name ExactOrPattern OPTIONAL }

ExactOrPattern ::= CHOICE {
       exact-match [0] ORName,
       pattern-match [1] ORName }
```

-- **Figura 2 – Parte 11 de 29**

```
RegistrationTypes ::=  SEQUENCE {
       standard-parameters [0] BIT STRING {
              user-name (0),
              user-address (1),
              deliverable-class (2),
              default-delivery-controls (3),
              redirections (4),
              restricted-delivery (5) } OPTIONAL,
       extensions [1] SET OF EXTENSION.&id ({ RegisterExtensions }) OPTIONAL }

-- Message Submission Envelope

MessageSubmissionEnvelope ::= SET {
       COMPONENTS OF PerMessageSubmissionFields,
       per-recipient-fields [1] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientMessageSubmissionFields }

PerMessageSubmissionFields ::= SET {
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       priority Priority DEFAULT normal,
       per-message-indicators PerMessageIndicators DEFAULT { },
       deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerMessageSubmissionExtensions }} DEFAULT { } }

PerMessageSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       latest-delivery-time |
       originator-return-address |
       originator-certificate |
       content-confidentiality-algorithm-identifier |
       message-origin-authentication-check |
       message-security-label |
       proof-of-submission-request |
       content-correlator |
       dl-exempted-recipients |
       certificate-selectors |
       multiple-originator-certificates |
       forwarding-request -- for MS Abstract Service only -- |
       PrivateExtensions, ... }

PerRecipientMessageSubmissionFields ::= SET {
       recipient-name RecipientName,
       originator-report-request [0] OriginatorReportRequest,
       explicit-conversion [1] ExplicitConversion OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerRecipientMessageSubmissionExtensions }}
              DEFAULT { } }

PerRecipientMessageSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       originator-requested-alternate-recipient |
       requested-delivery-method |
       physical-forwarding-prohibited |
       physical-forwarding-address-request |
       physical-delivery-modes |
       registered-mail-type |
       recipient-number-for-advice |
       physical-rendition-attributes |
       physical-delivery-report-request |
       message-token |
       content-integrity-check |
       proof-of-delivery-request |
       certificate-selectors-override |
       recipient-certificate |
       IPMPerRecipientEnvelopeExtensions |
       PrivateExtensions, ... }
```

```
--      Figura 2 – Parte 12 de 29

--      Probe Submission Envelope

ProbeSubmissionEnvelope ::= SET {
       COMPONENTS OF PerProbeSubmissionFields,
       per-recipient-fields [3] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientProbeSubmissionFields }

PerProbeSubmissionFields ::= SET {
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       content-length [0] ContentLength OPTIONAL,
       per-message-indicators PerMessageIndicators DEFAULT { },
       extensions [2] SET OF ExtensionField {{ PerProbeSubmissionExtensions }} DEFAULT { } }

PerProbeSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       originator-certificate |
       message-security-label |
       content-correlator |
       probe-origin-authentication-check |
       PrivateExtensions, ... }

PerRecipientProbeSubmissionFields ::= SET {
       recipient-name RecipientName,
       originator-report-request [0] OriginatorReportRequest,
       explicit-conversion [1] ExplicitConversion OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerRecipientProbeSubmissionExtensions }}
                                                                          DEFAULT { } }

PerRecipientProbeSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       originator-requested-alternate-recipient |
       requested-delivery-method |
       physical-rendition-attributes |
       PrivateExtensions, ... }

--      Message Delivery Envelope

MessageDeliveryEnvelope ::= SEQUENCE {
       message-delivery-identifier MessageDeliveryIdentifier,
       message-delivery-time MessageDeliveryTime,
       other-fields OtherMessageDeliveryFields }

OtherMessageDeliveryFields ::= SET {
       content-type DeliveredContentType,
       originator-name DeliveredOriginatorName,
       original-encoded-information-types [1] OriginalEncodedInformationTypes OPTIONAL,
       priority Priority DEFAULT normal,
       delivery-flags [2] DeliveryFlags OPTIONAL,
       other-recipient-names [3] OtherRecipientNames OPTIONAL,
       this-recipient-name [4] ThisRecipientName,
       originally-intended-recipient-name [5] OriginallyIntendedRecipientName OPTIONAL,
       converted-encoded-information-types [6] ConvertedEncodedInformationTypes OPTIONAL,
       message-submission-time [7] MessageSubmissionTime,
       content-identifier [8] ContentIdentifier OPTIONAL,
       extensions [9] SET OF ExtensionField {{ MessageDeliveryExtensions }} DEFAULT { } }
```

```
--      Figura 2 - Parte 13 de 29

MessageDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        conversion-with-loss-prohibited |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        originator-return-address |
        physical-delivery-report-request |
        originator-certificate |
        message-token |
        content-confidentiality-algorithm-identifier |
        content-integrity-check |
        message-origin-authentication-check |
        message-security-label |
        proof-of-delivery-request |
        dl-exempted-recipients |
        certificate-selectors |
        certificate-selectors-override |
        multiple-originator-certificates |
        recipient-certificate |
        IPMPerRecipientEnvelopeExtensions |
        redirection-history |
        dl-expansion-history |
        trace-information |
        internal-trace-information |
        PrivateExtensions, ... }

--      Report Delivery Envelope

ReportDeliveryEnvelope ::= SET {
        COMPONENTS OF PerReportDeliveryFields,
        per-recipient-fields SEQUENCE SIZE (1..ub-recipients) OF
                                                PerRecipientReportDeliveryFields }

PerReportDeliveryFields ::= SET {
        subject-submission-identifier SubjectSubmissionIdentifier,
        content-identifier ContentIdentifier OPTIONAL,
        content-type ContentType OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        extensions [1] SET OF ExtensionField {{ ReportDeliveryExtensions }} DEFAULT { } }

ReportDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        message-security-label |
        content-correlator |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        trace-information |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

PerRecipientReportDeliveryFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        report-type [1] ReportType,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        originally-intended-recipient-name [2] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [3] SupplementaryInformation OPTIONAL,
        extensions [4] SET OF ExtensionField {{ PerRecipientReportDeliveryExtensions }}
                                                                        DEFAULT { } }

PerRecipientReportDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }
```

```
--      Figura 2 – Parte 14 de 29

ReportType ::= CHOICE {
       delivery [0] DeliveryReport,
       non-delivery [1] NonDeliveryReport }

DeliveryReport ::= SET {
       message-delivery-time [0] MessageDeliveryTime,
       type-of-MTS-user [1] TypeOfMTSUser DEFAULT public }

NonDeliveryReport ::= SET {
       non-delivery-reason-code [0] NonDeliveryReasonCode,
       non-delivery-diagnostic-code [1] NonDeliveryDiagnosticCode OPTIONAL }

--      Envelope Fields

OriginatorName ::= ORAddressAndOrDirectoryName

DeliveredOriginatorName ::= ORAddressAndOptionalDirectoryName

OriginalEncodedInformationTypes ::= EncodedInformationTypes

ContentTypes ::= SET SIZE (1..ub-content-types) OF ContentType

ContentType ::= CHOICE {
       built-in BuiltInContentType,
       extended ExtendedContentType }

BuiltInContentType ::= [APPLICATION 6] INTEGER {
       unidentified (0),
       external (1),                -- identified by the object-identifier of the EXTERNAL content
       interpersonal-messaging-1984 (2),
       interpersonal-messaging-1988 (22),
       edi-messaging (35),
       voice-messaging (40) } (0..ub-built-in-content-type)

ExtendedContentType ::= OBJECT IDENTIFIER

DeliveredContentType ::= CHOICE {
       built-in [0] BuiltInContentType,
       extended ExtendedContentType }

ContentIdentifier ::= [APPLICATION 10] PrintableString (SIZE (1..ub-content-id-length))

PerMessageIndicators ::= [APPLICATION 8] BIT STRING {
       disclosure-of-other-recipients (0), -- disclosure-of-other-recipients-requested 'one',
                                           -- disclosure-of-other-recipients-prohibited 'zero';
                                           -- ignored for Probe-submission
       implicit-conversion-prohibited (1), -- implicit-conversion-prohibited 'one',
                                           -- implicit-conversion-allowed 'zero'
       alternate-recipient-allowed (2),            -- alternate-recipient-allowed 'one',
                                           -- alternate-recipient-prohibited 'zero'
       content-return-request (3),         -- content-return-requested 'one',
                                           -- content-return-not-requested 'zero';
                                           -- ignored for Probe-submission
       reserved (4),                       -- bit reserved by MOTIS 1986
       bit-5 (5),
       bit-6 (6),                          -- notification type-1 : bit 5 'zero' and bit 6 'one'
                                           -- notification type-2 : bit 5 'one' and bit 6 'zero'
                                           -- notification type-3 : bit 5 'one' and bit 6 'one'
                                           -- the mapping between notification type 1, 2, 3
                                           -- and the content specific notification types are defined
                                           -- in relevant content specifications
       service-message (7)                 -- the message content is for service purposes;
                                           -- it may be a notification related to a service message;
                                           -- used only by bilateral agreement -- }
       (SIZE (0..ub-bit-options))

RecipientName ::= ORAddressAndOrDirectoryName
```

```
--      Figura 2 - Parte 15 de 29

OriginatorReportRequest ::= BIT STRING {
       report (3),
       non-delivery-report (4)
       -- at most one bit shall be 'one':
       -- report bit 'one' requests a 'report';
       -- non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'zero' requests 'no-report' --  } (SIZE (0..ub-bit-options))

ExplicitConversion ::= INTEGER {
       ia5-text-to-teletex (0),
       -- values 1 to 7 are no longer defined
       ia5-text-to-g3-facsimile (8),
       ia5-text-to-g4-class-1 (9),
       ia5-text-to-videotex (10),
       teletex-to-ia5-text (11),
       teletex-to-g3-facsimile (12),
       teletex-to-g4-class-1 (13),
       teletex-to-videotex (14),
       -- value 15 is no longer defined
       videotex-to-ia5-text (16),
       videotex-to-teletex (17) } (0..ub-integer-options)

DeferredDeliveryTime ::= Time

Priority ::= [APPLICATION 7] ENUMERATED {
       normal (0),
       non-urgent  (1),
       urgent (2) }

ContentLength ::= INTEGER (0..ub-content-length)

MessageDeliveryIdentifier ::= MTSIdentifier

MessageDeliveryTime ::= Time

DeliveryFlags ::= BIT STRING {
       implicit-conversion-prohibited (1)  -- implicit-conversion-prohibited 'one',
                                           -- implicit-conversion-allowed 'zero' --  }
       (SIZE (0..ub-bit-options))

OtherRecipientNames ::= SEQUENCE SIZE (1..ub-recipients) OF OtherRecipientName

OtherRecipientName ::= ORAddressAndOptionalDirectoryName

ThisRecipientName ::= ORAddressAndOptionalDirectoryName

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName

ConvertedEncodedInformationTypes ::= EncodedInformationTypes

SubjectSubmissionIdentifier ::= MTSIdentifier

ActualRecipientName ::= ORAddressAndOrDirectoryName

TypeOfMTSUser ::= INTEGER {
       public (0),
       private (1),
       ms (2),
       dl (3),
       pdau (4),
       physical-recipient (5),
       other (6) } (0..ub-mts-user-types)
```

-- Figura 2 – Parte 16 de 29

```
NonDeliveryReasonCode ::= INTEGER {
        transfer-failure (0),
        unable-to-transfer (1),
        conversion-not-performed (2),
        physical-rendition-not-performed (3),
        physical-delivery-not-performed (4),
        restricted-delivery (5),
        directory-operation-unsuccessful (6),
        deferred-delivery-not-performed (7),
        transfer-failure-for-security-reason (8) } (0..ub-reason-codes)

NonDeliveryDiagnosticCode ::= INTEGER {
        unrecognised-OR-name (0),
        ambiguous-OR-name (1),
        mts-congestion (2),
        loop-detected (3),
        recipient-unavailable (4),
        maximum-time-expired (5),
        encoded-information-types-unsupported (6),
        content-too-long (7),
        conversion-impractical (8),
        implicit-conversion-prohibited (9),
        implicit-conversion-not-subscribed (10),
        invalid-arguments (11),
        content-syntax-error (12),
        size-constraint-violation (13),
        protocol-violation (14),
        content-type-not-supported (15),
        too-many-recipients (16),
        no-bilateral-agreement (17),
        unsupported-critical-function (18),
        conversion-with-loss-prohibited (19),
        line-too-long (20),
        page-split (21),
        pictorial-symbol-loss (22),
        punctuation-symbol-loss (23),
        alphabetic-character-loss (24),
        multiple-information-loss (25),
        recipient-reassignment-prohibited (26),
        redirection-loop-detected (27),
        dl-expansion-prohibited (28),
        no-dl-submit-permission (29),
        dl-expansion-failure (30),
        physical-rendition-attributes-not-supported (31),
        undeliverable-mail-physical-delivery-address-incorrect (32),
        undeliverable-mail-physical-delivery-office-incorrect-or-invalid (33),
        undeliverable-mail-physical-delivery-address-incomplete (34),
        undeliverable-mail-recipient-unknown (35),
        undeliverable-mail-recipient-deceased (36),
        undeliverable-mail-organization-expired (37),
        undeliverable-mail-recipient-refused-to-accept (38),
        undeliverable-mail-recipient-did-not-claim (39),
        undeliverable-mail-recipient-changed-address-permanently (40),
        undeliverable-mail-recipient-changed-address-temporarily (41),
        undeliverable-mail-recipient-changed-temporary-address (42),
        undeliverable-mail-new-address-unknown (43),
        undeliverable-mail-recipient-did-not-want-forwarding (44),
        undeliverable-mail-originator-prohibited-forwarding (45),
        secure-messaging-error (46),
        unable-to-downgrade (47),
        unable-to-complete-transfer (48),
        transfer-attempts-limit-reached (49),
        incorrect-notification-type (50),
        dl-expansion-prohibited-by-security-policy (51),
        forbidden-alternate-recipient (52),
        security-policy-violation (53),
        security-services-refusal (54),
        unauthorised-dl-member (55),
        unauthorised-dl-name (56),
        unauthorised-originally-intended-recipient-name (57),
        unauthorised-originator-name (58),
        unauthorised-recipient-name (59),
        unreliable-system (60),
        authentication-failure-on-subject-message (61),
```

```
--      Figura 2 - Parte 16 de 29

        decryption-failed (62),
        decryption-key-unobtainable (63),
        double-envelope-creation-failure (64),
        double-enveloping-message-restoring-failure (65),
        failure-of-proof-of-message (66),
        integrity-failure-on-subject-message (67),
        invalid-security-label (68),
        key-failure (69),
        mandatory-parameter-absence (70),
        operation-security-failure (71),
        repudiation-failure-of-message (72),
        security-context-failure (73),
        token-decryption-failed (74),
        token-error (75),
        unknown-security-label (76),
        unsupported-algorithm-identifier (77),
        unsupported-security-policy (78) } (0..ub-diagnostic-codes)

SupplementaryInformation ::= PrintableString (SIZE (1..ub-supplementary-info-length))
```

```
--      Figura 2 - Parte 17 de 29

--      Extension Fields

EXTENSION ::= CLASS {
       &id ExtensionType UNIQUE,
       &Type OPTIONAL,
       &absent &Type OPTIONAL,
       &recommended Criticality DEFAULT { } }
WITH SYNTAX {
       [&Type [IF ABSENT &absent],]
       [RECOMMENDED CRITICALITY &recommended,]
       IDENTIFIED BY &id }

ExtensionType ::= CHOICE {
       standard-extension [0] INTEGER (0..ub-extension-types),
       private-extension [3] OBJECT IDENTIFIER }

Criticality ::= BIT STRING {
       for-submission (0),
       for-transfer (1),
       for-delivery (2) } (SIZE (0..ub-bit-options))     -- critical 'one', non-critical 'zero'

ExtensionField {EXTENSION:ChosenFrom} ::= SEQUENCE {
       type EXTENSION.&id({ChosenFrom}),
       criticality [1] Criticality DEFAULT { },
       value [2] EXTENSION.&Type({ChosenFrom} {@type}) DEFAULT NULL:NULL }

PrivateExtensions EXTENSION ::= {
       -- Any value shall be relayed and delivered if not Critical (see Table 27)
       -- except those values whose semantics the MTA obeys which are defined to be removed when obeyed.
       -- Shall be IDENTIFIED BY ExtensionType.private-extension --  . . .  }

recipient-reassignment-prohibited EXTENSION ::= {
       RecipientReassignmentProhibited IF ABSENT recipient-reassignment-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:1 }

RecipientReassignmentProhibited ::= ENUMERATED {
       recipient-reassignment-allowed (0),
       recipient-reassignment-prohibited (1) }

originator-requested-alternate-recipient EXTENSION ::= {
       OriginatorRequestedAlternateRecipient,
       RECOMMENDED CRITICALITY {for-submission},
       IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOrDirectoryName
-- OriginatorRequestedAlternateRecipient as defined here differs from the field of the same name
-- defined in Figure 4, since on submission the OR-address need not be present, but on
-- transfer the OR-address must be present.

dl-expansion-prohibited EXTENSION ::= {
       DLExpansionProhibited IF ABSENT dl-expansion-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:3 }

DLExpansionProhibited ::= ENUMERATED {
       dl-expansion-allowed (0),
       dl-expansion-prohibited (1) }

conversion-with-loss-prohibited EXTENSION ::= {
       ConversionWithLossProhibited IF ABSENT conversion-with-loss-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:4 }
```

```
--      Figura 2 – Parte 18 de 29

ConversionWithLossProhibited ::= ENUMERATED {
       conversion-with-loss-allowed (0),
       conversion-with-loss-prohibited (1) }

latest-delivery-time EXTENSION ::= {
       LatestDeliveryTime,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:5 }

LatestDeliveryTime ::= Time

requested-delivery-method EXTENSION ::= {
       RequestedDeliveryMethod IF ABSENT { any-delivery-method },
       IDENTIFIED BY standard-extension:6 }

RequestedDeliveryMethod ::= SEQUENCE OF INTEGER { -- each different in order of preference,
                                                  -- most preferred first
       any-delivery-method (0),
       mhs-delivery (1),
       physical-delivery (2),
       telex-delivery (3),
       teletex-delivery (4),
       g3-facsimile-delivery (5),
       g4-facsimile-delivery (6),
       ia5-terminal-delivery (7),
       videotex-delivery (8),
       telephone-delivery (9) } (0..ub-integer-options)

physical-forwarding-prohibited EXTENSION ::= {
       PhysicalForwardingProhibited IF ABSENT physical-forwarding-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:7 }

PhysicalForwardingProhibited ::= ENUMERATED {
       physical-forwarding-allowed (0),
       physical-forwarding-prohibited (1) }

physical-forwarding-address-request EXTENSION ::= {
       PhysicalForwardingAddressRequest IF ABSENT physical-forwarding-address-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:8 }

PhysicalForwardingAddressRequest ::= ENUMERATED {
       physical-forwarding-address-not-requested (0),
       physical-forwarding-address-requested (1) }

physical-delivery-modes EXTENSION ::= {
       PhysicalDeliveryModes IF ABSENT ordinary-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:9 }

PhysicalDeliveryModes ::= BIT STRING {
       ordinary-mail (0),
       special-delivery (1),
       express-mail (2),
       counter-collection (3),
       counter-collection-with-telephone-advice (4),
       counter-collection-with-telex-advice (5),
       counter-collection-with-teletex-advice (6),
       bureau-fax-delivery (7)
       -- bits 0 to 6 are mutually exclusive
       -- bit 7 can be set independently of any of bits 0 to 6 -- } (SIZE (0..ub-bit-options))
```

```
--      Figura 2 - Parte 19 de 29

registered-mail-type EXTENSION ::= {
       RegisteredMailType IF ABSENT non-registered-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:10 }

RegisteredMailType ::= INTEGER {
       non-registered-mail (0),
       registered-mail (1),
       registered-mail-to-addressee-in-person (2) } (0..ub-integer-options)

recipient-number-for-advice EXTENSION ::= {
       RecipientNumberForAdvice,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:11 }

RecipientNumberForAdvice ::= TeletexString (SIZE (1..ub-recipient-number-for-advice-length))

physical-rendition-attributes EXTENSION ::= {
       PhysicalRenditionAttributes IF ABSENT id-att-physicalRendition-basic,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:12 }

PhysicalRenditionAttributes ::= OBJECT IDENTIFIER

originator-return-address EXTENSION ::= {
       OriginatorReturnAddress,
       IDENTIFIED BY standard-extension:13 }

OriginatorReturnAddress ::= ORAddress

physical-delivery-report-request EXTENSION ::= {
       PhysicalDeliveryReportRequest IF ABSENT return-of-undeliverable-mail-by-PDS,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:14 }

PhysicalDeliveryReportRequest ::= INTEGER {
       return-of-undeliverable-mail-by-PDS (0),
       return-of-notification-by-PDS (1),
       return-of-notification-by-MHS (2),
       return-of-notification-by-MHS-and-PDS (3) } (0..ub-integer-options)

originator-certificate EXTENSION ::= {
       OriginatorCertificate,
       IDENTIFIED BY standard-extension:15 }

OriginatorCertificate ::= Certificates

message-token EXTENSION ::= {
       MessageToken,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:16 }

MessageToken ::= Token

content-confidentiality-algorithm-identifier EXTENSION ::= {
       ContentConfidentialityAlgorithmIdentifier,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:17 }

ContentConfidentialityAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
--      Figura 2 - Parte 20 de 29

content-integrity-check EXTENSION ::= {
       ContentIntegrityCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:18 }

ContentIntegrityCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ContentIntegrityAlgorithmIdentifier OPTIONAL,
       content Content } }

ContentIntegrityAlgorithmIdentifier ::= AlgorithmIdentifier

message-origin-authentication-check EXTENSION ::= {
       MessageOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:19 }

MessageOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier MessageOriginAuthenticationAlgorithmIdentifier,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

MessageOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

message-security-label EXTENSION ::= {
       MessageSecurityLabel,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:20 }

MessageSecurityLabel ::= SecurityLabel

proof-of-submission-request EXTENSION ::= {
       ProofOfSubmissionRequest IF ABSENT proof-of-submission-not-requested,
       RECOMMENDED CRITICALITY {for-submission},
       IDENTIFIED BY standard-extension:21 }

ProofOfSubmissionRequest ::= ENUMERATED {
       proof-of-submission-not-requested (0),
       proof-of-submission-requested (1) }

proof-of-delivery-request EXTENSION ::= {
       ProofOfDeliveryRequest IF ABSENT proof-of-delivery-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:22 }

ProofOfDeliveryRequest ::= ENUMERATED {
       proof-of-delivery-not-requested (0),
       proof-of-delivery-requested (1) }

content-correlator EXTENSION ::= {
       ContentCorrelator,
       IDENTIFIED BY standard-extension:23 }

ContentCorrelator ::= CHOICE {
       ia5text IA5String,
       octets  OCTET STRING }

probe-origin-authentication-check EXTENSION ::= {
       ProbeOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:24 }
```

```
--      Figura 2 – Parte 21 de 29

ProbeOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProbeOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProbeOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

redirection-history EXTENSION ::= {
       RedirectionHistory,
       IDENTIFIED BY standard-extension:25 }

RedirectionHistory ::= SEQUENCE SIZE (1..ub-redirections) OF Redirection

Redirection ::= SEQUENCE {
       intended-recipient-name IntendedRecipientName,
       redirection-reason RedirectionReason }

IntendedRecipientName ::= SEQUENCE {
       intended-recipient ORAddressAndOptionalDirectoryName,
       redirection-time Time }

RedirectionReason ::= ENUMERATED {
       recipient-assigned-alternate-recipient (0),
       originator-requested-alternate-recipient (1),
       recipient-MD-assigned-alternate-recipient (2),
       -- The following values may not be supported by implementations of earlier versions of this Service Definition
       directory-look-up (3),
       alias (4),
       ... }

dl-expansion-history EXTENSION ::= {
       DLExpansionHistory,
       IDENTIFIED BY standard-extension:26 }

DLExpansionHistory ::= SEQUENCE SIZE (1..ub-dl-expansions) OF DLExpansion

DLExpansion ::= SEQUENCE {
       dl ORAddressAndOptionalDirectoryName,
       dl-expansion-time Time }

physical-forwarding-address EXTENSION ::= {
       PhysicalForwardingAddress,
       IDENTIFIED BY standard-extension:27 }

PhysicalForwardingAddress ::= ORAddressAndOptionalDirectoryName

recipient-certificate EXTENSION ::= {
       RecipientCertificate,
       IDENTIFIED BY standard-extension:28 }

proof-of-delivery EXTENSION ::= {
       ProofOfDelivery,
       IDENTIFIED BY standard-extension:29 }

originator-and-DL-expansion-history EXTENSION ::= {
       OriginatorAndDLExpansionHistory,
       IDENTIFIED BY standard-extension:30 }

OriginatorAndDLExpansionHistory ::= SEQUENCE SIZE (2..ub-orig-and-dl-expansions) OF
              OriginatorAndDLExpansion

OriginatorAndDLExpansion ::= SEQUENCE {
       originator-or-dl-name ORAddressAndOptionalDirectoryName,
       origination-or-expansion-time Time }
```

```
--      Figura 2 - Parte 22 de 29

reporting-DL-name EXTENSION ::= {
       ReportingDLName,
       IDENTIFIED BY standard-extension:31 }

ReportingDLName ::= ORAddressAndOptionalDirectoryName

reporting-MTA-certificate EXTENSION ::= {
       ReportingMTACertificate,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:32 }

ReportingMTACertificate ::= Certificates

report-origin-authentication-check EXTENSION ::= {
       ReportOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:33 }

ReportOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ReportOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL,
       per-recipient SEQUENCE SIZE (1..ub-recipients) OF PerRecipientReportFields } }

ReportOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

PerRecipientReportFields ::= SEQUENCE {
       actual-recipient-name ActualRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       report-type CHOICE {
              delivery [0] PerRecipientDeliveryReportFields,
              non-delivery [1] PerRecipientNonDeliveryReportFields } }

PerRecipientDeliveryReportFields ::= SEQUENCE {
       message-delivery-time MessageDeliveryTime,
       type-of-MTS-user TypeOfMTSUser,
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] ProofOfDelivery OPTIONAL }

PerRecipientNonDeliveryReportFields ::= SEQUENCE {
       non-delivery-reason-code NonDeliveryReasonCode,
       non-delivery-diagnostic-code NonDeliveryDiagnosticCode OPTIONAL }

originating-MTA-certificate EXTENSION ::= {
       OriginatingMTACertificate,
       IDENTIFIED BY standard-extension:34 }

OriginatingMTACertificate ::= Certificates

proof-of-submission EXTENSION ::= {
       ProofOfSubmission,
       IDENTIFIED BY standard-extension:35 }

ProofOfSubmission ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfSubmissionAlgorithmIdentifier,
       message-submission-envelope MessageSubmissionEnvelope,
       content Content,
       message-submission-identifier MessageSubmissionIdentifier,
       message-submission-time MessageSubmissionTime } }

ProofOfSubmissionAlgorithmIdentifier ::= AlgorithmIdentifier

reporting-MTA-name EXTENSION ::= {
       ReportingMTAName,
       IDENTIFIED BY standard-extension:39 }

ReportingMTAName ::= SEQUENCE {
       domain GlobalDomainIdentifier,
       mta-name MTAName,
       mta-directory-name [0] Name OPTIONAL }
```

```
--      Figura 2 – Parte 22 de 29

multiple-originator-certificates EXTENSION ::= {
       ExtendedCertificates,
       IDENTIFIED BY standard-extension:40 }

ExtendedCertificates ::= SET SIZE (1..ub-certificates) OF ExtendedCertificate

ExtendedCertificate ::= CHOICE {
       directory-entry [0] Name,   -- Name of a Directory entry where the certificate can be found
       certificate [1] Certificates}

dl-exempted-recipients EXTENSION ::= {
       DLExemptedRecipients,
       IDENTIFIED BY standard-extension:42 }

DLExemptedRecipients ::= SET OF ORAddressAndOrDirectoryName

certificate-selectors EXTENSION ::= {
       CertificateSelectors,
       IDENTIFIED BY standard-extension:45 }

CertificateSelectors ::= SET {
       encryption-recipient           [0] CertificateAssertion OPTIONAL,
       encryption-originator          [1] CertificateAssertion OPTIONAL,
       content-integrity-check        [2] CertificateAssertion OPTIONAL,
       token-signature                [3] CertificateAssertion OPTIONAL,
       message-origin-authentication  [4] CertificateAssertion OPTIONAL}

certificate-selectors-override EXTENSION ::= {
       CertificateSelectors (WITH COMPONENTS{...,
              message-origin-authentication ABSENT}),
       IDENTIFIED BY standard-extension:46 }

-- Some standard-extensions are defined elsewhere:
--       36 (forwarding-request) in ITU-T Rec. X.413 | ISO/IEC 10021-5;
--       37 (trace-information), and 38 (internal-trace-information) in Figure 4;
--       41 (blind-copy-recipients), 43 (body-part-encryption-token), and 44 (forwarded-content-token) in
--              ITU-T Rec. X.420 | ISO/IEC 10021-7
```

```
--      Figura 2 – Parte 23 de 29

--      Common Parameter Types

Content ::= OCTET STRING            -- when the content-type has the integer value external, the value of the
                                    -- content octet string is the ASN.1 encoding of the external-content;
                                    -- an external-content is a data type EXTERNAL

MTSIdentifier ::= [APPLICATION 4] SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       local-identifier LocalIdentifier }

LocalIdentifier ::= IA5String (SIZE (1..ub-local-id-length))

GlobalDomainIdentifier ::= [APPLICATION 3] SEQUENCE {
       country-name CountryName,
       administration-domain-name AdministrationDomainName,
       private-domain-identifier PrivateDomainIdentifier OPTIONAL }

PrivateDomainIdentifier ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

MTAName ::= IA5String (SIZE (1..ub-mta-name-length))

Time ::= UTCTime

--      OR Names

ORAddressAndOrDirectoryName ::= ORName

ORAddressAndOptionalDirectoryName ::= ORName

ORName ::= [APPLICATION 0] SEQUENCE {
       -- address -- COMPONENTS OF ORAddress,
       directory-name [0] Name OPTIONAL }

ORAddress ::= SEQUENCE {
       built-in-standard-attributes BuiltInStandardAttributes,
       built-in-domain-defined-attributes BuiltInDomainDefinedAttributes OPTIONAL,
       -- see also teletex-domain-defined-attributes
       extension-attributes ExtensionAttributes OPTIONAL }

--      The OR-address is semantically absent from the OR-name if the built-in-standard-attribute
--      sequence is empty and the built-in-domain-defined-attributes and extension-attributes are both omitted.

--      Built-in Standard Attributes

BuiltInStandardAttributes ::= SEQUENCE {
       country-name CountryName OPTIONAL,
       administration-domain-name AdministrationDomainName OPTIONAL,
       network-address [0] NetworkAddress OPTIONAL,
       -- see also extended-network-address
       terminal-identifier [1] TerminalIdentifier OPTIONAL,
       private-domain-name [2] PrivateDomainName OPTIONAL,
       organization-name [3] OrganizationName OPTIONAL,
       -- see also teletex-organization-name
       numeric-user-identifier [4] NumericUserIdentifier OPTIONAL,
       personal-name [5] PersonalName OPTIONAL,
       -- see also teletex-personal-name
       organizational-unit-names [6] OrganizationalUnitNames OPTIONAL
       -- see also teletex-organizational-unit-names -- }
```

```
--      Figura 2 – Parte 24 de 29

CountryName ::= [APPLICATION 1] CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
       numeric NumericString (SIZE (0..ub-domain-name-length)),
       printable PrintableString (SIZE (0..ub-domain-name-length)) }

NetworkAddress ::= X121Address
-- see also extended-network-address

X121Address ::= NumericString (SIZE (1..ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE (1..ub-terminal-id-length))

PrivateDomainName ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

OrganizationName ::= PrintableString (SIZE (1..ub-organization-name-length))
-- see also teletex-organization-name

NumericUserIdentifier ::= NumericString (SIZE (1..ub-numeric-user-id-length))

PersonalName ::= SET {
       surname [0] PrintableString (SIZE (1..ub-surname-length)),
       given-name [1] PrintableString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] PrintableString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] PrintableString (SIZE (1..ub-generation-qualifier-length))
                                                                          OPTIONAL}
-- see also teletex-personal-name

OrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
                                                          OrganizationalUnitName
-- see also teletex-organizational-unit-names

OrganizationalUnitName ::= PrintableString (SIZE (1..ub-organizational-unit-name-length))

--      Built-in Domain-defined Attributes

BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
                                    BuiltInDomainDefinedAttribute

BuiltInDomainDefinedAttribute ::= SEQUENCE {
       type PrintableString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value PrintableString (SIZE (1..ub-domain-defined-attribute-value-length)) }

--      Extension Attributes

ExtensionAttributes ::= SET SIZE (1..ub-extension-attributes) OF ExtensionAttribute

ExtensionAttribute ::= SEQUENCE {
       extension-attribute-type [0] EXTENSION-ATTRIBUTE.&id ({ExtensionAttributeTable}),
       extension-attribute-value [1] EXTENSION-ATTRIBUTE.&Type ({ExtensionAttributeTable}
                                                          {@extension-attribute-type}) }

EXTENSION-ATTRIBUTE ::= CLASS {
       &id    INTEGER (0..ub-extension-attributes) UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```

```
--      Figura 2 - Parte 25 de 29

ExtensionAttributeTable EXTENSION-ATTRIBUTE ::= {
       common-name |
       teletex-common-name |
       universal-common-name |
       teletex-organization-name |
       universal-organization-name |
       teletex-personal-name |
       universal-personal-name |
       teletex-organizational-unit-names |
       universal-organizational-unit-names |
       teletex-domain-defined-attributes |
       universal-domain-defined-attributes |
       pds-name |
       physical-delivery-country-name |
       postal-code |
       physical-delivery-office-name |
       universal-physical-delivery-office-name |
       physical-delivery-office-number |
       universal-physical-delivery-office-number |
       extension-OR-address-components |
       universal-extension-OR-address-components |
       physical-delivery-personal-name |
       universal-physical-delivery-personal-name |
       physical-delivery-organization-name |
       universal-physical-delivery-organization-name |
       extension-physical-delivery-address-components |
       universal-extension-physical-delivery-address-components |
       unformatted-postal-address |
       universal-unformatted-postal-address |
       street-address |
       universal-street-address |
       post-office-box-address |
       universal-post-office-box-address |
       poste-restante-address |
       universal-poste-restante-address |
       unique-postal-name |
       universal-unique-postal-name |
       local-postal-attributes |
       universal-local-postal-attributes |
       extended-network-address |
       terminal-type }

--      Extension Standard Attributes

common-name EXTENSION-ATTRIBUTE ::= {CommonName IDENTIFIED BY 1}

CommonName ::= PrintableString (SIZE (1..ub-common-name-length))

teletex-common-name EXTENSION-ATTRIBUTE ::= {TeletexCommonName IDENTIFIED BY 2}

TeletexCommonName ::= TeletexString (SIZE (1..ub-common-name-length))

universal-common-name EXTENSION-ATTRIBUTE ::= {UniversalCommonName IDENTIFIED BY 24}

UniversalCommonName ::= UniversalOrBMPString {ub-common-name-length}

teletex-organization-name EXTENSION-ATTRIBUTE ::= {TeletexOrganizationName IDENTIFIED BY 3}

TeletexOrganizationName ::= TeletexString (SIZE (1..ub-organization-name-length))

universal-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationName IDENTIFIED BY 25}

UniversalOrganizationName ::= UniversalOrBMPString {ub-organization-name-length}

teletex-personal-name EXTENSION-ATTRIBUTE ::= {TeletexPersonalName IDENTIFIED BY 4}

TeletexPersonalName ::= SET {
       surname [0] TeletexString (SIZE (1..ub-surname-length)),
       given-name [1] TeletexString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] TeletexString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] TeletexString (SIZE (1..ub-generation-qualifier-length))
                                                                              OPTIONAL }
```

```
--      Figura 2 – Parte 25 de 29

universal-personal-name EXTENSION-ATTRIBUTE ::= {UniversalPersonalName IDENTIFIED BY 26}

UniversalPersonalName ::= SET {
       surname [0] UniversalOrBMPString {ub-universal-surname-length},
       --      If a language is specified within surname, then that language applies to each of the following
       --      optional components unless the component specifies another language.
       given-name [1] UniversalOrBMPString {ub-universal-given-name-length} OPTIONAL,
       initials [2] UniversalOrBMPString {ub-universal-initials-length} OPTIONAL,
       generation-qualifier [3]
              UniversalOrBMPString {ub-universal-generation-qualifier-length} OPTIONAL }

teletex-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {TeletexOrganizationalUnitNames IDENTIFIED BY 5}

TeletexOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       TeletexOrganizationalUnitName

TeletexOrganizationalUnitName ::= TeletexString (SIZE (1..ub-organizational-unit-name-length))

universal-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationalUnitNames IDENTIFIED BY 27}

UniversalOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       UniversalOrganizationalUnitName
       --      If a unit name specifies a language, then that language applies to subordinate unit names unless
       --      the subordinate specifies another language.

UniversalOrganizationalUnitName ::= UniversalOrBMPString {ub-organizational-unit-name-length}

UniversalOrBMPString{INTEGER:ub-string-length} ::= SET {
       character-encoding CHOICE {
              two-octets BMPString (SIZE(1..ub-string-length)),
              four-octets UniversalString (SIZE(1..ub-string-length)) },
       iso-639-language-code PrintableString (SIZE(2|5)) OPTIONAL }

pds-name EXTENSION-ATTRIBUTE ::= {PDSName IDENTIFIED BY 7}

PDSName ::= PrintableString (SIZE (1..ub-pds-name-length))

physical-delivery-country-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryCountryName IDENTIFIED BY 8}
```

```
--      Figura 2 - Parte 26 de 29

PhysicalDeliveryCountryName ::= CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

postal-code EXTENSION-ATTRIBUTE ::= {PostalCode IDENTIFIED BY 9}

PostalCode ::= CHOICE {
       numeric-code NumericString (SIZE (1..ub-postal-code-length)),
       printable-code PrintableString (SIZE (1..ub-postal-code-length)) }

physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeName IDENTIFIED BY 10}

PhysicalDeliveryOfficeName ::= PDSParameter

universal-physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeName IDENTIFIED BY 29}

UniversalPhysicalDeliveryOfficeName ::= UniversalPDSParameter

physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeNumber IDENTIFIED BY 11}

PhysicalDeliveryOfficeNumber ::= PDSParameter

universal-physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeNumber IDENTIFIED BY 30}

UniversalPhysicalDeliveryOfficeNumber ::= UniversalPDSParameter

extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionORAddressComponents IDENTIFIED BY 12}

ExtensionORAddressComponents ::= PDSParameter

universal-extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionORAddressComponents IDENTIFIED BY 31}

UniversalExtensionORAddressComponents ::= UniversalPDSParameter

physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryPersonalName IDENTIFIED BY 13}

PhysicalDeliveryPersonalName ::= PDSParameter

universal-physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryPersonalName IDENTIFIED BY 32}

UniversalPhysicalDeliveryPersonalName ::= UniversalPDSParameter

physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOrganizationName IDENTIFIED BY 14}

PhysicalDeliveryOrganizationName ::= PDSParameter

universal-physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOrganizationName IDENTIFIED BY 33}

UniversalPhysicalDeliveryOrganizationName ::= UniversalPDSParameter

extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 15}

ExtensionPhysicalDeliveryAddressComponents ::= PDSParameter

universal-extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 34}

UniversalExtensionPhysicalDeliveryAddressComponents ::= UniversalPDSParameter
```

```
--      Figura 2 - Parte 26 de 29

unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UnformattedPostalAddress IDENTIFIED BY 16}

UnformattedPostalAddress ::= SET {
       printable-address SEQUENCE SIZE (1..ub-pds-physical-address-lines) OF
              PrintableString (SIZE (1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE (1..ub-unformatted-address-length)) OPTIONAL }

universal-unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UniversalUnformattedPostalAddress IDENTIFIED BY 35}

UniversalUnformattedPostalAddress ::= UniversalOrBMPString {ub-unformatted-address-length}

street-address EXTENSION-ATTRIBUTE ::= {StreetAddress IDENTIFIED BY 17}

StreetAddress ::= PDSParameter

universal-street-address EXTENSION-ATTRIBUTE ::= {UniversalStreetAddress IDENTIFIED BY 36}

UniversalStreetAddress ::= UniversalPDSParameter

post-office-box-address EXTENSION-ATTRIBUTE ::= {PostOfficeBoxAddress IDENTIFIED BY 18}

PostOfficeBoxAddress ::= PDSParameter

universal-post-office-box-address EXTENSION-ATTRIBUTE ::=
       {UniversalPostOfficeBoxAddress IDENTIFIED BY 37}

UniversalPostOfficeBoxAddress ::= UniversalPDSParameter

poste-restante-address EXTENSION-ATTRIBUTE ::= {PosteRestanteAddress IDENTIFIED BY 19}

PosteRestanteAddress ::= PDSParameter

universal-poste-restante-address EXTENSION-ATTRIBUTE ::=
       {UniversalPosteRestanteAddress IDENTIFIED BY 38}

UniversalPosteRestanteAddress ::= UniversalPDSParameter

unique-postal-name EXTENSION-ATTRIBUTE ::= {UniquePostalName IDENTIFIED BY 20}

UniquePostalName ::= PDSParameter

universal-unique-postal-name EXTENSION-ATTRIBUTE ::=
       {UniversalUniquePostalName IDENTIFIED BY 39}

UniversalUniquePostalName ::= UniversalPDSParameter

local-postal-attributes EXTENSION-ATTRIBUTE ::= {LocalPostalAttributes IDENTIFIED BY 21}

LocalPostalAttributes ::= PDSParameter
```

-- Figura 2 – Parte 27 de 29

```
universal-local-postal-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalLocalPostalAttributes IDENTIFIED BY 40}

UniversalLocalPostalAttributes ::= UniversalPDSParameter

PDSParameter ::= SET {
       printable-string PrintableString (SIZE(1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE(1..ub-pds-parameter-length)) OPTIONAL }

UniversalPDSParameter ::= UniversalOrBMPString {ub-pds-parameter-length}

extended-network-address EXTENSION-ATTRIBUTE ::= {ExtendedNetworkAddress IDENTIFIED BY 22}

ExtendedNetworkAddress ::= CHOICE {
       e163-4-address SEQUENCE {
              number [0] NumericString (SIZE (1..ub-e163-4-number-length)),
              sub-address [1] NumericString (SIZE (1..ub-e163-4-sub-address-length))
                                                                          OPTIONAL },
       psap-address [0] PresentationAddress }

terminal-type EXTENSION-ATTRIBUTE ::= {TerminalType IDENTIFIED BY 23}

TerminalType ::= INTEGER {
       telex (3),
       teletex (4),
       g3-facsimile (5),
       g4-facsimile (6),
       ia5-terminal (7),
       videotex (8) } (0..ub-integer-options)

-- Extension Domain-defined Attributes

teletex-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {TeletexDomainDefinedAttributes IDENTIFIED BY 6}

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       TeletexDomainDefinedAttribute

TeletexDomainDefinedAttribute ::= SEQUENCE {
       type TeletexString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value TeletexString (SIZE (1..ub-domain-defined-attribute-value-length)) }

universal-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalDomainDefinedAttributes IDENTIFIED BY 28}

UniversalDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       UniversalDomainDefinedAttribute

UniversalDomainDefinedAttribute ::= SEQUENCE {
       type UniversalOrBMPString {ub-domain-defined-attribute-type-length},
       value UniversalOrBMPString {ub-domain-defined-attribute-value-length} }

-- Encoded Information Types

EncodedInformationTypes ::= [APPLICATION 5] SET {
       built-in-encoded-information-types [0] BuiltInEncodedInformationTypes,
       -- non-basic-parameters -- COMPONENTS OF NonBasicParameters,
       extended-encoded-information-types [4] ExtendedEncodedInformationTypes OPTIONAL }

-- Built-in Encoded Information Types

BuiltInEncodedInformationTypes ::= BIT STRING {
       unknown (0),
       ia5-text (2),
       g3-facsimile (3),
       g4-class-1 (4),
       teletex (5),
       videotex (6),
       voice (7),
       sfd (8),
       mixed-mode (9) } (SIZE (0..ub-built-in-encoded-information-types))
```

```
--      Figura 2 - Parte 27 de 29
```

-- Extended Encoded Information Types

```
ExtendedEncodedInformationTypes ::= SET SIZE (1..ub-encoded-information-types) OF
              ExtendedEncodedInformationType

ExtendedEncodedInformationType ::= OBJECT IDENTIFIER
```

-- Non-basic Parameters

```
NonBasicParameters ::= SET {
       g3-facsimile [1] G3FacsimileNonBasicParameters DEFAULT { },
       teletex [2] TeletexNonBasicParameters DEFAULT { } }
```

-- Figura 2 – Parte 28 de 29

```
G3FacsimileNonBasicParameters ::= BIT STRING {
       two-dimensional (8),                -- As defined in ITU-T Recommendation T.30
       fine-resolution (9),                --
       unlimited-length (20),              -- These bit values are chosen such that when
       b4-length (21),                     -- encoded using ASN.1 Basic Encoding Rules
       a3-width (22),                      -- the resulting octets have the same values
       b4-width (23),                      -- as for T.30 encoding
       t6-coding (25),                     --
       uncompressed (30),                  -- Trailing zero bits are not significant.
       width-middle-864-of-1728 (37),      -- It is recommended that implementations
       width-middle-1216-of-1728 (38),     -- should not encode more than 32 bits unless
       resolution-type (44),               -- higher numbered bits are non-zero.
       resolution-400x400 (45),
       resolution-300x300 (46),
       resolution-8x15 (47),
       edi (49),
       dtm (50),
       bft (51),
       mixed-mode (58),
       character-mode (60),
       twelve-bits (65),
       preferred-huffmann (66),
       full-colour (67),
       jpeg (68),
       processable-mode-26 (71) }

TeletexNonBasicParameters ::= SET {
       graphic-character-sets [0] TeletexString OPTIONAL,
       control-character-sets [1] TeletexString OPTIONAL,
       page-formats [2] OCTET STRING OPTIONAL,
       miscellaneous-terminal-capabilities [3] TeletexString OPTIONAL,
       private-use [4] OCTET STRING OPTIONAL      -- maximum ub-teletex-private-use-length octets -- }
       -- as defined in CCITT Recommendation T.62

--     Token

Token ::= SEQUENCE {
       token-type-identifier [0] TOKEN.&id ({TokensTable}),
       token [1] TOKEN.&Type ({TokensTable} {@token-type-identifier}) }

TOKEN ::= TYPE-IDENTIFIER

TokensTable TOKEN ::= { asymmetric-token, ... }

asymmetric-token TOKEN ::= {AsymmetricToken IDENTIFIED BY id-tok-asymmetricToken}

AsymmetricToken ::= SIGNED { SEQUENCE {
       signature-algorithm-identifier AlgorithmIdentifier,
       name CHOICE {
              recipient-name RecipientName,
              mta [3] SEQUENCE {
                     global-domain-identifier GlobalDomainIdentifier OPTIONAL,
                     mta-name MTAName } },
       time Time,
       signed-data [0] TokenData OPTIONAL,
       encryption-algorithm-identifier [1] AlgorithmIdentifier OPTIONAL,
       encrypted-data [2] ENCRYPTED { TokenData } OPTIONAL } }

TokenData ::= SEQUENCE {
       type [0] TOKEN-DATA.&id ({TokenDataTable}),
       value [1] TOKEN-DATA.&Type ({TokenDataTable} {@type}) }

TOKEN-DATA ::= CLASS {
       &id INTEGER UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```

```
--      Figura 2 – Parte 29 de 29

TokenDataTable TOKEN-DATA ::= {
       bind-token-signed-data |
       message-token-signed-data |
       message-token-encrypted-data |
       bind-token-encrypted-data, ... }

bind-token-signed-data TOKEN-DATA ::= {BindTokenSignedData IDENTIFIED BY 1}

BindTokenSignedData ::= RandomNumber

RandomNumber ::= BIT STRING

message-token-signed-data TOKEN-DATA ::= {MessageTokenSignedData IDENTIFIED BY 2}

MessageTokenSignedData ::= SEQUENCE {
       content-confidentiality-algorithm-identifier [0]
              ContentConfidentialityAlgorithmIdentifier OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       proof-of-delivery-request [3] ProofOfDeliveryRequest OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

message-token-encrypted-data TOKEN-DATA ::= {MessageTokenEncryptedData IDENTIFIED BY 3}

MessageTokenEncryptedData ::= SEQUENCE {
       content-confidentiality-key [0] EncryptionKey OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       content-integrity-key [3] EncryptionKey OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

EncryptionKey ::= BIT STRING

bind-token-encrypted-data TOKEN-DATA ::= {BindTokenEncryptedData IDENTIFIED BY 4}

BindTokenEncryptedData ::= EXTERNAL

--      Security Label

SecurityLabel ::= SET {
       security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
       security-classification SecurityClassification OPTIONAL,
       privacy-mark PrivacyMark OPTIONAL,
       security-categories SecurityCategories OPTIONAL }

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
       unmarked (0),
       unclassified (1),
       restricted (2),
       confidential (3),
       secret (4),
       top-secret (5) } (0..ub-integer-options)

PrivacyMark ::= PrintableString (SIZE (1..ub-privacy-mark-length))

SecurityCategories ::= SET SIZE (1..ub-security-categories) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
       type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
       value [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type}) }

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= { ... }

END     -- of MTSAbstractService
```

Figura 2 – Definición de sintaxis abstracta del servicio abstracto del MTS (fin)

SECCIÓN 3 – SERVICIO ABSTRACTO DE AGENTE DE TRANSFERENCIA DE MENSAJES

10 Modelo perfeccionado del sistema de transferencia de mensajes

En la cláusula 6 se describe el MTS como un objeto, sin referencia a su estructura interna. La presente cláusula perfecciona el modelo del MTS, y expone sus objetos constituyentes y los puertos compartidos entre ellos.

La figura 3 proporciona un modelo del MTS y revela su estructura interna.

El MTS consta de una colección de objetos agente-transferencia-mensaje (MTA), que cooperan entre sí para formar el MTS y ofrecer a sus usuarios el servicio abstracto de MTS. Los MTA realizan las funciones activas del MTS, es decir, la transferencia de mensajes, sondas e informes, generación de informes, y conversión de contenidos.

Los objetos del MTA tienen igualmente puertos, algunos de los cuales son concretamente los que resultan igualmente visibles en la frontera del objeto del MTS, es decir, puertos-remisión, puertos-entrega y puertos-administración. Sin embargo, los MTA tienen igualmente otro tipo de puerto, el puerto-transferencia, que se ocupa de la distribución del servicio abstracto del MTS entre los MTA y que no resulta visible en la frontera del objeto MTS.

El puerto-transferencia permite a un MTA transferir mensajes, sondas e informes a otro MTA. En general, puede que haya que transferir un mensaje, una sonda o un informe, un cierto número de veces entre diferentes MTA hasta alcanzar el destino deseado.

Si se dirige un mensaje a múltiples destinatarios servidos por varios MTA diferentes, debe transferirse el mensaje a través del MTS a lo largo de varios trayectos diferentes. Desde la perspectiva del MTA que transfiere dicho mensaje, se pueden alcanzar algunos destinatarios a través de un trayecto mientras que a otros se llega a través de otro distinto. En dicho MTA, se crean dos copias del mensaje, transfiriéndose cada una de ellas al próximo MTA a lo largo de su trayecto respectivo. La copia y ramificación del mensaje se repiten hasta que cada copia haya alcanzado un MTA de destino final, donde pueda entregarse el mensaje a uno o más usuarios-MTS destinatarios.

Cada MTA a lo largo de un trayecto tomado por un mensaje, es responsable de la entrega o transferencia del mensaje a un subconjunto determinado de destinatarios-especificados-originalmente. Otros MTA se encargan de la entrega o transferencia a los restantes destinatarios, utilizando copias de los mensajes creados a lo largo del camino.

Los MTA generan informes sobre la entrega o no-entrega de un mensaje dirigido a uno o más usuarios-MTS destinatarios, de conformidad con la petición del originador del mensaje y del MTA-originador. Un MTA puede generar un informe-entrega al entregar con éxito una copia de un mensaje a un usuario-MTS destinatario. Puede generar un informe-no-entrega al determinar que una copia de un mensaje resulta imposible de entregar a uno o más destinatarios, es decir, el MTA no ha podido entregar el mensaje a los usuarios-MTS destinatarios, o no puede transferir el mensaje a un MTA adyacente que tomaría la responsabilidad de entregar o transferir el mensaje ulteriormente.

Para una mayor eficacia, un MTA puede generar un informe único, combinado, que sirva para varias copias de un único mensaje con múltiples destinatarios, del cual es responsable. Pueden combinarse conjuntamente tanto los informes-entrega como los informes-no-entrega. Sin embargo, para combinar los informes de esta manera, debe realizarse la misma conversión de contenido, si ha lugar, en los mensajes de todos los destinatarios a que se refiere el informe.

Los informes que se refieren a copias del mismo mensaje con múltiples destinatarios pero que fueron generados por MTA diferentes no se combinan en ningún MTA intermedio, sino que permanecen separados.

Cuando se necesite, un MTA puede realizar una conversión de contenido. Cuando ni la petición del usuario-MTS originador, ni la del usuario-MTS destinatario prohíben la conversión, un MTA puede realizar la conversión implícita de los tipos-información-codificada de un mensaje para adaptarse a los tipos-información-codificada a los que puede recibir el usuario-MTS destinatario. El usuario-MTS originador puede solicitar explícitamente la conversión de los tipos-información-codificada específicos para un determinado usuario-MTS destinatario.

Los puertos-remisión-entrega-y-administración de un MTA que resultan igualmente visibles en la frontera del MTS se definen en la sección 2 de esta Definición de servicio. Las restantes cláusulas de esta sección definen el puerto-transferencia de un MTA, y los procedimientos realizados por los MTA para garantizar una correcta operación distribuida del MTS.

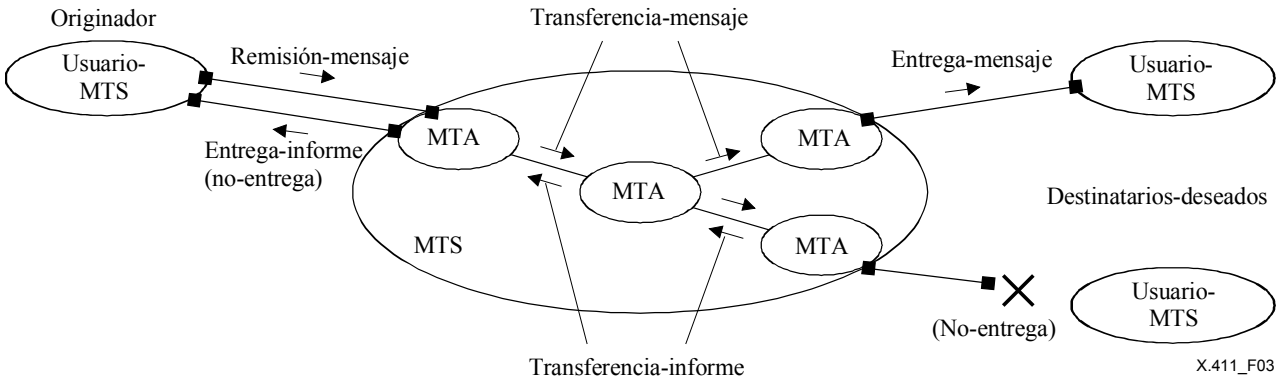


Figura 3 – Modelo perfeccionado del sistema de transferencia de mensajes

11 Visión de conjunto del servicio abstracto del agente de transferencia de mensajes

En la sección 2 se define el servicio abstracto MTS proporcionado por los puertos-remisión-entrega-y-administración de un MTA. En esta cláusula, se definen las operaciones-abstractas siguientes que proporcionan los puertos-transferencia de los MTA:

Vinculación-MTA y desvinculación-MTA

a) vinculación-MTA;

b) desvinculación-MTA.

Operaciones-abstractas de puerto de transferencia

c) transferencia-mensaje;

d) transferencia-sonda;

e) transferencia-informe.

11.1 Vinculación-MTA y desvinculación-MTA

La **vinculación-MTA** permite a un MTA establecer una asociación con otro MTA. En el contexto de una asociación establecida pueden invocarse únicamente operaciones-abstractas distintas de vinculación-MTA.

La **desvinculación-MTA** permite liberar una asociación establecida por el iniciador de la asociación.

11.2 Operaciones-abstractas de puerto de transferencia

La operación-abstracta **transferencia-mensaje** permite a un MTA transferir un mensaje a otro MTA.

La operación-abstracta **transferencia-sonda** permite a un MTA transferir una sonda a otro MTA.

La operación-abstracta **transferencia-informe** permite a un MTA transferir un informe a otro MTA.

12 Definición del servicio abstracto de agente de transferencia de mensajes

En la cláusula 8 se define el servicio abstracto de MTS. En esta cláusula, se define la semántica de los parámetros del servicio-abstracto proporcionados por los puertos-transferencia de los MTA.

En la cláusula 12.1 se define vinculación-MTA y desvinculación-MTA. La cláusula 12.2 define el puerto-transferencia. En la cláusula 12.3 se definen algunos tipos de parámetros comunes.

La sintaxis-abstracta del servicio abstracto de MTA se define en la cláusula 13.

12.1 Vinculación-MTA y desvinculación-MTA

Esta cláusula define los servicios-abstractos utilizados para establecer y liberar asociaciones entre MTA.

12.1.1 Vinculación-abstracta y desvinculación-abstracta

Esta cláusula define las siguientes vinculación-abstracta y desvinculación-abstracta:

a) vinculación-MTA;

b) desvinculación-MTA.

12.1.1.1 Vinculación-MTA

La vinculación-MTA permite a un MTA establecer una asociación con otro MTA.

La vinculación-MTA establece las **credenciales** de los MTA para interaccionar, y el **contexto-aplicación** y el **contexto-seguridad** de la asociación. Únicamente el iniciador de una asociación puede liberarla (utilizando desvinculación-MTA).

Las operaciones-abstractas diferentes de vinculación-MTA pueden invocarse únicamente en el contexto de una asociación establecida.

La finalización con éxito de vinculación-MTA significa el establecimiento de una asociación.

La interrupción de vinculación-MTA por un error-vinculación indica que la asociación no se ha establecido.

12.1.1.1.1 Argumentos

El cuadro 28 enumera los argumentos de vinculación-MTA y para cada argumento califica su presencia e indica la cláusula donde se define el argumento.

Cuadro 28 – Argumentos de vinculación-MTA

Argumento	Presencia	Cláusula
Argumentos de vinculación		
Nombre-iniciador	O	12.1.1.1.1.1
Credenciales-iniciador	O	12.1.1.1.1.2
Contexto-seguridad	O	12.1.1.1.1.3

12.1.1.1.1.1 Nombre-iniciador

Este argumento contiene un nombre para el iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

El nombre es un **nombre-MTA**.

12.1.1.1.1.2 Credenciales-iniciador

Este argumento contiene las **credenciales** del iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

Las **credenciales-iniciador** pueden utilizarse por el respondedor para autenticar la identidad del iniciador (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si se propone únicamente una autenticación-simple, las **credenciales-iniciador** constan de una **contraseña** simple asociada al **nombre-iniciador**.

Si se utiliza una autenticación-fuerte, las **credenciales-iniciador** constan de un **distintivo-vinculación-iniciador** y, opcionalmente un **certificado-iniciador** o un **selector-certificado**.

El **testigo-vinculación-iniciador** es un **testigo** generado por el iniciador de la asociación. Si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**, los **datos-firmados** incluyen un **número-aleatorio**. Los **datos-criptados** de un **testigo-asimétrico** pueden utilizarse para transportar información secreta relativa-seguridad (por ejemplo, una o más claves-criptación-simétricas) utilizadas para asegurar la asociación, o pueden estar ausentes de **testigo-vinculación-iniciador**.

En el citado **testigo-asimétrico** (véase 8.5.8) pueden emplearse algoritmos simétricos.

El **certificado-iniciador** es un **certificado** del iniciador de la asociación, generado por una fuente de confianza (por ejemplo, una autoridad-certificación) y, opcionalmente, certificados adicionales que proporcionan un trayecto-certificación para el certificado del iniciador. Puede ser suministrado por el iniciador de la asociación, si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**. El **certificado-iniciador** contendrá el **nombre-MTA** del iniciador en

un *nombre-mta* (véase A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) en el componente *otroNombre* de su campo de nombre alternativo de sujeto (véase 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), a menos que la política-de-seguridad proporcione una vinculación alternativa del certificado al MTA iniciador. El **certificado-iniciador** puede utilizarse para transportar una copia verificada de la clave-criptación-asimétrica-pública (**clave-pública-sujeto**) del iniciador de la asociación. La clave-criptación-pública-asimétrica del iniciador puede ser utilizada por el respondedor para validar el **testigo-vinculación-iniciada** y calcular los **datos-criptados** en el **testigo-vinculación-respondedor**. Si se sabe que el respondedor posee, o tiene acceso al **certificado** del iniciador (por ejemplo, a través del directorio), puede omitirse el **certificado-iniciador** cuando el iniciador tiene más de un certificado, puede proporcionarse un **selector-certificado** para identificar el certificado aplicando cualquier criterio de selección de certificado especificado para la concordancia del certificado (véase 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

12.1.1.1.1.3 Contexto-seguridad

Este argumento indica el **contexto-seguridad** que propone para funcionar el iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

El **contexto-seguridad** consta de una o más **etiquetas-seguridad** que definen la sensibilidad de las interacciones que pueden producirse entre los MTA durante la duración de la asociación, en línea con la política-seguridad en vigor. El **contexto-seguridad** debe ser uno de los autorizados por las **etiquetas-seguridad** asociadas a los MD (MTA).

Si no se establecen los **contextos-seguridad** entre los MTA, la sensibilidad de las interacciones que pueden producirse entre los MTA puede quedar a la discreción del invocador de una operación-abstracta.

12.1.1.1.2 Resultados

El cuadro 29 enumera los resultados de vinculación-MTA, y para cada resultado califica su presencia e indica la cláusula donde se define el resultado.

Cuadro 29 – Resultados de vinculación-MTA

Resultado	Presencia	Cláusula
Resultados de vinculación		
Nombre-respondedor	O	12.1.1.1.2.1
Credenciales-respondedor	O	12.1.1.1.2.2

12.1.1.1.2.1 Nombre-respondedor

Este argumento contiene un nombre para el respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

El nombre es un **nombre-MTA**.

12.1.1.1.2.2 Credenciales-respondedor

Este argumento contiene las **credenciales** del respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

Las **credenciales-respondedor** pueden utilizarse por el iniciador para autenticar la identidad del respondedor (véase la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si se propone únicamente una autenticación-simple, las **credenciales-respondedor** constan de una **contraseña** simple asociada al **nombre-respondedor.**

Si se utiliza una autenticación-fuerte, las **credenciales-respondedor** constan de un **testigo-vinculación-respondedor**, y opcionalmente, un **certificado-respondedor** o **selector-certificado**.

El **testigo-vinculación-respondedor** es un **testigo** generado por el respondedor de la asociación. El **testigo-vinculación-respondedor** debe ser del mismo tipo de **testigo** que el **testigo-vinculación-iniciador**. Si el **testigo-vinculación-respondedor** es un **testigo-asimétrico**, los **datos-firmados** incluyen un **número-aleatorio** (que puede estar relacionado con el **número-aleatorio** proporcionado en el **distintivo-vinculación-iniciador**). Los **datos-criptados** de un **testigo-asimétrico** pueden utilizarse para transportar información relativa-seguridad (por ejemplo, una o más claves-criptación-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-respondedor**.

En el citado **testigo-asimétrico** (véase 8.5.8) pueden emplearse algoritmos simétricos.

El **certificado-respondedor** es un **certificado** del respondedor de la asociación, generado por una fuente de confianza (por ejemplo, una autoridad-certificación) y, opcionalmente, certificados adicionales que proporcionan un trayecto-certificación para el certificado del respondedor. Puede proporcionarlo el respondedor de la asociación, siempre que el **testigo-vinculación-respondedor** sea un **testigo-asimétrico**. El **certificado-respondedor** contendrá el **nombre-MTA** del respondedor en un *nombre-mta* (véase A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) en el componente *otroNombre* de su campo de nombre alternativo de sujeto (véase 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), a menos que la política-de-seguridad proporcione una vinculación alternativa del certificado al MTA respondedor. El **certificado-respondedor** puede utilizarse para transportar una copia verificada de la clave-criptación-pública-asimétrica (**clave-pública-sujeto**) del respondedor de la asociación. El iniciador puede utilizar la clave-criptación-pública-asimétrica del respondedor para validar el **testigo-vinculación-respondedor**. Si se sabe que el iniciador dispone o tiene acceso al **certificado** del respondedor (por ejemplo, a través del directorio), puede omitirse el **certificado-respondedor** y, cuando el respondedor tiene más de un certificado, puede proporcionarse un **selector-certificado** para identificar el certificado aplicando cualquier criterio de selección de certificado especificado para la concordancia de certificados (véase 12.7.2 de la Rec. UIT-T 509 | ISO/CEI 9594-8).

12.1.1.1.3 Errores-vinculación

Los errores-vinculación que pueden interrumpir la operación vinculación-MTA se definen en 12.1.2.

12.1.1.2 Desvinculación-MTA

Desvinculación-MTA permite liberar una asociación establecida por el iniciador de la asociación.

12.1.1.2.1 Argumentos

El servicio desvinculación-MTA no tiene argumentos.

12.1.1.2.2 Resultados

El servicio desvinculación-MTA devuelve un resultado vacío como indicación de la liberación de la asociación.

12.1.1.2.3 Errores-desvinculación

No existen errores-desvinculación que puedan interrumpir la operación desvinculación-MTA.

12.1.2 Errores-vinculación

Esta cláusula define los siguientes errores-vinculación:

a) error-autenticación;
b) ocupado;
c) modo-diálogo-inaceptable;
d) contexto-seguridad-inaceptable.
e) confidencialidad-asociación-inadecuada.

12.1.2.1 Error-autenticación

El error-vinculación de error-autenticación notifica que no puede establecerse una asociación debido a un error de autenticación; las **credenciales** del iniciador no son aceptables o están indebidamente especificadas.

El error-vinculación de error-autenticación no tiene parámetros.

12.1.2.2 Ocupado

El error-vinculación ocupado informa que una asociación no puede establecerse porque el respondedor está ocupado.

El error-vinculación ocupado no tiene parámetros.

12.1.2.3 Modo-diálogo-inaceptable (error-vinculación)

El error-vinculación modo-diálogo-inaceptable informa que el modo-diálogo propuesto por el iniciador de la asociación resulta inaceptable para el respondedor (véase la cláusula 12 de la Rec. UIT-T X.419 | ISO/CEI 10021-6).

El error-vinculación de modo-diálogo-inaceptable no tiene parámetros.

12.1.2.4 Contexto-seguridad-inaceptable

El error-vinculación contexto-seguridad-inaceptable informa que el **contexto-seguridad** propuesto por el iniciador de la asociación resulta inaceptable para el respondedor.

El error-vinculación contexto-seguridad inaceptable no tiene parámetros.

12.1.2.5 Confidencialidad-asociación-inadecuada

El error-vinculación confidencialidad-asociación-inadecuada informa que una asociación no puede ser establecida porque la conexión subyacente no proporciona la confidencialidad necesaria.

12.2 Puerto de transferencia

Esta cláusula define las operaciones-abstractas y los errores-abstractos que se producen en un puerto-transferencia.

12.2.1 Operaciones-abstractas

Esta cláusula define las siguientes operaciones-abstractas de puerto-transferencia:

a) transferencia-mensaje;

b) transferencia-sonda;

c) transferencia-informe.

12.2.1.1 Transferencia-mensaje

La operación-abstracta transferencia-mensaje permite a un MTA transferir un mensaje a otro MTA.

12.2.1.1.1 Argumentos

El cuadro 30 enumera los argumentos de la operación-abstracta transferencia-mensaje y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

12.2.1.1.1.1 Identificador-mensaje

Este argumento consta de un **identificador-MTS** que distingue el mensaje de los restantes mensajes, sondas e informes en el interior del MTS. Deberá ser generado por el MTA-originador del mensaje, y tendrá el mismo valor que el **identificador-remisión-mensaje** suministrado al originador del mensaje cuando se remitió éste, y que el **identificador-entrega-mensaje** suministrado a los destinatarios del mensaje cuando se entrega el mensaje.

Al hacer copias de un mensaje para encaminarlo a múltiples destinatarios a través de diferentes MTA, cada copia del mensaje lleva el **identificador-mensaje** del original.

12.2.1.1.1.2 Información-bilateral-por-dominio

Este argumento contiene la información destinada a los MD que encontrará el mensaje al ser transferido a través del MTS. Puede ser generado por el MD-originador del mensaje.

Este argumento puede contener cero o más elementos, cada uno de los cuales incluye:

la **información-bilateral** destinada a un MD;

el **nombre-país**, y, facultativamente, el **nombre-dominio-administración** y, facultativamente, el **identificador-dominio-privado** del MD al que va destinado la **información-bilateral**.

12.2.1.1.1.3 Información-rastreo

Este argumento documenta las acciones realizadas sobre el mensaje (o sonda o informe) por cada MD a través del cual pasa el mensaje al ser transferido a través del MTS (véase 12.3.1). Debe ser generado por cada MD a través del cual pasa el mensaje (o sonda o informe).

Cuadro 30 – Argumentos de transferencia-mensaje

Argumento	Presencia	Cláusula
Argumentos de retransmisión		
Identificador-mensaje	M	12.2.1.1.1.1
Información-bilateral-por-dominio	C	12.2.1.1.1.2
Información-rastreo	M	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Historia-ampliación-DL	C	8.3.1.1.1.7
Argumento del originador		
Nombre-originador	M	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	M	8.2.1.1.1.2
Número-destinatario-especificado-originalmente	M	12.2.1.1.1.5
Responsabilidad	M	12.2.1.1.1.6
Ampliación-DL-prohibida	C	8.2.1.1.1.6
Revelación-de-otros-destinatarios	C	8.2.1.1.1.7
Destinatarios-exentos-DL	O	8.2.1.1.1.40
Argumentos de redireccionamiento		
Destinatario-alternativo-autorizado	C	8.2.1.1.1.3
Reasignación-destinatario-prohibida	C	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	C	8.2.1.1.1.5
Historia-redireccionamiento	C	8.3.1.1.1.5
Argumento de prioridad		
Prioridad	C	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Conversión-explícita	C	12.2.1.1.1.9
Argumentos de tiempo de entrega		
Tiempo-entrega-diferida	C	12.2.1.1.1.7
Último-tiempo-entrega	C	8.2.1.1.1.13
Argumento de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	C	8.2.1.1.1.15
Petición-dirección-envío-físico	C	8.2.1.1.1.16
Modos-entrega-física	C	8.2.1.1.1.17
Tipo-correo-certificado	C	8.2.1.1.1.18
Número-destinatario-para-aviso	C	8.2.1.1.1.19
Atributos-reproducción-física	C	8.2.1.1.1.20
Dirección-devolución-originador	C	8.2.1.1.1.21
Argumentos de petición de informe de entrega		
Petición-informe-originador	M	8.2.1.1.1.22
Petición-informe-MTA-originador	M	12.2.1.1.1.8
Petición-devolución-contenido	C	8.2.1.1.1.23
Petición-informe-entrega-física	C	8.2.1.1.1.24
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Testigo-mensaje	C	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	C	8.2.1.1.1.27
Verificación-integridad-contenido	C	8.2.1.1.1.28

Cuadro 30 – Argumentos de transferencia-mensaje

Argumento	Presencia	Cláusula
Verificación-autenticación-origen-mensaje	C	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Petición-prueba-de-entrega	C	8.2.1.1.1.32
Múltiples-certificados-originador	O	8.2.1.1.1.41
Certificados-por-destinatario	O	8.2.1.1.1.42
Selectores-certificado	O	8.2.1.1.1.43
Contraorden-selectores-certificado	O	8.2.1.1.1.44
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	M	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido	M	8.2.1.1.1.37
Tipo-notificación	O	8.2.1.1.1.38
Mensaje-servicio	O	8.2.1.1.1.39

12.2.1.1.1.4 Información-rastreo-interna

Este argumento documenta las acciones realizadas sobre el mensaje (o sonda o informe) por cada MTA a través del cual pasa el mensaje (o sonda o informe) al ser transferido en el interior de un MD (véase 12.3.1). Debe ser generado por cada MTA a través del cual pasa el mensaje (o sonda o informe) en el interior de un MD.

Queda como asunto de política local que un MTA pueda (no necesariamente) eliminar **información-rastreo-interno** relacionada con otros MD cuando realice la entrega o cuando haga una transferencia a otro MD o cuando reciba de otro MD.

12.2.1.1.1.5 Número-destinatario-especificado-originalmente

Este argumento, debe ser generado por el MTA-originador del mensaje. Se especifica un valor diferente de este argumento para cada destinatario especificado-originalmente de este mensaje.

El **número-destinatario-especificado-originalmente** es un valor entero en el intervalo comprendido entre uno y el número de destinatarios-especificados-originalmente.

Existe una relación biunívoca entre un determinado valor del **número-destinatario-especificado-originalmente** y un determinado **nombre-destinatario** en el momento de la remisión-mensaje; no debería suponerse que esta es una relación singular en el momento de la entrega-mensaje. Es decir, puede utilizarse un valor del **número-destinatario-especificado-originalmente** para distinguir un **nombre-destinatario** especificado originalmente, pero no un destinatario real que recibirá el mensaje.

12.2.1.1.1.6 Responsabilidad

Este argumento indica si el MTA-receptor debe tener la responsabilidad de entregar el mensaje a un destinatario o de transferirlo a otro MTA para su entrega subsiguiente al destinatario. Debe ser generado por el MTA-emisor. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno de los siguientes valores: **responsable** o **no responsable**.

12.2.1.1.1.7 Tiempo-entrega-diferida

Este argumento se define en 8.2.1.1.1.12. Puede aparecer en un mensaje en el puerto-transferencia si existe un acuerdo bilateral de que un MTA distinto del MTA-originador del mensaje diferirá la entrega del mensaje. Estará ausente una vez se haya satisfecho la demanda de aplazamiento.

En ausencia de acuerdo bilateral el MTA efectuará localmente las operaciones siguientes:

a) diferirá la entrega del mensaje; o

b) procesará el mensaje como si no estuviera presente el **tiempo-entrega-diferida**; o

c) si no ha transcurrido todavía el tiempo de entrega diferida, no entregará el mensaje con **código-motivo-no entrega** puesto a **entrega-diferida-no-efectuada** y el **código-diagnóstico-no entrega** puesto a **no-acuerdo-bilateral**.

12.2.1.1.1.8 Petición-informe-MTA-originador

Este argumento indica el tipo de informe solicitado por el MTA-originador. Debe ser generado por el MTA-originador del mensaje. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tomar uno de los siguientes valores:

informe-no-entrega: se devuelve un informe únicamente en el caso de no-entrega, y contiene únicamente la **última-información-rastreo**.

informe: se devuelve un informe tanto en el caso de entrega como de no-entrega y contiene únicamente la **última-información-rastreo**.

informe-auditado: se devuelve un informe tanto en el caso de entrega como de no-entrega, y contiene toda la **información-rastreo**.

El argumento de **petición-informe-MTA-originador** deberá especificar al menos el nivel del informe especificado en el argumento de **petición-informe-originador**, siendo el orden creciente de los niveles de informe: **no-informe**, **informe-no-entrega**, **informe**, **informe-auditado**.

12.2.1.1.1.9 Conversión-explícita

Este argumento se define en 8.2.1.1.1.11. Una vez efectuada la conversión explícita especificada, se suprimirá el argumento.

12.2.1.1.2 Resultados

La operación-abstracta transferencia-mensaje no devuelve resultado.

12.2.1.1.3 Errores-abstractos

No existen errores-abstractos que puedan interrumpir la operación-abstracta transferencia-mensaje.

12.2.1.2 Transferencia-sonda

La operación-abstracta transferencia-sonda permite a un MTA transferir una sonda a otro MTA.

12.2.1.2.1 Argumentos

El cuadro 31 enumera los argumentos de la operación-abstracta transferencia-sonda, y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

12.2.1.2.1.1 Identificador-sonda

Este argumento contiene un **identificador-MTS** que distingue la sonda de otros mensajes, sondas e informes en el interior del MTS. Debe ser generado por el MTA-originador de la sonda, y debe tener el mismo valor que el **identificador-remisión-sonda** suministrado al originador de la sonda cuando se remitió ésta.

12.2.1.2.2 Resultados

La operación-abstracta transferencia-sonda no devuelve resultados.

12.2.1.2.3 Errores-abstractos

No existen errores-abstractos que puedan interrumpir la operación-abstracta transferencia-sonda.

12.2.1.3 Transferencia-informe

La operación-abstracta transferencia-informe permite a un MTA transferir un informe a otro MTA.

Cuadro 31 – Argumentos de transferencia-sonda

Argumento	Presencia	Cláusula
Argumentos de retransmisión		
Identificador-sonda	M	12.2.1.2.1.1
Información-bilateral-por-dominio	C	12.2.1.1.1.2
Información-rastreo	M	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Argumento del originador		
Nombre-originador	M	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	M	8.2.1.1.1.2
Número-destinatario-especificado-originalmente	M	12.2.1.1.1.5
Responsabilidad	M	12.2.1.1.1.6
Ampliación-DL-prohibida	C	8.2.1.1.1.6
Argumentos de redireccionamiento		
Destinatario-alternativo-autorizado	C	8.2.1.1.1.3
Reasignación-destinatario-prohibida	C	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	C	8.2.1.1.1.5
Historia-redireccionamiento	C	8.3.1.1.1.5
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Conversión-explícita	C	8.2.1.1.1.11
Argumento de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumento de entrega física		
Atributos-reproducción-física	C	8.2.1.1.1.20
Argumentos de petición de informe		
Petición-informe-originador	M	8.2.1.1.1.22
Petición-informe-MTA-originador	M	12.2.1.1.1.8
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Verificación-autenticación-origen-sonda	C	8.2.1.2.1.1
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	M	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Longitud-contenido	C	8.2.1.2.1.2
Tipo-notificación	C	8.2.1.1.1.38
Mensaje-servicio	O	8.2.1.1.1.39

12.2.1.3.1 Argumentos

El cuadro 32 enumera los argumentos de la operación-abstracta transferencia-informe, y para cada argumento califica su presencia e identifica la cláusula donde se define el argumento.

Cuadro 32 – Argumentos de transferencia-informe

Argumento	Presencia	Cláusula
Argumentos de retransmisión		
Identificador-informe	M	12.2.1.3.1.1
Información-rastreo	M	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Historia-redireccionamiento	C	8.3.1.2.1.5
Argumento de origen del informe		
Nombre-MTA-informador	C	8.3.1.2.1.17
Argumento de destino del informe		
Nombre-destino-informe	M	12.2.1.3.1.2
Argumento de petición del informe		
Petición-informe-originador	M	8.2.1.1.1.22
Argumentos de rastreo del sujeto		
Identificador-sujeto	M	12.2.1.3.1.3
Número-destinatario-especificado-originalmente	M	12.2.1.1.1.5
Información-rastreo-intermedia-sujeto	C	12.2.1.3.1.4
Tiempo-llegada	M	12.2.1.3.1.5
Originador-e-historia-ampliación-DL	C	8.3.1.2.1.3
Nombre-DL-informadora	C	8.3.1.2.1.4
Argumento de conversión		
Tipos-información-codificada-convertidos	C	8.3.1.2.1.6
Argumentos de información suplementaria		
Información-suplementaria	C	8.3.1.2.1.7
Dirección-envío-físico	C	8.3.1.2.1.8
Argumentos de redireccionamiento del sujeto		
Nombre-destinatario-real	M	8.3.1.2.1.2
Nombre-destinatario-deseado-originalmente	C	8.3.1.1.1.4
Historia-redireccionamiento	C	8.3.1.1.1.5
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	C	8.3.1.2.1.15
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido-devuelto	C	8.3.1.2.1.16
Argumentos de entrega		
Tiempo-entrega-mensaje	C	
Tipo-de usuario-MTS	C	8.3.1.2.1.9
Argumentos de no-entrega		8.3.1.2.1.10
Código-motivo-no-entrega	C	
Código-diagnóstico-no-entrega	C	8.3.1.2.1.11
Argumentos de seguridad		8.3.1.2.1.12
Certificado-destinatario	C	
Prueba-de-entrega	C	8.3.1.1.2.1
Certificado-MTA-que-informa	C	8.3.1.1.2.2
Verificación-autenticación-origen-informe	C	8.3.1.2.1.13
Etiqueta-seguridad-mensaje	C	8.3.1.2.1.14
Argumento de información adicional		8.2.1.1.1.30
Información-adicional	C	12.2.1.3.1.6

12.2.1.3.1.1 Identificador-informe

Este argumento contiene un **identificador-MTS** que distingue el informe de los demás mensajes, sondas e informes en el interior del MTS. Debe ser generado por el MTA-originador del informe.

12.2.1.3.1.2 Nombre-destino-informe

Este argumento contiene el **nombre-OR** del destino inmediato del informe. Debe ser generado por el MTA-originador del informe, y modificado subsiguientemente por los puntos-ampliación de DL si se ha ampliado alguna DL para añadir destinatarios al sujeto.

El MTA-originador del informe debe fijar este argumento en el **nombre-originador** del sujeto si éste no tiene una **historia-ampliación-DL**, o en el último **nombre-OR** de la **historia-ampliación-DL** si está presente en el sujeto.

Un punto-ampliación de DL puede sustituir su propio **nombre-OR** en este argumento, por el **nombre-OR** que precede inmediatamente a su propio **nombre-OR** en el **originador-e-historia-ampliación-DL** del informe, o por algún otro **nombre-OR** según la política-informadora de la DL.

12.2.1.3.1.3 Identificador-sujeto

Este argumento contiene el **identificador-mensaje** (o el **identificador-sonda**) del sujeto (**identificador-MTS**). Debe ser generado por el MTA-originador del sujeto.

12.2.1.3.1.4 Información-rastreo-intermedia-sujeto

Este argumento contiene la **información-rastreo** presente en el sujeto cuando se transfirió al MD-informador. Debe estar presente si, y únicamente si se solicitó un informe-auditado-y-confirmado por el MTA-originador del sujeto. Puede ser generado por el MTA-informador.

NOTA – La inclusión en la **información-rastreo-intermedia-sujeto** de la **información-rastreo-interna** presente en el sujeto cuando se transfirió al MTA-informador queda pendiente de ulterior normalización.

12.2.1.3.1.5 Tiempo-llegada

Este argumento contiene el **tiempo** en que el sujeto indicó al MD que hiciera el informe. Debe ser generado por el MD-originador del informe. Puede especificarse un valor diferente de este argumento para cada destinatario del sujeto a que se refiere el informe.

12.2.1.3.1.6 Información-adicional

La especificación del contenido de este argumento se realiza mediante acuerdo bilateral entre MD.

12.2.1.3.2 Resultados

La operación-abstracta transferencia-informe no devuelve resultados.

12.2.1.3.3 Errores abstractos

No existen errores-abstractos que pueden interrumpir la operación-abstracta transferencia-informe.

12.2.2 Errores abstractos

El puerto-transferencia no tiene errores-abstractos.

12.3 Tipos de parámetros comunes

Esta cláusula define cierto número de tipos de parámetros comunes del servicio abstracto de MTA.

12.3.1 Información-rastreo e información-rastreo-interna

La **información-rastreo** documenta las acciones efectuadas sobre un mensaje, sonda o informe por cada MD, a través del cual pasa al ser transferido a través del MTS.

La **información-rastreo-interna** documenta las acciones efectuadas sobre un mensaje, sonda o informe por cada MTA, a través del cual pasa al ser transferido a través de un MD. La **información-rastreo-interna** podrá ser eliminada del mensaje, sonda o informe antes de ser transferida fuera de un MD. Un MD puede (pero no debe obligatoriamente) suprimir la **información-rastreo-interna** relativa a otros MD.

La **información-rastreo** (o **información-rastreo-interna**) consta de una secuencia de **elementos-información-rastreo** (o **elementos-información-rastreo-interna**). El primer **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) es el suministrado por el MD-o-MTA originador del mensaje, sonda o informe. El segundo **elemento-**

información-rastreo (o **elemento-información-rastreo-interna**) es el suministrado por el siguiente MD (o MTA) encontrado por el mensaje, sonda o informe, y así sucesivamente. Cada MD (o MTA) añade su **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) al final de la secuencia existente. La **información-rastreo** la añade el primer MTA que encuentren el mensaje, la sonda o el informe en cada MD por el que atraviesen y, si fuera necesario, la modifica los siguientes MTA en ese MD.

Cada **elemento-información-rastreo** incluye el **identificador-dominio-global** del MD que suministra el **elemento-información-rastreo**.

Cada **elemento-información-rastreo-interna** incluye el **nombre-MTA** del MTA que suministra el **elemento-información-rastreo-interna** y el **identificador-dominio-global** del MD al que pertenece el MTA.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) incluye el **tiempo-llegada** en el cual el mensaje, sonda o informe entró en el MD (o MTA). En el caso del MD-o-MTA) originador del mensaje, sonda o informe, el **tiempo-llegada** es el tiempo de la remisión-mensaje, remisión-sonda o generación del informe, respectivamente.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) especifica la **acción-encaminamiento** que el MD (o MTA) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) adoptó respecto del mensaje, sonda o informe. **Retransmitido** constituye la **acción-encaminamiento** normal de transferencia de mensaje, sonda o informe a otro MD o MTA. **Reencaminado** indica que se había realizado previamente un intento de reencaminar el mensaje, sonda o informe hacia un **dominio-deseado** (o **MTA-deseado**); se incluye el **identificador-dominio-global** del **dominio-deseado** en el **elemento-información-rastreo**; si el intento de reencaminamiento iba dirigido hacia otro MTA dentro del mismo MD, se incluye entonces el **nombre-MTA** del **MTA-deseado** en el **elemento-información-rastreo-interna**; si el intento de reencaminamiento iba dirigido hacia otro MD se incluye en el **elemento-información-rastreo-interna** el **identificador-dominio-global** en vez de un **nombre-MTA**.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) especifica igualmente cualquier **acción-adicional** que el MD (o MTA) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) efectuó con respecto al mensaje, sonda o informe. Las indicaciones de cualquiera de estas **acciones-adicionales** que aparecen en los **elementos-información-rastreo-interna** durante la travesía de un MD deberán reflejarse igualmente en los **elementos-información-rastreo** correspondientes a la travesía del MD.

Si la entrega diferida provocó que el MD (o MTA) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) retuviera el mensaje durante un periodo de tiempo, el **tiempo-diferido** en que inició el tratamiento del mensaje para su entrega o transferencia se incluye igualmente en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Este parámetro no está presente en los **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) de las sondas e informes.

Si el MD (o MTA) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) somete un mensaje a conversión, los **tipos-información-codificada-convertidos** resultantes de la conversión se incluyen igualmente en **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Para una sonda, un MD (o MTA) que hubiera convertido el mensaje-sujeto indica en su **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) los **tipos-información-codificada** que el mensaje-sujeto contendría después de la conversión. Este parámetro no está presente en la **información-rastreo** (o **información-rastreo-interna**) de los informes.

Si el MD (o MTA) redirige un mensaje o una sonda (a cualquiera, pero no necesariamente a todos los destinatarios de un mensaje o una sonda), se indica **redirigido** en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**).

Si el MD (o MTA) amplía la DL de un mensaje o de una sonda, se indica **operación-dl** en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Si el MD (o MTA) es un punto-ampliación de DL y sustituye su propio **nombre-OR** en el **nombre-destino-informe** de un informe por otro **nombre-OR** (véase 12.2.1.3.1.2), la **operación-dl** se indica en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) del informe. Este parámetro no está presente en la **información-rastreo** (o la **información-rastreo-interna**) de las sondas.

Un MD (o MTA) realiza la detección y supresión de un bucle cuando se recibe un mensaje, sonda o informe procedente de otro MD (o MTA). Los mensajes, sondas e informes pueden volver a entrar legítimamente en un MD (o MTA) debido a varias razones (**reencaminado**, etc.) y en consecuencia, un mensaje, sonda o informe puede tener **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) disjuntos procedentes del mismo MD (o MTA). Cada vez que un mensaje, sonda o informe se transfiere a través de un MD (o MTA), la generación de los **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) se ejecuta de la forma siguiente:

i) se agrega un **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) marcado como **retransmitido**;

ii) si se ha de producir una tentativa de reencaminamiento, el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) añadido en i) se cambia por **reencaminado** (y el número de **elemento-información-rastreo** (o **elementos-información-rastreo-interna**) añadidos por el MD (o MTA) para esta travesía del MD (o MTA) permanece en uno);

iii) si se producen tentativas subsiguientes de reencaminamiento, se añade un nuevo **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) (marcado como **reencaminado**) para reflejar cada nueva tentativa de reencaminamiento.

Pueden producirse varias tentativas de reencaminamiento hacia el mismo MD (o MTA).

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) añadido por un MD (o MTA) puede contener indicaciones de **acciones-adicionales** realizadas por el MD (o MTA) sobre el mensaje o sonda (es decir **tiempo-diferido** (no presentes en **información-rastreo** (o **información-rastreo-interna**) en las sondas), **tipos-información-codificada-convertidos**, y **redirigidos** u **operación-dl**). Para indicar el orden en que se han producido el redireccionamiento y la ampliación DL, las indicaciones **redirigido** y **operación-dl** no aparecerán ambas en un mismo **elemento-información-rastreo** (o **elemento-información-rastreo-interno**).

13 Definición de la sintaxis abstracta de agente de transferencia de mensajes

La sintaxis-abstracta del servicio abstracto del MTA se define en la figura 4.

La sintaxis-abstracta del servicio abstracto de MTA se define utilizando la notación de sintaxis abstracta (ASN.1) definida en la Rec. UIT-T X.680 | ISO/CEI 8824-1, la Rec. UIT-T X.681 | ISO/CEI 8824-2, la Rec. UIT-T X.682 | ISO/CEI 8824-3 y la Rec. UIT-T X.683 | ISO/CEI 8824-4 y los convenios de definición del servicio abstracto descritos en la Rec. UIT-T X.402 | ISO/CEI 10021-2, que utiliza la notación de operaciones distantes definida en la Rec. UIT-T X.880 | ISO/CEI 13712-1.

La definición de sintaxis-abstracta del servicio abstracto MTA tiene las siguientes partes principales:

Prólogo: declaraciones de las exportaciones desde el módulo de servicio abstracto MTA, y las importaciones a éste (figura 4, parte 1).

Objetos y puertos: definiciones del objeto del MTA, y su puerto-transferencia (figura 4, parte 2).

Vinculación-MTA y desvinculación-MTA: definiciones de vinculación-MTA y desvinculación-MTA utilizadas para establecer y liberar asociaciones entre MTA (figura 4, parte 2).

Puerto de transferencia: definiciones de las operaciones-abstractas de puerto-transferencia: transferencia-mensaje, transferencia-sonda y transferencia-informe (figura 4, parte 3).

Sobre de transferencia de mensaje: definición del sobre-transferencia-mensaje (figura 4, partes 3 y 4).

Sobre de transferencia de sonda: definición del sobre-transferencia-sonda (figura 4, parte 4).

Sobre y contenido de transferencia de informe: definición del sobre-transferencia-informe y del contenido-transferencia-informe (figura 4, parte 5).

Campos de sobre y contenido del informe: definiciones de campos de sobre y de contenido del informe (figura 4, partes 5 y 7).

Campos de ampliación: definiciones de los campos-ampliación (figura 4, parte 7).

Tipos de parámetros comunes: definiciones de los tipos de parámetros comunes (figura 4, partes 7 y 8).

NOTA – El módulo implica ciertos cambios en el protocolo P1 definido en la Recomendación X.411 del CCITT (1984). Dichos cambios se resaltan en la versión inglesa mediante subrayado.

Cada **campo-ampliación** definido en la figura 4 (parte 6) transporta consigo una indicación sobre su **criticidad** para la remisión, transferencia y entrega. El mecanismo de **criticidad** se describe en 9.2 y los procedimientos relativos a los **campos-ampliación** y a las indicaciones de su **criticidad** se definen ulteriormente en la cláusula 14.

```
MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mta-abstract-service(2)
            version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONNECTION-PACKAGE, CONTRACT
                ----
                FROM Remote-Operations-Information-Objects {joint-iso-itu-t remote-operations(4)
                        informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions {joint-iso-itu-t remote-operations(4)
                        useful-definitions(7) version1(0) }

        -- MTS Abstract Service Parameters

        ABSTRACT-ERROR, ABSTRACT-OPERATION, administration, AdministrationDomainName,
        certificate-selectors, certificate-selectors-override, Content, ContentIdentifier,
        ContentLength, ContentType, content-confidentiality-algorithm-identifier,
        content-correlator, content-integrity-check, conversion-with-loss-prohibited,
        ConvertedEncodedInformationTypes, CountryName, DeferredDeliveryTime, delivery,
        dl-exempted-recipients, dl-expansion-history, dl-expansion-prohibited,
        ExplicitConversion, EXTENSION, ExtensionField { }, GlobalDomainIdentifier,
        InitiatorCredentials, latest-delivery-time, message-origin-authentication-check,
        message-security-label, message-token, MHS-OBJECT, MTAName, MTSIdentifier,
        multiple-originator-certificates, ORAddressAndOptionalDirectoryName,
        OriginalEncodedInformationTypes, originator-and-DL-expansion-history,
        originator-certificate, originator-return-address, PerMessageIndicators,
        physical-delivery-modes, physical-delivery-report-request, physical-forwarding-address,
        physical-forwarding-address-request, physical-forwarding-prohibited,
        physical-rendition-attributes, PORT, Priority, PrivateDomainIdentifier,
        PrivateExtensions, probe-origin-authentication-check, proof-of-delivery,
        proof-of-delivery-request, recipient-certificate, recipient-number-for-advice,
        recipient-reassignment-prohibited, redirection-history, registered-mail-type,
        reporting-DL-name, reporting-MTA-certificate, reporting-MTA-name, ReportType,
        report-origin-authentication-check, requested-delivery-method, ResponderCredentials,
        SecurityContext, submission, SupplementaryInformation, Time
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- IPM Information Objects

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                        information-objects(2) version-1999(1) }

        -- Object Identifiers

        id-cp-mta-connect, id-ct-mta-transfer, id-ot-mta, id-pt-transfer
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 1 de 8)

```
        -- Upper Bounds

        ub-bit-options, ub-integer-options, ub-recipients, ub-transfers
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                        version-1999(1) };

--      Objects

mta MHS-OBJECT ::= {
        BOTH  { mta-transfer }
        ID    id-ot-mta }

--      Contracts

mta-transfer CONTRACT ::= {
        CONNECTION     mta-connect
        OPERATIONS OF  { transfer }
        ID             id-ct-mta-transfer }

--      Connection package

mta-connect CONNECTION-PACKAGE ::= {
        BIND        mta-bind
        UNBIND      mta-unbind
        ID          id-cp-mta-connect }

--      Ports

transfer PORT ::= {
        OPERATIONS  { message-transfer | probe-transfer | report-transfer }
        ID          id-pt-transfer }

--      MTA-bind and MTA-unbind

mta-bind ABSTRACT-OPERATION ::= {
        ARGUMENT  MTABindArgument
        RESULT    MTABindResult
        ERRORS    { mta-bind-error } }

mta-unbind ABSTRACT-OPERATION ::= emptyUnbind

MTABindArgument ::= CHOICE {
        unauthenticated NULL,        -- if no authentication is required
        authenticated [1] SET {      -- if authentication is required
                initiator-name [0] MTAName,
                initiator-credentials [1] InitiatorCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ),
                security-context [2] SecurityContext OPTIONAL } }

MTABindResult ::= CHOICE {
        unauthenticated NULL,        -- if no authentication is required
        authenticated [1] SET {      -- if authentication is required
                responder-name [0] MTAName,
                responder-credentials [1] ResponderCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ) } }

mta-bind-error ABSTRACT-ERROR ::= {
        PARAMETER  INTEGER {
                busy (0),
                authentication-error (2),
                unacceptable-dialogue-mode (3),
                unacceptable-security-context (4),
                inadequate-association-confidentiality (5) } (0..ub-integer-options) }
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 2 de 8)

```
--      Transfer Port

message-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Message }

probe-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Probe }

report-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Report }

Message ::= SEQUENCE {
              envelope MessageTransferEnvelope,
              content Content }

Probe ::= ProbeTransferEnvelope

Report ::= SEQUENCE {
              envelope ReportTransferEnvelope,
              content ReportTransferContent }

--      Message Transfer Envelope

MessageTransferEnvelope ::= SET {
       COMPONENTS OF PerMessageTransferFields,
       per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientMessageTransferFields }

PerMessageTransferFields ::= SET {
       message-identifier MessageIdentifier,
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       priority Priority DEFAULT normal,
       per-message-indicators PerMessageIndicators DEFAULT { },
       deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
       per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
              PerDomainBilateralInformation OPTIONAL,
       trace-information TraceInformation,
       extensions [3] SET OF ExtensionField {{ MessageTransferExtensions }} DEFAULT { } }

MessageTransferExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       latest-delivery-time |
       originator-return-address |
       originator-certificate |
       content-confidentiality-algorithm-identifier |
       message-origin-authentication-check |
       message-security-label |
       content-correlator |
       dl-exempted-recipients |
       certificate-selectors |
       multiple-originator-certificates |
       dl-expansion-history |
       internal-trace-information |
       PrivateExtensions, ... }

PerRecipientMessageTransferFields ::= SET {
       recipient-name RecipientName,
       originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
       per-recipient-indicators [1] PerRecipientIndicators,
       explicit-conversion [2] ExplicitConversion OPTIONAL,
       extensions [3] SET OF ExtensionField {{ PerRecipientMessageTransferExtensions }}
                                                                    DEFAULT { } }
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 3 de 8)

```
PerRecipientMessageTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        physical-delivery-report-request |
        message-token |
        content-integrity-check |
        proof-of-delivery-request |
        certificate-selectors-override |
        recipient-certificate |
        redirection-history |
        IPMPerRecipientEnvelopeExtensions |
        PrivateExtensions, ... }

--      Probe Transfer Envelope

ProbeTransferEnvelope ::= SET {
        COMPONENTS OF PerProbeTransferFields,
        per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
PerRecipientProbeTransferFields}

PerProbeTransferFields ::= SET {
        probe-identifier ProbeIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT { },
        per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
                PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extensions [3] SET OF ExtensionField {{ ProbeTransferExtensions }} DEFAULT { } }

ProbeTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        recipient-reassignment-prohibited |
        dl-expansion-prohibited |
        conversion-with-loss-prohibited |
        originator-certificate |
        message-security-label |
        content-correlator |
        probe-origin-authentication-check |
        internal-trace-information |
        PrivateExtensions, ... }

PerRecipientProbeTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extensions [3] SET OF ExtensionField {{ PerRecipientProbeTransferExtensions }}
                                                                        DEFAULT { } }

PerRecipientProbeTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-rendition-attributes |
        redirection-history |
        PrivateExtensions, ... }
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 4 de 8)

```
--      Report Transfer Envelope

ReportTransferEnvelope ::= SET {
        report-identifier ReportIdentifier,
        report-destination-name ReportDestinationName,
        trace-information TraceInformation,
        extensions [1] SET OF ExtensionField {{ ReportTransferEnvelopeExtensions }}
                                                                        DEFAULT { } }

ReportTransferEnvelopeExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        message-security-label |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

--      Report Transfer Content

ReportTransferContent ::= SET {
        COMPONENTS OF PerReportTransferFields,
        per-recipient-fields [0] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientReportTransferFields}

PerReportTransferFields ::= SET {
        subject-identifier SubjectIdentifier,
        subject-intermediate-trace-information SubjectIntermediateTraceInformation OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType OPTIONAL,
        content-identifier ContentIdentifier OPTIONAL,
        returned-content [1] Content OPTIONAL,
        additional-information [2] AdditionalInformation OPTIONAL,
        extensions [3] SET OF ExtensionField {{ ReportTransferContentExtensions }}
                                                                        DEFAULT { } }

ReportTransferContentExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        content-correlator |
        PrivateExtensions, ... }

PerRecipientReportTransferFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        originally-specified-recipient-number [1] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [2] PerRecipientIndicators,
        last-trace-information [3] LastTraceInformation,
        originally-intended-recipient-name [4] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [5] SupplementaryInformation OPTIONAL,
        extensions [6] SET OF ExtensionField {{ PerRecipientReportTransferExtensions }}
                                                                        DEFAULT { } }

PerRecipientReportTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }

--      Envelope & Report Content Fields

MessageIdentifier ::= MTSIdentifier

OriginatorName ::= ORAddressAndOptionalDirectoryName
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 5 de 8)

```
PerDomainBilateralInformation ::= SEQUENCE {
       COMPONENTS OF BILATERAL.&id,
       bilateral-information BILATERAL.&Type }

BILATERAL ::= CLASS {
       &id BilateralDomain UNIQUE,
       &Type }
WITH SYNTAX { &Type, IDENTIFIED BY &id }

BilateralDomain ::= SEQUENCE {
       country-name CountryName,
       domain CHOICE {
              administration-domain-name AdministrationDomainName,
              private-domain SEQUENCE {
                     administration-domain-name [0] AdministrationDomainName,
                     private-domain-identifier [1] PrivateDomainIdentifier } } }

RecipientName ::= ORAddressAndOptionalDirectoryName

OriginallySpecifiedRecipientNumber ::= INTEGER (1..ub-recipients)

PerRecipientIndicators ::= BIT STRING {
       responsibility (0),
       -- responsible 'one', not-responsible 'zero'
       originating-MTA-report (1),
       originating-MTA-non-delivery-report (2),
       -- either originating-MTA-report, or originating-MTA-non-delivery-report,
       -- or both, shall be 'one':
       -- originating-MTA-report bit 'one' requests a 'report';
       -- originating-MTA-non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'one' requests an 'audited-report';
       -- bits 0 - 2 'don't care' for Report Transfer Content
       originator-report (3),
       originator-non-delivery-report (4),
       -- at most one bit shall be 'one':
       -- originator-report bit 'one' requests a 'report';
       -- originator-non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'zero' requests 'no-report'
       reserved-5 (5),
       reserved-6 (6),
       reserved-7 (7)
       -- reserved- bits 5 - 7 shall be 'zero' -- } (SIZE (8..ub-bit-options))

ProbeIdentifier ::= MTSIdentifier

ReportIdentifier ::= MTSIdentifier

ReportDestinationName ::= ORAddressAndOptionalDirectoryName

SubjectIdentifier ::= MessageOrProbeIdentifier

MessageOrProbeIdentifier ::= MTSIdentifier

SubjectIntermediateTraceInformation ::= TraceInformation

--      AdditionalInformation is retained for backwards compatibility only,
--      and use in new systems is strongly deprecated

ADDITIONAL ::= CLASS { &Type }

AdditionalInformation ::= ADDITIONAL.&Type  -- maximum ub-additional-info octets including all encoding

ActualRecipientName ::= ORAddressAndOptionalDirectoryName
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 6 de 8)

```
LastTraceInformation ::= SET {
       arrival-time [0] ArrivalTime,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       report-type [1] ReportType }

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName


--      Extension Fields

originator-requested-alternate-recipient EXTENSION ::= {
       OriginatorRequestedAlternateRecipient,
       IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOptionalDirectoryName

trace-information EXTENSION ::= {
       TraceInformation,
       IDENTIFIED BY standard-extension:37 }

internal-trace-information EXTENSION ::= {
       InternalTraceInformation,
       IDENTIFIED BY standard-extension:38 }

InternalTraceInformation ::= SEQUENCE SIZE (1..ub-transfers) OF
InternalTraceInformationElement

InternalTraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       mta-name MTAName,
       mta-supplied-information MTASuppliedInformation }

MTASuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted CHOICE {
              mta MTAName,
              domain GlobalDomainIdentifier } OPTIONAL,
       -- additional-actions -- COMPONENTS OF InternalAdditionalActions }

InternalAdditionalActions ::= AdditionalActions


--      Common Parameter Types

TraceInformation ::= [APPLICATION 9] SEQUENCE SIZE (1..ub-transfers) OF
TraceInformationElement

TraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       domain-supplied-information DomainSuppliedInformation }

DomainSuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted-domain GlobalDomainIdentifier OPTIONAL,
       -- additional-actions -- COMPONENTS OF AdditionalActions }

AdditionalActions ::= SET {
       deferred-time [1] DeferredTime OPTIONAL,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       other-actions [3] OtherActions DEFAULT { } }

RoutingAction ::= ENUMERATED {
       relayed (0),
       rerouted (1) }
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 7 de 8)

```
DeferredTime ::= Time

ArrivalTime ::= Time

OtherActions ::= BIT STRING {
       redirected (0),
       dl-operation (1) } (SIZE (0..ub-bit-options))

END     -- of MTA Abstract Service
```

Figura 4 – Definición de la sintaxis abstracta del servicio abstracto del MTA (Parte 8 de 8)

SECCIÓN 4 – PROCEDIMIENTOS DE FUNCIONAMIENTO DISTRIBUIDO DEL MTS

14 Procedimientos de funcionamiento distribuido del MTS

En esta cláusula, se especifican los procedimientos para el funcionamiento distribuido del MTS, que ejecutan los MTA. Cada MTA aplica individualmente los procedimientos descritos a continuación; la acción colectiva de todos los MTA presta el servicio abstracto de MTS a los usuarios del MTS.

Aunque los procedimientos incluyen la mayoría de las acciones importantes requeridas de un MTA, se ha omitido gran cantidad de detalles para una mayor claridad de exposición y para evitar cualquier redundancia innecesaria. Para un tratamiento definitivo de las acciones del MTA deberían consultarse las definiciones del servicio-abstracto.

14.1 Visión de conjunto del modelo del MTA

14.1.1 Organización y técnica de realización de los modelos

La descripción de los procedimientos para un MTA único se basa en el modelo mostrado en las figuras 5 a 11 que se describe a continuación. Debe observarse que se incluye el modelo con fines descriptivos únicamente y no se pretende limitar en modo alguno la realización de un MTA.

Ni los procedimientos mostrados ni el orden de los pasos de procesamiento en ellos, implican necesariamente características específicas de un MTA real.

El modelo distingue entre *módulos* y *procedimientos*. Los *módulos*, en el sentido en que se utilizan aquí, son entidades de proceso autónomas que pueden ser invocadas por otros módulos u otros sucesos externos al MTA, los cuales pueden a su vez invocar otros módulos o generar otros sucesos externos. Los módulos no están unidos entre sí mediante una estructura de control descrita explícitamente; sino que la estructura de control entre los módulos surge de su esquema de invocaciones recíprocas. Los módulos corresponden a *objetos* en el sentido de la programación orientada-objeto.

Se utilizan aquí los *procedimientos* en el sentido convencional de programación. Los procedimientos están orientados a tareas o funciones. Los procedimientos pueden llamar a otros procedimientos, en forma de subrutinas, con devolución de control al procedimiento llamante cuando ha finalizado el procedimiento llamado. Tales llamadas pueden anidarse hasta una profundidad arbitraria, pudiendo, asimismo, autollamarse el procedimiento de forma recurrente. Los procedimientos están unidos entre sí mediante estructuras de control definidas explícitamente, construidas a partir de llamadas a procedimientos y de dispositivos de programación convencional como iteraciones y ejecuciones condicionales.

En el modelo, existen procedimientos dentro de los módulos. Cada módulo contiene al menos un procedimiento y puede contener varios. En el último caso, los procedimientos y la estructura de control de gobierno se describen explícitamente. En el primer caso, la existencia de un procedimiento único de módulos se trata generalmente como implícita.

Utilizando estas técnicas para la aplicación de modelos, puede perfeccionarse un proceso de aplicación del MTA de la forma siguiente: para cada operación-abstracta (tanto usuaria como suministradora) que puede existir entre un MTA y los usuarios-MTS que sirve, o entre un MTA y los otros MTA con los que coopera, hay un módulo único denominado *módulo externo*. El conjunto de módulos externos es responsable de la entrada y salida de mensajes, sondas e informes al MTA y del soporte de operaciones tales como vinculación-MTS, desvinculación-MTS, registro, control-remisión y control-entrega. Los módulos externos se muestran en la figura 5 y se describen en 14.5 a 14.10, agrupados por puertos.

Para realizar las diferentes operaciones-abstractas de las cuales es responsable, un MTA debe ejecutar ciertas operaciones de proceso sobre cada mensaje, sonda o informe que entra o se origina en él. En el modelo, esto es competencia de los *módulos internos*, mostrados en figura 6 y descritos en 14.2 a 14.4.

Los módulos externos e internos se relacionan entre sí de la forma siguiente: un módulo externo se comunica únicamente con un módulo interno, y no con otro módulo externo o directamente con un procedimiento dentro de un módulo interno. Así, los módulos internos no sólo soportan el volumen de proceso dentro de un MTA, sino que sirven igualmente como enlaces entre sus módulos externos. Además de los módulos internos, la figura 6 muestra igualmente los módulos con los que se comunican.

El MTA está dirigido por sucesos en el sentido que permanece en reposo hasta que se detecta un suceso en uno de sus puertos. Muchos de los sucesos, tales como la invocación de una operación-abstracta vinculación-MTS, control-remisión, control-entrega o registro por parte de un usuario-MTS u otro MTA se tratan directa y completamente por el módulo asignado a esta operación-abstracta. Sin embargo, otros sucesos arrancan un proceso que puede reverberar a

través del MTA, perdurar durante un cierto tiempo y finalmente provocar uno o más sucesos de salida. Estos sucesos hacen intervenir los módulos de proceso internos y son:

a) un mensaje o sonda originado por un usuario-MTS soportado localmente entra a través del puerto-remisión;

b) un mensaje, sonda o informe retransmitido desde otro MTA entra a través del puerto-transferencia.

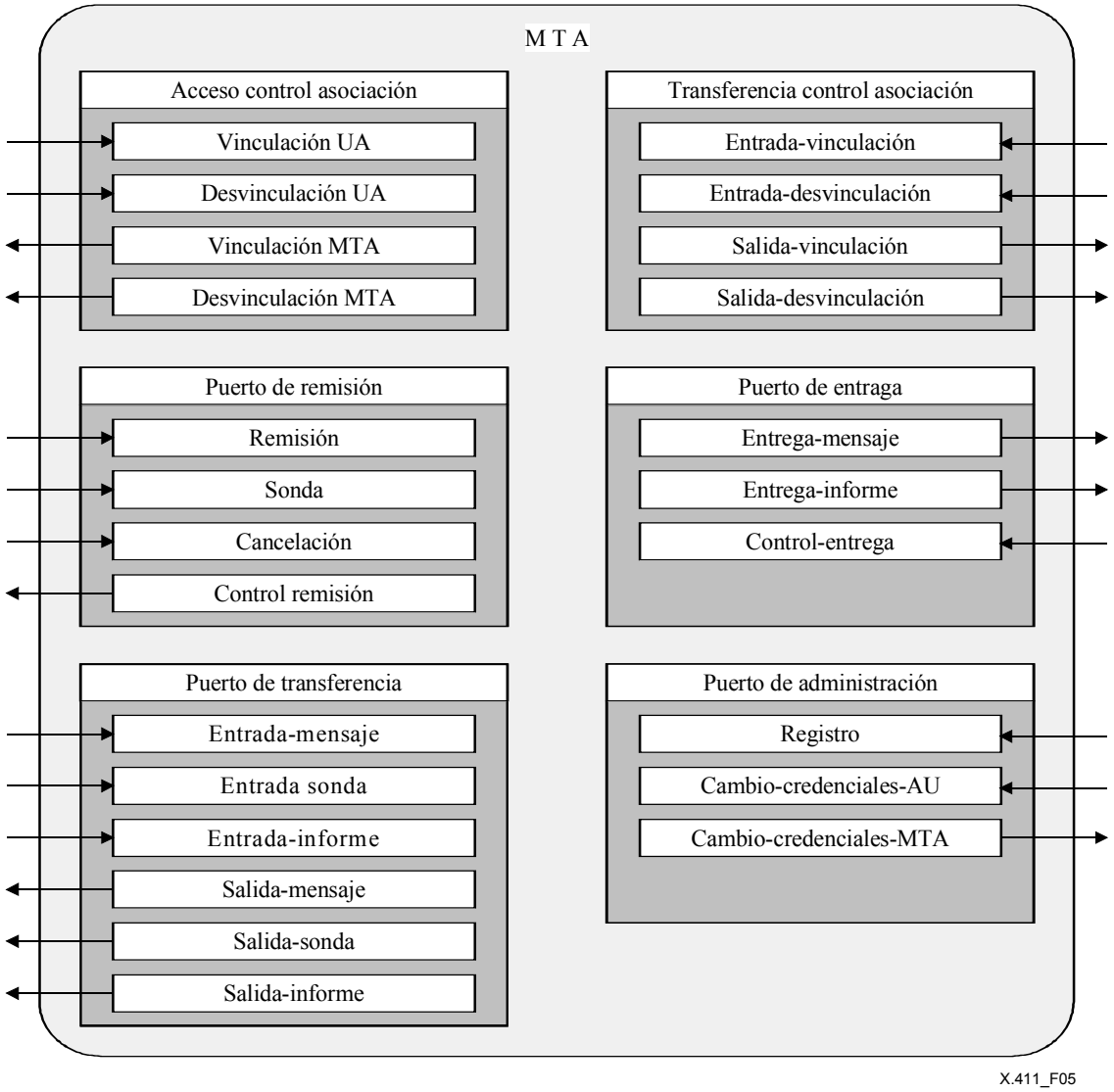


Figura 5 – Puertos y módulos de un MTA

Puesto que el proceso en el interior de un MTA puede resultar bastante complejo, especialmente para mensajes con múltiples destinatarios, el módulo supone, como dispositivo interno de contabilidad, que cada mensaje transporta consigo un conjunto de instrucciones, uno para el mensaje en su conjunto y uno para cada destinatario. Estas instrucciones ayudan a guiar un mensaje a través de los pasos de proceso y transportan la información entre los módulos y procedimientos internos al MTA.

NOTA 1 – Los procedimientos descritos aquí están dirigidos al proceso de un mensaje único. Esto resulta adecuado para todos los efectos menos para uno: la disposición en cola de mensajes y la prioridad relativa de invocación de los procedimientos están gobernados explícitamente por el argumento **prioridad** en el caso de un mensaje que entra a través del puerto-remisión o puerto-transferencia, o implícitamente (de prioridad urgente) en el caso de un informe o una prueba que se genera internamente o que entra a través del puerto-transferencia.

NOTA 2 – Un MTA puede especificar por defecto varias ventanas de tiempo de entrega para cada prioridad de mensaje (por ejemplo, aquellos valores definidos en las Recomendaciones de la serie F.400). El MTS y por tanto, cada MTA afectado debería tener en cuenta dichos valores durante el proceso del mensaje. Por ejemplo, el MTA puede aplicar un plazo máximo de entrega. Si este periodo de tiempo expira antes de la entrega, el MTA genera un informe-no-entrega y descarta el mensaje. Las acciones requeridas en este caso son idénticas a las acciones requeridas cuando se alcanza el **último-tiempo-entrega**.

NOTA 3 – El examen de la información-rastreo es incompleto debido a su naturaleza compleja. Se señalan algunos detalles importantes pero el tratamiento completo y definitivo del informe-rastreo aparece en 12.3.1.

NOTA 4 – En la Rec. UIT-T X.412 | ISO/CEI 10021-10 se especifican adiciones y sustituciones de los procedimientos descritos en esta Definición de servicio, que se aplican a los MTA conformes a la Rec. UIT-T X.412 | ISO/CEI 10021-10.

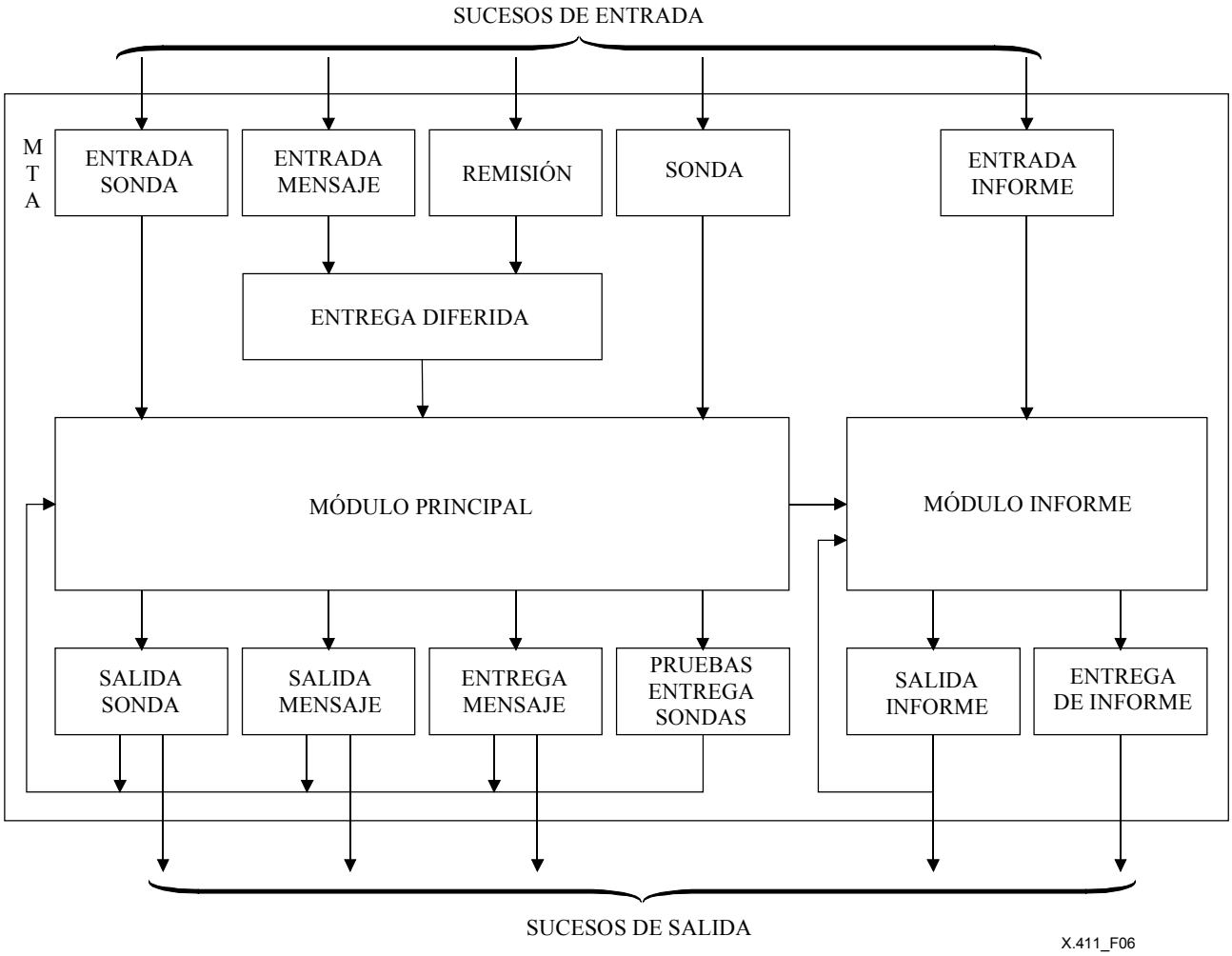


Figura 6 – Relación entre los módulos internos y externos

14.2 Módulo de entrega diferida

Este módulo proporciona el elemento-de-servicio de entrega diferida. Es invocado por los módulos de remisión-mensaje y entrada-mensaje que pasan un mensaje para comprobar la petición de entrega diferida y retenerla, si es necesario. Invoca el módulo principal, pasando sucesivamente el mensaje hasta la finalización de su procedimiento interno único.

14.2.1 Procedimiento de entrega diferida

14.2.1.1 Argumentos

Un mensaje para comprobación de la petición de entrega diferida y retención, si es necesario.

14.2.1.2 Resultados

Se devuelve el mensaje después de expirar el tiempo-entrega-diferida. Si se ha producido ésta, el mensaje va acompañado de un estampillado de fecha.

14.2.1.3 Errores

El mensaje con las instrucciones que detallan el problema en cuestión.

14.2.1.4 Descripción del procedimiento

1) Se comprueba en el mensaje la presencia del campo de **tiempo-entrega-diferida**. Si está ausente, el procedimiento devuelve el mensaje y finaliza. Si está presente, se compara el **tiempo-entrega-diferida** con el tiempo presente. Si el **tiempo-entrega-diferida** ha expirado, el procedimiento devuelve el mensaje con el campo **tiempo-entrega-diferida** y finaliza.
2) Esta etapa sólo corresponde a un mensaje del módulo entrada-mensaje. El MTA comprueba la existencia de un acuerdo bilateral que le pida que proporcione la entrega diferida de este mensaje. Si existe este acuerdo, el procesamiento continúa en el paso 3. Si no lo hay, se efectúa una de las operaciones siguientes:
   a) El procedimiento devuelve el mensaje sin diferirlo, y finaliza.
   b) El procedimiento devuelve el mensaje con una instrucción de generación de informe con un **código-motivo-no-entrega** de **entrega-diferida-no-efectuada** y un **código-diagnóstico-no-entrega** de **no-acuerdo-bilateral**. Después termina el procedimiento.
3) Según la política en vigor, se efectúa una de las operaciones siguientes:
   a) Si con el o los dominios o el o los MTA a los cuales se transferirá el mensaje existe un acuerdo bilateral en virtud del cual ese o esos dominios o ese o esos MTA se encargarán de la petición de aplazamiento, el procedimiento devuelve el mensaje sin diferirlo. Después termina el procedimiento.
   b) Se anota el instante actual como instante de llegada del mensaje, y el mensaje se retiene hasta la expiración del **tiempo-entrega-diferida**. Se devuelve entonces el mensaje con el campo **tiempo-entrega-diferida** suprimido y el estampillado de llegada, y termina el procedimiento.

NOTA – Una vez completada la dilación debe suprimirse el campo **tiempo-entrega-diferida** a fin de que cuando el mensaje se transfiera a otro dominio o MTA no exista peligro de no-entrega (véase el paso 2 b)) si los relojes no están sincronizados.

14.3 Módulo principal

El módulo principal ejecuta el grueso de tratamiento de los mensajes y sondas que entran en el MTA. La figura 6 muestra las relaciones entre el módulo principal y los módulos que puede invocar o por los que puede ser invocado. El módulo principal está sujeto a la invocación por:

1) el módulo entrada-sonda, que transfiere una sonda;
2) el módulo entrega-diferida, que transfiere un mensaje;
3) el módulo sonda, que transfiere una sonda.

En el caso de una condición de error o de la necesidad de un informe positivo de entrega, el módulo principal puede ser invocado igualmente por:

4) el módulo salida-mensaje, que transfiere un mensaje con una instrucción por-mensaje que indica el problema encontrado;
5) el módulo salida-sonda, que transfiere una sonda con una instrucción por-mensaje que indica el problema encontrado;
6) el módulo entrega-mensaje, que transfiere un mensaje con instrucciones por-destinatario que indica el problema o problemas o el suceso o sucesos encontrados;
7) el módulo prueba-entrega-sonda, que transfiere una sonda con instrucciones por-destinatario que indica el problema o problemas o el suceso o sucesos encontrados;
8) el módulo de entrega-diferida, que transfiere un mensaje con instrucciones que indican el problema encontrado.

El módulo principal contiene procedimientos que, colectivamente, proporcionan las siguientes funciones:

procesamiento de rastreo;

detección de bucle;

encaminamiento y reencaminamiento;

redireccionamiento del destinatario;

conversión de contenido;

ampliación de lista de distribución;

réplica del mensaje;

autenticación del origen de los mensajes y de las sondas;

resolución del nombre.

Los procedimientos que ejecutan estas funciones se llaman mediante el procedimiento de control que gestiona el tratamiento de cada mensaje o sonda recibido por el módulo principal. La figura 7 muestra la organización de los procedimientos de control y subsidiarios dentro del módulo principal. La figura 8 muestra el flujo de información a través de estos procedimientos.

Para cada mensaje o sonda recibido, el módulo principal llama al procedimiento de control con dicho mensaje o sonda como argumento. Como resultado, el procedimiento de control devuelve una o más réplicas del mensaje o sonda con las instrucciones apropiadas adjuntas. Dependiendo de la naturaleza de esas instrucciones el módulo principal invoca entonces:

1) el módulo de salida-mensaje, al cual cursa cada mensaje con una instrucción de transferencia por-mensaje;
2) el módulo de salida-sonda, al cual cursa cada sonda con una instrucción de transferencia por-mensaje;
3) el módulo de entrega-mensaje, al cual cursa cada mensaje con una o más instrucciones de entrega por-destinatario;
4) el módulo de prueba-entrega-sonda, al cual cursa cada sonda con una o más instrucciones de entrega por-destinatario;
5) el módulo de informe, al cual cursa cada mensaje o sonda con una instrucción por-mensaje y/o una o más instrucciones por-destinatario que indican la generación de un informe.

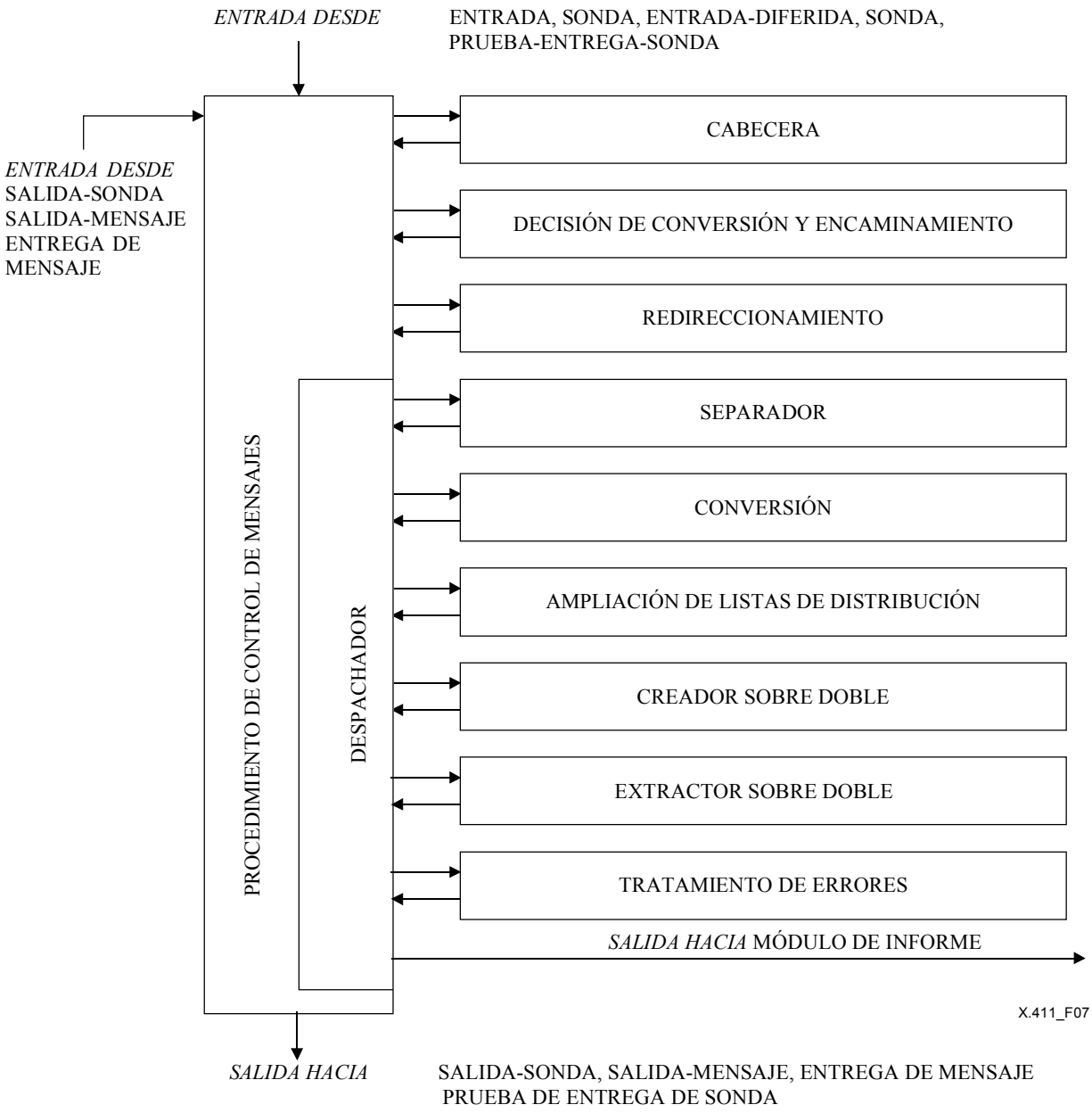
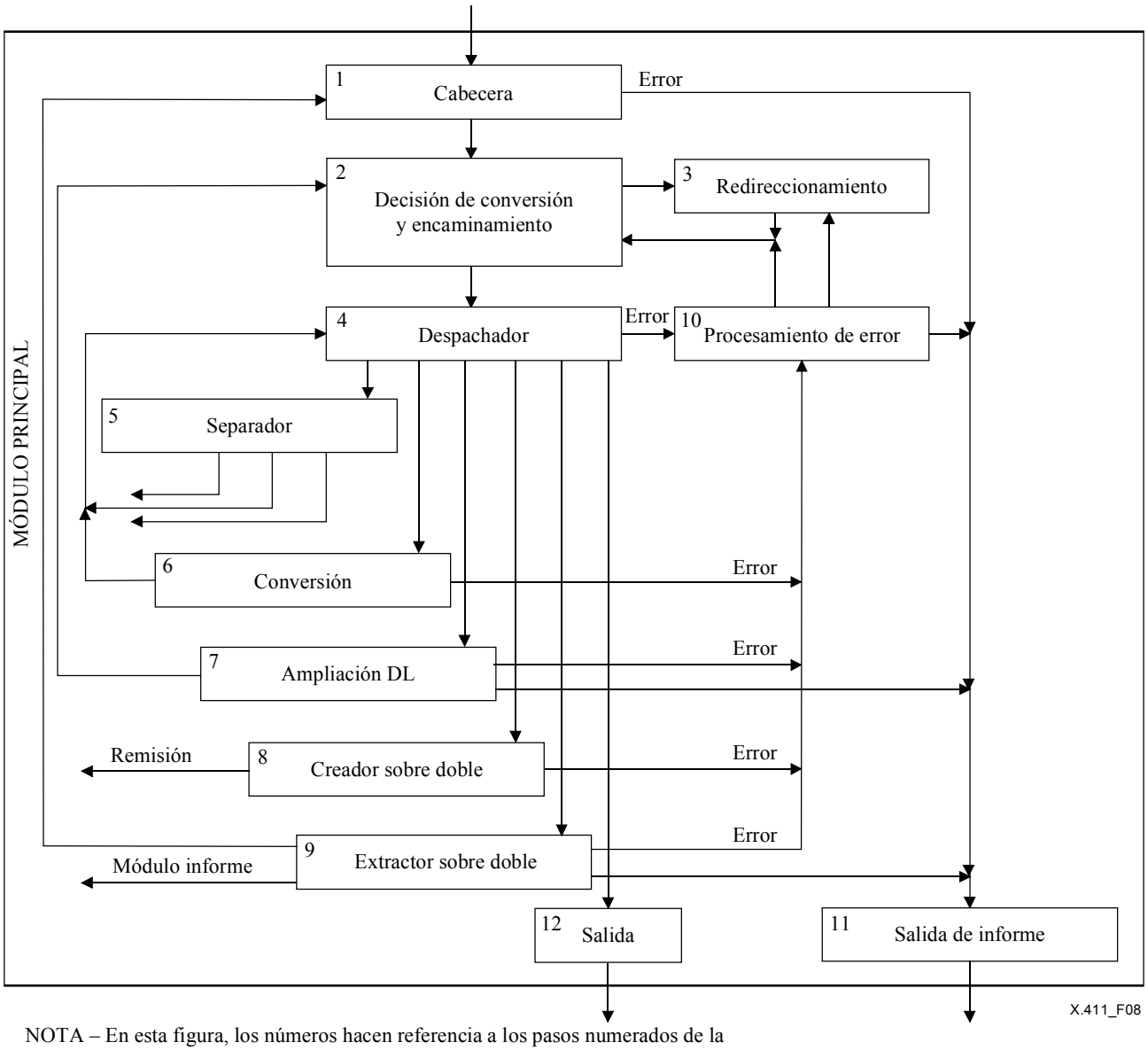


Figura 7 – Organización de los procedimientos en el módulo principal



NOTA – En esta figura, los números hacen referencia a los pasos numerados de la lógica del procedimiento de control (véase 14.3.1.4).

Figura 8 – Flujo de información dentro del módulo principal

14.3.1 Procedimiento de control

Este procedimiento dirige cada mensaje o sonda entrantes a través de los procedimientos restantes del módulo principal. El flujo global de información se muestra en la figura 8.

14.3.1.1 Argumentos

Uno de los siguientes (estos argumentos corresponden a los mensajes y sondas que pueden cursarse al módulo principal, después de invocación):

1) un mensaje o sonda sin instrucciones (procedentes del módulo de entrada-sonda o sonda);
2) un mensaje sin instrucciones, pero con indicación de tiempo opcional de instante de llegada (procedente del módulo de entrega-diferida);
3) un mensaje o sonda con una instrucción por-mensaje que describe un problema de transferencia (procedente del módulo de salida-mensaje o salida-sonda);
4) un mensaje o sonda con instrucciones por-destinatario que describen los problemas de entrega o los éxitos (procedente del módulo de entrega-mensaje o prueba-entrega-sonda).

14.3.1.2 Resultados

1) una o más réplicas del argumento del mensaje o de la sonda, cada una acompañada por una instrucción por-mensaje que indica la transferencia; y/o
2) una o más réplicas del argumento del mensaje o sonda, cada una de ellas acompañada por una o más instrucciones por-destinatario que indican la entrega o la prueba de entrega; y/o
3) una o más réplicas del argumento del mensaje o sonda, cada una acompañada por una o más instrucciones por-destinatario que indican la generación de un informe.

14.3.1.3 Errores

Ninguno. Las condiciones de error se tienen en cuenta en los resultados descritos anteriormente.

14.3.1.4 Descripción del procedimiento

1) Mensaje o sonda sin instrucciones:

   Se llama primero al procedimiento de cabecera para efectuar la inicialización del rastreo y varias comprobaciones mensaje por-mensaje, como la de expiración de mensaje y la detección de bucle de encaminamiento.

   Al recibir una devolución con instrucción de informe que indique un problema en relación con el mensaje, el proceso continúa en el paso 11.

   En todas las otras devoluciones el procedimiento continúa como sigue:

2) Se llama al procedimiento de decisión-conversión-y-encaminamiento para calcular las instrucciones de encaminamiento y conversión por-destinatario. (Son instrucciones completas que dirigirán el mensaje o sonda a través del resto de los procedimientos.)

   Si se indica una instrucción de redireccionamiento (por ejemplo, **destinatario-alternativo-asignado-destinatario**), el proceso continúa en el paso 3.

   En los demás casos restantes, el proceso continúa en el paso 4 (despachador.)

3) Se llama al redireccionamiento. Al recibir una devolución con éxito, el proceso continúa en el paso 2.

   En el caso de una devolución infructuosa, el proceso continúa en el paso 10 (manipulador-error.)

4) Despachador. El despachador actúa sobre las instrucciones generadas y transfiere el control al primero de los siguientes procedimientos que resulte aplicable:
   - división (paso 5);
   - conversión (paso 6);
   - ampliación-lista-distribución (paso 7);
   - creación-sobre-doble (paso 8);
   - extracción-sobre-doble (paso 9);
   - tratamiento-error (paso 10) en el caso en que el proceso de decisión encontró un problema, por ejemplo, error de encaminamiento;
   - salida (paso 12).

5) Se llama al divisor para la realización de réplicas, cuando se solicita en las instrucciones por-destinatario generadas en el procedimiento de decisión-conversión-y-encaminamiento. Para cada réplica el proceso continúa por separado en el paso 4 (despachador).

6) Se llama a la conversión para cada mensaje o sonda que necesite conversión.

   Al devolver con éxito el mensaje o sonda, el proceso continúa en el paso 4 (despachador).

   Después de una devolución con instrucción de informe que indica un error de conversión, el proceso continúa en el paso 10 (manipulador-error).

7) Se llama al procedimiento de ampliación-DL.

   Después de la devolución con éxito de un mensaje, el proceso continúa en el paso 2 de forma que los destinatarios resultantes de la ampliación de la DL puedan tratarse convenientemente.

   Si se devuelve una copia del mensaje con instrucciones de informe de entrega, en lugar de, o además de, la devolución anterior, el proceso continúa en el paso 11.

   Una sonda que retorna con éxito llevará instrucciones de informe; el proceso continúa en el paso 11 (generación-informe).

Después de la devolución de un mensaje o sonda con una instrucción de informe que indique una ampliación de DL, el proceso-error continúa en el paso 10.

8) Se utiliza el procedimiento de creación-de-doble-sobre cuando la instrucción de encaminamiento exige que el mensaje esté incrustado en un **contenido-del-tipo-de-sobre-interior**.

   El procedimiento termina si se obtiene el resultado esperado, ya que el servicio abstracto del sistema de transferencia de mensaje (MTA) no tiene que hacer ningún otro tratamiento en el mensaje original.

   Si no se obtiene el resultado esperado, el tratamiento continúa en el paso 10 (manipulador-error).

9) Se utiliza el procedimiento de extracción-de-doble sobre cuando se tiene una instrucción de encaminamiento para extraer el sobre interior del **contenido**.

   Si el sistema retorna un mensaje extraído o una sonda, el tratamiento del mensaje o la sonda se reanuda en el paso 1. Si el sistema retorna un informe extraído, el tratamiento del informe extraído continúa como se indica en 14.4.1. El tratamiento de las instrucciones de informe en el mensaje original también continúa, en ambos casos, en el paso 11.

   Si no se obtiene el resultado esperado, el tratamiento continúa en el paso 10 (manipulador-error).

10) Éste es el punto de recogida que alcanza el proceso al detectar que un mensaje o sonda no puede ser tratado por los procedimientos de línea principales. Se llama al procedimiento de proceso-error para buscar otro método de entrega o un destinatario-sustitutivo. Después de una devolución con éxito, el procedimiento de proceso-error indica el nuevo destinatario en una instrucción al procedimiento de decisión-conversión-y-encaminamiento (paso 2), donde continúa el proceso.

    Si no es posible el redireccionamiento, el mensaje o sonda se pasa al generador del informe (paso 11).

11) El procedimiento de control finaliza en este punto y devuelve un mensaje o sonda con las instrucciones de generación de informe.

12) Cuando un mensaje o sonda alcanza este punto, finaliza el procedimiento de control.

14.3.2 Procedimiento de cabecera

Este procedimiento efectúa la iniciación del rastreo, la detección de la expiración del mensaje, la comprobación inicial de seguridad, la detección de bucles y la comprobación de la criticidad.

14.3.2.1 Argumentos

Un mensaje o sonda y una indicación de tiempo opcional de instante de llegada.

14.3.2.2 Resultados

El mensaje o sonda con información inicializada de rastreo para este MTA.

14.3.2.3 Errores

El mensaje o sonda con instrucciones de generación del informe que detalla el problema encontrado.

14.3.2.4 Descripción del procedimiento

1) Si el mensaje ha cruzado una frontera entre dominios, se añade un **elemento-información-rastreo** de este dominio a la **retransmisión** como acción. Si el mensaje va acompañado de un tiempo llegada, es que ha habido dilación de entrega; se fija entonces **tiempo-diferido** en el instante actual, y **tiempo-llegada** en el valor de la indicación de tiempo de fecha acompañante. En caso contrario, no ha habido dilación, y se fija **tiempo-llegada** al valor del instante actual. Se añade igualmente un **elemento-información-rastreo-interno** tanto si el mensaje ha cruzado la frontera entre dominios como si no lo ha hecho.

2) Si lo requiere la política de seguridad en vigor y/o si la **verificación-autenticación-origen-mensaje** es incorrecta, el procedimiento devuelve una instrucción de generación de informe. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se fijan en **incapaz-de-transferir** y **error-mensajería-segura**, respectivamente.

3) Si alguno de los campos de ampliación **por-mensaje** o los campos de ampliación **por-destinatario** para los destinatarios cuya **responsabilidad** está puesta a **responsable** está marcado como **crítico-para-la-transferencia** pero el MTA no lo entiende semánticamente, el procedimiento devuelve una instrucción de generación de informe. Si las instrucciones de generación de informe han sido generadas por alguno (no por todos) de los destinatarios cuya **responsabilidad** tiene el valor **responsable**, se devuelve entonces una instrucción para dividir el mensaje. El **código-motivo-no-entrega** se pone en **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** en **función-crítica-no-soportada**. Finaliza entonces el procedimiento.

NOTA – Implementaciones anteriores pueden utilizar otro valor del código-motivo-no-entrega que haya sido especificado en ediciones anteriores de esta Definición de servicio.

4) Si se ha sobrepasado el **último-tiempo-entrega**, o si ha transcurrido el máximo tiempo de tránsito del sistema para la **prioridad** del mensaje, el procedimiento devuelve una instrucción de generación de informe. El **código-motivo-no-entrega** se pone en **fallo-transferencia** o en **incapaz-de-transferir** según corresponda y el **código-diagnóstico-no-entrega** se pone a **tiempo-máximo-expirado**. Finaliza entonces el procedimiento.

5) Se realiza la detección de bucles. El algoritmo de detección de bucles se encuentra fuera del alcance de esta Definición de servicio. Sin embargo, en 14.3.11 se facilita un ejemplo de algoritmo combinado de encaminamiento y de detección de bucles. Si se detecta un bucle, el procedimiento devuelve una instrucción de generación de informe. El **código-motivo-no-entrega** se pone en **fallo-transferencia** y el **código-diagnóstico-no-entrega** se pone en **bucle-detectado**. Finaliza entonces el procedimiento.

6) Según su política, el MTA puede verificar al ser remitido que el valor del **tipo-notificación** corresponde al **contenido**. Si el MTA no verifica el **tipo-notificación**, o si corresponde al **contenido**, el procedimiento termina satisfactoriamente. Si el MTA verifica el **tipo-notificación** y no corresponde al **contenido**, se efectúa una de las operaciones siguientes, según la política en vigor:

   a) se ignora la no-correspondencia y el procedimiento termina satisfactoriamente;

   b) si el **tipo-notificación** no se pone en uno de los valores tipo-1, tipo-2 o tipo-3, el **tipo-notificación** se pone al valor correcto y termina el procedimiento;

   c) si el **tipo-notificación** se pone incorrectamente en uno de los valores tipo-1, tipo-2 o tipo-3, el procedimiento devuelve una instrucción de generación de informe con un **código-motivo-no-entrega** de **incapaz-de-transferir** y un **código-diagnóstico-no-entrega** de **tipo-notificación-incorrecta**. El procedimiento termina.

El MTA puede verificar **el mensaje-servicio** con procedimientos similares.

14.3.3 Procedimiento de decisión-conversión-encaminamiento

Para cada destinatario de un mensaje o sonda cuyo responsable es el MTA, este procedimiento determina las acciones de encaminamiento y conversión, si ha lugar, que ha de tomar este MTA. Las acciones se registran como instrucciones por-destinatario asociadas al mensaje. Las acciones se llevan a cabo subsiguientemente mediante otros subprocedimientos dentro del procedimiento interno o en cualquier otro lugar del MTA.

NOTA – Para cada mensaje particular, es posible invocar más de una vez este procedimiento. En ese caso, el procedimiento ignora las instrucciones por destinatario generadas por anteriores invocaciones que aún no se han hecho actuar sobre ningún otro ente.

14.3.3.1 Argumentos

1) Un mensaje o sonda con **responsabilidad** puesta en **responsable** para aquellos destinatarios bajo la tutela de este MTA.

14.3.3.2 Resultados

El mensaje o sonda que formaron el argumento del procedimiento más las instrucciones por-destinatario nuevas o revisadas que indican el encaminamiento y la posible acción de conversión que debería emprender este MTA.

14.3.3.3 Errores

Ninguno. Las condiciones de error, si las hay, se señalan en las instrucciones por-destinatario.

14.3.3.4 Descripción del procedimiento

Se considera cada vez un destinatario. Si la **responsabilidad** está puesta en **no-responsable**, se ignora el destinatario. En caso contrario, se llama a los procedimientos de decisión-conversión y decisión-encaminamiento para cada destinatario. Cuando se han considerado todos los destinatarios se finaliza el procedimiento. Véase la figura 9.

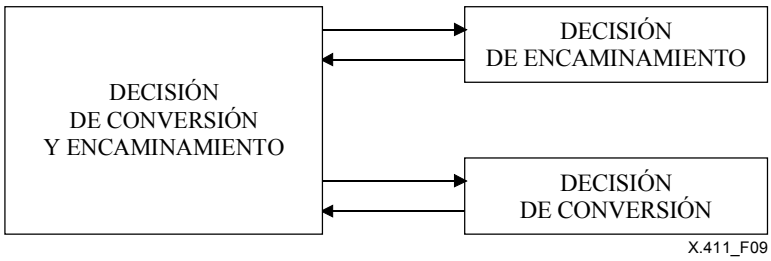


Figura 9 – Organización de los procedimientos dentro del procedimiento de decisión de conversión y en encaminamiento

14.3.4 Procedimiento de decisión-encaminamiento

Este procedimiento genera una instrucción de encaminamiento para un destinatario único del mensaje.

14.3.4.1 Argumentos

1) Un destinatario de mensaje más la instrucción por-destinatario, si la hay, aplicable a este destinatario.
2) La instrucción por-mensaje, si la hay, aplicable a este mensaje. Otros campos de mensaje resultan igualmente accesibles al procedimiento si se necesitan.

14.3.4.2 Resultados

Una instrucción de encaminamiento nueva o posiblemente revisada aplicable a este destinatario. Las posibles instrucciones son:

a) retransmisión a otro MTA;
b) entrega a un destinatario local;
c) ampliar la lista de distribución representada por este destinatario;
d) generar un informe que indique el fallo de la entrega. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** se incluyen en la instrucción;
e) redirigir a una dirección preferida o a un destinatario alternativo especificado por un destinatario.

14.3.4.3 Errores

Ninguno. Las condiciones de error se registran en la instrucción de encaminamiento.

14.3.4.4 Descripción del procedimiento

El procedimiento se describe según los siguientes pasos.

NOTA – Para garantizar que no se viole la política-seguridad durante el encaminamiento se debería comprobar que la **etiqueta-seguridad-entrega** resulta apropiada respecto del **contexto-seguridad**.

1) Si existe una instrucción por-mensaje que indica un fallo previo de retransmisión, el procedimiento calcula entonces un destino alternativo del próximo salto para este destinatario. La elección del algoritmo de encaminamiento está fuera del alcance de esta Definición de servicio. Sin embargo, en 14.3.11 se incluye un ejemplo de algoritmo aplicable. Si tuvo éxito, la **información-rastreo-interna** del mensaje se actualiza con una acción reencaminamiento **reencaminado** para reflejar el hecho de que se ha reencaminado el mensaje (véase 12.3.1). Si el mensaje tuviera que haber cruzado una frontera de dominio se actualizaría, la **información-rastreo** en consecuencia. El procedimiento devuelve una instrucción de retransmisión al destino alternativo y finaliza.

   Si no existe un siguiente salto alternativo disponible o todos los saltos siguientes disponibles han sido ensayados infructuosamente o están prohibidos, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** se pone a **fallo-transferencia** y el **código-diagnóstico-no-entrega** se pone en consonancia con el fallo de retransmisión encontrado. El procedimiento finaliza entonces.
2) Si la instrucción por-destinatario indica un fallo de entrega, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** son los suministrados por el procedimiento de entrega-mensaje o verificación-entrega-sonda. El procedimiento finaliza entonces.

3) Si el destinatario está especificado por un **nombre-OR** que sólo consta de un **nombre-directorio** (lo cual puede ocurrir a continuación de la ampliación de una lista de distribución si el miembro DL se especifica sólo por un **nombre-directorio)**, el MTA intenta conseguir en el directorio la **dirección-OR**. Si no puede determinarse la **dirección-OR,** el procedimiento devuelve una instrucción de generación de informe para este destinatario y se da por terminado. Si el **código-motivo-no-entrega** se pone a **operación-directorio-infructuosa**, y el **código-diagnóstico-no-entrega** puede ponerse en consonancia con el problema encontrado.

   En todos los demás casos, se siguen los siguientes pasos.

4) Si la **dirección-OR** del destinatario especifica sin ambigüedad un destinatario real, pero no es una dirección preferida de dicho destinatario, se genera una instrucción de redireccionamiento que consta del **nombre-OR** preferido del destinatario y el **alias** del motivo del redireccionamiento, dándose por terminado el procedimiento.

5) Si el destinatario es una lista de distribución para la cual este MTA sirve como punto de ampliación, se examina entonces el argumento de **ampliación-DL-prohibida** del mensaje. Si el valor es **ampliación-DL-autorizada** el procedimiento devuelve una instrucción de encaminamiento (sujeta a la política-seguridad en vigor) para ampliar la lista de distribución y finaliza.

   Si el valor es **ampliación-DL-prohibida** o la política-seguridad prohíbe la utilización de una DL, el procedimiento devuelve entonces una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** se pone a **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** a **ampliación-DL-prohibida**. El procedimiento finaliza entonces.

6) Si el **nombre-OR** del destinatario corresponde a un extractor-de-doble-sobre en este MTA, y el **tipo-de-contenido** de este mensaje es **sobre-interior**, el procedimiento retornará una instrucción de encaminamiento para extraer el sobre interior del **contenido**. Entonces terminará el procedimiento.

7) Si el destinatario resulta ser local, es decir, un usuario-MTS directamente soportado por este MTA, se siguen los siguientes pasos:

   a) Si la **dirección-OR** no especifica inequívocamente un destinatario local real, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-de-motivo-de-no-entrega** se pone a **incapaz-de-transferir** y el **código-de-diagnóstico-de-no-entrega** se pone a **nombre-OR-no-reconocido** o **nombre-OR-ambiguo**, según corresponda. El procedimiento finaliza entonces.

   b) Si la **dirección-OR** especifica inequívocamente un destinatario local real, se comprueban los parámetros de registro del destinatario para las **redirecciones-asignadas-por-el-destinatario**. En la determinación de un destinatario alternativo se debe comprobar la **etiqueta-de-seguridad-de-usuario** respecto de la **etiqueta-de-seguridad-del-mensaje** para garantizar que no se produce ninguna violación de la política de seguridad.

      Si para este destinatario se han registrado **redirecciones-asignadas-por-el-destinatario**, están autorizadas por el campo **reasignación-de-destinatario-prohibida**, y lo permite la política de seguridad, se compara los **tipos-de-información-codificada**, la **longitud-de-contenido**, el **tipo-de-contenido**, las **etiquetas-de-seguridad-del-mensaje**, la **prioridad**, el **nombre-del-originador**, la **historia-de-redireccionamiento** y la **historia-de-ampliación-DL** del mensaje, con cada **clase-de-redireccionamiento** del **destinatario-alternativo-asignado-por-el-destinatario** hasta que se encuentra una **clase-de-redireccionamiento** cuyos valores especificados concuerdan con los del mensaje. Si se encuentra esta clase-de-redireccionamiento, el **destinatario-alternativo-asignado-por-el-destinatario-asociado** constituye el primer argumento de una llamada al procedimiento de redireccionamiento. Los otros argumentos son una indicación del destinatario que debe ser sustituido, el mensaje y el motivo-de-redireccionamiento **destinatario-alternativo-asignado-por-el-destinatario**.

      Una vez completado normalmente el procedimiento de redireccionamiento, se reintroduce el procedimiento de decisión de encaminamiento. Si el procedimiento de redireccionamiento indica un error de bucle de redirección, el control pasa al procedimiento de procesamiento de error.

   c) Si las **redirecciones-asignadas-por-el-destinatario** no han causado el redireccionamiento del mensaje, y se ha registrado una o más **clases-entregables**, el MTS determina si el mensaje satisface los criterios especificados al menos por una **clase-entregable**, y puede ser entregado.

Para cada **clase-entregable**, los **tipos-de-información-codificados** del mensaje se comparan con las **constricciones-de-los-tipos-de-información-codificada** del destinatario, el **tipo-de-contenido** del mensaje se compara con los **tipos-de-contenido-entregables** del destinatario, la **longitud-de-contenido** del mensaje se compara con la **longitud-de-contenido-máxima-entregable** del destinatario, y las **etiquetas-de-seguridad** del mensaje se comparan con las **etiquetas-de-seguridad-entregables** del destinatario.

Para decidir si un mensaje puede ser entregado, el componente **constricciones-de-tipos-de-información-codificada** se utiliza junto con los **tipos-de-información-codificada** especificados en el mensaje (los **tipos-de-información-codificada-convertida** del último elemento de información de rastreo que lo contiene, o en los demás casos, los **tipos-de-información-codificada-original**):

Si en el mensaje no se especifica **tipo-de-información-codificada**, o si el componente **constricciones-de-tipo-de-información-codificada** está ausente, el mensaje satisface las **constricciones-de-tipo-de-información-codificada** de esta **clase-entregable**.

En los demás casos, si se especifican **tipos-de-información-codificada-no-aceptables**, y el mensaje contiene al menos un **tipo-de-información-codificada** que concuerda, el mensaje no satisface las **constricciones-de-tipo-de-información-codificada** de esta **clase-entregable**.

En los demás casos, si se especifican **tipos-de-información-codificada-aceptables**, y el mensaje contiene al menos un **tipo-de-información-codificada** que concuerda, el mensaje satisface las **constricciones-de-tipos-de-información-codificada** de esta **clase-entregable**.

En los demás casos, si se especifican **tipos-de-información-codificada-exclusivamente-aceptable**, y el mensaje contiene al menos un **tipo-de-información-codificada** que no concuerda con ninguno en la lista, el mensaje no satisface las **constricciones-de-tipo-de-información-codificada** de esta **clase-entregable**.

En los demás casos, el mensaje satisface las **constricciones-de-tipos-de-información-codificada** de esta **clase-entregable**.

El MTS no entregará el mensaje a menos que satisfaga todas las constricciones de al menos una de las **clases-entregables** registradas.

d) El parámetro de registro **entrega-restringida** se utiliza para decidir si se puede entregar el mensaje:

Si el parámetro **entrega-restringida** no está registrado, el mensaje puede ser entregado.

Si se ha registrado una o más **restricciones**, se compara el **nombre-del-originador**, el **nombre-OR** para cada elemento de **historia-de-ampliación-DL**, y el **nombre-OR** de cada elemento de **historia-de-redireccionamiento** del mensaje con cada **restricción** registrada (que tiene objetos puestos a mensajes o ambos) hasta que se produzca una concordancia. Si se permite la entrega en la restricción concordante, se devuelve una instrucción de entrega, y si no se permite, se devuelve una instrucción de generación de informe.

El procedimiento para determinar una concordancia-exacta de **nombres-OR** se describe en la regla de concordancia-de-nombres-OR en 12.4.4, y la concordancia según modelo en la regla de concordancia de los elementos-de-nombres-OR en 12.4.5, de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

e) Si no se encuentra ningún problema, el procedimiento de decisión-de-encaminamiento devuelve una instrucción de entrega para este destinatario y termina.

Si existe un problema en el mensaje y los parámetros de registro, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-de-motivo-de-no-entrega** se pone en **incapaz-de-transferir** y el **código-de-diagnóstico-de-no-entrega** se pone en consonancia con el problema de mensaje encontrado y el procedimiento termina.

8) Si el destinatario no es local para este MTA, se tiene en cuenta las consideraciones de entrega del paso 6. Si éstas no generan una instrucción, el procedimiento de decisión-encaminamiento intenta determinar una siguiente instrucción de salto (sujeta a la política-seguridad en vigor) para este destinatario. Si tiene éxito, se devuelve una instrucción de retransmisión al siguiente salto y finaliza el procedimiento.

Si los principios de seguridad establecen que es necesario un doble sobre para el siguiente salto identificado, y el **tipo-de-contenido** del mensaje no es **sobre-interior**, el procedimiento retornará una instrucción de encaminamiento para intercalar ese mensaje dentro del **contenido** de un nuevo mensaje, siguiendo el procedimiento que se especifica en 14.3.13. Entonces terminará el procedimiento.

Si no puede determinarse el salto siguiente, el procedimiento devuelve una instrucción de generación de informe a este destinatario. El **código-motivo-no-entrega** se pone en **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone en consonancia con el problema encontrado. Finaliza entonces el procedimiento.

14.3.5 Procedimiento de decisión-conversión

Este procedimiento genera una instrucción de conversión para un destinatario único del mensaje.

14.3.5.1 Argumentos

1) Un destinatario de un mensaje o sonda más la instrucción por destinatario, si existe, aplicable a este destinatario.
2) Otros campos de mensaje son considerados igualmente por el procedimiento:
   a) los **tipos-información-codificada** actuales, dados por los últimos **tipos-información-codificada-convertida** en la **información-rastreo**, si existe tal campo, o por **tipos-información-codificada-original;**
   b) **conversión-implícita-prohibida;**
   c) **conversión-con-pérdida-prohibida;**
   d) **conversión-explícita.**

14.3.5.2 Resultados

1) una instrucción de conversión de contenido aplicable a este destinatario y, posiblemente;
2) una instrucción revisada de encaminamiento que indica la salida-retransmisión o salida-sonda hacia un MTA capaz de realizar la conversión-requerida o, en lugar de los 1) y 2) anteriores;
3) una instrucción para generar un informe que indica un fallo de entrega. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** se incluyen en esta instrucción.

14.3.5.3 Errores

Ninguno. Las condiciones de error se registran en la instrucción de encaminamiento.

14.3.5.4 Descripción del procedimiento

NOTA – Como las circunstancias bajo las cuales MTA realiza la conversión pueden estar sujetas a ulterior normalización, no resulta práctico describir un procedimiento para decidir qué EIT se requieren para la salida de la conversión. Por ejemplo, si un MTA intermedio desarrolla la conversión, no existe ningún camino normalizado para conocer los EIT que puede manejar un usuario-MTS. En consecuencia, las siguientes cláusulas suponen que el MTA conoce los EIT para la conversión.

1) Si se requiere una conversión explícita para este destinatario, el procedimiento comienza en el paso 6.
2) Si se requiere una conversión implícita pero el destinatario no está abonado a la facilidad de conversión implícita, el procedimiento devuelve una instrucción de informe negativo en el **código-motivo-no-entrega** de **conversión-no-realizada** y el **código-diagnóstico-no-entrega** de **conversión-implícita-no-abonada**. Finaliza entonces el procedimiento.
3) Si la conversión requerida no resulta práctica, el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada** y el **código-diagnóstico-no-entrega** de **conversión-no-práctica**. Finaliza entonces el procedimiento.
4) Si se requiriese, la conversión del mensaje pero estuviese prohibida, el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada**, y el **código-diagnóstico-no-entrega** de **conversión-prohibida**. Finaliza entonces el procedimiento.
5) Si la conversión requerida causara una pérdida de información y el campo de **conversión-con-pérdida-prohibida** adopta el valor de **con-pérdida-prohibido**; el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada** y uno de los siguientes **código-motivo-no-entrega**, según proceda:

   línea-demasiado-larga;

   página-partida;

   pérdida-símbolo-pictórico;

   pérdida-símbolo-puntuación;

   pérdida-carácter-alfabético; o

   pérdida-información-múltiple.

   Seguidamente, termina el procedimiento.

6) Si la conversión requerida no puede ser realizada por este MTA, y se sabe que otro MTA puede efectuarla, no se genera instrucción de conversión. La instrucción de encaminamiento previamente generada se cambia por salida-transferencia o salida-sonda, con un destino del próximo salto apropiado para el MTA en cuestión. Debe tratarse de evitar un bucle de encaminamiento. Seguidamente, termina el procedimiento.

7) Si la conversión requerida puede ser efectuada por este MTA, el procedimiento devuelve una instrucción de efectuar la conversión, y finaliza.

14.3.6 Procedimiento de proceso-error

Cuando otro procedimiento encuentra un error de capacidad de entrega o encaminamiento, se llama a este procedimiento para determinar si pueden lograrse la entrega o el encaminamiento mediante la reasignación del destinatario o eligiendo una **dirección-OR** diferente para el mismo destinatario. En caso contrario, debe señalarse la no-entrega al módulo de informe. Los errores que provocan una llamada a este procedimiento son:

- **nombre-destinatario** que no identifica un usuario-MTS o DL;
- fallo de entrega;
- un MTA que es incapaz de realizar la conversión necesaria;
- problemas del trayecto de transferencia;
- problemas de ampliación DL;
- violaciones de seguridad;
- conflicto con parámetros de registro.

NOTA – La acción emprendida en relación con el proceso-error deberá estar sujeta a la política-seguridad en vigor.

14.3.6.1 Argumentos

1) Un mensaje o sonda con los campos por-destinatario que provocaron el problema.
2) Instrucciones de informe que indican el error.

14.3.6.2 Resultados

El mensaje o sonda en cuestión con un campo de **nombre-destinatario**, actualizado, o

1) el mensaje o sonda en cuestión;
2) instrucciones de informe.

14.3.6.3 Errores

Ninguno.

14.3.6.4 Descripción del procedimiento

NOTA – Un determinado destinatario puede llamar a este procedimiento múltiples veces. Ocasionalmente agotará todas las alternativas y ejecutará el paso 5 para informar del fallo.

1) Los argumentos se comprueban respecto de un **nombre-directorio**. Si hay uno presente, se hace una llamada al procedimiento de resolución de nombre de directorio (véase 14.3.12) para determinar una nueva **dirección-OR**. Si ésta es diferente de la **dirección-OR** original se combina con el **nombre-directorio** para constituir el **nombre-OR** de un destinatario alternativo. Se llama entonces al procedimiento de redireccionamiento para redireccionar el mensaje a su destinatario alternativo, con el motivo-redireccionamiento **búsqueda-directorio**.

2) En caso contrario, el procedimiento determina si se especificó un **destinatario-alternativo-solicitado-originador** para el destinatario en cuestión. Si es así, y es distinto del **nombre-destinatario** actual se llama al procedimiento de redireccionamiento junto con el mensaje, indicados los campos pertinentes como argumento. Al volver satisfactoriamente del redireccionamiento, el procedimiento finaliza devolviendo como resultado el mensaje ahora redirigido.

3) En caso contrario, el procedimiento efectúa una comprobación para el error de entrega y si está presente comprueba la causa del error examinando el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega**. Si la **dirección-OR** del destinatario no identifica un usuario-MTS o un DL, se comprueban los **indicadores-por-mensaje** en relación con el **destinatario-alternativo-autorizado**. Si el valor encontrado resulta ser **destinatario-alternativo-autorizado** y se ha configurado el MTA con un destinatario-alternativo para esta clase de destinatario que es distinto del **nombre-destinatario** actual, se llama entonces al redireccionamiento para dirigir el mensaje al destinatario-alternativo. Al volver

satisfactoriamente del redireccionamiento, finaliza el procedimiento devolviendo entonces como resultado el mensaje redirigido.

4) La manipulación de los errores que pueden resolverse, pero que son debidos a otros problemas diferentes del direccionamiento constituye un asunto local, por ejemplo, el encaminamiento a otro MTA dentro del dominio debido a problemas de conversión.

5) Si el error de entrega es de otro tipo diferente de los citados anteriormente, o si el valor del **destinatario-alternativo-autorizado** es un **destinatario-alternativo-prohibido**, o si no existe ningún destinatario-alternativo-especificado-MD que resulte adecuado, el procedimiento devuelve una instrucción de informe y finaliza.

14.3.7 Procedimiento de redireccionamiento

Este procedimiento redirecciona un mensaje.

NOTA – La utilización de las facilidades de redireccionamiento deberá ajustarse a la política-seguridad en vigor.

14.3.7.1 Argumentos

1) El **nombre-OR** del destinatario sustitutivo a quien se ha de redirigir el mensaje.
2) Los campos del mensaje por-destinatario para el destinatario que va a ser sustituido por uno alternativo.
3) El mensaje o sonda que ha de redirigirse.
4) Motivo del redireccionamiento.

14.3.7.2 Resultados

El mensaje o sonda suministrado en el tercer argumento con el destinatario identificado en el segundo argumento sustituido por el destinatario sustitutivo especificado en el primer argumento.

14.3.7.3 Errores

Indicación de que se ha detectado un bucle de redireccionamiento.

14.3.7.4 Descripción del procedimiento

1) El procedimiento garantiza primero que el redireccionamiento al destinatario sustitutivo especificado no provocará un bucle de redireccionamiento. La **dirección-OR** del destinatario sustitutivo suministrado en el argumento 1 se compara con cada **nombre-destinatario-deseado** de la secuencia de la **historia-redireccionamiento** procedente de los campos por-destinatario identificados en el argumento 2. Después de una concordancia, el procedimiento finaliza indicando que se ha detectado un bucle de redireccionamiento.
2) Se añade un elemento a la **historia-redireccionamiento** (que se crea si no está presente), utilizando el **nombre-destinatario** del argumento 2 para formar el **nombre-destinatario-deseado**, obteniendo el **motivo-redireccionamiento** a partir del argumento 4 e incluyendo el instante en que se efectúa ese redireccionamiento. El **nombre-OR** suministrado por el primer argumento se sustituye entonces por ese **nombre-destinatario**.
3) En el campo de **otras-acciones** de la **información-rastreo** e **información-rastreo-interna** vigente, si la **operación-dl** no está ya indicada, se indica entonces el valor **redirigido**; en otro caso se crean los nuevos elementos **información-rastreo** e **información-rastreo-interna** con el valor **redirigido** indicado.
4) El sobre de transferencia del mensaje se actualiza de la forma siguiente:

nombre-destinatario:	sustituido;
información-rastreo/información-rastreo-interna:	indica **redirigido**;
historia-redireccionamiento:	añadir **nombre-destinatario** previo y **motivo-redireccionamiento**;
destinatario-alternativo-solicitado-originador:	suprimido si y sólo si el **motivo-redireccionamiento** indica el **destinatario-alternativo-solicitado-originador**.

14.3.8 Procedimiento de división

El divisor produce réplicas de los mensajes y de las sondas según se necesiten para un proceso ulterior. Se modifican estas réplicas según proceda, para indicar la distribución de la **responsabilidad** para los diferentes destinatarios procedentes del original. Cada réplica se acompaña de una instrucción por-mensaje que indica su disposición ulterior dentro del MTA.

NOTA – La utilización de las facilidades del divisor deberá ajustarse a la política-seguridad en vigor.

14.3.8.1 Argumentos

Un mensaje o sonda. Para cada destinatario con **responsabilidad** puesta en **responsable**, acompaña al mensaje una instrucción de encaminamiento/conversión.

14.3.8.2 Resultados

Una o más réplicas del mensaje original o de la sonda con la **responsabilidad** convenientemente indicada, y una instrucción por mensaje que indique la ulterior disposición de la réplica dentro del MTA.

14.3.8.3 Errores

Ninguno.

14.3.8.4 Descripción del procedimiento

El separador examina las instrucciones generadas por el procedimiento de decisión-encaminamiento-y-conversión para segregar (conceptualmente) los destinatarios con **responsabilidad** puesta en **responsable** en grupos. Se crea una réplica para cada grupo. El proceso posterior para dichas réplicas (en otros procedimientos) depende de las instrucciones de conversión y encaminamiento aplicables al grupo que representa.

NOTA 1 – En un MTA se necesita una réplica del módulo debido al tratamiento posiblemente diferenciador que necesitan los diferentes destinatarios de un mensaje. Estas diferencias surgen de la necesidad de más de un trayecto de retransmisión para salir de un MTA, de la necesidad de llevar a cabo más de una conversión sobre el contenido del mensaje y de la necesidad de ampliar las listas de distribución. Por ejemplo, cuando existe más de un trayecto de retransmisión, debe crearse una copia separada del mensaje para cada uno de dichos trayectos, con los valores de **responsabilidad** adecuados para los destinatarios que se encuentran a lo largo del trayecto.

NOTA 2 – La determinación de cuáles son las réplicas que se necesitan es un asunto local, que se realiza de forma que se reduzca al mínimo el número total de las réplicas creadas. Los párrafos siguientes sugieren un enfoque pero no pretenden en forma alguna imponer limitaciones al método seguido en una aplicación real.

NOTA 3 – Para mayor sencillez de exposición, se describe el divisor como un algoritmo de un solo-paso. Es decir, se crean todas las réplicas necesarias antes de cualquier proceso posterior. Una optimización importante consistiría en dividir de forma mínima el mensaje para conversión, y completar entonces la separación de las copias convertidas.

1) El procedimiento considera primero aquellos destinatarios para los cuales existen instrucciones de conversión de contenido. Estos destinatarios se agrupan de forma que los miembros de cada grupo estén sujetos a instrucciones de conversión idénticas. Se crea una réplica para cada grupo con **responsabilidad** puesta en **responsable** para los destinatarios de este grupo y **no-responsable** para todos los demás.
2) Se examinan entonces los destinatarios para los cuales existen instrucciones de ampliación-DL. Se crea una réplica para cada destinatario de dicha DL con **responsabilidad** puesta en **no-responsable** para todos los destinatarios excepto para la única DL que produjo la réplica.
3) Se subdividen posteriormente los grupos en base a las llamadas de instrucciones de encaminamiento por-destinatario para salida-transferencia o salida-sonda. Estos destinatarios se agrupan de forma que cada grupo comparta un destino común para el próximo salto. Se crea una réplica para cada uno de estos grupos con **responsabilidad** puesta en **responsable** para los destinatarios del grupo, y **no-responsable** para todos los restantes. Para todos los destinatarios de cada uno de estos grupos, éste será el primer intento de retransmisión o un intento de reencaminamiento. En el último caso, se modifica la información-rastreo para el mensaje o sonda con el fin de indicar que éste es el primer reencaminamiento o uno subsiguiente.
4) Finalmente, las instrucciones de encaminamiento para algunos destinatarios llamarán a entrega-mensaje o a generación-informe. Se crea una réplica para cada uno de estos subgrupos con **responsabilidad** puesta en **responsable** para los destinatarios del grupo y **no-responsable** para todos los demás.
5) Si no se solicita la **revelación-de-otros-destinatarios**, pueden suprimirse los destinatarios cuya **responsabilidad** esté puesta a **no-responsable**.
6) Cualquier ampliación-por-destinatario para aquellos destinatarios cuya **responsabilidad** está puesta a **no-responsable** puede suprimirse.
7) Finaliza entonces el procedimiento.

14.3.9 Procedimiento-conversión

Este procedimiento realiza conversiones sobre mensajes e indica aquellas conversiones que habrían sido realizadas sobre las sondas.

14.3.9.1 Argumentos

Un mensaje o sonda con indicación de la conversión o conversiones requeridas.

14.3.9.2 Resultados

El mensaje o sonda con conversiones realizadas e indicadas (sólo indicadas en el caso de una sonda).

14.3.9.3 Errores

El mensaje o sonda con instrucciones de informe que detallan los problemas de conversión encontrados.

14.3.9.4 Descripción del procedimiento

1) Para un mensaje, se realizan los procedimientos de conversión para EIT incorporados según se define en la Recomendación X.408 del CCITT. Los procedimientos de conversión entre los EIT definidos externamente y entre los EIT incorporados y los definidos externamente están fuera del alcance de esta Definición de servicio.
2) Después de la conversión, se actualiza la **información-rastreo** del mensaje o de la sonda para este dominio y la **información-rastreo-interno** para este MTA para mostrar los EIT convertidos. Finaliza entonces el procedimiento.

14.3.10 Procedimiento de ampliación-lista-distribución

Este procedimiento toma un mensaje con un único destinatario de la DL y devuelve un mensaje cuya lista de destinatarios incluye los miembros de la DL. Para una sonda, verifica si se produciría una ampliación-DL, si ésta se solicita.

NOTA – La utilización de la ampliación-DL deberá estar sujeta a la política-seguridad en vigor.

14.3.10.1 Argumentos

1) un mensaje con información que indique la DL de destinatarios que debe ampliarse; o
2) una sonda con información que indique la DL de destinatarios cuya ampliación ha de verificarse.

14.3.10.2 Resultados

1) el mensaje con cero o más destinatarios que representan los miembros de la DL. Pueden actualizarse otros campos según se indica a continuación en la descripción del procedimiento;
2) opcionalmente, el mensaje con instrucciones para generación de informe que indica una entrega con éxito, o
3) la sonda con instrucciones para generación de informe.

14.3.10.3 Errores

1) Una instrucción de informe que indica un fallo de entrega. Los valores para el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** son los indicados en la descripción del siguiente procedimiento.
2) En el caso de una DL recurrente, el procedimiento finaliza sin devolver ni errores ni resultados.

14.3.10.4 Descripción del procedimiento

1) Para un mensaje (no para una sonda), hacer la detección de recurrencia: se examinan los componentes del campo de la **historia-ampliación-DL** para detectar la aparición del nombre de un destinatario de la DL. La ampliación DL se realiza utilizando un asiento almacenado en el directorio o mediante una configuración local de los miembros de la DL. Cuando la DL se amplía utilizando el directorio, el **nombre-directorio** distinguido de la DL se comparará, tras eliminar la referencia a cualquiera de los alias, con el **nombre-directorio** de cada **nombre-OR** en la **historia-ampliación-DL**, y se ignorará la **dirección-OR**. Cuando la DL se amplía utilizando una configuración local, cada MTA capaz de ampliar la DL debe conocer todas las **direcciones-OR** de la DL, se realiza una detección recurrente comparando las **direcciones-OR**.

   Si el nombre de los destinatarios de la DL se encuentra presente en la **historia-ampliación-DL**, se define la DL de forma recurrente y no deberá ser ampliada ulteriormente. Se descarta el mensaje y no se devuelven ni informes ni otros resultados. Finaliza el procedimiento de ampliación.

2) Adquisición de la DL: El procedimiento de ampliación intenta adquirir los atributos de la DL.

   Si no tiene éxito, el procedimiento devuelve una instrucción de informe con el **código-motivo-no-entrega** de **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** que procedan. Finaliza entonces el procedimiento.

3) Verificación del permiso de remisión: Si se trata de un mensaje (no de una sonda), el último elemento del campo de la **historia-ampliación-DL** (si ha lugar) diferente del **nombre-originador** se considera como el emisor del mensaje. Para una sonda, el originador es el emisor del mensaje.

   El nombre del emisor se compara con los componentes del permiso-remisión-DL. Si no existe coincidencia, se devuelve una instrucción de informe con el **código-motivo-no-entrega** de **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** de **no-permiso-remisión-DL**. Finaliza entonces el procedimiento.

4) Para una sonda: Si ninguna otra política local impidiera una entrega deseada, se devolvería entonces una instrucción de informe para indicar la entrega con éxito. Finaliza entonces el procedimiento.

5) Para un mensaje: La bandera **responsabilidad** del destinatario de la DL se pone a **no-responsable**. Si el MTA que realiza la expansión de DL soporta el argumento **destinatario-exentos-DL**, los miembros de la DL son comparados con los valores de este argumento. Si cualquier valor del argumento **destinatario-exentos-DL** carece de un componente **dirección-OR**, éste se obtiene del atributo direcciones OR del MHS de la inserción de directorio de ese argumento. Si están presentes múltiples direcciones OR en ese atributo de directorio, cada valor se incorpora en el argumento. Los componentes **dirección-OR** y **nombre-directorio** del atributo destinatario-exentos-DL son comparados para verificar la igualdad con los valores **dirección-OR** o **nombre-directorio** (utilizando la regla **concordancia-nombre-OR** descrita en 12.4.4 de la Rec. UIT-T X.413 | ISO/CEI 10021-5) para cada miembro de la DL. Si el componente **dirección-OR** o **nombre-directorio** concuerda para un miembro de la DL, ese miembro no será añadido como un nuevo destinatario del mensaje. El argumento **destinatario-exentos-DL** será retenido sin modificación en el sobre, con independencia de cuántos elementos concordaron satisfactoriamente con los miembros de la DL. Todos los miembros de la DL que no concuerdan con un valor de **destinatario-exentos-DL** serán añadidos como nuevos destinatarios del mensaje. Los campos por-destinatario para cada nuevo destinatario se copian de los del destinatario de la DL, salvo lo que sigue:

   nombre destinatario: miembro de la DL.

   Los siguientes campos por-destinatario se copian o cambian según la política de DL local:

   petición-informe-MTA-originador (véase la nota 1);

   petición-informe-originador (véase la nota 1);

   destinatario-alternativo-solicitado-originador (véase la nota 2);

   conversión-explícita;

   prueba-de-petición-entrega (véase la nota 4);

   método-entrega-solicitado;

   testigo-mensaje (véase la nota 6);

   testigo-cifrado-parte-cuerpo (véase la nota 6);

   testigo-contenido-reenviado (véase la nota 6).

NOTA 1 – Debe copiarse y no modificarse si la política-DL debe devolver los informes; puede modificarse en caso de necesidad si la política-DL no debe devolver los informes.

NOTA 2 – El **destinatario-alternativo-solicitado-originador** puede eliminarse o sustituirse, según la política de la DL local, o copiarse, pero sólo si la política-de-DL local lo exige explícitamente.

NOTA 3 – Cualquiera de los miembros-DL que identifican las DL que aparecen en la **historia-ampliación-DL** puede ser excluido de la ampliación de la DL y no ser incluido entre los nuevos destinatarios del mensaje.

NOTA 4 – El que la **petición-prueba-de-entrega** produzca una **prueba-de-entrega** desde el punto de ampliación DL, o de los miembros DL, o de ambos, o de ninguno de los dos, depende de la política DL y de la política de seguridad en vigor.

NOTA 5 – Cuando un miembro de la DL se identifica sólo con un nombre de directorio, el proceso necesario para obtener una **dirección-OR** está descrito en el procedimiento de decisión de encaminamiento.

NOTA 6 – Cuando se amplia un mensaje que contiene datos criptados en un testigo para el destinatario de la DL, los datos criptados se descriptan utilizando la clave privada de la DL y se crea un nuevo testigo para cada destinatario miembro con los datos descriptados redescriptados utilizando el primer algoritmo en el preferencia-algoritmo-criptación-testigo que es soportado por el MTA que amplia la DL y por ese miembro DL y el nuevo testigo firmado utilizando el primer algoritmo en la preferencia-algoritmo-firma-testigo que es soportado por el MTA que amplía la DL y por ese miembro DL.

6) En el campo de **otras-acciones** de la **información-rastreo** e **información-rastreo-interna** vigente, si **redirigido** no está ya indicado, se indica entonces el valor **operación-dl**; en otro caso se crean los nuevos elementos **información-rastreo** e **información-rastreo-interna** con el valor **operación-dl** indicado.

7) El valor del **nombre-destinatario** del destinatario de la DL (que incluye su **nombre-directorio** distinguido, tras la eliminación de cualquier alias, si es que tiene alguno) y el instante en que se ha producido la expansión se añaden al campo de **historia-ampliación-DL** del mensaje.

NOTA 7 – El valor actual del **nombre-destinatario** será un valor preferido como resultado de las acciones especificadas en 14.3.4.4, elemento 3).

8) Si los valores de la nueva petición de informe (determinados en el paso 5) o la política local de DL impiden que el originador reciba de los miembros de la DL un informe de entrega solicitado, se construye una copia del mensaje, con instrucciones de petición del informe de entrega para la DL ampliada, y se devuelve junto con el mensaje.

   En este caso (cuando la política de DL no envía informes desde los miembros de la DL hacia el originador), si cualquier miembro de la DL tiene asociado el contexto de originador-de-reiniciación-de-DL (véase la Rec. UIT-T X.402 | ISO/CEI 10021-2), se utiliza un procedimiento parecido al procedimiento de separación para hacer dos copias del mensaje: una copia para los miembros sin el contexto de originador-de-reiniciación-de-DL y el otro para miembros con el contexto de originador-de-reiniciación-de-DL. En la copia para los miembros con el contexto de originador-de-reiniciación-de-DL, el campo de nombre-de-originador se cambia al nombre-OR del propietario de la DL.

9) El procedimiento devuelve el mensaje revisado y la petición de informe facultativa, tras lo cual finaliza.

14.3.11 Algoritmos de detección de bucle y de encaminamiento

Los algoritmos de encaminamiento y de detección de bucle para su utilización entre dominios y dentro de un dominio se encuentran fuera del alcance de esta Definición de servicio. Para exponer los aspectos que deben considerarse, la parte restante de esta cláusula define un método para el encaminamiento y la detección de bucle. Este texto es informativo.

Los párrafos que siguen describen un método sencillo de detección de bucle junto con un algoritmo de encaminamiento mínimo. El algoritmo es mínimo en el sentido de que presupone únicamente un conocimiento mínimo de cada MD y realiza los pasos de transferencia para evitar bucles (en el sentido que se indica a continuación). Por supuesto, este algoritmo puede mejorarse cuando un MD conoce mejor la topología de la red de los MD.

El algoritmo reconoce el hecho de que, en general, está legitimado (es decir, no deberían detectarse bucles) para entrar de nuevo en un MD si otro MD ha realizado una operación específica desde el último paso a través del MD antes de entrar de nuevo en él. Las operaciones legítimas son: conversión, ampliación-DL y redireccionamiento.

1) Notación: La secuencia de información de rastreo está constituida por **elementos-información-rastreo** designados de una forma simplificada como [MD, acción-encaminamiento, operación], donde MD es el nombre de un MD, la acción de encaminamiento es "retransmitido" o "reencaminado", la operación es "conversión", "operación-DL", "redireccionamiento" o "nada". M designa el mensaje que hay que transferir. MD(o) designa el MD vigente (aquel que detecta en ese momento el bucle). Los vecinos representan el conjunto de los MD adyacentes seleccionados [vecinos del MD(o)] que constituyen posibles MD-retransmisores para M. Info-rastreo* es la secuencia de info-rastreo obtenida considerando la cola de la secuencia info de rastreo que comienza con el último elemento de info de rastreo [MD, r, op] donde op no es nada (nada indica que no ha sido realizada ninguna operación por ningún MD).

2) Detección de bucle: Se examina info-rastreo para los bucles. Se detecta un bucle si la secuencia de info-rastreo contiene una subsecuencia posterior [MD(o), retransmitido, op(o)] ... [MD(p), retransmitido, op(p)] donde para todos los j tales que $o < j \leq p$ el elemento de info de rastreo asociado es [MD(j), retransmitido, op(j)] y op(j) = nada. Es decir, se detecta un bucle si M llega a un MD que lo ha retransmitido ya y después cada MD lo ha retransmitido igualmente sin realizar ninguna otra operación que no sea la de encaminamiento. Si se detecta un bucle, entonces el algoritmo devuelve un error que indica el problema y finaliza.

3) Establecimiento del encaminamiento: Si no se detecta ningún bucle, se ajusta el conjunto, vecinos, si procede, para los pasos de transferencia de evitar-bucle en el contexto del presente mensaje. (El ajuste no afecta a ningún otro mensaje.)

   a) Si no existe ningún bucle ni ninguna aparición de [MD(o), r, op] en Info-rastreo* no se modifica vecinos.

b) Si no existe ningún bucle pero hay una aparición de [MD(o), r, op] en Info-rastreo* se eliminan de vecinos todos los MD que aparezcan en este sufijo del Info-rastreo* que comienza con [MD(o), r, op]. Se modifica el elemento de info de rastreo añadido por el dominio vigente para mostrar reencaminado como acción de reencaminar. Se añade un parámetro MD-previo determinado de la forma siguiente: se coloca el último elemento de info de rastreo [MD(o), r, op] en info de rastreo. El MD-previo es el MD que aparece en el primer elemento de info de rastreo después del último elemento de info de rastreo de [MD(o), r, op].

c) En los casos a) y b) si vecinos está vacío, el algoritmo devuelve un error indicando el problema y finaliza.

4) Acción de reencaminamiento. Se selecciona un próximo salto desde vecinos para cada destinatario que haya de ser retransmitido.

14.3.12 Procedimiento de resolución de nombre de directorio

Mediante este procedimiento se obtiene una **dirección-OR** para un usuario identificado mediante un nombre de directorio.

14.3.12.1 Argumentos

El nombre de directorio del usuario, el **método-entrega-solicitado** del originador, si se especifica, y la **historia-redireccionamiento**, si está presente.

14.3.12.2 Resultados

Una **dirección-OR** del usuario.

14.3.12.3 Errores

Una indicación de que el nombre de directorio no puede resolverse.

14.3.12.4 Descripción del procedimiento

1) El MTA accede al directorio utilizando el nombre de directorio suministrado. Si el nombre no identifica un asiento en el directorio, el procedimiento devuelve un error y finaliza.

2) Si no se suministra el argumento del **método-entrega-solicitado**, o bien es **cualquier-método-entrega**, el MTA intenta obtener el atributo del *método-entrega-preferido* del asiento en el directorio. Si los restantes pasos permiten construir más de un tipo de dirección, la elección entre los mismos se basará en una combinación del **método-entrega-solicitado** (o *método-entrega-preferido*) y de la política local. Si debe hacerse una elección entre **direcciones-OR** y existe un argumento de **historia-redireccionamiento,** cualquier **dirección-OR** que esté presente en la **historia-redireccionamiento** se excluye antes de realizar la elección.

3) Si el atributo *direcciones-or-mhs* está presente, se puede devolver un valor de dicho atributo. Dicho valor se considera para satisfacer una petición para el método de **entrega-mhs**. Si existen múltiples valores del atributo, la elección entre ellos es un asunto local. La elección puede estar influenciada por las capacidades de la UA del destinatario (determinado a partir de otros atributos de directorio o del conocimiento local) y por las características del mensaje.

4) El MTA puede configurarse con información de varias unidades de acceso cuya utilización está permitida cuando se constituye una **dirección-OR** a partir de información suministrada por el directorio. La información configurada incluirá los valores de atributo de la **dirección-OR**, que pueden combinarse con información recuperada del directorio para formar una **dirección-OR** completa y con el método de entrega propio de dicha dirección. Si el MTA se configura con información de más de una unidad de acceso del mismo tipo, la elección está sujeta a la política local. El MTA puede configurarse con información relativa a alguno o ninguno de los siguientes tipos de unidades de acceso:

   a) entrega-física: Se configuran valores de **nombre-país**, **nombre-dominio-administración**, facultativamente **nombre-dominio-privado** y **nombre-pds**. La **dirección-OR** se construye a partir de los componentes configurados, los valores de **dirección-postal-no-formateada** y **código-postal** obtenido a partir de los atributos de directorio *dirección postal* y *código postal*, y del **nombre-país-entrega-física** derivado del componente *nombre país* del nombre distinguido de la entrada al directorio. Se considera que así se satisface el método de **entrega-física**.

   b) entrega-facsímil-g3: Se configuran valores de **nombre-país**, **nombre-dominio-administración** y, facultativamente **nombre-dominio-privado**. La **dirección-OR** se construye a partir de los componentes configurados y de una **dirección-red** obtenida a partir del valor del atributo de directorio *número teléfono facsímil* y **tipo-de-terminal** puesto al valor *facsímil-g3*. Se considera que así se satisface el método de **entrega-facsímil-g3**.

c) entrega-télex: se configuran valores de **nombre-país**, **nombre-dominio-administración** y facultativamente **nombre-dominio-privado**, y **tipo-de-terminal**. La **dirección-OR** se construye a partir de los componentes configurados, y se obtiene una **dirección-red** de los valores de los componentes número de télex e indicativo de país del atributo de directorio *número télex*, se obtiene un **identificador-de-terminal** del valor del componente del distintivo del atributo de directorio *número télex* y se pone **tipo-de-terminal** al valor *télex*. Se considera que así se satisface el método **entrega-télex**.

14.3.13 Procedimiento de sobre doble

Este procedimiento toma un mensaje, sonda o informe y coloca todo el objeto dentro de un nuevo mensaje que se envía a un extractor-sobre-doble distante y se presenta como un nuevo mensaje con **tipo-contenido** de **sobre-interior**.

14.3.13.1 Argumentos

1) Mensaje, sonda o informe que debe envolverse con un sobre-exterior.
2) El **nombre-OR** del extractor-sobre-doble distante.
3) El **nombre-OR** de este sobre-doble.
4) Los servicios de seguridad que deben aplicarse para proteger el contenido del sobre-interior y la información de algoritmo específica o las preferencias de algoritmo para estos (confidencialidad-contenido, datos-criptados-testigo-mensaje, datos-firmados-testigo-mensaje y verificación-autenticación-origen-mensaje).

14.3.13.2 Resultados

Ninguno, ya que el MTA no tiene ningún otro proceso que llevar a cabo con el mensaje original.

NOTA – Hay dos eventos de salida de este procedimiento: uno es la presentación de un nuevo mensaje que contenga el sobre-interior y el segundo es un registro de información suficiente para permitir al doble-sobre construir un informe de no-entrega en el mensaje original en el caso de que reciba un informe de no-entrega en el nuevo mensaje.

14.3.13.3 Errores

Indicación de un error-seguridad si no puede proporcionarse un servicio solicitado.

NOTA – El hecho de que se produzca tal error-seguridad indica un error de configuración (como por ejemplo, que no se disponga de un algoritmo configurado) o de la clave-privada del MTA para el mismo.

14.3.13.4 Descripción del procedimiento

La totalidad de la MTS-APDU que contiene el mensaje, sonda o informe del sujeto se coloca dentro de un nuevo mensaje, cuyo originador es el **nombre-OR** de este sobre-doble y cuyo destinatario es el **nombre-OR** del extractor-doble-sobre distante. La petición-informe-originador para este destinatario se fija en informe y el tipo-contenido se fija en sobre-interior.

Si se especifican preferencias de algoritmos para los servicios de seguridad solicitados y el nombre-directorio aparece en el **nombre-OR** del extractor-sobre-doble distante, se lee el asiento en el directorio para obtener sus algoritmos soportados y el atributo certificado de usuario. Se selecciona el primer algoritmo por orden de preferencia que sea soportado tanto por este MTA como por el extractor-sobre-doble distante para cada servicio de seguridad solicitado (es decir, confidencialidad-contenido, datos-criptados-testigo-mensaje, datos-firmados-testigo-mensaje y verificación-autenticación-origen-mensaje). La información-algoritmo contiene un identificador-algoritmo y, opcionalmente, información para seleccionar un certificado apropiado para dicho algoritmo para el originador, o el destinatario, o ambos (dependiendo de los requisitos del algoritmo). La información selector-certificado se necesita únicamente si el asiento en el directorio puede contener más de un certificado para el algoritmo identificado. Si no aparece el nombre-directorio, se selecciona la primera preferencia y se requerirá la configuración local de la clave pública de criptación del extractor-sobre-doble distante.

El contenido se cifra utilizando el algoritmo-confidencialidad-contenido seleccionado (o configurado), que puede ser un algoritmo asimétrico o, si se trata de un algoritmo simétrico, se genera una clave-confidencialidad-contenido aleatoria y se utiliza para criptar el contenido, se crea un testigo-mensaje con esta clave criptada utilizando el algoritmo-criptación-testigo-mensaje seleccionado (o configurado) (que debe ser un algoritmo asimétrico) y se firma utilizando el algoritmo-firma-testigo-mensaje seleccionado (o configurado) (que debe ser un algoritmo de firma). La clave pública utilizada con el algoritmo de criptación asimétrico se encuentra por medio del identificador-algoritmo y el selector-certificado-destinatario para seleccionar un certificado apropiado a partir del asiento en el directorio.

Si se ha especificado una autenticación-origen-mensaje, la verificación-autenticación-origen-mensaje se calcula con una firma del contenido cifrado utilizando el algoritmo seleccionado (o configurado), junto con la clave privada de este MTA correspondiente a su certificado identificado por el selector-certificado-originador.

Se remite el nuevo mensaje que contiene el sobre-interior, y se crea un registro de su identificador-remisión-mensaje junto con la información suficiente como para permitir al sobre-doble construir un mensaje de no-entrega del mensaje original en el caso de que reciba un informe de no-entrega del nuevo mensaje.

14.3.14 Procedimiento de extractor-sobre-doble

Este procedimiento toma un mensaje con tipo-contenido de sobre-interior y extrae de su interior un mensaje, sonda o informe que el MTA procesa como si hubiese sido transferido normalmente.

14.3.14.1 Argumentos

Un mensaje con tipo-contenido de sobre-interior.

14.3.14.2 Resultados

Un mensaje, sonda o informe.

14.3.14.3 Errores

Una indicación de error-seguridad si falla la verificación del argumento de seguridad.

En respuesta a una sonda, o a un mensaje con tipo-contenido diferente de sobre-interior, instrucción de generación de informe incapaz-de-transferir, nombre-OR-no-reconocido.

14.3.14.4 Descripción del procedimiento

Se sigue el procedimiento de entrega-mensaje (véase 14.7.1) (según convenga), incluyendo la generación de una instrucción de informe cuando así se requiera.

Si está presente verificación-autenticación-origen-mensaje, se verifica. Se descripta el contenido, se extrae el mensaje, sonda o informe y se pasa al procedimiento-de-cabecera (o de cabecera-informe).

14.4 Módulo del informe

El módulo del informe puede ser invocado por:

1) el módulo de entrada-informe, que transfiere un informe; o
2) el módulo principal, que transfiere un mensaje o una sonda con instrucciones de informe; o
3) el módulo de salida-informe, que transfiere un informe con descripción de fallo.

Si se encuentra un error mediante los procedimientos internos de este módulo, no se genera ninguna salida. En caso contrario, el módulo de informe invoca el módulo de salida-informe o entrega-informe, que pasa un informe con instrucciones de transferencia o entrega, respectivamente. Véase la figura 10.

NOTA – La utilización de los informes deberá estar sujeta a la política-seguridad en vigor.

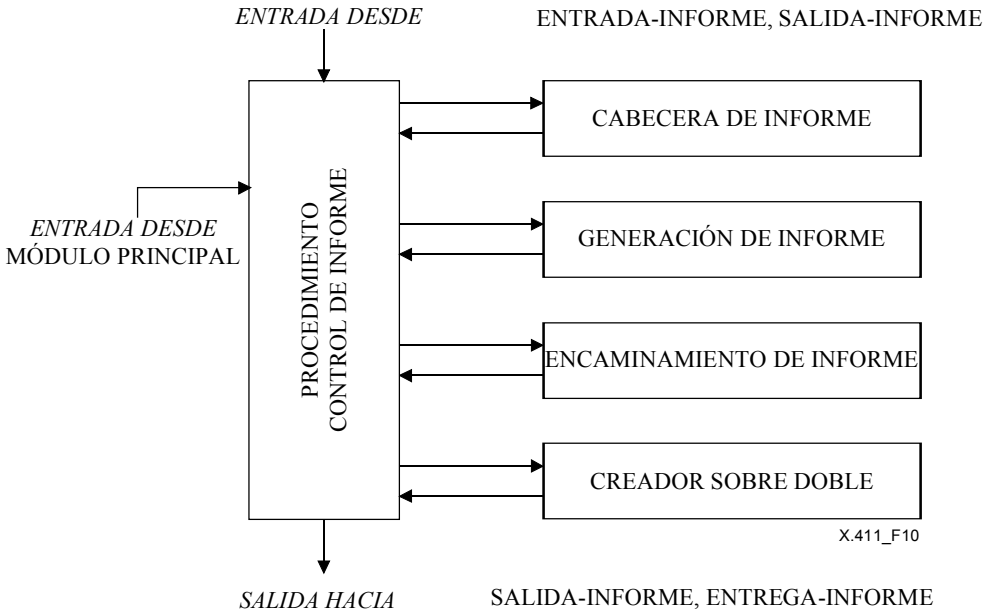


Figura 10 – Organización de los procedimientos dentro del módulo del informe

14.4.1 Procedimiento de control

14.4.1.1 Argumentos

1) un informe; o
2) un mensaje o sonda con instrucción de informe.

14.4.1.2 Resultados

1) un informe con instrucciones de retransmisión o entrega; o
2) ningún resultado en el caso de encontrarse un error.

14.4.1.3 Errores

Ninguno. El informe, mensaje o sonda se descarta si se encuentra un error.

14.4.1.4 Descripción del procedimiento

1) Para un informe procedente de entrada-informe se llama primero al procedimiento de cabecera-informe para realizar la iniciación del rastreo y varios pasos iniciales de verificación. Una devolución nula indica un error; se descarta el informe y termina el proceso. En caso contrario, el proceso continúa en el paso 3 siguiente.
2) Para un mensaje o sonda se llama primero al procedimiento de generación-informe para crear un informe. Una devolución nula indica un error; se descarta el mensaje o la sonda y termina el proceso. Si se devuelve un informe el proceso continúa en el paso 3 siguiente.
3) Se llama al procedimiento de encaminamiento-informe para generar una instrucción de encaminamiento para el informe. Una devolución nula indica un error; se descarta el informe y termina el proceso. El procedimiento de control devuelve el informe finalizado junto con la instrucción de encaminamiento y termina, sujeto a la política-seguridad.

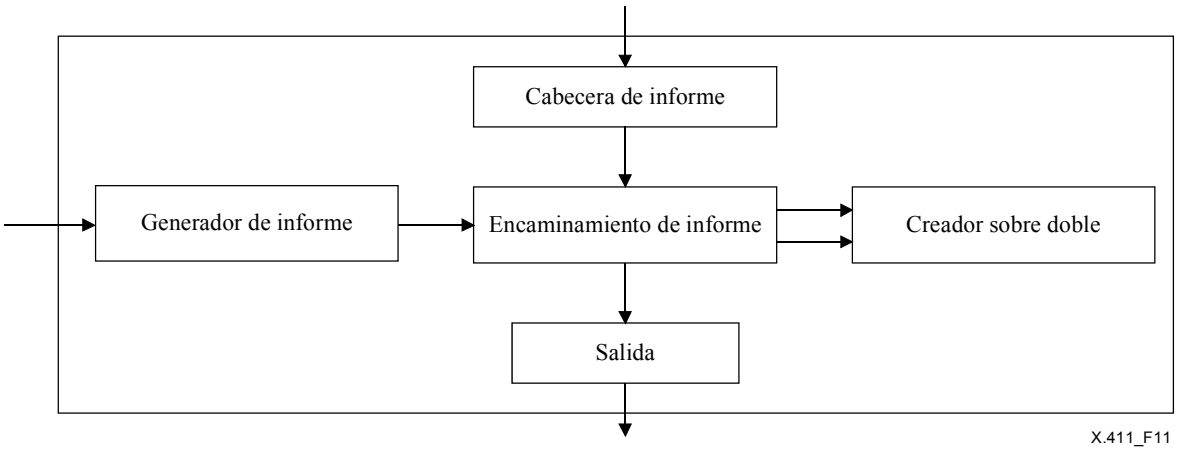


Figura 11 – Flujo de información dentro del módulo del informe

14.4.2 Procedimiento de cabecera-informe

Este procedimiento realiza la inicialización de traza, la detección de las violaciones de la expiración-mensaje, la comprobación inicial de seguridad, la detección de bucles y la comprobación de criticidad.

14.4.2.1 Argumentos

Un informe.

14.4.2.2 Resultados

El informe con la **información-rastreo** iniciada para este MTA.

14.4.2.3 Errores

Ninguno. Si se detecta un error se descarta el informe.

14.4.2.4 Descripción del procedimiento

1) Si el informe ha cruzado una frontera entre dominios, se añade un **elemento-información-rastreo** para este dominio con el tiempo presente como **tiempo-llegada** y **retransmisión** como **acción**. Se añade igualmente un **elemento-información-rastreo-interna** indicando si el informe ha cruzado o no una frontera de dominio.
2) Si la política-seguridad en vigor lo requiere, y/o si la **comprobación-autenticación-origen-informe** resulta incorrecta, se descarta el informe y se termina el proceso.
3) Si alguno de los campos de ampliación es marcado como crítico para la transferencia pero el MTA no lo entiende semánticamente, se descarta el informe. Finaliza entonces el procedimiento.
4) Se realiza la detección de bucles. El algoritmo de detección de bucles está fuera del alcance de esta Definición de servicio. Sin embargo, en 14.3.11 figura, como ejemplo, un algoritmo combinado de encaminamiento y de detección de bucles. Si se detecta un bucle, se descarta el informe y finaliza el procedimiento.

14.4.3 Procedimiento de generación-informe

Este procedimiento genera un informe que describe el éxito y/o el fallo de las operaciones deseadas por parte del MTA.

14.4.3.1 Argumentos

Un mensaje o sonda. Para cada destinatario con **responsabilidad** puesta en **responsable**, se incluye una instrucción por-destinatario que indica el éxito o el problema encontrado.

14.4.3.2 Resultados

Un informe que describe los éxitos y fallos que hay que comunicar.

14.4.3.3 Errores

Ninguno.

14.4.3.4 Descripción del procedimiento

Si el campo de **petición-informe-MTA-originador** del sujeto así lo indica, se construye el informe con los argumentos descritos en el cuadro 32, ampliado posteriormente por lo siguiente.

Se toman los argumentos de entrega (**tiempo-entrega-mensaje**, **tipo-de-usuario-MTS**) o argumentos de no-entrega (**código-motivo-no-entrega**, **código-diagnóstico-no-entrega**) para cada destinatario a partir de las instrucciones por-destinatario que acompañaban al mensaje sujeto. Si se comunica una entrega con éxito para un destinatario de una DL, el **tipo-de-usuario-MTS** se pone a **DL**. El **nombre-destinatario-informe** es el último elemento de la **historia-ampliación-DL**, si dicho elemento existe. Para mensajes sin **historia-ampliación-DL** y para todas las sondas, el **nombre-destino-informe** es el **nombre-originador** del sujeto. El **originador-y-ampliación-DL** contendrá el **nombre-originador** y el **tiempo-presentación-mensaje** del sujeto seguido del contenido de la **historia-ampliación-DL**. Un **elemento-información-rastreo** para este dominio se crea con el tiempo actual como **tiempo-llegada** y **retransmisión** como **acción**. También se crea un **elemento-información-rastreo-interno**. Si el sujeto contiene una **historia-redireccionamiento** o una **historia-ampliación-dl**, el **nombre-destinatario-originalmente-deseado** se copiará del primer elemento de la **historia-redireccionamiento** o de la **historia-ampliación-dl**, según cual ocurra en primer lugar (la secuencia de dichos eventos vendrá determinada por la **información-rastreo**).

NOTA – No se genera el **nombre-DL-informadora** bajo ninguna de estas condiciones.

En el caso en que las instrucciones reflejen múltiples fallos, el informe debería reflejar el problema original, en vez del fallo de las acciones de recuperación subsiguientes.

El MTA designa valores de **criticidad** para campos copiados del sujeto (asunto). Estos nuevos valores reflejan la criticidad con respecto al informe, no al asunto. El MTA no copiará en el informe ninguna función crítica que no admita.

14.4.4 Procedimiento de encaminamiento-informe

Este procedimiento determina la acción de encaminamiento, si ha lugar, que ha de adoptarse en un informe. El encaminamiento-informe refleja las condiciones especiales que requiere un procedimiento de encaminamiento diferente del aplicable a los mensajes o sondas:

1) un informe tiene un solo destinatario – el originador del mensaje que constituye el sujeto del informe, un punto-de-ampliación de DL, o, si la política local lo permite, un propietario de DL;
2) fallos insuperables encontrados al encaminar un informe hacen que se descarte el informe. No se hace ningún intento para generar un informe ulterior, sobre la dificultad encontrada.

Las acciones de proceso que exigen estas condiciones, se describen en los puntos siguientes. Debería observarse que el encaminamiento de los informes está sujeto a la política-seguridad.

14.4.4.1 Argumentos

Uno de los siguientes:

1) un informe transferido a este MTA desde otro MTA y procesado con éxito por el procedimiento de cabecera-informe;
2) un informe creado por el procedimiento generación-informe interno a este MTA;
3) un informe devuelto desde el procedimiento de salida-informe junto con una descripción del fallo de transferencia encontrado.

14.4.4.2 Resultados

Uno de los siguientes:

1) el informe, junto con las instrucciones de retransmisión para el MTA del próximo salto;
2) el informe, junto con una indicación del usuario-MTS soportado localmente que debe recibir la entrega-informe.

14.4.4.3 Errores

Ninguno. Si no puede determinarse ningún destinatario local o ningún próximo salto, se descarta el informe.

14.4.4.4 Descripción del procedimiento

1) Los informes retransmitidos a este MTA o generados localmente reciben una atención de encaminamiento normal como se describe a continuación.

   a) Si el destino-informe no es local en este MTA, se necesita la retransmisión. El encaminamiento-informe intenta determinar la dirección del próximo salto. En esta determinación se compara la **etiqueta-seguridad-mensaje** del informe con el **contexto-seguridad** para garantizar que no se reproducen violaciones de la política-seguridad. Si tiene éxito, se devuelve el informe, junto con esta información como resultado del procedimiento. Finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento de salida-informe.

      Si los principios de seguridad establecen que es necesario un doble sobre para el siguiente salto identificado, el procedimiento retornará una instrucción para intercalar el informe dentro del **contenido** de un nuevo mensaje, siguiendo el procedimiento especificado en 14.3.13. Entonces terminará el procedimiento.

      Si no puede determinarse la dirección del próximo salto, se descarta entonces el informe y finaliza el procedimiento sin devolver ningún resultado.

   b) Si el destino-informe especifica sin ambigüedad un destinatario real, pero no es una dirección preferida de dicho destinatario, se genera una orden de redireccionamiento que contiene el **nombre-OR** preferido del destinatario y el **alias** del motivo del redireccionamiento, terminando así el procedimiento.

      Si el destino-informe especifica sin ambigüedad un destinatario local real, se comprueban los parámetros de registro del destinatario para el **redireccionamiento-asignado-destinatario** y si éste está en vigor, la longitud del contenido devuelto, si la hubiere, se compara con la **longitud-de-contenido** y el tipo de contenido, si está presente, con el **tipo-de-contenido** de cada **clase-de-redireccionamiento** de redireccionamientos asignados por destinatario (que tiene objetos fijados a informes o ambos) a su vez hasta que se encuentra una **clase-de-redireccionamiento** cuyos valores especificados para estos campos concuerdan con los del informe, pasando por alto **clases-de-redireccionamiento** con valores especificados para otros componentes. Si una **clase-de-redireccionamiento** concuerda, entonces se genera una orden de redireccionamiento, dándose por terminado el procedimiento.

   c) Si el destino-informe es un usuario-MTS local en este MTA, y el campo de **petición-informe-originador** lo indica, se solicita la entrega-informe (sujeta a la política-seguridad en vigor). El encaminamiento-informe intenta determinar la dirección-OR del destino del informe. Si tiene éxito, se devuelve entonces el informe, junto con esta información, como resultado del procedimiento, finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento de entrega-informe.

      Si el destino-informe no identifica un usuario-MTS y el MTA se ha configurado con la dirección de un destinatario-alternativo para esta clase de destino-informe, se genera una orden de redireccionamiento con motivo de redireccionamiento destinatario-alternativo-asignado-MD-destinatario, finalizando entonces el procedimiento.

      Si no se solicitó el informe o no puede determinarse la dirección de destino del informe, se descarta éste y el procedimiento finaliza sin devolver ningún resultado.

   d) Si el **nombre-destino-informe** corresponde a una DL local en este MTA, este informe se encuentra en el proceso de encaminamiento hacia atrás a lo largo de un trayecto de sucesivos puntos-ampliación de la DL. En el campo de **otras-acciones** del **elemento-información-rastreo** y **elemento-información-rastreo-interno** se indica el valor **operación-dl**.

      Cualquier proceso basado en una política de DL local podría producirse aquí; por ejemplo, puede construirse una copia del informe y enviarla al propietario de la DL. En este caso el **nombre-destino-informe** será el del propietario de la DL y se construirá el **nombre-DL-informadora** para que contenga el nombre de la DL del sujeto. Esta copia del informe no deberá contener el **contenido-devuelto**. Además se puede realizar aquí la supresión de los informes.

   NOTA 1 – Queda en estudio la posibilidad de que un propietario DL sea en sí mismo una DL.

   NOTA 2 – Cuando se procesa un informe no se considera el permiso-remisión-DL.

Si no se va a suprimir el informe, el MTA sustituye el **nombre-OR** existente en el campo de **nombre-destino-informe** por el **nombre-OR** que precede inmediatamente al del campo del **originador-e-historia-ampliación-DL**. De esta forma, el informe adquiere, como nuevo destino, la nueva entrada junto con la cadena de entradas del campo del **originador-e-historia-ampliación-DL**:

nombre-destino-informe: **nombre-OR** previo de la DL de la copia procedente de **originador-e-historia-ampliación-DL**.

nombre-DL-informadora: Generado únicamente en el caso de informes al propietario de la DL.

Para encaminar el informe a su nuevo destino el procedimiento de encaminamiento-informe se llama ahora a sí mismo de forma recurrente. Se devuelve el resultado devuelto procedente de esta llamada recurrente, si lo hay y finaliza el procedimiento.

e) Si el **nombre-destino-informe** identifica un creador de doble sobre en este MTA, se aplicará el procedimiento descrito en 14.4.5 y el procedimiento terminará. Los eventuales nuevos informes resultantes serán tratados desde el principio de este procedimiento.

2) Un informe devuelto por el procedimiento de salida-informe ha encontrado un fallo de transferencia en el procedimiento de retransmisión a otro MTA. El procedimiento de encaminamiento-informe intenta reencaminar dicho informe, es decir, calcula una dirección alternativa para el próximo salto (sujeta a la política-seguridad en vigor). Si se encuentra una dirección alternativa para el próximo salto, se devuelve entonces el informe, junto con esta información y la información de rastreo convenientemente modificada, a modo de resultado del procedimiento. Finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento de salida-informe.

Si no puede determinarse una dirección alternativa para el próximo salto, se descarta entonces el informe y finaliza el procedimiento sin devolver ningún resultado.

14.4.5 Procedimiento de sobre-doble

Este procedimiento toma un informe de un mensaje (creado por este MTA) con un tipo-contenido de sobre-interior, y si es un informe de no-entrega, éste sustituye a un informe de no-entrega del mensaje que estaba en el sobre-interior.

14.4.5.1 Argumentos

Un informe.

14.4.5.2 Resultados

Otro informe si el argumento es un informe de no-entrega, o ninguno en cualquier otro caso.

14.4.5.3 Errores

Ninguno.

14.4.5.4 Descripción del procedimiento

Si el informe es un informe de no-entrega, se lee el registro de los mensajes con sobre-doble remitidos para obtener la información necesaria con la que crear un informe de no-entrega en el mensaje del sobre-interior. Este nuevo informe de no-entrega sustituye al informe de no-entrega del sobre-exterior.

Si el informe es un informe de entrega, no se requiere ninguna otra transferencia del mismo.

En cualquier caso, se añade al registro de los mensajes con sobre-doble remitidos información sobre el informe de entrega o no-entrega. El MTA puede incorporar un procedimiento adicional, activado por la expiración de un temporizador, para generar un informe de no-entrega del mensaje del sobre-interior si no se ha recibido ningún informe de entrega del mensaje del sobre-exterior.

14.5 Vinculación-MTS y desvinculación-MTS

14.5.1 Procedimiento de vinculación-MTS iniciado por usuario-MTS

Esta cláusula describe el comportamiento del MTA cuando un usuario-MTS invoca vinculación-MTS.

14.5.1.1 Argumentos

Los argumentos de vinculación-MTS se definen en 8.1.1.1.1.

14.5.1.2 Resultados

Los resultados de vinculación-MTS se definen en 8.1.1.1.2.

14.5.1.3 Errores

Los errores-vinculación se definen en 8.1.2.

14.5.1.4 Descripción del procedimiento

1) Si los recursos de los MTA no permiten normalmente el establecimiento de una nueva asociación, el procedimiento devuelve un error-vinculación de ocupado y finaliza.

2) En caso contrario, si la política-seguridad exige autenticación, el MTA intenta tanto autenticar el usuario-MTS a través de las **credenciales-iniciador** suministradas, como comprobar la posibilidad de aceptación del **contexto-seguridad**.

   Si **credenciales-iniciador** contiene **credenciales-fuertes**, se verifica la firma del testigo-vinculación-iniciador utilizando la clave pública del **certificado** del usuario-MTS para el algoritmo de firma identificado. El **certificado** del usuario-MTS puede estar incluido en credenciales-iniciador dentro del argumento de la vinculación, o ser identificado por un **selector-certificado** y, si todavía no está disponible para el MTA, puede obtenerse del atributo certificado de usuario del usuario-MTS en el directorio. También se verifica la validez del **certificado** y de su trayecto-certificación. Adicionalmente se comprueba que el nombre de directorio del campo de sujeto de ese certificado es el del usuario-MTS. Se comprueba que el **nombre-OR** del campo de nombre-alternativo-sujeto de ese certificado corresponde al **nombre-OR** del usuario-MTS, y al **nombre-OR** que aparece en el campo de nombre-iniciador de vinculación. Se comprueba que el nombre-mta y el identificador-dominio-global dentro del testigo-vinculación-iniciador son los de este MTA. Se compara el tiempo del testigo con el tiempo presente para asegurarse de que el periodo de validez del testigo aceptable para este MTA no ha expirado.

   El testigo-vinculación-respondedor es generado utilizando el mismo algoritmo de firma (a menos que se sepa que el usuario-MTS puede soportar una alternativa mejor) y esta clave privada del MTA para firmar un testigo que comprende el identificador-algoritmo para el algoritmo de firma, el **nombre-OR** del usuario-MTS, el tiempo presente y un número aleatorio como datos-firmados-testigo-vinculación. Este testigo-vinculación-respondedor junto con el **selector-certificado** o el **certificado** (y los certificados adicionales que proporcionan su trayecto-certificación) para esta clave pública del MTA para este algoritmo constituyen las credenciales-respondedor en el resultado de la vinculación.

   Si no pueden autenticarse las **credenciales-iniciador**, el procedimiento devuelve un error-autenticación y finaliza. Si el **contexto-seguridad** no resulta aceptable, el procedimiento devuelve un error-vinculación de contexto-seguridad-inaceptable y finaliza.

3) Si la autenticación tiene éxito y el **contexto-seguridad** resulta aceptable, el MTA acepta la asociación solicitada. El procedimiento devuelve el **nombre-MTA** y las **credenciales-respondedor**. Se devuelven igualmente los **mensajes-esperando** si el usuario-MTS está abonado al elemento-de-servicio retención para entrega. Finaliza entonces el procedimiento.

4) Si no se requiere autenticación, se devuelve una **espera-mensaje** si el usuario-MTS se abona al elemento-de-servicio retención para entrega, y el procedimiento finaliza.

14.5.2 Procedimiento de desvinculación-MTS iniciado por usuario-MTS

Esta cláusula describe el comportamiento del MTA cuando un usuario-MTS invoca desvinculación-MTS para liberar una asociación existente establecida por el usuario-MTS.

14.5.2.1 Argumentos

Ninguno.

14.5.2.2 Resultados

El procedimiento de desvinculación-MTS devuelve un resultado vacío como indicación de la liberación de la asociación.

14.5.2.3 Errores

Ninguno.

14.5.2.4 Descripción del procedimiento

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.5.3 Procedimiento de vinculación-MTS iniciado por MTA

Esta cláusula describe los pasos dados por el MTA cuando emprende la tarea de establecer una asociación con un usuario-MTS.

14.5.3.1 Argumentos

Los argumentos de vinculación-MTS se definen en 8.1.1.1.1.

14.5.3.2 Resultados

Un identificador interno para la asociación establecida.

14.5.3.3 Errores

El procedimiento devuelve una indicación de fallo en el caso de que no pudiera establecerse la asociación.

14.5.3.4 Descripción del procedimiento

1) El procedimiento establece los valores para los argumentos definidos en 8.1.1.1.1. Pueden suministrarse **mensajes-esperando** si el usuario-MTS está abonado al elemento-de-servicio de retención para entrega. Se toman los valores del **nombre-iniciador**, **contexto-seguridad** y **credenciales-iniciador** de la información interna.

   Si **credenciales-iniciador** debe contener **credenciales-fuerte**, el MTA selecciona un algoritmo de firma soportado por el usuario-MTS y utiliza este algoritmo para firmar un testigo-vinculación-iniciador que comprenda el identificador-algoritmo para ese algoritmo, el **nombre-OR** del usuario-MTS, el tiempo presente y un número aleatorio como datos-firmados-testigo-vinculación. Este testigo-vinculación-iniciador junto con un **selector-certificado** o el **certificado** (y los certificados adicionales que proporcionan su trayecto-certificación) para esta clave pública del MTA para este algoritmo constituyen las credenciales-iniciador en el argumento de la vinculación.

2) El procedimiento determina la **dirección-usuario** del usuario-MTS e intenta establecer una asociación con los argumentos del 8.1.1.1.1. Si no tiene éxito, se devuelve una indicación de fallo y finaliza el procedimiento.

3) Si tiene éxito, se examinan los resultados devueltos por el usuario-MTS (definidos en el 8.1.1.1.2). Se comprueba la corrección del **nombre-respondedor** y se realiza un intento de autenticar el usuario-MTS a través de las **credenciales-respondedor** devueltas.

   Cuando se recibe el resultado de la vinculación, se comprueba la firma del testigo-vinculación-respondedor por medio de la clave pública del **certificado** del usuario-MTS para el algoritmo de firma identificado. (Podría tratarse de un algoritmo de firma diferente al utilizado para firmar el testigo-vinculación-iniciador.) El **certificado** del usuario-MTS puede estar incluido en el resultado de la vinculación, o ser identificado por un **selector-certificado** y, si todavía no está disponible para el MTA, puede obtenerse del atributo certificado de usuario del usuario-MTS en el directorio. También se verifica la validez del **certificado** y de su trayecto-certificación. Adicionalmente, se comprueba que el nombre de directorio del campo de sujeto de ese **certificado** es el del usuario-MTS (es decir, que el usuario-MTS que responde es el objetivo de la vinculación). Se comprueba que el **nombre-OR** del campo de nombre-alternativo-sujeto de ese **certificado** corresponde al **nombre-OR** del usuario-MTS y al **nombre-OR** que aparece en el campo de nombre-respondedor del resultado de la vinculación. Se comprueba que el nombre-mta y el identificador-dominio-global dentro del testigo-vinculación-respondedor son los de este MTA. Se compara el tiempo del testigo con el tiempo presente para asegurarse de que el periodo de validez del testigo aceptable para este MTA no ha expirado.

   Si la comprobación falla, el procedimiento cierra la conexión, devuelve una indicación de fallo y finaliza.

4) Si ambas comprobaciones tienen éxito, el procedimiento devuelve el identificador de la asociación y finaliza.

14.5.4 Procedimiento de desvinculación-MTS iniciado por el MTA

Se llama a este procedimiento para liberar una asociación con un usuario-MTS.

14.5.4.1 Argumentos

El identificador interno para la asociación que ha de liberarse.

14.5.4.2 Resultados

El procedimiento de desvinculación-MTS devuelve un resultado vacío como indicación de la liberación de la asociación.

14.5.4.3 Errores

Ninguno.

14.5.4.4 Descripción del procedimiento

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.6 Puerto de remisión

14.6.1 Procedimiento de remisión-mensaje

Esta cláusula describe el comportamiento del MTA cuando el usuario-MTS invoca la operación-abstracta de remisión-mensaje en un puerto de remisión.

14.6.1.1 Argumentos

Los argumentos de remisión-mensaje enumerados en el cuadro 3 y descritos en las cláusulas indicadas en ese cuadro.

14.6.1.2 Resultados

1) Los resultados de remisión-mensaje enumerados en el cuadro 5 y descritos en las cláusulas indicadas en dicho cuadro se devuelven al usuario-MTS.
2) Se invoca el módulo de entrega diferida y se transfiere el mensaje remitido.

14.6.1.3 Errores

Véase 8.2.1.1.3 para las descripciones de los errores-abstractos pertinentes.

14.6.1.4 Descripción del procedimiento

1) Comprobación de errores

   El procedimiento de remisión-mensaje comprueba las condiciones de error. Si se encuentra alguna, se devuelve el error-abstracto indicado y termina todo proceso ulterior. El MTA no acepta la responsabilidad del mensaje deseado.

   Errores de interés especial:

   a) Errores de seguridad. Si la **etiqueta-seguridad-mensaje** no es compatible con el **contexto-seguridad** o, si procede, la **comprobación-autenticación-origen-mensaje** resulta incorrecta se genera un error-seguridad.

   b) Errores de criticidad. Si alguno de los campos de ampliación es marcado como **crítico-para-remisión**, pero el MTA no lo entiende semánticamente, se devuelve un error-función-crítica-no-permitida.

      Si no se encuentran errores en esta etapa, continúa el proceso en el paso 2. Pueden encontrarse errores adicionales en estas últimas etapas del proceso, en cuyo caso el MTA adopta las medidas descritas anteriormente.

2) Procesamiento del nombre

   El procedimiento siguiente se aplica al **nombre-originador**, al **nombre-destinatario** y al **destinatario-alternativo-solicitado-originador**, a menos que se señale lo contrario.

   a) Si el **nombre-OR** contiene únicamente un **nombre-directorio**, el MTA intenta obtener la **dirección-OR**.

      En el caso del **nombre-destinatario**, se llama al procedimiento de resolución de nombre de directorio (véase 14.3.12) a fin de determinar una nueva **dirección-OR**.

      Si no puede encontrarse una **dirección-OR**, deberá devolverse al originador del mensaje un error abstracto de **especificado-indebidamente-destinatario** o un informe de no-entrega.

   b) Si el **nombre-OR** contiene tanto el **nombre-directorio** como la **dirección-OR** no es necesario dar validez a su asociación.

   c) La validación de la **dirección-OR**, tanto si se pasó como argumento de la remisión-mensaje como si se obtuvo resolviendo el **nombre-directorio**, consta de dos pasos. El primer paso da validez a que la **dirección-OR** implicada tiene la combinación de atributos necesarios para ser una **dirección-OR** válida (véase 8.5.5). El segundo paso, que se aplica únicamente al **nombre-originador** da validez a que la **dirección-OR** es, de hecho, una **dirección-OR** del usuario-MTS que remite el mensaje.

3) Transferencia de responsabilidad, devolución de resultados

Si no se detecta ningún error en el proceso anterior, el MTA acepta la responsabilidad del mensaje y así lo indica devolviendo los resultados de la remisión-mensaje al usuario-MTS. Los resultados de la remisión-mensaje se describen en 8.2.1.1.2. El MTA construye los argumentos del **identificador-remisión-mensaje** y del **tiempo-remisión-mensaje** según proceda. El **identificador-contenido** es idéntico al argumento correspondiente de remisión-mensaje. Si lo solicitó el originador, el MTA-originador genera la **prueba-de-remisión** utilizando el algoritmo identificado por **identificador-algoritmo-prueba-de-remisión** y los argumentos definidos en 8.2.1.1.2.4. Además se devuelve el **certificado-MTA-originador**.

4) Construcción del mensaje

Se construye un mensaje a partir de los argumentos de remisión-mensaje, posiblemente modificados en los pasos anteriores del proceso, más los argumentos adicionales suministrados por el MTA, especificados en 12.2.1.1.

Cuando está finalizado, el procedimiento de remisión-mensaje termina y se pasa el mensaje al módulo de entrega diferida para un proceso ulterior.

14.6.2 Procedimiento de remisión-sonda

Esta cláusula describe el comportamiento del MTA cuando el usuario-MTS invoca la operación-abstracta de usuario-MTS en un puerto de remisión.

14.6.2.1 Argumentos

Los argumentos de remisión-sonda enumerados en el cuadro 7 y descritos en las cláusulas indicadas en ese cuadro.

14.6.2.2 Resultados

1) Los resultados de remisión-sonda enumerados en el cuadro 8 y descritos en las cláusulas indicadas en dicho cuadro se devuelven al usuario-MTS.
2) Se invoca el módulo principal y se transfiere la sonda remitida.

14.6.2.3 Errores

Véase 8.2.1.2.3 para las descripciones de los errores-abstractos pertinentes.

14.6.2.4 Descripción del procedimiento

1) Comprobación de errores

El procedimiento de remisión-sonda comprueba las condiciones de error. Si se encuentra alguna, se devuelve el error-abstracto indicado. El MTA no acepta la responsabilidad de la sonda deseada.

Errores de interés especial:

a) Errores de seguridad. Si la **etiqueta-seguridad-mensaje** no es compatible con el contexto-seguridad o si la **comprobación-autenticación-origen-sonda** resulta incorrecta se genera un error-seguridad.

b) Errores de criticidad. Si uno de los argumentos externos resulta ser **crítico-para-remisión**, pero el MTA no lo entiende semánticamente, se devuelve un error-función-crítica-no-permitida.

Si no se encuentran errores en esta etapa, continúa el proceso en el paso 2. Pueden encontrarse errores adicionales en estas últimas etapas del proceso, en cuyo caso el MTA adopta las medidas descritas anteriormente.

2) Procesamiento del nombre

Se aplica el procedimiento siguiente al **nombre-originador**, **nombre-destinatario** y **destinatario-alternativo-solicitado-originador**, a menos que se señale lo contrario.

a) Si el **nombre-OR** contiene únicamente un **nombre-directorio**, el MTA intenta obtener la **dirección-OR**.

En el caso del **nombre-destinatario**, se llama al procedimiento de resolución de nombre de directorio (véase 14.3.12) a fin de determinar una nueva **dirección-OR**.

Si no puede encontrarse una **dirección-OR**, deberá devolverse al originador del mensaje un error abstracto de **especificado-indebidamente-destinatario** o un informe de no-entrega.

b) Si el **nombre-OR** contiene tanto el **nombre-directorio** como la **dirección-OR**, no es necesario dar validez a su asociación.

c) La validación de la **dirección-OR**, tanto si se transfirió como argumento de remisión-sonda, como si se obtuvo resolviendo el **nombre-directorio**, consta de dos pasos. El primer paso da validez a que la **dirección-OR** implicada tiene la combinación de atributos necesarios para ser una **dirección-OR** válida (véase 8.5.5). El segundo paso, que se aplica únicamente al **nombre-originador**, da validez a que la **dirección-OR** es, de hecho, la **dirección-OR** del usuario-MTS que remite el mensaje.

3) Transferencia de responsabilidad, devolución de resultados

Si no se detecta ningún error en los pasos anteriores, el MTA acepta la responsabilidad del mensaje y así lo indica devolviendo los resultados de remisión-sonda al usuario-MTS. Los resultados de remisión-sonda se describen en 8.2.1.2.2. El MTA construye los argumentos de **identificador-remisión-sonda** y del **tiempo-remisión-sonda** según convenga. El **identificador-contenido** es idéntico al argumento correspondiente a remisión-sonda.

4) Construcción de la sonda

Se construye una sonda a partir de los argumentos de remisión-sonda, posiblemente modificados en los pasos anteriores del proceso, más los argumentos adicionales suministrados por el MTA.

Cuando está finalizado, el procedimiento de remisión-sonda termina y se pasa la sonda al módulo principal para un proceso ulterior.

14.6.3 Procedimiento de cancelación-entrega-diferida

Esta cláusula describe el comportamiento del MTA cuando el usuario-MTS invoca la operación-abstracta de cancelación-entrega-diferida en un puerto-de-remisión para cancelar la entrega diferida de un mensaje previamente remitido al MTA.

14.6.3.1 Argumentos

Los argumentos de cancelación-entrega-diferida enumerados en el cuadro 10 y descritos en las cláusulas indicadas en ese cuadro.

14.6.3.2 Resultados

Como indicación de cancelación satisfactoria, se transfiere al usuario-MTS un resultado vacío.

14.6.3.3 Errores

Véase 8.2.1.3.3 para las descripciones de los errores-abstractos pertinentes.

14.6.3.4 Descripción del procedimiento

1) Si ya ha sido proporcionada una **prueba-de-remisión**, el MTA devuelve el error-abstracto de demasiado-tarde-para-cancelar. No se cancela la entrega diferida del mensaje.

2) Si el MTA reconoce el argumento del **identificador-remisión-mensaje** como válido y asociado con un mensaje que está reteniendo el MTA para su entrega-diferida, el MTA descarta este mensaje como cancelado y supone que ya no tiene ninguna responsabilidad sobre él.

3) Si el MTA reconoce el argumento del **identificador-remisión-mensaje** como válido pero referido a un mensaje ya entregado o transferido a otro MTA, el MTA invoca el error-abstracto demasiado-tarde-para-cancelar. No se cancela la entrega diferida del mensaje.

4) Si no se reconoce como válido el argumento del **identificador-remisión-mensaje** (porque el MTA nunca asignó dicho valor o porque el MTA ya no tiene depositado el registro histórico de un mensaje de entrega diferida que ha sido transferido o entregado) el MTA devuelve entonces el error-abstracto de identificador-remisión-mensaje-inválido o demasiado-tarde-para-cancelar, siendo la elección un asunto local.

14.6.4 Procedimiento control-remisión

Esta cláusula describe el comportamiento del MTA al invocar la operación-abstracta de control-remisión en un puerto-remisión, para limitar transitoriamente las operaciones-abstractas del puerto-remisión que puede invocar el usuario-MTS. Estos controles permanecen en vigor durante la asociación presente, a menos que sean anulados por una operación-abstracta del control-remisión.

NOTA – La utilización de control-remisión deberá estar sujeta a la política-seguridad en vigor. El argumento de control-remisión de **contexto-seguridad-permisible** limita el **contexto-seguridad** establecido durante la vinculación-MTS.

14.6.4.1 Argumentos

Los argumentos de control-remisión enumerados en el cuadro 12 y descritos en las cláusulas indicadas en ese cuadro.

14.6.4.2 Resultados

El usuario-MTS devuelve al MTA los resultados de control-remisión enumerados en el cuadro 13 y descritos en las cláusulas indicados en ese cuadro.

14.6.4.3 Errores

El usuario-MTS puede devolver un error-seguridad. Véase 8.2.1.4.3 para la descripción de este error-abstracto.

14.6.4.4 Descripción del procedimiento

Las circunstancias que hacen que un MTA invoque la operación-abstracta de control-remisión son asunto local, como lo son las medidas adoptadas durante y después de su consecución.

14.7 Puerto de entrega

14.7.1 Procedimiento de entrega-mensaje

Esta cláusula describe los pasos dados por un MTA cuando se encarga de entregar un mensaje a uno o más usuarios-MTS.

La mayoría de las disposiciones de esta cláusula se aplicarán igualmente al caso en que el MTA haya recibido una sonda con uno o más destinatarios locales. A menos que se señale lo contrario, todos los pasos del procedimiento, excepto la entrega física, se aplican al manejo de las sondas.

NOTA – La generación de informes estará sujeta a la política-seguridad.

14.7.1.1 Argumentos

1) Un mensaje desde el módulo principal con instrucciones por-destinatario para entregar a uno o más usuarios-MTS locales.
2) Los argumentos de entrega-mensaje enumerados en el cuadro 15 y descritos en las cláusulas indicadas en ese cuadro se pasan al usuario-MTS destinatario.

14.7.1.2 Resultados

1) Un resultado vacío o, si se solicita, una **prueba-de-entrega** y, opcionalmente, un **certificado-destinatario** devuelto por el usuario-MTS como indicación de una entrega con éxito sin requisitos de información.
2) Si se requiere un informe, se invoca el módulo principal y se pasa el mensaje con instrucciones por-destinatario describiendo los problemas de entrega encontrados y/o indicando las entregas con éxito sobre las que hay que informar.

14.7.1.3 Errores

Los errores-abstractos de entrega-mensaje que pueden ser devueltos por el usuario-MTS al MTA se describen en 8.3.1.1.3. Estas condiciones de error se comunican al módulo principal en los resultados descritos anteriormente.

14.7.1.4 Descripción del procedimiento

1) Si se alcanza la expiración del mensaje, se genera una instrucción de informe para cada destinatario local. Los valores de **código-motivo-no-entrega** y **código-diagnóstico-no-entrega** son respectivamente **incapaz-de-transferir** y **máximo-tiempo-expirado**. Finaliza entonces el procedimiento.
2) Si cualquiera de los **campos-ampliación** por-mensaje se pone en **crítico-para-entrega** pero el MTA no lo entiende semánticamente, se genera una instrucción de informe por cada destinatario local. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen en **incapaz-de-transferir** y **función-crítica-no-permitida** respectivamente.
3) En caso contrario, se establecen los valores para aquellos argumentos de la operación-abstracta entrega-mensaje que se aplican a todos los destinatarios (los argumentos de entrega-mensaje se describen en 8.3.1.1.1).
4) Para cada destinatario con **responsabilidad** puesta en **responsable** se ejecutan los pasos 5 a 16. Finaliza entonces el procedimiento.

5) Para garantizar que durante la entrega, no se viola la política-seguridad, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si la política-seguridad impide la entrega entonces, con sujeción a la política de seguridad, se genera una instrucción de informe para ese destinatario. Los valores de **código-motivo-no-entrega** y **código-diagnóstico-no-entrega** son **incapaz-de-transferir** y **error-mensajería-segura**, respectivamente.

6) Si los controles de entrega impuestos por una operación-abstracta de registro o de control-entrega invocada previamente impiden la entrega, el MTA entonces, sujeto a la política-seguridad en vigor, retendrá el mensaje hasta que se levanten los controles aplicables. Los controles de entrega no son aplicables a las sondas.

7) Si expira el máximo tiempo de retención para un mensaje retenido (siendo el valor máximo de este tiempo un asunto local excepto en que se deberá tener en cuenta el **último-tiempo-entrega** si está presente y cuando sea **crítico-para-entrega**) con las restricciones aplicables todavía en vigor, se genera una instrucción de informe para este destinatario. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen respectivamente en **incapaz-de-transferir** y **destinatario-indisponible**. Termina entonces el proceso para este destinatario.

NOTA 1 – Los pasos de proceso (6 y 7 anteriores) asociados con las restricciones de control no se aplican en el caso de las sondas.

8) Si se hace cumplir la entrega restringida, y el remitente está en la categoría de remitente no autorizado, entonces se genera una instrucción de informe para ese destinatario. Se fija **código-motivo-no-entrega** en el valor **entrega-restringida**. En ese momento, termina el procesamiento para ese destinatario.

9) El MTA establece los argumentos de la operación-abstracta de entrega-mensaje que se aplican únicamente al destinatario individual: los valores **identificador-entrega-mensaje** y **tiempo-entrega-mensaje** se describen en las cláusulas 8.3.1.1.1.1 y 8.3.1.1.1.2. Si el mensaje contiene una **historia-redireccionamiento** o una **historia-ampliación-dl** se copiará entonces el **nombre-destinatario-originalmente-deseado** del primer elemento de la **historia-redireccionamiento** o de la **historia-ampliación-dl**, en función de cuál ocurra en primer lugar (la secuencia de dichos eventos vendrá determinada por la **información-rastreo**). Todos los restantes argumentos se toman directamente de los campos correspondientes del mensaje a entregar. Con las excepciones indicadas a continuación, todos los argumentos indicados en el cuadro 15 se incluyen en cada invocación de entrega-mensaje.

10) Si **revelación-de-otros-destinatarios** tiene el valor **revelación-de-otros destinatarios-solicitada**, el argumento de **nombre-otro-destinatario** se pone para que incluya lo siguiente:

   a) Los **nombres-OR** de todos los destinatarios especificados-originalmente con un **número-destinatario-especificado-originalmente** distinto del destinatario actual. Para cualquiera de esos destinatarios para el cual se haya registrado un redireccionamiento, el **nombre-OR** del destinatario especificado-originalmente es el de la primera entrada en la historia-redireccionamiento correspondiente.

   b) Si se ha producido una ampliación de la lista de distribución, el **nombre-OR** de la primera entrada de la **historia-ampliación-DL**.

      Si el destinatario es un miembro de una lista de distribución, en el argumento de **nombre-otro-destinatario** no deben incluirse otros miembros de esta lista de distribución. El destinatario es un miembro de la lista de distribución si el campo de **historia-ampliación-DL** es no-vacío.

11) Si alguno de los **campos-ampliación** por-destinatario se pone en **crítico-para-entrega**, pero el MTA no lo entiende semánticamente, se genera una instrucción de informe para este destinatario. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen respectivamente en **incapaz-de-transferir** y **función-crítica-no-permitida**.

12) En el caso de entrega de una unidad de acceso de entrega física, los argumentos de entrega física se incluyen en la entrega-mensaje. Estos argumentos se describen en las cláusulas 8.2.1.1.1.14 a 8.2.1.1.1.23.

13) Una vez satisfechas todas las condiciones para una entrega con éxito, el MTA entregará físicamente el mensaje. La consecución de la entrega a un usuario-MTS destinatario coubicado es un asunto local. En el caso de un usuario-MTS destinatario distante, el MTA establece una asociación con este usuario-MTS (o utiliza uno existente) e invoca la operación-abstracta de entrega-mensaje a través de esta asociación. Al realizar una entrega con éxito, la responsabilidad distante o local del mensaje pasa del MTA al usuario-MTS destinatario.

14) Al realizar una entrega con éxito, si la **petición-informe-entrega-MTA-originador** tiene el valor de **informe** o de **informe-auditado**, se genera una instrucción de informe señalando la entrega con éxito. Se termina el proceso para este destinatario.

15) En el caso de un usuario-MTS destinatario distante, si no existe o no puede establecerse inicialmente una asociación o si existe un fallo de transferencia a través de la asociación, el MTA puede repetir el intento de establecimiento de asociación y/o transferir, siendo el número máximo y/o la duración de las repeticiones un asunto local (excepto en que se deberá tener en cuenta el **último-tiempo-entrega** si está presente y cuando sea **crédito-para-entrega**). Si, después de repetidas tentativas no se ha conseguido la transferencia, el mensaje es considerado como inentregable y, se genera una instrucción de informe, sujeta a la política-seguridad en vigor. Los valores del **código-motivo-no-entrega** y del **código-diagnóstico-no-entrega** son respectivamente **fallo-transferencia** y **destinatario-indisponible**. Termina entonces el proceso para este destinatario.

NOTA 2 – Los pasos del proceso asociados con la transferencia física de un mensaje al usuario-MTS destinatario no se aplican en el caso de la sonda.

16) Devolución de los resultados y errores por el usuario-MTS

Si la operación-abstracta de entrega-mensaje tiene éxito, el usuario-MTS devuelve como indicación de éxito o bien un resultado vacío o bien, si se solicitase, una **prueba-de-entrega** y un **certificado-destinatario** facultativo.

Si la operación-abstracta de entrega-mensaje viola uno o más de los controles impuestos por la operación-abstracta de control-entrega o de registro, el usuario-MTS devuelve un error de control-entrega-violado. Si el **contexto-seguridad** dicta que el usuario-MTS no puede admitir la operación-abstracta solicitada porque violaría la política-seguridad, el usuario-MTS devuelve entonces un error-seguridad. En este caso, la invocación de la entrega-mensaje ha fracasado y el MTA conserva la responsabilidad del mensaje respecto de este destinatario. El mensaje es retenido para hacer un reintento a continuación, o es enviado al módulo principal para la generación de un informe. Termina entonces el proceso para este destinatario.

14.7.2 Procedimiento de prueba-entrega-sonda

Esta cláusula describe los pasos dados por un MTA cuando emprende la tarea de comprobar la posibilidad de entregar una sonda.

NOTA – La utilización de informes estará sujeta a la política-seguridad.

14.7.2.1 Argumentos

1) Sonda del procedimiento interno con instrucciones por-destinatario para la prueba-entrega-sonda a uno a más usuarios MTS locales.

14.7.2.2 Resultados

Se invoca el módulo principal y se transfiere la sonda con instrucciones por destinatario que describen si habría ocurrido o no la entrega ficticia, y si no, por qué motivo.

14.7.2.3 Errores

Ninguno.

14.7.2.4 Descripción del procedimiento

En 14.7.1 se describe la lógica de la entrega-mensaje. Se ejecutan todos los pasos de esta cláusula, excepto aquellos indicados específicamente como no aplicables a la sonda.

14.7.3 Procedimiento de entrega-informe

Esta cláusula describe los pasos dados por un MTA cuando se encarga de entregar un informe al usuario-MTS. Se llama a la entrega-informe cuando un MTA recibe un informe, procedente de la entrada-informe o al generarse dentro del MTA, cuyo campo de **nombre-originador** especifica un usuario-MTS servido por este MTA.

14.7.3.1 Argumentos

1) Un informe del módulo de informe con instrucciones por-destinatario para entregarlas a un destinatario local.

2) Los argumentos de entrega-informe enumerados en el cuadro 18 y descritos en las cláusulas indicadas en dicho cuadro se transfieren al usuario-MTS destinatario.

14.7.3.2 Resultados

Un resultado vacío devuelto por el usuario-MTS como indicación de una entrega con éxito.

14.7.3.3 Errores

Los errores de entrega-informe que pueden devolver el usuario-MTS al MTA se describen en 8.3.1.2.3.

14.7.3.4 Descripción del procedimiento

1) Para garantizar que no se viola la política-seguridad durante la entrega-informe, se comprueba la **etiqueta-seguridad-mensaje** respecto del contexto-seguridad. Si la entrega-informe está prohibida por la política-seguridad, se descarta el informe.

2) Si las restricciones impuestas por una operación-abstracta de registro o control-entrega invocada previamente prohíben la entrega-informe, el MTA retendrá, sujeto a la política-seguridad en vigor, el informe hasta que cesen la restricción o las restricciones aplicables. Los argumentos de la operación-abstracta de control-entrega o de registro establecen las restricciones según se describe en 8.3.1.3.1.

   Si expira el máximo tiempo de retención para un informe retenido (siendo el valor máximo de este tiempo un asunto local) con las restricciones aplicables todavía en vigor, se descarta el informe.

3) Los argumentos para la operación-abstracta de entrega-informe se toman de los correspondientes campos del informe.

4) Si cualquiera de los **campos-ampliación** por-mensaje o por-destinatario se pone en **crítico-para-entrega**, pero no es entendido semánticamente por el MTA, se descarta el informe.

5) La consecución de la entrega-informe a un usuario-MTS coubicado es un asunto local. En el caso de un usuario-MTS distante, el MTA establece una asociación con dicho usuario-MTS (o utiliza uno existente) e invoca la operación-abstracta de entrega-informe a través de la asociación. Al tener éxito una entrega-informe, la responsabilidad distante o local del informe pasa del MTA al usuario-MTS.

6) En el caso de un usuario-MTS distante, si no puede establecerse inicialmente una asociación, el MTA puede repetir la tentativa, siendo el número máximo y la duración de las repeticiones un asunto local. Si, después de varias tentativas no se ha establecido la asociación, el informe se considera inentregable y se descarta.

7) Devolución de resultados y errores por el usuario-MTS.

   Si la operación-abstracta de entrega-informe tiene éxito, el usuario-MTS devuelve un resultado vacío como indicación del éxito.

   Si la operación-abstracta de entrega-informe viola uno o más controles impuestos por una operación-abstracta de control-entrega o de registro, el usuario-MTS devuelve un error de control-entrega-violado. En este caso, la invocación de entrega-informe ha fracasado y el MTA conserva la responsabilidad del informe.

14.7.4 Procedimiento de control-entrega

Esta cláusula describe el comportamiento del MTA cuando un usuario-MTS servido por dicho MTA invoca la operación-abstracta de control-entrega. Esta última impone y levanta restricciones sobre las operaciones-abstractas de entrega-mensaje y entrega-informe. Estos controles permanecen vigentes durante la presente asociación, a menos que sean anulados por un control-entrega subsiguientes. Los controles-entrega limitan de forma transitoria el **contexto-seguridad**, pero no pueden provocar ninguna violación de la política-seguridad.

Estos controles no se aplican al tratamiento de las sondas por el MTA.

14.7.4.1 Argumentos

Los argumentos de control-entrega enumerados en el cuadro 20 y descritos en 8.3.1.3.1.

14.7.4.2 Resultados

1) Los resultados del control-entrega enumerados en el cuadro 21 que se describen en 8.3.1.3.2, son devueltos por el MTA al usuario-MTS.

2) Varios parámetros de control de usuario-MTS retenidos por este MTA se sustituyen por valores transportados en los argumentos de control-entrega.

14.7.4.3 Errores

Véase 8.3.1.3.3 para una descripción de los errores-abstractos pertinentes.

14.7.4.4 Descripción del procedimiento

1) Si el valor del argumento **restricción** es **eliminación**, todos los controles establecidos por cualquier control-entrega previo se eliminan; la operación-abstracta está terminada y se devuelve el resultado al usuario-MTS.

2) Si el valor del argumento **restricción** es **actualización**, y no existe ningún otro argumento presente, se considera válida la petición y se devuelve el resultado al usuario-MTS.

   En dichos casos todos los valores de control vigentes en ese momento permanecen sin modificación.

3) Si el valor del argumento **restricción** es **actualización**, y están presentes otros argumentos, se comprueba la compatibilidad de estos argumentos con las condiciones a largo plazo especificadas por la invocación más reciente de la operación-abstracta de restricción en el puerto-administración (véase 14.4.1). Si no se detecta ninguna incompatibilidad y está permitida la actualización dentro de la política-seguridad, se llevan a cabo las actualizaciones indicadas, la operación-abstracta finaliza y se devuelve el resultado al usuario-MTS.

4) Si se detecta alguna de las siguientes incompatibilidades con condiciones a largo plazo, el MTA devuelve un error-abstracto de control-viola-registro:

   a) Los **tipos-información-codificada-admisibles** tiene un tipo no especificado entre los permitidos a largo plazo.

   b) Los **tipos-contenido-admisibles** tiene un contenido no especificado entre los permitidos a largo plazo.

   c) La **longitud-máxima-contenido-admisible** excede la longitud autorizada a largo plazo.

   d) Se viola el **contexto-seguridad-admisible**.

   En cualquiera de estos casos de error, se descarta el control-entrega y no se lleva a cabo.

14.8 Puerto de administración

14.8.1 Procedimiento de registro

Esta cláusula describe el comportamiento del MTA cuando un usuario-MTS servido por este MTA invoca la operación-abstracta de registro.

14.8.1.1 Argumentos

Los argumentos de registro enumerados en el cuadro 23 y descritos en las cláusulas indicadas en dicho cuadro.

14.8.1.2 Resultados

1) Si el argumento **extracción-de-registros** está presente, la información registrada solicitada se devuelve en el resultado. Un argumento extensión de registro puede hacer que se devuelva también información adicional. En los demás casos, se devuelve un resultado vacío.

2) Varios parámetros del usuario-MTS retenidos por el MTA se sustituyen por valores transportados en los argumentos de registro.

14.8.1.3 Errores

Para una descripción de los errores abstractos pertinentes, véase 8.4.1.1.3.

14.8.1.4 Descripción del procedimiento

1) Se comprueba la correcta especificación de los argumentos de registro. Si alguno está incorrectamente especificado, el procedimiento de registro devuelve un error rechazado-registro y finaliza. Sujeto a la política local o a suscripción, el MTA puede imponer restricciones adicionales a los registros que puede realizar el usuario-MTS; si no se cumplen dichas restricciones, se devuelve un error-abstracto al usuario-MTS y no se realizan pasos ulteriores.

2) Si los argumentos de registro están especificados correctamente, los valores de los parámetros del usuario-MTS son sustituidos por los de los argumentos del registro. Si el argumento **redireccionamientos-asignados-por-destinatario** contiene una sola **restricción** en la cual todos los tipos-de-fuente están permitidos y el nombre-fuente se omite, (en el Contexto de Aplicación de 1994), o el **nombre-OR** del usuario-MTS (en el Contexto de Aplicación de 1988), no se registra el **destinatario-alternativo-asignado** por destinatario. Si el argumento **extracción-de-registros** está presente, se devuelve la información registrada solicitada.

14.8.2 Procedimiento de cambio-de-credenciales iniciado por el usuario-MTS

Esta cláusula describe el comportamiento del MTA cuando el usuario-MTS invoca la operación-abstracta de cambio-de-credenciales.

NOTA – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

14.8.2.1 Argumentos

Los argumentos de cambio-de-credenciales enumerados en el cuadro 25 y descritos en 8.4.1.2.1.

14.8.2.2 Resultados

1) El procedimiento de cambio-de-credenciales devuelve un resultado vacío al usuario-MTS como indicación de éxito.
2) Las credenciales del usuario-MTS retenidas por el MTA se modifican de acuerdo con el argumento de **nuevas-credenciales**.

14.8.2.3 Errores

El error-abstracto de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, descrito en 8.4.1.2.3 y enumerado en el cuadro 26.

14.8.2.4 Descripción del procedimiento

NOTA – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

1) Si el valor del argumento de **antiguas-credenciales** no es el mismo que el de las credenciales retenidas por el MTA para el usuario-MTS que invoca la operación-abstracta, se devuelve al usuario-MTS un error de antiguas-credenciales-incorrectamente-especificadas y finaliza el procedimiento de cambio-de-credenciales.
2) En caso contrario, se comprueba la validez del argumento de **nuevas-credenciales**. Si se encuentra que es no válido (asunto local dictado por la política-seguridad) se devuelve al usuario-MTS un error de nuevas-credenciales-inaceptables y finaliza el procedimiento de cambio-de-credenciales.
3) En caso contrario, las credenciales del usuario-MTS retenidas por este MTA se sustituyen por el valor del argumento de las **nuevas-credenciales**, se devuelve un resultado vacío al usuario-MTS como indicación de éxito y finaliza el procedimiento de cambio-de-credenciales.

14.8.3 Procedimiento de cambio-de-credenciales iniciado por el MTA

Esta cláusula describe el comportamiento del MTA al cambiar sus credenciales retenidas por un usuario-MTS soportado localmente.

NOTA – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

14.8.3.1 Argumentos

Los argumentos de cambio-de-credenciales enumerados en el cuadro 25 y descrito en 8.4.1.2.1.

14.8.3.2 Resultados

El usuario-MTS devuelve un resultado vacío al procedimiento de cambio-de-credenciales como indicación de éxito.

14.8.3.3 Errores

El usuario-MTS puede devolver un error de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, según se describe en 8.4.1.2.3 y se enumera en el cuadro 26.

14.8.3.4 Descripción del procedimiento

NOTA – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

1) El procedimiento invoca la operación-abstracta de cambio-de-credenciales para cambiar las credenciales del MTA retenidas por un usuario-MTS soportado localmente. Las condiciones que hacen que un MTA cambie sus credenciales constituyen un asunto local.
2) Si se recibe del usuario-MTS el error de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, el MTA debe suponer que sus credenciales no han cambiado. A nivel local se puede emprender una actuación ulterior, después de la cual finaliza el procedimiento.
3) Si se recibe la devolución de un resultado vacío procedente del usuario-MTS, el MTA puede suponer que el procedimiento ha tenido éxito y que sus credenciales han cambiado. El procedimiento termina.

14.9 Vinculación-MTA y desvinculación-MTA

14.9.1 Procedimiento de entrada-vinculación-MTA

Esta cláusula describe el comportamiento del MTA cuando otro MTA invoca vinculación-MTA.

14.9.1.1 Argumentos

Los argumentos de vinculación-MTA se definen en 12.1.1.1.1 y se enumeran en el cuadro 28.

14.9.1.2 Resultados

Los resultados de vinculación-MTA se definen en 12.1.1.1.2 y se enumeran en el cuadro 29.

14.9.1.3 Errores

Los errores-vinculación se definen en 12.1.2.

14.9.1.4 Descripción del procedimiento

1) Si los recursos de los MTA no permiten normalmente el establecimiento de una nueva asociación, el procedimiento devuelve un error-vinculación de ocupado y finaliza.

2) En caso contrario, si la política-seguridad exige la autenticación, el MTA intenta tanto autenticar el MTA llamante a través de las **credenciales-iniciador** suministradas como comprobar la posibilidad de aceptación del contexto-seguridad.

   Si **credenciales-iniciador** contiene **credenciales-fuertes**, se verifica la firma del testigo-vinculación-iniciador utilizando la clave pública del **certificado** del MTA iniciador para el algoritmo de firma identificado. El **certificado** del MTA iniciador puede estar incluido en credenciales-iniciador dentro del argumento de la vinculación, o ser identificado por un **selector-certificado** y, si todavía no está disponible para el MTA, puede obtenerse del atributo certificado de usuario del MTA iniciador en el directorio. También se verifica la validez del **certificado** y de su trayecto-certificación. Adicionalmente se comprueba que el nombre de directorio del campo de sujeto de ese certificado es el del MTA iniciador. Se comprueba que el nombres-mta del campo de nombre-alternativo-sujeto de ese certificado corresponde al nombre MTA y al identificador de dominio global del MTA llamante, y al nombre-mta que aparece en el campo de nombre-iniciador de vinculación. Se comprueba que el nombre-mta y el identificador-dominio-global dentro del testigo-vinculación-iniciador son los de este MTA. Se compara el tiempo del testigo con el tiempo presente para asegurarse de que el periodo de validez del testigo aceptable para este MTA no ha expirado.

   El testigo-vinculación-respondedor es generado utilizando el mismo algoritmo de firma (a menos que se sepa que el iniciador puede soportar una alternativa mejor) y esta clave privada del MTA para firmar un testigo que comprende el identificador-algoritmo para el algoritmo de firma, el nombre-mta y el identificador de dominio global del MTA iniciador, el tiempo presente y un número aleatorio como datos-firmados-testigo-vinculación. Este testigo-vinculación-respondedor junto con el **selector-certificado** o el **certificado** (y los certificados adicionales que proporcionan su trayecto-certificación) para esta clave pública del MTA para este algoritmo constituyen las credenciales-respondedor en el resultado de la vinculación.

   Si no pueden autenticarse las **credenciales-iniciador**, el procedimiento devuelve un error-autenticación y finaliza. Si el **contexto-seguridad** no resulta aceptable, el procedimiento devuelve un error de contexto-seguridad-inaceptable y finaliza.

3) Si la autenticación es satisfactoria y el **contexto-seguridad** resulta aceptable, el MTA establece la asociación solicitada. El procedimiento devuelve el **nombre-MTA** y las **credenciales-respondedor**. Finaliza entonces el procedimiento.

4) Si no se requiere autenticación, no hay resultados que devolver y el procedimiento finaliza.

14.9.2 Procedimiento de entrada-desvinculación-MTA iniciado por usuario-MTS

Esta cláusula describe el comportamiento del MTA cuando otro MTA invoca desvinculación-MTA para liberar una asociación existente.

14.9.2.1 Argumentos

Ninguno.

14.9.2.2 Resultados

El procedimiento de entrada-desvinculación-MTA devuelve un resultado vacío como indicación de la liberación de la asociación.

14.9.2.3 Errores

Ninguno.

14.9.2.4 Descripción del procedimiento

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.9.3 Procedimiento de salida-vinculación-MTA

Esta cláusula describe los pasos dados por el MTA cuando emprende la tarea de establecer una asociación con otro MTA.

14.9.3.1 Argumentos

1) El **nombre-MTA** del MTA con quién se ha establecido la asociación.
2) El **contexto-seguridad** para la asociación.

14.9.3.2 Resultados

Un identificador interno para la asociación establecida.

14.9.3.3 Errores

El procedimiento devuelve una indicación de fallo en caso de no poderse establecer la asociación.

14.9.3.4 Descripción del procedimiento

1) El procedimiento establece los valores para los argumentos definidos en 12.1.1.1.1. Se toman los valores de **nombre-iniciador**, **contexto-seguridad** y **credenciales-iniciador** de la información interna.

   Si **credenciales-iniciador** debe contener **credenciales-fuertes**, el MTA selecciona un algoritmo de firma soportado por el MTA destinatario y utiliza este algoritmo para firmar un testigo-vinculación-iniciador que comprenda el identificador-algoritmo para ese algoritmo, el nombre-mta y el identificador de dominio global del MTA destinatario, el tiempo presente y un número aleatorio como datos-firmados-testigo-vinculación. Este testigo-vinculación-iniciador junto con un **selector-certificado** o el **certificado** (y los certificados adicionales que proporcionan su trayecto-certificación) para esta clave pública del MTA para este algoritmo constituyen las credenciales-iniciador en el argumento de vinculación.

2) El procedimiento determina la dirección del MTA e intenta establecer una asociación con los argumentos de 12.1.1.1.1. Si no tiene éxito, se devuelve una indicación de fallo y finaliza el procedimiento.

3) Si tiene éxito, se examinan los resultados devueltos por el MTA llamado (definido en 12.1.1.1.2). Se comprueba la corrección del **nombre-respondedor** y se realiza un intento de autenticar el MTA a través de las **credenciales-respondedor** devueltas.

   Cuando se recibe el resultado de la vinculación, se comprueba la firma del testigo-vinculación-respondedor por medio de la clave pública del **certificado** del MTA respondedor para el algoritmo de firma identificado. (Podría tratarse de un algoritmo de firma diferente al utilizado para firmar el testigo-vinculación-iniciador.) El **certificado** del MTA respondedor puede estar incluido en el resultado de la vinculación, o ser identificado por un **selector-certificado** y, si todavía no está disponible para el MTA, puede obtenerse del atributo certificado de usuario del MTA respondedor en el directorio. También se verifica la validez del **certificado** y de su trayecto-certificación. Adicionalmente, se comprueba que el nombre de directorio del campo de sujeto de ese **certificado** es el del MTA destinatario (es decir, que el MTA que responde es el objetivo de la vinculación). Se comprueba que el nombre-mta del campo de nombre-alternativo-sujeto de ese **certificado** corresponde al nombre MTA y al identificador de dominio global del MTA destinatario y al nombre-mta que aparece en el campo de nombre-respondedor del resultado de la vinculación. Se comprueba que el nombre-mta y el identificador-dominio-global dentro del testigo-vinculación-respondedor son los de este MTA. Se compara el tiempo del testigo con el tiempo presente para asegurarse de que el periodo de validez del testigo aceptable para este MTA no ha expirado.

   Si alguna de las comprobaciones falla, el procedimiento cierra la conexión, devuelve una indicación de fallo al llamante y finaliza.

4) Si ambas comprobaciones tienen éxito, el procedimiento devuelve el identificador de la asociación y finaliza.

14.9.4 Procedimiento de salida-desvinculación-MTA

Se llama a este procedimiento para liberar una asociación con otro MTA.

14.9.4.1 Argumentos

El identificador interno de la asociación que ha de liberarse.

14.9.4.2 Resultados

El procedimiento de salida-desvinculación-MTA devuelve un resultado vacío como indicación de la liberación de la asociación.

14.9.4.3 Errores

Ninguno.

14.9.4.4 Descripción del procedimiento

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.10 Puerto de transferencia

NOTA – Las medidas adoptadas en el puerto-transferencia están sujetas a la política-seguridad en vigor.

14.10.1 Procedimiento de entrada-mensaje

Esta cláusula describe el comportamiento del MTA cuando el otro MTA invoca la operación-abstracta de transferencia-mensaje en un puerto de transferencia.

14.10.1.1 Argumentos

Los argumentos de transferencia-mensaje enumerados en el cuadro 30 y descritos en los puntos indicados en ese cuadro.

14.10.1.2 Resultados

Se invoca el módulo entrega-diferida y se pasa el mensaje transferido.

14.10.1.3 Errores

Ninguno.

14.10.1.4 Descripción del procedimiento

Al recibir un mensaje, mediante la consecución de una operación-abstracta de transferencia-mensaje (invocada desde un MTA vecino), se invoca el procedimiento de entrada-mensaje. Este procedimiento transfiere simplemente el mensaje al módulo entrega-diferida para determinar las acciones que debe emprender este MTA.

La responsabilidad sobre el mensaje pasa al MTA-receptor con la transferencia efectuada satisfactoriamente.

14.10.2 Procedimiento de entrada-sonda

Esta cláusula describe el comportamiento del MTA cuando otro MTA invoca la operación-abstracta de transferencia-sonda en un puerto-transferencia.

14.10.2.1 Argumentos

Los argumentos de transferencia-sonda enumerados en el cuadro 31 y descritos en las cláusula indicadas en dicho cuadro.

14.10.2.2 Resultados

Se invoca el módulo principal y se pasa la sonda transferida.

14.10.2.3 Errores

Ninguno.

14.10.2.4 Descripción del procedimiento

Al recibir una sonda mediante la aparición de una operación-abstracta de transferencia-sonda (invocada desde un MTA vecino), se invoca el procedimiento de entrada-sonda. Este procedimiento simplemente pasa la sonda al módulo principal para determinar las acciones que debe emprender este MTA.

La responsabilidad de la sonda pasa al MTA receptor si la transferencia se realizó con éxito.

14.10.3 Procedimiento de entrada-informe

Esta cláusula describe el comportamiento del MTA al recibir un informe en un puerto-transferencia mediante la aparición de una operación-abstracta de transferencia-informe invocada por otro MTA o al recibir una indicación para la generación de un informe procedente de una unidad de acceso tal como una PDAU.

14.10.3.1 Argumentos

Los argumentos de informe enumerados en el cuadro 32 y descritos en las cláusulas indicadas en ese cuadro.

14.10.3.2 Resultados

Se invoca el módulo informe y se pasa el informe transferido.

14.10.3.3 Errores

Ninguno.

14.10.3.4 Descripción del procedimiento

Al recibir una sonda mediante la aparición de una operación-abstracta de transferencia-sonda (invocada desde un MTA vecino), o al recibir una indicación para una generación de un informe procedente de una unidad de acceso tal como una PDAU, se invoca el procedimiento de entrada-informe. Este procedimiento simplemente transfiere el informe al módulo informe para determinar las acciones que debe emprender este MTA.

La responsabilidad de la sonda pasa al MTA receptor si la transferencia se realizó satisfactoriamente.

14.10.4 Procedimiento de salida-mensaje

Esta cláusula describe los pasos dados por un MTA cuando éste se encarga de transferir un mensaje a otro MTA.

14.10.4.1 Argumentos

Un mensaje del procedimiento interno con instrucciones de encaminamiento para transferir a otro MTA. Los campos de este mensaje forman los argumentos de la operación-abstracta de transferencia-mensaje enumerados en el cuadro 30.

14.10.4.2 Resultados

Ninguno.

14.10.4.3 Errores

En el caso de un fallo de transferencia se invoca el módulo-principal y se pasa el mensaje con una instrucción por-mensaje que indica el motivo del fallo.

14.10.4.4 Descripción del procedimiento

El mensaje que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-mensaje. Debe observarse que el mensaje puede reflejar el proceso (por ejemplo, conversión de contenido, redireccionamiento, ampliación de la lista de distribución) llevado a cabo en este o en anteriores MTA.

1) Para garantizar que no se viola la política-seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohíbe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.
2) En caso contrario, el MTA establece una asociación con el MTA-receptor (o utiliza uno existente) e invoca la operación-abstracta de transferencia-mensaje a través de esta asociación. La consecución de la salida-mensaje indica que la transferencia ha tenido éxito y que el MTA-receptor acepta ahora la responsabilidad del mensaje. Finaliza ahora el procedimiento de salida-mensaje.

   Si el MTA-remitente ha recibido del sistema receptor instrucciones de abortar la transferencia, el procesamiento continúa en el paso 3 siguiente.

Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el MTA puede repetir el intento de establecimiento de asociación y/o transferencia, siendo el máximo número y/o la duración de las repeticiones un asunto local, excepto en que se deberá tener en cuenta el **último-tiempo-entrega** si está presente y cuando sea **crédito-para-entrega**.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, o el MTA-remitente ha recibido instrucciones de abortar la transferencia en el paso 2, se considera el mensaje como no transferible y se devuelve, con el motivo del fallo indicado, al módulo principal para un posible reencaminamiento o redireccionamiento. La responsabilidad del mensaje permanece en el MTA emisor. Termina entonces el procedimiento de salida-mensaje.

NOTA – La instrucción de abortar una transferencia es generada por el proveedor-RTSE destinatario si es permanentemente incapaz de completar la transferencia; por ejemplo, cuando la transferencia es de un tamaño tal que nunca podría ser aceptada.

14.10.5 Procedimiento de salida-sonda

Esta cláusula describe los pasos dados por un MTA cuando éste se encarga de transferir una sonda a otro MTA.

14.10.5.1 Argumentos

Una sonda del procedimiento interno con instrucciones de encaminamiento para transferir a otro MTA. Los campos de esta sonda forman los argumentos de la operación-abstracta de transferencia-sonda enumerados en el cuadro 31.

14.10.5.2 Resultados

Ninguno.

14.10.5.3 Errores

En el caso de un fallo de transferencia se invoca el módulo principal y se transfiere la sonda con una instrucción por-mensaje que indica el motivo del fallo.

14.10.5.4 Descripción del procedimiento

La sonda que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-sonda. Debe observarse que la sonda puede reflejar el proceso (por ejemplo, redireccionamiento) llevado a cabo en este o en anteriores MTA.

1) Para garantizar que no se viola la política de seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohíbe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.

2) El MTA establece una asociación con el MTA receptor (o utiliza uno existente) e invoca la operación-abstracta de transferencia-sonda a través de esta asociación. La consecución de la salida-sonda indica que la transferencia ha tenido éxito y que el MTA-receptor acepta ahora la responsabilidad de la sonda. Finaliza ahora el procedimiento de salida-sonda.

   Si el MTA-remitente ha recibido del sistema receptor instrucciones de abortar la transferencia, el procesamiento continúa en el paso 3 siguiente.

   Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el MTA puede repetir la tentativa de establecimiento de asociación y/o transferencia, siendo el máximo número y/o duración de las repeticiones un asunto local.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, o el MTA-remitente ha recibido instrucciones de abortar la transferencia en el paso 2, se considera la sonda como no transferible y se devuelve, con el motivo del fallo indicado, al módulo principal para un posible reencaminamiento o redireccionamiento. La responsabilidad del mensaje permanece en el MTA emisor. Termina entonces el procedimiento de salida-sonda.

NOTA – La instrucción de abortar una transferencia es generada por el proveedor-RTSE destinatario si es permanentemente incapaz de completar la transferencia; por ejemplo, cuando la transferencia es de un tamaño tal que nunca podría ser aceptada.

14.10.6 Procedimiento de salida-informe

Esta cláusula describe los pasos dados por un MTA cuando se enfrenta con la transferencia de un informe a otro MTA.

14.10.6.1 Argumentos

Un informe del procedimiento interno con instrucciones de encaminamiento para transferir a otro MTA. Los campos de este informe forman los argumentos de la operación-abstracta de transferencia-informe enumerados en el cuadro 32.

14.10.6.2 Resultados

Ninguno.

14.10.6.3 Errores

El informe, junto con el motivo del fallo de transferencia se devuelve al módulo informe.

14.10.6.4 Descripción del procedimiento

El informe que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-informe. Debe observarse, que el informe puede reflejar el proceso (por ejemplo, redireccionamiento) llevado a cabo en éste o en anteriores MTA.

1) Para garantizar que no se viola la política de seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohíbe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.

2) El MTA establece una asociación con el MTA receptor (o utiliza una existente) e invoca la operación-abstracta de transferencia-informe a través de esta asociación. La consecución de la salida-informe indica que la transferencia ha tenido éxito y que el MTA-receptor acepta ahora la responsabilidad del informe. Finaliza ahora el procedimiento de salida-informe.

   Si el MTA-remitente ha recibido del sistema receptor instrucciones de abortar la transferencia, el procesamiento continúa en el paso 3 siguiente.

   Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el MTA puede repetir la tentativa de establecimiento de asociación y/o transferencia, siendo el máximo número y/o la duración de las repeticiones un asunto local.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, o el MTA-remitente ha recibido instrucciones de abortar la transferencia en el paso 2, se considera el informe como no transferible y se devuelve, con el motivo del fallo indicado, al módulo informe para un posible reencaminamiento o redireccionamiento. La responsabilidad del informe permanece en el MTA emisor. Termina entonces el procedimiento de salida-informe.

NOTA – La instrucción de abortar una transferencia es generada por el proveedor-RTSE destinatario si es permanentemente incapaz de completar la transferencia; por ejemplo, cuando la transferencia es de un tamaño tal que nunca podría ser aceptada.

Anexo A

Definición de referencia de los identificadores de objeto del MTS

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

Este anexo define como referencia varios identificadores de objeto citados en los módulos ASN.1 en el texto de esta Definición de servicio. Los identificadores de objetos se asignan en la figura A.1.

Todos los identificadores de objeto que asigna esta Definición de servicio se indican en este anexo. El anexo es definitivo para todos, salvo para los módulos ASN.1 y el propio sistema de transferencia de mensajes. Las asignaciones definitivas para los primeros se producen en los propios módulos; en las cláusulas IMPORT aparecen otras referencias a ellas. Esas cláusulas están fijadas.

```
MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0) object-identifiers(0)
            version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Prologue

-- Exports everything

IMPORTS-- nothing --  ;

ID ::= OBJECT IDENTIFIER

-- Message Transfer System

id-mts ID ::= { joint-iso-itu-t mhs(6) mts(3) } -- not definitive

-- Categories of Object Identifiers

id-mod  ID ::= { id-mts 0 } -- modules
id-ot   ID ::= { id-mts 1 } -- object types
id-pt   ID ::= { id-mts 2 } -- port types
id-cont ID ::= { id-mts 3 } -- content types
id-eit  ID ::= { id-mts 4 } -- encoded information types
id-att  ID ::= { id-mts 5 } -- attributes
id-tok  ID ::= { id-mts 6 } -- token types
id-sa   ID ::= { id-mts 7 } -- secure agent types
id-ct   ID ::= { id-mts 8 } -- contracts
id-cp   ID ::= { id-mts 9 } -- connection packages

-- Modules

id-mod-object-identifiers   ID ::= { id-mod 0 } -- not definitive
id-mod-mts-abstract-service ID ::= { id-mod 1 } -- not definitive
id-mod-mta-abstract-service ID ::= { id-mod 2 } -- not definitive
id-mod-upper-bounds         ID ::= { id-mod 3 } -- not definitive

-- Object Types

id-ot-mts      ID ::= { id-ot 0 }
id-ot-mts-user ID ::= { id-ot 1 }
id-ot-mta      ID ::= { id-ot 2 }
```

Figura A.1 – Definición de la sintaxis abstracta de los identificadores de objeto del MTS (Parte 1 de 2)

```
--      Port Types

id-pt-submission     ID  ::= { id-pt 0 }
id-pt-delivery       ID  ::= { id-pt 1 }
id-pt-administration ID  ::= { id-pt 2 }
id-pt-transfer       ID  ::= { id-pt 3 }

--      Content Types

id-cont-unidentified   ID ::= { id-cont 0 } -- For use by MS and Directory
id-cont-inner-envelope ID ::= { id-cont 1 }


--      Encoded Information Types

id-eit-unknown      ID ::= { id-eit 0 }
        -- Value { id-eit 1 } is no longer defined
id-eit-ia5-text     ID ::= { id-eit 2 }
id-eit-g3-facsimile ID ::= { id-eit 3 }
id-eit-g4-class-1   ID ::= { id-eit 4 }
id-eit-teletex      ID ::= { id-eit 5 }
id-eit-videotex     ID ::= { id-eit 6 }
id-eit-voice        ID ::= { id-eit 7 }
id-eit-sfd          ID ::= { id-eit 8 }
id-eit-mixed-mode   ID ::= { id-eit 9 }

--      Attributes

id-att-physicalRendition-basic         ID ::= { id-att 0 }
id-att-physicalRendition-no-cover-page ID ::= { id-att 1 }

--      Token Types

id-tok-asymmetricToken ID ::= { id-tok 0 }

--      Secure Agent Types

id-sa-ua ID ::= { id-sa 0 }
id-sa-ms ID ::= { id-sa 1 }

--      Contracts

id-ct-mts-access        ID ::= {id-ct 0}
id-ct-mts-forced-access ID ::= {id-ct 1}
id-ct-mta-transfer      ID ::= {id-ct 2}

--      Connection Packages

id-cp-mts-connect       ID ::= {id-cp 0}
id-cp-mta-connect       ID ::= {id-cp 1}

END    -- of MTSObjectIdentifiers
```

Figura A.1 – Definición de la sintaxis abstracta de los identificadores de objeto del MTS (Parte 2 de 2)

Anexo B

Definición de referencia de los límites superiores de los parámetros del MTS

(Este anexo es parte integrante de esta Recomendación UIT-T, pero no de la Norma Internacional ISO/CEI)

Este anexo presenta como referencia los límites superiores de varios tipos de datos de longitud variable, cuyas sintaxis abstractas se definen en los módulos ASN.1 del texto de esta Definición de servicio. Los límites superiores se definen en la figura B.1.

```
MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3) version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

--      Prologue

--      Exports everything

IMPORTS-- nothing --  ;

--      Upper Bounds

ub-additional-info INTEGER ::= 1024

ub-bilateral-info INTEGER ::= 1024

ub-bit-options INTEGER ::= 16

ub-built-in-content-type INTEGER ::= 32767

ub-built-in-encoded-information-types INTEGER ::= 32

ub-certificates INTEGER ::= 64

ub-common-name-length INTEGER ::= 64

ub-content-correlator-length INTEGER ::= 512

ub-content-id-length INTEGER ::= 16

ub-content-length INTEGER ::= 2147483647          -- the largest integer in 32 bits

ub-content-types INTEGER ::= 1024

ub-country-name-alpha-length INTEGER ::= 2

ub-country-name-numeric-length INTEGER ::= 3

ub-diagnostic-codes INTEGER ::= 32767

ub-deliverable-class INTEGER ::= 256

ub-dl-expansions INTEGER ::= 512

ub-domain-defined-attributes INTEGER ::= 4
```

Figura B.1 – Definición de la sintaxis abstracta de los límites superiores del MTS (Parte 1 de 3)

```
ub-domain-defined-attribute-type-length INTEGER ::= 8

ub-domain-defined-attribute-value-length INTEGER ::= 128

ub-domain-name-length INTEGER ::= 16

ub-encoded-information-types INTEGER ::= 1024

ub-extension-attributes INTEGER ::= 256

ub-extension-types INTEGER ::= 256

ub-e163-4-number-length INTEGER ::= 15

ub-e163-4-sub-address-length INTEGER ::= 40

ub-generation-qualifier-length INTEGER ::= 3

ub-given-name-length INTEGER ::= 16

ub-initials-length INTEGER ::= 5

ub-integer-options INTEGER ::= 256

ub-labels-and-redirections INTEGER ::= 256

ub-local-id-length INTEGER ::= 32

ub-mta-name-length INTEGER ::= 32

ub-mts-user-types INTEGER ::= 256

ub-numeric-user-id-length INTEGER ::= 32

ub-organization-name-length INTEGER ::= 64

ub-organizational-unit-name-length INTEGER ::= 32

ub-organizational-units INTEGER ::= 4

ub-orig-and-dl-expansions INTEGER ::= 513   -- ub-dl-expansions plus one

ub-password-length INTEGER ::= 62

ub-pds-name-length INTEGER ::= 16

ub-pds-parameter-length INTEGER ::= 30

ub-pds-physical-address-lines INTEGER ::= 6

ub-postal-code-length INTEGER ::= 16

ub-privacy-mark-length INTEGER ::= 128

ub-queue-size INTEGER ::= 2147483647                    -- the largest integer in 32 bits

ub-reason-codes INTEGER ::= 32767

ub-recipient-number-for-advice-length INTEGER ::= 32

ub-recipients INTEGER ::= 32767

ub-redirection-classes INTEGER ::= 256

ub-redirections INTEGER ::= 512
```

Figura B.1 – Definición de la sintaxis abstracta de los límites superiores del MTS (Parte 2 de 3)

```
ub-restrictions INTEGER ::= 1024

ub-security-categories INTEGER ::= 64

ub-security-labels INTEGER ::= 256

ub-security-problems INTEGER ::= 256

ub-supplementary-info-length INTEGER ::= 256

ub-surname-length INTEGER ::= 40

ub-teletex-private-use-length INTEGER ::= 128

ub-terminal-id-length INTEGER ::= 24

ub-transfers INTEGER ::= 512

ub-tsap-id-length INTEGER ::= 16

ub-unformatted-address-length INTEGER ::= 180

ub-universal-generation-qualifier-length INTEGER ::= 16

ub-universal-given-name-length INTEGER ::= 40

ub-universal-initials-length INTEGER ::= 16

ub-universal-surname-length INTEGER ::= 64

ub-x121-address-length INTEGER ::= 16

END    -- of MTSUpperBounds
```

Figura B.1 – Definición de la sintaxis abstracta de los límites superiores del MTS (Parte 3 de 3)

NOTA – Como se especifica en 45.5.4 de la Rec. UIT-T X.680 | ISO/CEI 8824-1, los límites superiores de cada cadena teletex se miden en caracteres. Un número de octetos considerablemente mayor se requerirá para mantener este valor. Como mínimo, se debe autorizar 16 octetos, o dos veces el límite superior especificado, el que sea mayor.

Anexo C

Definición del servicio abstracto del sistema de transferencia de mensajes de 1988

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

Este anexo define una versión del servicio abstracto de transferencia de mensaje que, cuando se realice en forma de protocolo interfuncionará con el protocolo correspondiente definido en la edición anterior de esta Norma. Se proporciona sólo para facilitar la transición. Se prevé suprimir este anexo en la próxima edición.

El servicio abstracto del sistema de transferencia de mensajes de 1988 es idéntico a la versión de 1994 definida en la cláusula 8, salvo para las operaciones de registro y control de entrega que se definen a continuación, y en los siguientes casos: en los parámetros MTSBindArgument, MTSBindResult, InitiatiorCredentials, ResponderCredentials, MessageDeliveryResult, y ReportDeliveryResult definidos en la figura 2, los componentes que aparecen después de la elipsis ("...") no están definidos para contextos de aplicación de 1998.

C.1 Registro-88

La operación-abstracta registro-88 permite a un usuario-MTS realizar cambios a largo plazo en varios parámetros del usuario-MTS retenido por el MTS afectado por la entrega de mensajes al usuario-MTS.

Dichos cambios permanecen vigentes hasta ser superados por la nueva invocación de la operación-abstracta de registro-88. Sin embargo, algunos parámetros pueden ser transitoriamente reemplazados mediante la invocación de la operación-abstracta-88 control-entrega.

NOTA 1 – Esta operación-abstracta debe ser invocada antes de que pueda utilizarse cualquier otro puerto-remisión, puerto-entrega u operación-abstracta de puerto-administración o habrá tenido lugar un registro equivalente localmente.

NOTA 2 – Esta operación-abstracta no incluye los parámetros existentes involucrados por el elemento-de-servicio destinatario alternativo autorizado definido en la Rec. UIT-T X.400 | ISO/CEI 10021-1. La forma en que se suministran y modifican dichos parámetros es asunto local.

C.1.1 Argumentos

El cuadro C.1 enumera los argumentos de la operación-abstracta registro-88 y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro C.1 – Argumentos de registro-88

Argumento	Presencia	Cláusula
Argumentos de registro		
Dirección-usuario	O	8.4.1.1.1.1
Tipos-información-codificada-entregables	O	8.4.1.1.1.2
Tipos-contenido-entregables	O	C.1.1.1
Longitud-contenido-máxima-entregable	O	C.1.1.2
Destinatario-alternativo-asignado-destinatario	O	C.1.1.3
Etiquetas-seguridad-usuario	O	C.1.1.4
Dirección-usuario	O	C.1.1.5
Argumentos de control de entrega por defecto		8.4.1.1.1.7
Limitaciones	O	8.3.1.3.1.1
Operaciones-admisibles	O	8.3.1.3.1.2
Prioridad-inferior-admisible	O	8.3.1.3.1.3
Tipos-información-codificada-admisibles	O	C.2.1.1
Tipos-contenido-admisibles	O	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	O	8.3.1.3.1.6

C.1.1.1 Tipos-información-codificada-entregables

Este argumento indica los **tipos-información-codificada** que el MTS permitirá que aparezcan en los mensajes entregados al usuario-MTS, si éstos deben modificarse. Pueden ser generados por el usuario-MTS.

El MTS debe rechazar como inentregable cualquier mensaje para un usuario-MTS que no esté registrado para aceptar la entrega de los **tipos-información-codificada** del mensaje. El usuario-MTS puede registrarse para recibir el **tipo-información-codificada-desconocido**. Los **tipos-información-codificada-entregables** indican también los posibles **tipos-información-codificada** cuya conversión implícita puede efectuar.

En ausencia de este argumento, los **tipos-información-codificada-entregables** permanecerán sin modificar.

C.1.1.2 Tipos-contenido-entregables

Este argumento indica los **tipos-contenido** que el MTS debe permitir que aparezcan en los mensajes entregados al usuario-MTS, si han de modificarse. Puede ser generado por el usuario-MTS.

El MTS debe rechazar como inentregable cualquier mensaje para un usuario-MTS que no esté registrado para aceptar la entrega de los **tipos-contenido** del mensaje. El usuario-MTS puede registrarse para recibir el **tipo-contenido-no-identificado**.

En ausencia de este argumento, los **tipos-contenido-entregables** deben permanecer sin modificar.

C.1.1.3 Longitud-máxima-contenido-entregable

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el MTS debe permitir que aparezca en los mensajes entregados al usuario-MTS, si han de modificarse. Puede ser generado por el usuario-MTS.

El MTS deberá rechazar como imposible de entregar, cualquier mensaje para un usuario-MTS que no esté registrado para aceptar la entrega de mensajes de este tamaño.

En ausencia de este argumento, la longitud **máxima-contenido-entregable** del mensaje debe permanecer sin modificar.

C.1.1.4 Destinatario-alternativo-asignado-destinatario

En caso que deba modificarse la asignación de destinatarios-alternativos, este argumento contiene una lista ordenada de los **nombres-OR** de los destinatarios-alternativos y especificado por el usuario-MTS, a los que se redirigirán los mensajes. Puede ser generado por el usuario-MTS. Puede especificarse un criterio diferente de este argumento para cada valor de **etiquetas-seguridad-usuario**.

Si se ha registrado un **destinatario-alternativo-asignado-destinatario**, asociado a un valor de **etiqueta-seguridad-usuario**, los mensajes que cumplen los criterios de **etiqueta-seguridad-mensaje** serán redirigidos al destinatario-alternativo. Los mensajes que llevan una **etiqueta-seguridad-mensaje**, para los cuales no se ha registrado un **destinatario-alternativo-asignado-destinatario**, no serán redirigidos a un **destinatario-alternativo-asignado-destinatario**.

Si se ha registrado un **destinatario-alternativo-asignado-destinatario** único, y no está asociado a un valor de **etiqueta-seguridad-usuario**, todos los mensajes serán redirigidos a ese destinatario alternativo.

El **destinatario-alternativo-asignado-destinatario** deberá contener el **nombre-OR** del destinatario-alternativo. Si el **destinatario-alternativo-asignado-destinatario** contiene el **nombre-OR** del usuario-MTS (véase 8.4.1.1.1.1) no se registra ningún **destinatario-alternativo-asignado-destinatario**.

En ausencia de este argumento el **destinatario-alternativo-asignado-destinatario**, si lo hubiere, permanece sin modificar.

C.1.1.5 Etiquetas-seguridad-usuario

Este argumento contiene las **etiquetas-seguridad** del usuario-MTS, si han de modificarse. Puede ser generado por el usuario-MTS.

Puede registrarse un **destinatario-alternativo-asignado-destinatario** para cualquier valor de las **etiquetas-seguridad-usuario**.

En ausencia de este argumento, las **etiquetas-seguridad-usuario** permanecen sin modificar.

Algunas políticas-seguridad puede que permitan únicamente modificar las **etiquetas-seguridad-usuario** de esta forma si se utiliza un enlace seguro. Pueden proporcionarse otros medios locales de modificar las **etiquetas-seguridad-usuario** de forma segura.

C.1.2 Resultados

La operación-abstracta registro-88 devuelve un resultado vacío como indicación del éxito.

C.1.3 Errores-abstractos

El cuadro C.2 enumera los errores-abstractos que pueden interrumpir la operación-abstracta de registro-88 y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro C.2 – Errores-abstractos de registro-88

Error-abstracto	Cláusula
Registro-rechazado	8.4.2.1
Error-vinculación-distante	8.2.2.10

C.2 Control-entrega-88

La operación-abstracta control-entrega-88 permite al usuario-MTS limitar de forma transitoria las operaciones abstractas de puerto-entrega que puede invocar el MTS, y los mensajes que puede entregar el usuario-MTS a través de la operación-abstracta entrega-mensaje.

El MTS debe retener hasta un tiempo posterior, en vez de abandonar, las operaciones-abstractas y los mensajes prohibidos.

La ejecución satisfactoria de la operación-abstracta significa que los controles especificados están actualmente en vigor. Estos controles sobreseen cualquier otro previamente en vigor, y permanecen vigentes hasta que se libera la asociación, el usuario-MTS invoca la operación-abstracta de registro-88 en el puerto-administración para imponer limitaciones más rigurosas que los controles especificados.

La operación-abstracta devuelve una indicación de cualquier operación-abstracta que invocara el MTS, o cualquier tipo de mensaje que entregaría o sobre el que informaría el MTS, a no ser por los controles que prevalecen.

C.2.1 Argumentos

El cuadro C.3 enumera los argumentos de la operación-abstracta control-entrega-88 y para cada argumento califica la presencia e identifica la cláusula donde se define el argumento.

Cuadro C.3 – Argumentos de control-entrega-88

Argumento	Presencia	Cláusula
Argumentos de control de entrega		
Limitación	O	8.3.1.3.1.1
Operaciones-admisibles	O	8.3.1.3.1.2
Prioridad-inferior-admisible	O	8.3.1.3.1.3
Tipos-información-codificada-admisible	O	C.2.1.1
Tipos-contenido-admisibles	O	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	O	8.3.1.3.1.6
Contexto-seguridad-admisible	O	8.3.1.3.1.7

C.2.1.1 Tipos-información-codificada-admisibles

Este argumento indica los **tipos-información-codificada**, que deben aparecer en los mensajes que el MTS entregará al usuario-MTS a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-MTS.

Los **tipos-información-codificada-admisibles** especificados deben estar entre los autorizados a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**tipos-información-codificada-entregables**).

En ausencia de este argumento, los **tipos-información-codificada-admisibles** de un mensaje que el MTS puede entregar al usuario-MTS permanecen sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se debe aplicar el control por defecto registrado con el MTS mediante la operación-abstracta de registro del puerto-administración.

C.2.2 Resultados

Los resultados de la operación-abstracta control-entrega-88 son idénticos a los resultados de la operación-abstracta control-entrega como se define en 8.3.1.3.2.

C.2.3 Errores-abstractos

El cuadro C.4 enumera los errores-abstractos que pueden interrumpir la operación-abstracta control-entrega-88, y para cada error-abstracto identifica la cláusula donde se define el error-abstracto.

Cuadro C.4 – Errores-abstractos de control-entrega-88

Error-abstracto	Cláusula
Control-viola-registro	8.3.2.2
Error-seguridad	8.3.2.3

```
MTSAbstractService88 { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
              version-1988(1988) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONTRACT
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
                        remote-operations(4) informationObjects(5) version1(0) }

        -- MTS Abstract Service Parameters

        ABSTRACT-OPERATION, change-credentials, ContentLength, ContentTypes, Controls,
        control-violates-registration, DefaultDeliveryControls, EncodedInformationTypes,
        message-delivery, MHS-OBJECT, mts-connect, operationObject1, PORT,
        RecipientAssignedAlternateRecipient, register-rejected, report-delivery, SecurityLabel,
        security-error, submission, UserAddress, UserName, Waiting
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- Object Identifiers

        id-ct-mts-access, id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user,
        id-pt-administration, id-pt-delivery
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }

        -- Operation Codes

        op-delivery-control, op-register
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                        mts-access-protocol(1) version-1999(1) }
```

```
        -- Upper Bounds

        ub-content-types, ub-labels-and-redirections
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                        version-1999(1) };

--      Objects

mts-88 MHS-OBJECT ::= {
        INITIATES       { mts-forced-access-contract-88 }
        RESPONDS        { mts-access-contract-88 }
        ID              {id-ot-mts 88} }

mts-user-88 MHS-OBJECT ::= {
        INITIATES       { mts-access-contract-88 }
        RESPONDS        { mts-forced-access-contract-88 }
        ID              { id-ot-mts-user 88 } }
```

Figura C.1 – Definición de la sintaxis abstracta del servicio abstracto MTS 1988 (Parte 1 de 2)

```
-- Contracts

mts-access-contract-88 CONTRACT ::= {
        CONNECTION              mts-connect
        INITIATOR CONSUMER OF   { submission | delivery-88 | administration-88 }
        ID                      { id-ct-mts-access 88 } }

mts-forced-access-contract-88 CONTRACT ::= {
        CONNECTION              mts-connect
        RESPONDER CONSUMER OF   { submission | delivery-88 | administration-88 }
        ID                      { id-ct-mts-forced-access 88 } }

--      Ports

delivery-88 PORT ::= {
        OPERATIONS {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        CONSUMER INVOKES {delivery-control-88,...} -- This IOS needs to be extensible for
Forward{} of X.880--
        SUPPLIER INVOKES {message-delivery | report-delivery,...} -- This IOS needs to be
extensible for Forward{} of X.880--
        ID {id-pt-delivery 88}}

administration-88 PORT ::= {
        OPERATIONS {change-credentials,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        CONSUMER INVOKES {register-88,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        SUPPLIER INVOKES {operationObject1,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        ID {id-pt-administration 88}
  }

--      Delivery Port

delivery-control-88 ABSTRACT-OPERATION ::= {
        ARGUMENT            DeliveryControls88
        RESULT              Waiting
        ERRORS              { control-violates-registration | security-error }
        LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        INVOKE-PRIORITY     { 3 }
        CODE                op-delivery-control }

DeliveryControls88 ::= SET {
        COMPONENTS OF Controls (WITH COMPONENTS {
                ... ,
                permissible-encoded-information-types ABSENT } ),
        permissible-encoded-information-types-88 EncodedInformationTypes OPTIONAL }
```

```
--      Administration Port

register-88 ABSTRACT-OPERATION ::= {
       ARGUMENT          Register88
       RESULT            NULL
       ERRORS            { register-rejected }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }

Register88 ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-encoded-information-types EncodedInformationTypes OPTIONAL,
       deliverable-maximum-content-length [1] EXPLICIT ContentLength OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       deliverable-content-types [3] ContentTypes OPTIONAL,
       labels-and-redirections [4] SET SIZE (1..ub-labels-and-redirections) OF
              LabelAndRedirection OPTIONAL }

LabelAndRedirection ::= SET {
       user-security-label [0] UserSecurityLabel OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                          OPTIONAL }

UserSecurityLabel ::= SecurityLabel

END     -- of MTSAbstractService88
```

Figura C.1 – Definición de la sintaxis abstracta del servicio abstracto MTS 1988 (Parte 2 de 2)

Anexo D

Diferencias entre las versiones de ISO/CEI 10021-4 y la Recomendación UIT-T X.411

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

En este anexo se identifican las diferencias técnicas entre la Rec. UIT-T X.411 | ISO/CEI 10021-4.

Estas diferencias son:

1) En la Rec. UIT-T X.411 se establecen limitaciones de tamaño a un cierto número de campos de protocolo (véase el anexo B). En ISO/CEI 10021-4, los valores reales de las limitaciones no forman parte de la Norma.

Anexo E

Índice

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

Este anexo contiene un índice (en inglés) de esta Definición de servicio, en el que se indican los números de página (de la versión inglesa) en los que aparece la definición de cada elemento de las diversas categorías.

El índice se divide en las siguientes categorías:

a) Abreviaturas.
b) Términos.
c) Definiciones de los parámetros del MTS.
d) Módulos ASN.1.
e) Clases de objetos de información ASN.1.
f) Tipos ASN.1.
g) Valores ASN.1.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos y comunicación entre sistemas abiertos**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

17397

Impreso en Suiza
Ginebra, 2004