



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.402

(06/1999)

SERIE X: REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS

Sistemas de tratamiento de mensajes

**Tecnología de la información – Sistemas de
tratamiento de mensajes: Arquitectura global**

Recomendación UIT-T X.402

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
SEGURIDAD DE LAS TELECOMUNICACIONES	X.1000–

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

**Tecnología de la información – Sistemas de
tratamiento de mensajes: Arquitectura global**

Resumen

Esta Recomendación | Norma Internacional contiene definiciones de atributos y clases de objeto del directorio, algunas de ellas nuevas y las restantes revisadas, que se utilizan en las nuevas Recomendaciones X.500. La ASN.1 ha sido enteramente revisada para usar las nuevas Recomendaciones X.680 y X.880. Se incorporan numerosas correcciones de defectos. Esta Recomendación | Norma Internacional incorpora además mejoras sobre la autoridad de registro internacional, la utilización de caracteres ISO/CEI 10646 en direcciones OR, el cambio de credenciales protegidas y la utilización del directorio de 1997.

Orígenes

La Recomendación UIT-T X.402 fue aprobada el 18 de junio de 1999. Se publica también un texto idéntico como Norma Internacional ISO/CEI 10021-2.

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.402 agrupa la Rec. UIT-T X.402 (11/1995), el corrigendum técnico 1 a la X.402 (08/1997) y la enmienda 1 a la X.402 (12/1997).

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.

© UIT 2004

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

SECCIÓN 1 – INTRODUCCIÓN.....	1
1 Objeto.....	1
2 Referencias normativas.....	3
2.1 Interconexión de sistemas abiertos.....	3
2.2 Sistemas de directorio.....	4
2.3 Sistemas de tratamiento de mensajes.....	4
2.4 Indicativos de país.....	5
2.5 Direcciones de la red.....	5
2.6 Código de lenguaje.....	5
2.7 Juegos de caracteres.....	5
3 Definiciones.....	5
3.1 Interconexión de sistemas abiertos.....	5
3.2 Sistemas de directorio.....	7
3.3 Sistemas de tratamiento de mensajes.....	7
4 Abreviaturas.....	7
5 Convenios.....	7
5.1 ASN.1.....	7
5.2 Grado.....	7
5.3 Términos.....	8
SECCIÓN 2 – MODELOS ABSTRACTOS.....	8
6 Visión de conjunto.....	8
7 Modelo funcional.....	8
7.1 Objetos funcionales primarios.....	9
7.1.1 Sistema de tratamiento de mensajes.....	9
7.1.2 Usuarios.....	9
7.1.3 Lista de distribución.....	9
7.2 Objetos funcionales secundarios.....	10
7.2.1 Sistema de transferencia de mensajes.....	10
7.2.2 Agentes de usuario.....	10
7.2.3 Memorias de mensajes.....	10
7.2.4 Unidades de acceso.....	11
7.3 Objetos funcionales terciarios.....	11
7.3.1 Agentes de transferencia de mensajes.....	11
7.4 Tipos de AU seleccionados.....	11
7.4.1 Entrega física.....	11
7.4.2 Telemática.....	12
7.4.3 Télex.....	12
8 Modelo de información.....	12
8.1 Mensajes.....	12
8.2 Sondas.....	13
8.3 Informes.....	13
9 Modelo operacional.....	14
9.1 Transmisión.....	14
9.2 Funciones de la transmisión.....	15
9.3 Pasos de la transmisión.....	16
9.3.1 Origen.....	16
9.3.2 Depósito.....	17
9.3.3 Importación.....	17
9.3.4 Transferencia.....	17
9.3.5 Exportación.....	17
9.3.6 Entrega.....	17

	<i>Página</i>
9.3.7 Recuperación.....	18
9.3.8 Recepción.....	18
9.4 Eventos de la transmisión.....	18
9.4.1 División.....	18
9.4.2 Combinación.....	19
9.4.3 Resolución de nombre.....	19
9.4.4 Ampliación de DL.....	19
9.4.5 Redireccionamiento.....	19
9.4.6 Conversión.....	19
9.4.7 No entrega.....	19
9.4.8 No afirmación.....	19
9.4.9 Afirmación.....	20
9.4.10 Encaminamiento.....	20
10 Modelo de seguridad.....	20
10.1 Políticas de seguridad.....	21
10.2 Servicios de seguridad.....	21
10.2.1 Servicios de seguridad de autenticación de origen.....	22
10.2.2 Servicio de seguridad de gestión de acceso seguro.....	23
10.2.3 Servicios de seguridad de confidencialidad de datos.....	23
10.2.4 Servicios de seguridad de integridad de datos.....	23
10.2.5 Servicio de seguridad de no rechazo.....	24
10.2.6 Servicio de seguridad del etiquetado de seguridad de mensajes.....	25
10.2.7 Servicios de gestión de la seguridad.....	25
10.3 Elementos de seguridad.....	25
10.3.1 Elementos de seguridad de autenticación.....	25
10.3.2 Elementos de seguridad de gestión de acceso seguro.....	27
10.3.3 Elementos de seguridad de confidencialidad de datos.....	27
10.3.4 Elementos de seguridad de integridad de datos.....	28
10.3.5 Elementos de seguridad de no rechazo.....	28
10.3.6 Elementos de seguridad de la etiqueta de seguridad.....	29
10.3.7 Elemento de seguridad de gestión de la seguridad.....	29
10.3.8 Técnica del sobre doble.....	29
10.3.9 Codificación para encriptación y troceado (hashing).....	29
SECCIÓN 3 – CONFIGURACIONES.....	29
11 Visión de conjunto.....	29
12 Configuraciones funcionales.....	30
12.1 Respecto al directorio.....	30
12.2 Respecto a la memoria de mensajes.....	30
13 Configuraciones físicas.....	30
13.1 Sistemas de mensajería.....	30
13.1.1 Sistemas de acceso.....	32
13.1.2 Sistemas de almacenamiento.....	32
13.1.3 Sistemas de acceso y almacenamiento.....	32
13.1.4 Sistemas de transferencia.....	32
13.1.5 Sistemas de acceso y transferencia.....	32
13.1.6 Sistemas de almacenamiento y transferencia.....	32
13.1.7 Sistema de acceso, almacenamiento y transferencia.....	32
13.2 Configuraciones representativas.....	32
13.2.1 Totalmente centralizada.....	32
13.2.2 Transferencia y almacenamiento de mensajes centralizados.....	33
13.2.3 Transferencia de mensajes centralizada.....	33
13.2.4 Totalmente distribuida.....	33
14 Configuraciones organizativas.....	33
14.1 Dominios de gestión.....	33
14.1.1 Dominio de gestión de administración.....	34
14.1.2 Dominio de gestión privado.....	34

	<i>Página</i>
14.2 Configuraciones representativas	34
14.2.1 Totalmente centralizada	34
14.2.2 Conectada directamente	34
14.2.3 Conectada indirectamente	34
15 El MHS global.....	35
SECCIÓN 4 – DENOMINACIÓN, DIRECCIONAMIENTO Y ENCAMINAMIENTO	35
16 Visión de conjunto.....	35
17 Denominación	35
17.1 Nombres de directorio	36
17.2 Nombres OR	36
18 Direccionamiento	36
18.1 Lista de atributos	37
18.2 Juegos de caracteres	37
18.3 Atributos normalizados	38
18.3.1 Nombre-dominio-administración	39
18.3.2 Nombre-común	39
18.3.3 Nombre-país.....	40
18.3.4 Componentes-ampliación-dirección-OR-postal	40
18.3.5 Componentes-ampliación-dirección-entrega-física.....	40
18.3.6 Atributos-postales-locales	40
18.3.7 Dirección-red	40
18.3.8 Identificador-usuario-numérico.....	40
18.3.9 Nombre-organización.....	41
18.3.10 Nombres-unidades-organizativas.....	41
18.3.11 Nombre-servicio-entrega-física.....	41
18.3.12 Nombre-personal.....	41
18.3.13 Nombre-país-entrega-física.....	41
18.3.14 Nombre-oficina-entrega-física	41
18.3.15 Número-oficina-entrega-física	41
18.3.16 Nombre-organización-entrega-física.....	42
18.3.17 Nombre-personal-entrega-física.....	42
18.3.18 Dirección-apartado-correos.....	42
18.3.19 Código-postal	42
18.3.20 Dirección-lista-correos.....	42
18.3.21 Nombre-dominio-privado	42
18.3.22 Dirección-calle.....	42
18.3.23 Identificador-terminal	42
18.3.24 Tipo-terminal	42
18.3.25 Dirección-postal-no-formatada	43
18.3.26 Nombre-postal-exclusivo	43
18.4 Equivalencia de listas de atributos	43
18.5 Formas de direcciones OR	44
18.5.1 Dirección OR nemotécnica	44
18.5.2 Dirección OR numérica.....	45
18.5.3 Dirección OR postal.....	45
18.5.4 Dirección OR terminal.....	45
18.5.5 Determinación de las formas de dirección	46
18.6 Atributos condicionales.....	46
19 Encaminamiento.....	46
Versión ISO/CEI:	47
SECCIÓN 5 – USO DEL DIRECTORIO	48
20 Visión de conjunto.....	48
21 Autenticación	48
22 Resolución de nombres	48
23 Ampliación de DL.....	48
24 Evaluación de capacidades.....	48

SECCIÓN 6 – REALIZACIÓN POR OSI	49
25 Visión de conjunto.....	49
26 Elementos de servicio de aplicación.....	49
26.1 El concepto de ASE	49
26.2 ASE simétricos y asimétricos.....	50
26.3 ASE de tratamiento de mensajes.....	51
26.3.1 Transferencia de mensajes	52
26.3.2 Depósito de mensajes.....	52
26.3.3 Entrega de mensajes.....	52
26.3.4 Recuperación de mensajes	52
26.3.5 Administración de mensajes	52
26.4 ASE de apoyo.....	52
26.4.1 Operaciones distantes.....	53
26.4.2 Transferencia fiable.....	53
26.4.3 Control de asociación.....	53
27 Contextos de aplicación.....	53
SECCIÓN 7 – CONVENIOS SOBRE DEFINICIÓN DEL SERVICIO ABSTRACTO	54
28 Visión de conjunto.....	54
29 Componentes del modelo abstracto.....	54
29.1 Objetos abstractos	54
29.2 Contratos abstractos	54
29.3 Paquetes de conexión	54
29.4 Puertos abstractos.....	55
29.5 Operaciones abstractas y errores abstractos	55
30 Realización de ROS (servicio de operaciones a distancia).....	55
Anexo A – Clases de objetos de directorio y atributos	56
A.1 Clases de objetos.....	56
A.1.1 Lista de distribución del MHS	56
A.1.2 Memoria de mensajes del MHS	56
A.1.3 Agente de transferencia de mensajes del MHS	57
A.1.4 Usuario del MHS	57
A.1.5 Agente de usuario del MHS	57
A.2 Atributos.....	57
A.2.1 EIT aceptables del MHS	57
A.2.2 Clases entregables del MHS.....	58
A.2.3 Tipos de contenido entregable del MHS	58
A.2.4 Servicio de archivo de DL del MHS	58
A.2.5 Miembros del DL del MHS.....	58
A.2.6 Política de DL del MHS.....	58
A.2.7 Listas relacionadas con DL del MHS.....	59
A.2.8 Permisos de depósito de DL del MHS	59
A.2.9 Servicio de suscripción a DL del MHS	59
A.2.10 EIT exclusivamente aceptables del MHS.....	59
A.2.11 Longitud de contenido máxima del MHS	59
A.2.12 Nombre de directorio memoria de mensajes del MHS	60
A.2.13 Direcciones OR del MHS.....	60
A.2.14 Direcciones OR con capacidades del MHS.....	60
A.2.15 Atributos permitidos por el MHS.....	60
A.2.16 Acciones automáticas permitidas por el MHS	60
A.2.17 Tipos de contenido permitidos por el MHS	61
A.2.18 Reglas de concordancia permitidas por el MHS	61
A.2.19 EIT no aceptables del MHS	61
A.3 Sintaxis de atributos.....	61
A.3.1 Permiso de depósito de DL	61
A.3.2 Política de DL	63

	<i>Página</i>
A.3.3 Dirección OR	65
A.3.4 Dirección OR con capacidades	65
A.3.5 Nombre OR	65
A.4 Contextos	66
A.4.1 Anotación de administrador DL	66
A.4.2 DL anida de DL	66
A.4.3 Reiniciación de originador DL	67
A.5 Nombres alternativos de sujeto de certificado	67
A.5.1 Nombre de MTA	67
Anexo B – Definición de referencia de identificadores de objetos	68
Anexo C – Definición de referencia de clases de objetos y atributos de directorio	70
Anexo D – Amenazas contra la seguridad	77
D.1 Suplantación	77
D.2 Secuenciamiento de mensajes	77
D.3 Modificación de información	78
D.4 Denegación de servicio	79
D.5 Rechazo	79
D.6 Fuga de información	79
D.7 Otras amenazas	79
Anexo E – Provisión de servicios de seguridad en la Recomendación UIT-T X.411 ISO/CEI 10021-4	80
Anexo F – Representación de las direcciones OR para su utilización por el hombre	81
F.1 Finalidad	81
F.2 Objeto	81
F.3 Formato	81
F.3.1 Generalidades	81
F.3.2 Formato etiquetado	82
F.3.3 Formato autoexplicativo	84
F.4 Interfaz del usuario	84
Anexo G – La utilización de direcciones OR por parte de las organizaciones multinacionales	86
G.1 Principios de direccionamiento	86
G.2 Ejemplos de configuraciones	86
G.2.1 PRMD independientes múltiples	87
G.2.2 Un PRMD único, nombrado a partir del país de origen	87
G.2.3 Un PRMD único con múltiples nombres de dominio y de país	88
G.3 Seudónimos de direcciones OR	89
Anexo H – Utilización de contraseñas protegidas para el acceso a almacenamiento de mensajes	90
Anexo I – Diferencias entre la ISO/CEI 10021-2 y la Recomendación UIT-T X.402	93
Anexo J – Resumen de los cambios con respecto a ediciones anteriores	94
J.1 Diferencias entre ISO/CEI 10021-2:1990 y la Recomendación X.402 del CCITT (1992)	94
J.2 Diferencias entre la Recomendación X.402 del CCITT (1992) y la Recomendación UIT-T X.402 (1995) ISO/CEI 10021-2:1996	94
J.3 Diferencias entre la Recomendación UIT-T X.402 (1995) ISO/CEI 10021-2:1996 y la Recomendación UIT-T X.402 (1999) ISO/CEI 10021-2:1999	94
Anexo K – Índice	95

Introducción

La presente Especificación forma parte de una serie de Recomendaciones | Normas Internacionales sobre el tratamiento de mensajes. Esta serie proporciona un amplio esquema de sistemas de tratamiento de mensajes (MHS) constituidos por cualquier número de sistemas abiertos cooperantes.

Un MHS tiene por objeto permitir a los usuarios el intercambio de mensajes, sobre la base de su almacenamiento y retransmisión. Un mensaje presentado en nombre de un usuario, el originador, es transportado por el sistema de transferencia de mensajes (MTS) y entregado a continuación a los agentes de uno o más usuarios adicionales, los destinatarios. Las unidades de acceso (AU) enlazan el MTS con sistemas de comunicación de otro tipo (por ejemplo, sistemas postales). El usuario recibe la ayuda de un agente de usuario (UA) para la preparación, el almacenamiento y la visualización de los mensajes. Facultativamente, puede recibir la ayuda de un dispositivo de almacenamiento de mensajes (MS) para almacenarlos. El MTS consta de cierto número de agentes de transferencia de mensajes (MTA) que, de manera colectiva, realizan la función de transferencia de almacenamiento y retransmisión de mensajes.

Esta Especificación especifica la arquitectura global del MHS, y sirve como introducción técnica al mismo.

La presente Especificación ha sido elaborada conjuntamente por el UIT-T y la ISO/CEI. Se publica como texto común como Rec. UIT-T X.402 | ISO/CEI 10021-2.

**NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T**

**Tecnología de la información – Sistemas de
tratamiento de mensajes: Arquitectura global**

SECCIÓN 1 – INTRODUCCIÓN

1 Objeto

Esta Recomendación | Norma Internacional define la arquitectura global del MHS y sirve como introducción técnica al mismo.

En otras Recomendaciones | partes de ISO/CEI 10021 se especifican otros aspectos del tratamiento de mensajes. La Rec. UIT-T X.400 | ISO/CEI 10021-1 da una visión general, no técnica, del tratamiento de mensajes. La prueba de conformidad de los componentes del MHS se describe en la Rec. X.403. Las reglas detalladas según las cuales el MTS convierte los contenidos de los mensajes de un EIT a otro se definen en la Rec. X.408. El servicio abstracto que proporciona el MTS y el procedimiento que gobierna su operación distribuida se definen en la Rec. UIT-T X.411 | ISO/CEI 10021-4. El servicio abstracto proporcionado por el MS se define en la Rec. UIT-T X.413 | ISO/CEI 10021-5. Los protocolos de aplicación que gobiernan las interacciones de los componentes del MHS se especifican en la Rec. UIT-T X.419 | ISO/CEI 10021-6. El sistema de mensajería interpersonal, que es una aplicación del tratamiento de mensajes, se define en la Rec. UIT-T X.420 | ISO/CEI 10021-7. El acceso telemático al sistema de mensajería interpersonal se especifica en la Rec. T.330. El servicio de mensajería del EDI se describe en la Rec. CCITT F.435 | ISO/CEI 10021-8. El sistema de mensajería del EDI, que es otra aplicación del tratamiento de mensajes, se define en la Rec. CCITT X.435 | ISO/CEI 10021-9. Los medios por los cuales los mensajes pueden encaminarse a través del MHS se especifican en ISO/CEI 10021-10. La información de gestión de los componentes del MHS se define en las Recomendaciones de la serie X.460 | ISO/CEI 11588.

En el cuadro 1 se indican de manera resumida las Normas Internacionales de la ISO/CEI y las Recomendaciones del UIT-T relacionadas con el tratamiento de mensajes.

Cuadro 1 – Especificaciones para sistemas de tratamiento de mensajes

ISO/CEI	UIT-T	TEMA TRATADO
+-----+-----+-----+-----+		
+- Introducción - - - - -		
10021-1	X.400	Visión de conjunto de sistemas y servicios
10021-2	X.402	Arquitectura global
+- Aspectos diversos - - - - -		
-	X.408	Reglas de conversión de tipo de información codificada
+- Servicios abstractos - - - - -		
10021-4	X.411	Definición del servicio abstracto del MTS y procedimientos de operación distribuida
10021-5	X.413	Definición del servicio abstracto del MS
+- Protocolos - - - - -		
10021-6	X.419	Especificaciones de protocolo
+- Sistema de mensajería interpersonal - - - - -		
10021-7	X.420	Sistema de mensajería interpersonal
-	T.330	Acceso telemático al IPMS
+- Sistema de mensajería con intercambio electrónico de datos - - - - -		
10021-8	F.435	Servicio de mensajería EDI
10021-9	X.435	Sistema de mensajería EDI
+- Encaminamiento - - - - -		
10021-10	X.412	Encaminamiento MHS
10021-11	X.404	Encaminamiento MHS: Guía para los gestores de sistemas
+- Gestión de MHS - - - - -		
11588-1	X.460	Gestión: Modelo y arquitectura
11588-3	X.462	Información de registro cronológico
11588-8	X.467	Gestión de agente de transferencia de mensajes
+-----+-----+-----+-----+		

El Directorio, que es el instrumento principal para la difusión de la información relacionada con las comunicaciones entre los componentes del MHS, se define en las Recomendaciones de la serie X.500 | ISO/CEI 9594. Véase el cuadro 2.

Cuadro 2 – Especificaciones para los directorios

ISO/CEI	UIT-T	TEMA TRATADO
9594-1	X.500	Visión de conjunto
9594-2	X.501	Modelos
9594-3	X.511	Definición del servicio abstracto
9594-4	X.518	Procedimientos de operación distribuida
9594-5	X.519	Especificaciones de protocolos
9594-6	X.520	Tipos de atributos seleccionados
9594-7	X.521	Clases de objetos seleccionados
9594-8	X.509	Marco de autenticación
9594-9	X.525	Duplicación
9594-10	X.530	Utilización de la gestión de sistemas para la administración del directorio

El fundamento arquitectural del tratamiento de mensajes figura en otras Recomendaciones | Normas Internacionales. El modelo de referencia de OSI se define en la Rec. UIT-T X.200 | ISO/CEI 7498. 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, Rec. UIT-T X.683 | ISO/CEI 8824-4 y Rec. UIT-T X.690 | ISO/CEI 8825-1 se define la notación ASN.1 para la especificación de las estructuras de datos de los servicios abstractos y los protocolos de aplicación y las reglas de codificación asociadas. La manera de establecer y liberar asociaciones, el ACSE, se especifica en la Rec. UIT-T X.217 | ISO/CEI 8649 y Rec. UIT-T X.227 | ISO/CEI 8650-1. En la Rec. UIT-T X.218 | ISO/CEI 9066-1 y en la Rec. CCITT X.228 e ISO/CEI 9066-2 se define el método RTSE de transporte fiable de las APDU por las asociaciones. La manera de efectuar peticiones a otros sistemas abiertos, el ROSE, se especifica en la Rec. UIT-T X.880 | ISO/CEI 13712-1, Rec. UIT-T X.881 | ISO/CEI 13712-2 y Rec. UIT-T X.882 | ISO/CEI 13712-3.

En el cuadro 3 se indican, en síntesis las Normas Internacionales de la ISO/CEI y las Recomendaciones del UIT-T básicas para el tratamiento de mensajes.

Cuadro 3 – Especificaciones para los fundamentos del MHS

ISO/CEI	UIT-T	TEMA TRATADO
+- Model		
7498-1	X.200	Modelo de referencia de OSI
+- ASN.1		
8824-1	X.680	Notación de sintaxis abstracta uno
8824-2	X.681	ASN.1 Objetos de información
8824-3	X.682	ASN.1 Especificación de constricciones
8824-4	X.683	ASN.1 Parametrización
8825-1	X.690	Reglas básicas de codificación
+- Control de asociación		
8649	X.217	Definición de servicios
8650	X.227	Especificación del protocolo
+- Transferencia fiable		
9066-1	X.218	Definición de servicios
9066-2	X.228	Especificación del protocolo
+- Operaciones a distancia		
13712-1	X.880	Conceptos, modelo y notación
13712-2	X.881	Definición del servicio
13712-3	X.882	Especificación del protocolo

La presente Recomendación | Norma Internacional está estructurada como a continuación se indica. La sección 1 es la de introducción. En la sección 2 se presentan los modelos abstractos de tratamiento de mensajes. En la sección 3 se especifica la manera de configurar el MHS para satisfacer una diversidad de exigencias de tipo funcional, físico u organizativo. En la sección 4 se describe la denominación y el direccionamiento de usuarios y listas de distribución y el encaminamiento hacia ellos de los objetos de información. En la sección 5 se indican los usos que el MHS puede hacer del directorio. En la sección 6 se describe cómo se realiza el MHS utilizando la OSI. Los convenios utilizados en la definición de los servicios abstractos proporcionados por los componentes del MHS se describen en la sección 7. Los anexos contienen importante información suplementaria.

No se establecen requisitos de conformidad en relación con esta Recomendación | Norma Internacional.

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 Especificación y en otras de la misma serie se citan las siguientes especificaciones de la OSI:

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación CCITT X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*
- Recomendación UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de presentación.*
- Recomendación UIT-T X.217 (1995) | ISO/CEI 8649:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición de servicio para el elemento de servicio de control de asociación.*
- Recomendación UIT-T X.218 (1993), *Transferencia fiable: Modelo y definición del servicio.*
ISO/CEI 9066-1:1989, *Information processing systems – Text communication – Reliable Transfer – Part 1: Model and service definition.*
- Recomendación UIT-T X.227 (1995) | ISO/CEI 8650-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo con conexión para el elemento de servicio de control de asociación: Especificación de protocolo.*
- Recomendación CCITT X.228 (1988), *Transferencia fiable: Especificación del protocolo.*
ISO/CEI 9066-2:1989, *Information processing systems – Text communication – Reliable Transfer – Part 2: Protocol specification.*
- Recomendación UIT-T X.666 (1997) | ISO/CEI 9834-7:1998, *Tecnología de la información – Interconexión de sistemas abiertos – Procedimientos para la operación de las autoridades de registro en la interconexión de sistemas abiertos: Asignación de nombres internacionales para uso en contextos específicos.*
- 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.690 (1997) | ISO/CEI 8825-1:1998, *Tecnología de la información – Reglas de codificación de la notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida.*
- Recomendación UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Tecnología de la información – Operaciones a distancia: Conceptos, modelos y notación.*

ISO/CEI 10021-2:2004 (S)

- Recomendación UIT-T X.881 (1994) | ISO/CEI 13712-2:1995, *Tecnología de la información – Operaciones a distancia – Realizaciones de interconexión de sistemas abiertos: Definición de servicio del elemento de servicio de operaciones a distancia.*
- Recomendación UIT-T X.882 (1994) | ISO/CEI 13712-3:1995, *Tecnología de la información – Operaciones a distancia – Realizaciones de interconexión de sistemas abiertos: Especificación de protocolo del elemento de servicio de operaciones a distancia.*

2.2 Sistemas de directorio

En esta Especificación y en otras de la misma serie 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.*

2.3 Sistemas de tratamiento de mensajes

En esta Especificación y en otras de la misma serie se citan las siguientes especificaciones de sistemas de tratamiento de mensajes:

- Recomendación CCITT T.330 (1988), *Acceso telemático al sistema de mensajería interpersonal.*
- 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 CCITT X.408 (1988), *Sistemas de tratamiento de mensajes: Reglas de conversión de tipos de información codificada.*
- Recomendación UIT-T X.411 (1999) | ISO/CEI 10021-4:2002, *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes – Definición del servicio abstracto y procedimientos.*
- 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 10021-6:2002, *Tecnología de la información – Sistemas de tratamiento de mensajes: Especificaciones de protocolo.*
- Recomendación UIT-T X.420 (1999) | ISO/CEI 10021-7:2002, *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería interpersonal.*
- Recomendación UIT-T F.435 (1999), *Tratamiento de mensajes: Servicio de mensajería con intercambio electrónico de datos.*

- ISO/CEI 10021-8:1999, *Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service.*
- Recomendación UIT-T X.435 (1999) | ISO/CEI 10021-9:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería con intercambio electrónico de datos.*
 - 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 UIT-T X.404 (1999) | ISO/CEI TR 10021-11:1999, *Tecnología de la información – Sistemas de tratamiento de mensajes: Encaminamiento en sistemas de tratamiento de mensajes – Guía para los gestores de sistemas de mensajería.*
 - Recomendación UIT-T X.460 (1995) | ISO/CEI 11588-1:1996, *Tecnología de la información – Gestión de sistemas de tratamiento de mensajes: Modelo y arquitectura.*
 - Recomendación UIT-T X.462 (1996) | ISO/CEI 11588-3:1997, *Tecnología de la información – Gestión de sistemas de tratamiento de mensajes: Información de registro cronológico.*
 - Recomendación UIT-T X.467 (1996) | ISO/CEI 11588-8:1997, *Tecnología de la información – Gestión de sistemas de tratamiento de mensajes: Gestión de agente de transferencia de mensajes.*

2.4 Indicativos de país

En esta Especificación se indican las siguientes especificaciones de indicativos de país:

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

2.5 Direcciones de la red

En esta Especificación se indica la siguiente especificación de dirección de la red:

- Recomendación CCITT E.164 (1991), *Plan de numeración para la era de la red digital de servicios integrados.*

2.6 Código de lenguaje

En esta Especificación se indica la siguiente especificación de código de lenguaje:

- ISO 639:1988, *Code for the representation of names of languages.*

2.7 Juegos de caracteres

En esta Especificación se indica la siguiente especificación de juego de caracteres:

- ISO 10646-1:1993, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane.*

3 Definiciones

Las definiciones que se indican a continuación se aplican a efectos de la presente Especificación y de otras de la misma serie.

3.1 Interconexión de sistemas abiertos

En esta Especificación y en otras de la misma serie se emplean los nombres de las siete capas del modelo de referencia así como los siguientes términos definidos en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

- a) sintaxis abstracta;
- b) entidad de aplicación (AE, *application entity*);
- c) proceso de aplicación;
- d) unidad de datos de protocolo de aplicación (APDU, *application protocol data unit*);
- e) elemento de servicio de aplicación (ASE, *application service element*);
- f) tarea de tratamiento de la información distribuida;

ISO/CEI 10021-2:2004 (S)

- g) capa;
- h) sistema abierto;
- i) interconexión de sistemas abiertos (OSI, *open systems interconnection*);
- j) par;
- k) contexto de presentación;
- l) protocolo;
- m) modelo de referencia;
- n) sintaxis de transferencia;
- o) elemento de usuario (UE, *user element*).

En esta Especificación y en otras de la misma serie se emplean los siguientes términos definidos 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, así como los nombres de los tipos y valores de datos ASN.1:

- a) notación de sintaxis abstracta uno (ASN.1, *abstract syntax notation one*);
- b) reglas básicas de codificación;
- c) explícito;
- d) exportación;
- e) implícito;
- f) importación;
- g) clase de objeto de información;
- h) módulo;
- i) rótulo;
- j) tipo;
- k) valor.

En esta Especificación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. UIT-T X.217 | ISO/CEI 8649:

- a) asociación de aplicación; asociación;
- b) contexto de aplicación (AC, *application context*);
- c) elemento de servicio de control de asociación (ACSE, *association control service element*);
- d) iniciador;
- e) respondedor.

En esta Especificación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. UIT-T X.218 | ISO/CEI 9066-1:

- a) transferencia fiable (RT, *reliable transfer*);
- b) elemento de servicio de transferencia fiable (RTSE, *reliable transfer service element*).

En esta Especificación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. UIT-T X.880 | ISO/CEI 13712-1:

- a) argumento;
- b) asíncrono;
- c) vinculado;
- d) parámetro;
- e) error distante;
- f) operación distante;
- g) operaciones a distancia (RO, *remote operations*);
- h) elemento de servicio de operaciones a distancia (ROSE, *remote operations service element*);
- i) resultado;
- j) síncrono;
- k) no vinculado.

3.2 Sistemas de directorio

En esta Especificación y en otras de la misma serie se emplean los siguientes términos definidos en las Recomendaciones de la serie X.500 | ISO/CEI 9594:

- a) atributo;
- b) certificado;
- c) autoridad certificadora;
- d) trayecto de la certificación;
- e) inscripción en el directorio; inscripción;
- f) agente de sistema de directorio (DSA, *directory system agent*);
- g) directorio;
- h) función troceado ("hash");
- i) nombre;
- j) clase de objeto;
- k) objeto;
- l) autenticación simple;
- m) autenticación fuerte.

3.3 Sistemas de tratamiento de mensajes

A efectos de la presente Especificación, son de aplicación los términos cuya relación figura en el anexo K.

4 Abreviaturas

A efectos de la presente Especificación, son de aplicación las siglas cuya relación figura en el anexo K.

5 Convenios

En esta Especificación se utilizan los convenios descriptivos indicados a continuación.

5.1 ASN.1

Esta Especificación emplea, en sus anexos A y C, diversos convenios de descripción basados en la ASN.1 para definir información propia del tratamiento de mensajes, que pueda contener el directorio. La ASN.1 se define 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. En particular, esta Especificación utiliza las clases de objeto de información OBJECT-CLASS y ATTRIBUTE de la Rec. UIT-T X.501 | ISO/CEI 9594-2 para definir las clases de objetos y los atributos propios del tratamiento de mensajes.

La ASN.1 aparece en el anexo A como ayuda a la explicación y en el anexo C, innecesariamente en buena medida, como referencia. Cuando hay diferencias entre ambos, se indica una especificación de error.

Los rótulos de identificación de ASN.1 están implícitos en todo el módulo ASN.1 que se define en el anexo C; el módulo es definitivo a este respecto.

Aunque la sintaxis abstracta de esta definición de servicio contiene marcadores de ampliación, no se ha verificado si éstos están presentes en todos los casos en que ello sería necesario antes de que puedan utilizarse con seguridad reglas de codificación compactada.

5.2 Grado

Cuando en esta Especificación se describe una clase de estructura de datos (por ejemplo, direcciones OR) que tiene componentes (por ejemplo, atributos), a cada componente se le asigna uno de los siguientes grados:

- a) obligatorio (M, *mandatory*): Un componente obligatorio estará presente en cada caso de la clase.
- b) optativo (O): Un componente optativo estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que suministra ese caso. No hay valor por defecto.

- c) defectible por defecto (D): Un componente defectible estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que ofrece ese caso. En su ausencia se aplica un valor por defecto especificado por esta Especificación.
- d) condicional (C): Un componente condicional estará presente en un caso de la clase, en las circunstancias prescritas por esta Especificación.

5.3 Términos

En el resto de la presente Especificación, los términos se escriben en **negritas** al definirlos, en *bastardilla* cuando se hace referencia a los mismos antes de su definición y sin realce especial en otras ocasiones.

Los términos que son nombres propios se presentan en letras mayúsculas; no así los términos genéricos.

SECCIÓN 2 – MODELOS ABSTRACTOS

6 Visión de conjunto

En esta sección se presentan modelos abstractos de *tratamiento de mensajes*, que proporcionan la arquitectura básica para la elaboración de las especificaciones, más detalladas, que figuran en otras Especificaciones del MHS.

El tratamiento de mensajes es una tarea distribuida del tratamiento de la información, que comprende las siguientes subtareas intrínsecamente relacionadas:

- a) transferencia de mensajes: transmisión diferida de objetos de información entre usuarios, empleando computadores como intermediarios;
- b) almacenamiento de mensajes: almacenamiento automático, para su posterior recuperación, de objetos de información, transportados mediante la transferencia de mensajes.

Esta sección abarca los siguientes temas:

- a) modelo funcional;
- b) modelo de información;
- c) modelo operacional;
- d) modelo de seguridad.

NOTA – El tratamiento de mensajes tiene una pluralidad de aplicaciones, una de las cuales es la mensajería interpersonal que se describe en la Rec. UIT-T X.420 | ISO/CEI 10021-7.

7 Modelo funcional

En esta cláusula se da un modelo funcional de tratamiento de mensajes. De la realización concreta del modelo se ocupan otras Especificaciones del MHS.

El entorno de tratamiento de mensajes (MHE, *message handling environment*) comprende objetos funcionales "primarios" de varios tipos: el *sistema de tratamiento de mensajes* (MHS, *message handling system*), los *usuarios* y las *listas de distribución*. A su vez, el MHS, puede descomponerse en objetos funcionales "secundarios", de menor nivel y de varios tipos: el *sistema de transferencia de mensajes* (MTS, *message transfer system*); los *agentes de usuario*, las *memorias de mensajes* y las *unidades de acceso*. El MTS, en fin, puede descomponerse en objetos funcionales "terciarios", aún de menor nivel y de un solo tipo, los *agentes de transferencia de mensajes*.

Los tipos de objetos funcionales primarios, secundarios y terciarios y los tipos de *unidades de acceso* seleccionadas se definen y describen por separado en los puntos que siguen.

Tal como se precisa a continuación, los objetos funcionales se adaptan a veces a una o más aplicaciones del tratamiento de mensajes, por ejemplo la mensajería interpersonal (véanse la Rec. UIT-T X.420 | ISO/CEI 10021-7 y la Rec. CCITT T.330). Un objeto funcional, que ha sido adaptado a una aplicación, comprende la sintaxis y la semántica del contenido de los mensajes intercambiados en esa aplicación.

Como asunto local, los objetos funcionales pueden tener capacidades superiores a las especificadas en esta Especificación o en otras Especificaciones del MHS. En concreto, un *agente de usuario* típico tiene capacidades de preparación, reproducción y almacenamiento de mensajes que no están normalizadas.

7.1 Objetos funcionales primarios

El MHE comprende el *sistema de tratamiento de mensajes*, los *usuarios* y las *listas de distribución*. Entre estos objetos funcionales primarios se produce una interacción. A continuación se definen y describen los tipos de objetos.

En la figura 1 se representa de manera esquemática esa interacción.

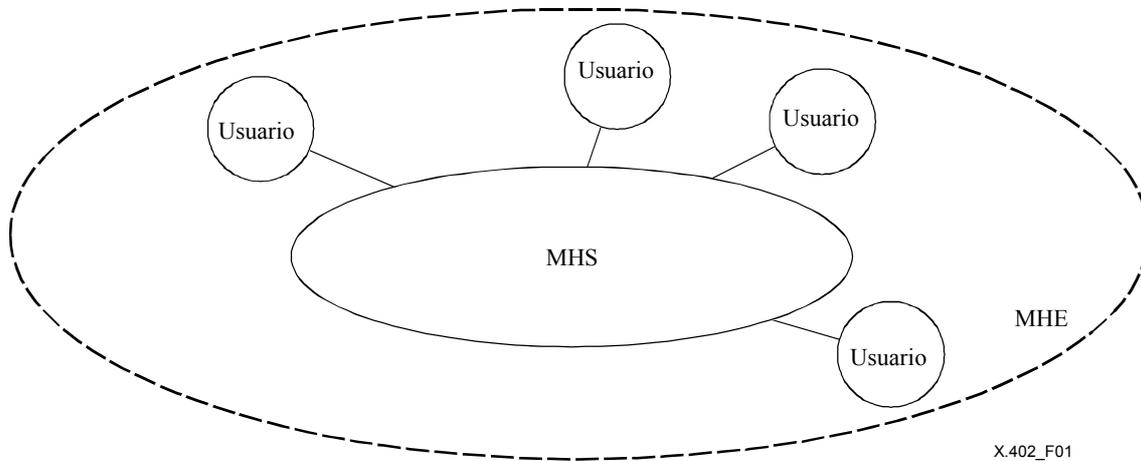


Figura 1 – Entorno del tratamiento de mensajes

7.1.1 Sistema de tratamiento de mensajes

La finalidad principal del tratamiento de mensajes es transportar objetos de información de un usuario a otro. Al objeto funcional que lleva a cabo esta tarea se le denomina sistema de tratamiento de mensajes (MHS, *message handling system*).

El MHE consta de un solo MHS.

7.1.2 Usuarios

La finalidad principal del MHS es transportar objetos de información entre *usuarios*. Al objeto funcional (por ejemplo, una persona) que más que proporcionar tratamiento de mensajes, participa en ese tratamiento, se le denomina usuario.

Cabe distinguir las siguientes clases de usuarios:

- a) usuario directo: usuario que participa en el tratamiento de mensajes utilizando directamente el MHS;
- b) usuario indirecto: usuario que participa en el tratamiento de mensajes utilizando indirectamente el MHS, es decir, a través de otro sistema de comunicaciones (por ejemplo, un sistema postal o una red télex) al que está enlazado el MHS.

El MHE consta de un número cualquiera de usuarios.

7.1.3 Lista de distribución

Mediante el MHS, un usuario puede hacer llegar objetos de información a grupos de usuarios previamente especificados, así como a usuarios individuales. Se llama lista de distribución (DL, *distribution list*) al objeto funcional que representa a un grupo de usuarios previamente especificado y a otras DL.

Una DL representa cero o más usuarios y DL, a los que se les denomina sus miembros. De estas últimas DL (si es que hay alguna) se dice que están jerarquizadas. Pedir al MHS que transporte un objeto de información (por ejemplo, un *mensaje*) a una DL equivale a pedirle que lo transporte a sus miembros. Téngase en cuenta que se trata de un proceso recurrente.

El derecho a transportar *mensajes* a una DL determinada, o el permiso para hacerlo, puede estar bajo control. A ese derecho, se le denomina permiso de depósito. Como asunto local, es posible restringir más aún el uso de una DL.

El MHE consta de un número cualquiera de DL.

NOTA – Una DL podría estar más restringida, limitándola por ejemplo al transporte de *mensajes* con un determinado *tipo de contenido*.

7.2 Objetos funcionales secundarios

El MHS comprende el *sistema de transferencia de mensajes*, los *agentes de usuarios*, las *memorias de mensajes* y las *unidades de acceso*. Entre estos objetos funcionales secundarios se produce una interacción. Más adelante se definen y describen los tipos de objetos.

En la figura 2 se representa de forma esquemática esa interacción.

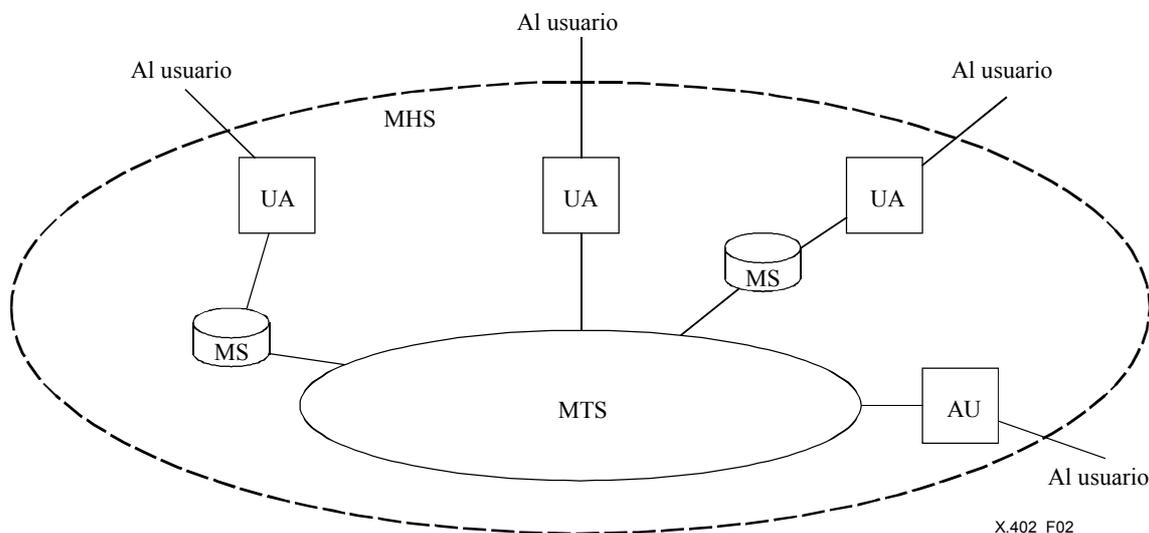


Figura 2 – Sistema de tratamiento de mensajes

7.2.1 Sistema de transferencia de mensajes

En el MHS se produce un transporte de objetos de información a usuarios individuales y a los miembros de las DL. El objeto funcional que realmente los transporta se llama sistema de transferencia de mensajes (MTS, *message transfer system*). El MTS es un sistema de comunicación de almacenamiento y retransmisión, del que se puede decir que es la columna vertebral del MHS.

El MTS es de uso general y soporta toda clase de aplicaciones del tratamiento de mensajes. Además, el MTS puede adaptarse a una o más aplicaciones particulares, es decir, puede efectuar una *conversión*.

El MHS consta de un solo MTS.

7.2.2 Agentes de usuario

El objeto funcional por medio del cual un usuario directo aislado participa en el tratamiento de mensajes se denomina agente de usuario (UA, *user agent*).

Un UA típico está adaptado a una o más aplicaciones particulares del tratamiento de mensajes.

El MHS consta de un número cualquiera de UA.

NOTA – En el caso de un UA que preste servicio a un usuario humano, lo típico es que la interacción entre agente y usuario se establezca a través de un dispositivo de entrada/salida (por ejemplo, un teclado, una pantalla, un dispositivo explorador, una impresora o una combinación de algunos de estos dispositivos).

7.2.3 Memorias de mensajes

El usuario típico debe almacenar la información que recibe. El objeto funcional que proporciona a un usuario directo (aislado) la capacidad de almacenar mensajes se llama memoria de mensajes (MS, *message store*). Cada MS está asociada a un UA, pero no todos los UA tienen MS asociada.

Las MS son de uso general y facilitan todas las aplicaciones de tratamiento de mensajes. Además, una MS puede adaptarse a una o más aplicaciones particulares, de tal modo que pueda, con mayor facilidad, *presentar* mensajes y soportar la *recuperación de mensajes* asociados a esa aplicación.

El MHS consta de un número cualquiera de MS.

NOTA – Como asunto local, un UA puede proporcionar capacidad de almacenamiento de objetos de información que complemente o sustituya la de una MS.

7.2.4 Unidades de acceso

El objeto funcional que enlaza al MTS con otro sistema de comunicaciones (por ejemplo, un sistema postal o la red télex) y, a través del cual, sus autoridades participan en el tratamiento de mensajes como usuarios indirectos, se denomina unidad de acceso (AU, *access unit*).

Una AU típica está adaptada a un sistema de comunicaciones particular y a una o más aplicaciones particulares del tratamiento de mensajes.

El MHS consta de un número cualquiera de AU.

7.3 Objetos funcionales terciarios

El MTS está formado por *agentes de transferencia de mensajes*. Entre estos objetos funcionales terciarios se produce una interacción. Más adelante se definen y describen los tipos de objetos terciarios.

En la figura 3 se representa de manera esquemática esa interacción.

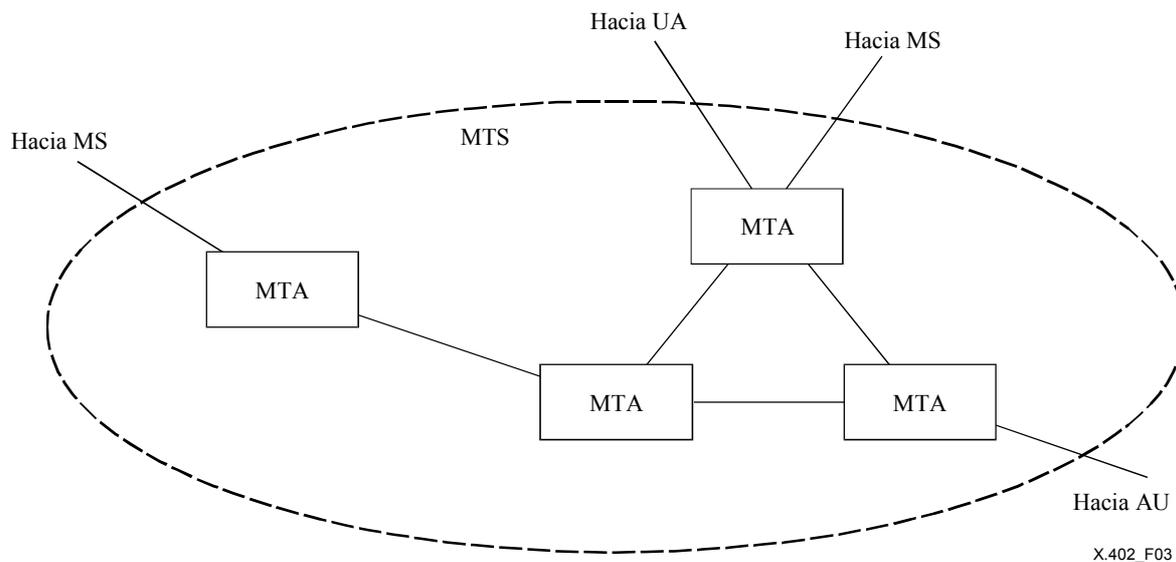


Figura 3 – Sistema de transferencia de mensajes

7.3.1 Agentes de transferencia de mensajes

El MTS transporta objetos de información a usuarios y DL según el modo de almacenamiento y retransmisión. Al objeto funcional que proporciona el eslabón de la cadena de almacenamiento y retransmisión del MTS se le denomina agente de transferencia de mensajes (MTA, *message transfer agent*).

Los MTA son de uso general y soportan las aplicaciones del tratamiento de mensajes. Además, un MTA se puede adaptar a una o más aplicaciones particulares, es decir, puede efectuar una *conversión*.

El MTS consta de un número cualquiera de MTA.

7.4 Tipos de AU seleccionados

Como se ha descrito anteriormente, entre el MHS y otros tipos de sistemas de comunicaciones se produce un interfuncionamiento a través de las AU. En las subcláusulas que siguen se presentan varios tipos de AU seleccionados: de *entrega física*, de acceso telemático y por télex.

7.4.1 Entrega física

Una unidad de acceso de entrega física (PDAU, *physical delivery access unit*) es una AU que somete los *mensajes* (pero no las *sondas* ni los *informes*) a *reproducción física*, y transporta los *mensajes físicos* resultantes a un *sistema de entrega física*.

A la transformación de un *mensaje* en un *mensaje físico* se le denomina *reproducción física*. Un *mensaje físico* es un objeto físico (por ejemplo, una carta y su sobre de papel) que contiene un *mensaje*.

ISO/CEI 10021-2:2004 (S)

Un sistema de entrega física (PDS, *physical delivery system*) es un sistema que efectúa la *entrega física*. El sistema postal es un tipo importante de PDS. Se llama entrega física a la transferencia de un mensaje físico a una autoridad de un PDS, uno de los usuarios indirectos a los que la PDAU proporciona capacidades de tratamiento de mensajes.

La mensajería interpersonal es una de las aplicaciones del tratamiento de mensajes proporcionadas por todas las PDAU (véase la Rec. UIT-T X.420 | ISO/CEI 10021-7).

7.4.2 Telemática

En la Rec. UIT-T X.420 | ISO/CEI 10021-7 se presentan las unidades de acceso telemático, que proporcionan, en exclusiva, la mensajería interpersonal.

7.4.3 Télex

En la Rec. UIT-T X.420 | ISO/CEI 10021-7 se presentan las unidades de acceso télex, que proporcionan, en exclusiva, la mensajería interpersonal.

8 Modelo de información

En esta cláusula se presenta un modelo de información del tratamiento de mensajes. La realización concreta del modelo es objeto de otras Especificaciones del MHS.

El MHS y el MTS pueden transportar objetos de información de tres clases: *mensajes*, *sondas* e *informes*. En la primera columna del cuadro 4 figuran esas tres clases. Para cada una de ellas se indican, en la segunda columna, los tipos de objetos funcionales – usuario, UA, MS, MTA y AU – que son origen y destino final de tales objetos.

Cuadro 4 – Objetos de información transportables

Objeto de información	Objeto funcional				
	usuario	UA	MS	MTA	AU
Mensaje	SD	-	-	-	-
Sonda	S	-	-	D	-
Informe	D	-	-	S	-

+ - Leyenda ----- +
| S Último origen |
| D Último destino |
+-----+

En las subcláusulas que siguen se definen y describen los objetos de información cuyo resumen figura en el cuadro.

8.1 Mensajes

La finalidad principal de la transferencia de mensajes es el transporte de objetos de información llamados mensajes de un usuario a otros. Un mensaje, como se muestra en la figura 4, consta de las siguientes partes:

- sobre: objeto de información cuya composición varía de un *paso de transmisión* a otro, y que identifica de manera diversa al *originador* del mensaje y a los *destinatarios potenciales*, informa sobre el transporte previo y dirige el siguiente por el MTS, y caracteriza el *contenido* del mensaje;
- contenido: objeto de información que el MTS ni examina ni modifica, si no es a efectos de *conversión*, mientras transporta el mensaje.

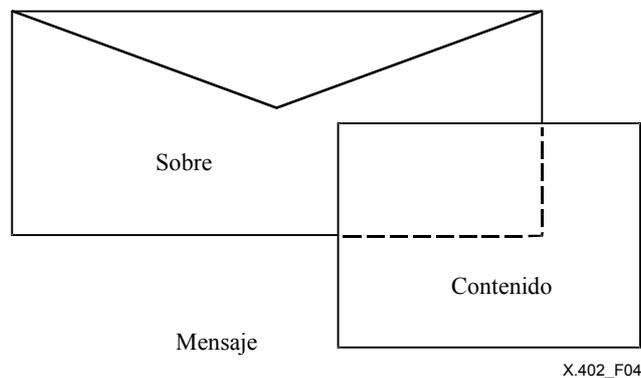


Figura 4 – Sobre y contenido de un mensaje

Una parte de información, que figura en el sobre, identifica el tipo de contenido. El tipo de contenido es un identificador (un identificador de objeto o entero ASN.1) que indica la sintaxis y la semántica del contenido en su conjunto. Ese identificador permite al MTS determinar si el mensaje ha de *entregarse* o no a usuarios particulares, y permite a los UA y MS interpretar y tratar el contenido.

Otra parte de información, que figura asimismo en el sobre, identifica los tipos de información codificada representada en el contenido. Un tipo de información codificada (EIT, *encoded information type*) es un identificador que indica el soporte y el formato (por ejemplo, texto IA5 o facsímil del grupo 3) de partes individuales del contenido. Permite además al MTS determinar si el mensaje se ha de entregar o no a usuarios particulares, e identificar las oportunidades de *hacer* el mensaje entregable, convirtiendo una porción del contenido de un EIT a otro.

8.2 Sondas

Un segundo objetivo de la transferencia de mensajes es transportar objetos de información llamados sondas desde un usuario a otros (es decir, llevarlos hasta los MTA que prestan servicio a esos usuarios). Una sonda describe una clase de mensajes y se utiliza para determinar la *entregabilidad* de dichos mensajes.

A un mensaje descrito por una sonda se le llama mensaje descrito.

La sonda consta de un solo sobre. El sobre contiene, en gran parte, la misma información que para un mensaje. Además del tipo de contenido y los tipos de información codificada del mensaje descrito, en el sobre figura la longitud de su contenido.

El *depósito* de una sonda da lugar a un comportamiento del MTS que es, en buena medida, el mismo que suscitaría el *depósito* de cualquier mensaje descrito, salvo que en el caso de la sonda, se prescinde de la *ampliación y de la entrega de la DL*. En concreto, y aparte de las consecuencias de la supresión de la *ampliación de la DL*, la sonda da lugar a los mismos *informes* a que daría lugar cualquier mensaje descrito. En esto reside la utilidad de las sondas.

8.3 Informes

Un tercer objetivo de la transferencia de mensajes es transportar a los usuarios unos objetos de información, llamados informes. Un informe, generado por el MTS, comunica el resultado o la marcha de la *transmisión* de un mensaje o de una sonda a uno o más *destinatarios potenciales*.

Al mensaje o a la sonda que sean objeto de un informe se les llama mensaje objeto o sonda objeto, respectivamente.

Un informe referido a un determinado *destinatario potencial* se lleva hasta el *originador* del mensaje o de la sonda objeto, a menos que el *destinatario potencial* sea un *destinatario miembro*. En este último caso, el informe es transportado a la DL a la que pertenezca el *destinatario miembro*. Como asunto local, (es decir, cuando exista una política establecida para esa DL particular), el transporte del informe puede proseguir hasta el propietario de la DL, bien a la DL que la contenga (en caso de jerarquización) o al originador del mensaje objeto (en el caso contrario), o a ambos.

Los resultados a los que puede referirse un informe único son de las siguientes clases:

- a) informe de entrega: *entrega, exportación o afirmación* del mensaje objeto o de la sonda objeto, o bien *ampliación de la DL*;
- b) informe de no entrega: *no entrega o no afirmación* del mensaje objeto o de la sonda objeto.

Un informe puede comprender uno o más informes de entrega y/o no entrega. Un mensaje o una sonda puede dar lugar a varios informes de entrega y/o no entrega relativos a un determinado *destinatario potencial*. Cada uno de ellos marca el tránsito de un *paso* o *evento* de transmisión diferente.

9 Modelo operacional

En esta cláusula se presenta un modelo operacional de tratamiento de mensajes. La realización concreta del modelo es objeto de otras Especificaciones del MHS.

El MHS puede transportar un objeto de información a usuarios individuales, DL o una combinación de ambos. El transporte se lleva a cabo por un proceso llamado *transmisión*, que comprende *pasos* y *eventos*. A continuación se definen y describen el proceso y sus subdivisiones, así como el papel que los usuarios y las DL desempeñan en éste.

9.1 Transmisión

Se llama *transmisión* al transporte o tentativa de transporte de un mensaje o de una sonda. La transmisión abarca el transporte del mensaje desde su *originador* a sus *destinatarios potenciales*, y el transporte de la sonda desde su *originador* hasta los MTA facultados para *afirmar* la *entregabilidad* o no del mensaje descrito a los *destinatarios potenciales* de aquélla. La transmisión comprende también el transporte o tentativa de transporte al *originador* de cuantos informes provoquen el mensaje o la sonda.

La transmisión se desarrolla a través de una secuencia de *pasos de transmisión* y *eventos*. Un paso de transmisión (o paso) consiste en el transporte de un mensaje, una sonda o un informe desde un objeto funcional a otro "adyacente" al primero. Un evento de transmisión (o evento) consiste en el tratamiento de un mensaje, una sonda o un informe en un objeto funcional, tratamiento que puede influir en la selección, por parte del objeto funcional, del siguiente paso o evento.

En la figura 5 se presenta de manera esquemática el flujo de información de la transmisión. Se muestran en ella los tipos de objetos funcionales –usuarios directos, usuarios indirectos, UA, MS, MTA y AU– que pueden tomar parte en una transmisión, los objetos de información –mensajes, sondas, e informes– que pueden ser transportados entre aquéllos y los nombres de los pasos de transmisión mediante los cuales se efectúan esos transportes.

La figura 5 destaca el hecho de que un mensaje o informe pueden ser extraídos repetidamente y que sólo el primer transporte de un objeto extraído desde el UA al usuario constituye *recepción*.

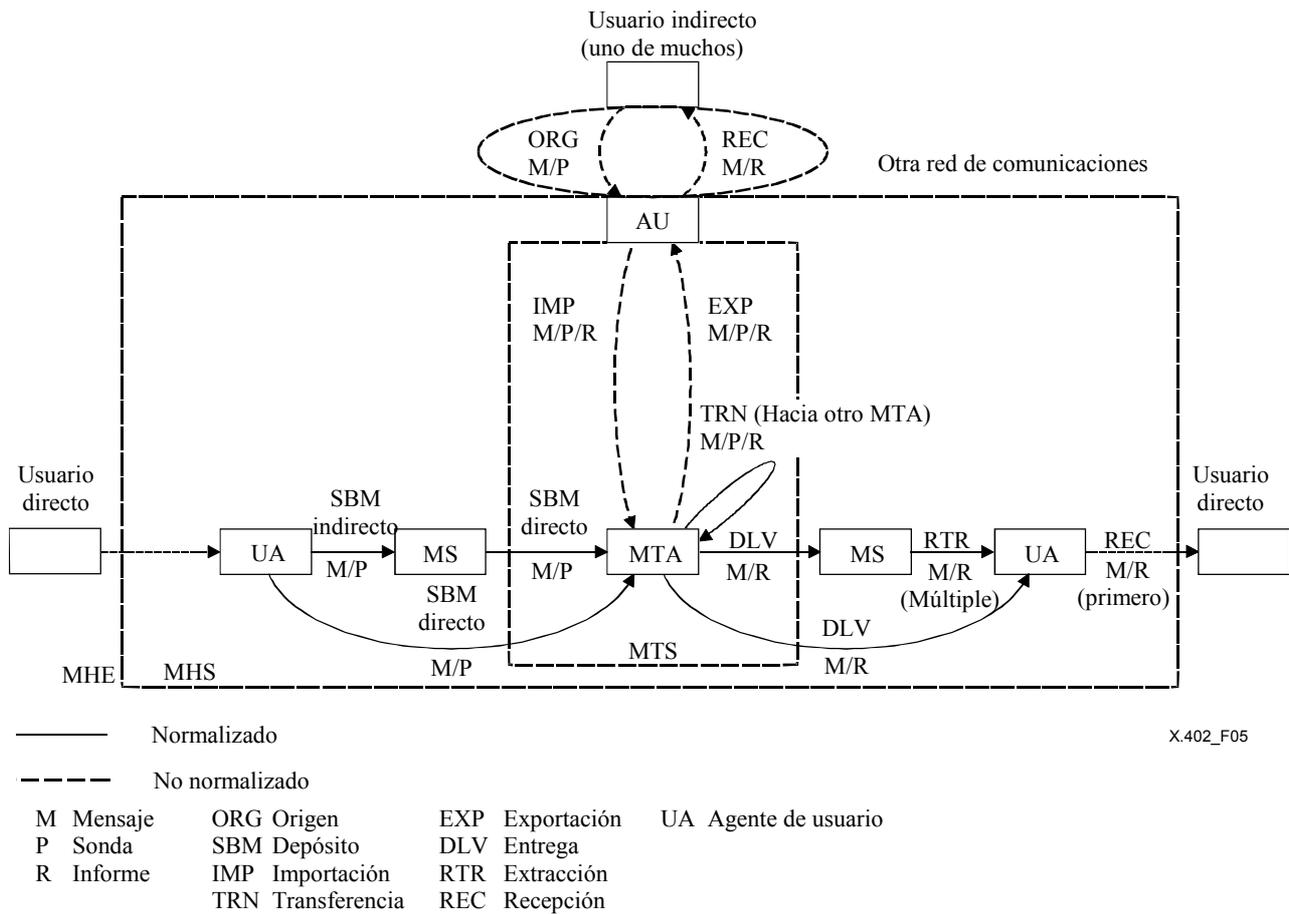


Figura 5 – Flujo de información de la transmisión

El evento tiene un papel destacado en la transmisión. La *división* duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus *destinatarios inmediatos*. Se llaman destinatarios inmediatos a los destinatarios potenciales asociados a un caso particular de un mensaje o sonda. Un MTA efectúa una división si el siguiente paso o evento, necesario para transportar un mensaje o sonda a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros. En cada una de las descripciones de pasos y eventos que a continuación se hacen, se supone que el paso o evento es adecuado para todos los destinatarios inmediatos, situación que puede crearse, si es preciso, por división.

9.2 Funciones de la transmisión

Los usuarios y las DL desempeñan una diversidad de papeles en la transmisión de un mensaje o una sonda. A esos papeles se les clasifica, de manera informal, en papeles "fuente", papeles "destino" y categorías a las que se pueden elevar los usuarios o las DL.

Un usuario puede desempeñar el siguiente papel "fuente" en la transmisión de un mensaje o sonda:

- originador: usuario (no DL) que es origen último de un mensaje o sonda.

Un usuario o una DL pueden desempeñar alguno de los siguientes papeles "destino" en la transmisión de un mensaje o sonda:

- destinatario deseado: uno de los usuarios o de las DL que el originador especifica como destinos de un mensaje o una sonda;
- destinatario alternativo especificado por el originador: usuario (o DL si hay alguna) al que el originador pide que sea transportado un mensaje o sonda, si no puede transportarse a un determinado destinatario deseado;

- c) destinatario miembro: DL o usuario al cual se transporta un mensaje (pero no una sonda), como resultado de una *ampliación de DL*;
- d) destinatario alternativo designado por el destinatario: usuario (o DL si hay alguna) el cual haya sido elegido por un destinatario deseado, destinatario alternativo especificado por el originador, o destinatario miembro para *redireccionar* los mensajes.

Un usuario o una DL pueden adquirir alguna de las siguientes categorías durante la transmisión de un mensaje o una sonda:

- a) destinatario potencial: cualquier DL o usuario hacia el cual se transporta un mensaje o sonda en cualquier momento durante la transmisión. Ha de tratarse necesariamente de un destinatario deseado, alternativo especificado por el originador, miembro o destinatario alternativo designado por el destinatario;
- b) destinatario efectivo (o receptor): un destinatario potencial para el cual tiene lugar la *entrega* o la *afirmación*.

9.3 Pasos de la transmisión

En la primera columna del cuadro 5 figura una lista de los tipos de pasos que pueden producirse en una transmisión. Para cada tipo de la lista se indica, en la segunda columna, si ese paso está normalizado o no; en la tercera columna, las clases de objetos de información –mensajes, sondas e informes– cuyo transporte está permitido en ese paso y en la cuarta columna, las clases de objetos funcionales –usuarios, UA, MS, MTA y AU– que pueden participar en ese paso como origen o destino del objeto.

El cuadro 5 está dividido en tres secciones. Los pasos de la primera sección corresponden a la "creación" de mensajes y sondas, los de la última a la "distribución" de mensajes e informes y los de la de en medio a la "retransmisión" de mensajes, sondas e informes.

Cuadro 5 – Pasos de transmisión

Paso de transmisión	¿Norma- lizado?	Objetos de información			Objetos funcionales				
		M	P	R	usuar.	UA	MS	MTA	AU
Origen	No	x	x	-	S	D	-	-	-
Depósito	Sí	x	x	-	-	S	SD	D	-
Importación	No	x	x	x	-	-	-	D	S
Transferencia	Sí	x	x	x	-	-	-	SD	-
Exportación	No	x	x	x	-	-	-	S	D
Entrega	Sí	x	-	x	-	D	D	S	-
Recuperación	Sí	x	-	x	-	D	S	-	-
Recepción	No	x	-	x	D	S	-	-	-

+- Leyenda		
M mensaje	S origen	x permitido
P sonda	D destino	
R informe		

En las subcláusulas que siguen se definen y describen cada uno de los tipos de pasos de transmisión cuya relación figura en el cuadro 5.

9.3.1 Origen

En un paso de origen, un usuario directo transporta un mensaje o una sonda a su UA, o bien un usuario indirecto hace otro tanto al sistema de comunicaciones que le presta servicio. Este paso genera el mensaje o la sonda y constituye el primero de su transmisión.

El referido usuario es el originador del mensaje o de la sonda. Como tal originador identifica los destinatarios deseados de uno u otro objetos funcionales. Además, para cada destinatario deseado, puede identificar un destinatario alternativo, aunque no es preciso que lo haga.

9.3.2 Depósito

En un paso de depósito se transporta a un MTA, un mensaje o sonda que quedan a cargo del MTS. Cabe distinguir los dos tipos siguientes de depósito:

- a) depósito indirecto: paso de transmisión en el que el UA del originador transporta un mensaje o sonda a su MS y en el que la MS efectúa un *depósito directo*. Este paso sigue al de origen.

Es un paso que sólo puede darse si el usuario dispone de una MS.

- b) depósito directo: paso de transmisión en el que el UA o la MS del originador transportan un mensaje o sonda a un MTA. Este paso sigue al de origen o se produce como parte de un depósito indirecto.

Es posible dar este paso tanto si el usuario está equipado con una MS como si no lo está.

El depósito indirecto y el directo son funcionalmente equivalentes, salvo en lo que se refiere a las capacidades adicionales de las que es posible disponer con el primero. El depósito indirecto puede diferir del directo en otros aspectos (por ejemplo, en el número de sistemas abiertos con los que debe establecer una interacción aquel que incorpore un UA) y ser por ello preferible al depósito directo.

Al UA o a la MS que participa en el depósito directo se le llama agente de depósito. Un agente de depósito se da a conocer al MTS mediante un proceso de registro, como resultado del cual el agente de depósito y el MTS quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.3 Importación

En un paso de importación, una AU transporta un mensaje, una sonda o un informe a un MTA. Este paso introduce en el MTS un objeto de información llevado en otro sistema de comunicaciones, y se produce a continuación de su transporte por dicho sistema.

NOTA – El concepto de importación es un concepto genérico. La manera cómo se efectúe este paso varía, naturalmente, de una AU a otra.

9.3.4 Transferencia

En un paso de transferencia, un MTA transporta un mensaje, una sonda o un informe a otro MTA. En este paso, el transporte del objeto de información tiene lugar a lo largo de distancias físicas y, a veces, organizativas. Se produce a continuación del depósito directo o de la importación o de una transferencia previa.

Por supuesto, este paso sólo puede darse si el MTS consta de varios MTA.

Cabe distinguir, según sea el número de *MD* afectados, los siguientes tipos de transferencia:

- a) transferencia interna: transferencia que implica a varios MTA en un solo *MD*;
- b) transferencia externa: transferencia que implica a varios MTA en diferentes *MD*.

9.3.5 Exportación

En un paso de exportación, un MTA transporta un mensaje, una sonda o un informe a una AU. En este paso, se lanza un objeto de información desde el MTS hacia otro sistema de comunicaciones. El paso se produce a continuación del depósito directo, de la importación o de la transferencia.

El MTA puede generar, como parte de este paso, un informe de entrega. Dependiendo de los requisitos para el tipo de unidad de acceso definidos en las especificaciones de tratamiento de mensajes pertinentes, un informe de entrega positivo indica la buena aceptación de un mensaje (o sonda) por parte de la unidad de acceso, o bien que la unidad de acceso ha realizado satisfactoriamente un transporte ulterior de dicho mensaje o sonda.

NOTA – El concepto de exportación es un concepto genérico. La manera cómo se efectúe este paso varía, naturalmente, de una AU a otra.

9.3.6 Entrega

En un paso de entrega, un MTA transporta un mensaje o un informe a una MS o a un UA. La MS y el UA corresponden a un destinatario potencial del mensaje o al originador del mensaje o sonda objeto del informe. En este paso se confía el objeto de información a un representante del usuario y se produce tras el depósito directo, la importación o la transferencia. Además, se eleva al usuario en cuestión a la categoría de destinatario efectivo.

En el caso de un mensaje el MTA puede generar, como parte de este paso, un informe de entrega.

Se llama agente de entrega a la MS o al UA que participan en la misma. Un agente de entrega se da a conocer al MTS mediante un proceso de registro, como resultado del cual el agente de entrega y el MTS quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.7 Recuperación

En un paso de recuperación, la MS de un usuario transporta un mensaje o un informe a su UA. El usuario en cuestión es un destinatario efectivo del mensaje o el originador del mensaje o de la sonda objeto. Este paso extrae del almacenamiento el objeto de información de manera no destructiva. Se produce tras el paso de entrega o de una recuperación previa.

El paso de recuperación sólo puede darse si el usuario está equipado con una MS.

9.3.8 Recepción

En un paso de recepción, un UA transporta un mensaje o informe a su usuario directo, o bien el sistema de comunicaciones que presta servicio a un usuario indirecto transporta ese objeto de información a dicho usuario. En cualquier caso, este paso transporta el objeto a su destino último.

Si se trata de un usuario directo, este paso sucede a la entrega del objeto o a la primera recuperación (solamente). Si se trata de un usuario indirecto, sucede al transporte de un objeto de información por el sistema de comunicaciones que sirve al usuario. En cualquiera de los dos casos, el usuario es un destinatario potencial (pero si es usuario directo, es también destinatario efectivo) del mensaje en cuestión, o el originador del mensaje objeto o la sonda objeto.

9.4 Eventos de la transmisión

En la primera columna del cuadro 6 se da una relación de los tipos de eventos que pueden producirse en una transmisión. Para cada tipo de evento se indica, en la segunda columna, los tipos de objetos de información –mensajes, sondas e informes– para los que pueden desarrollarse tales eventos, y en la tercera columna, los tipos de objetos funcionales –usuarios, UA, MS, MTA y AU– a los que les está permitido desarrollarlos.

Todos los eventos se producen dentro del MTS.

Cuadro 6 – Eventos de transmisión

Evento de transmisión	Objetos de información			Objetos funcionales				
	M	P	R	usuario	UA	MS	MTA	AU
división	x	x	-	-	-	-	x	-
combinación	x	x	x	-	-	-	x	-
resolución de nombre	x	x	-	-	-	-	x	-
ampliación de DL	x	-	-	-	-	-	x	-
redireccionamiento	x	x	-	-	-	-	x	-
conversión	x	x	-	-	-	-	x	-
no entrega	x	-	x	-	-	-	x	-
no afirmación	-	x	-	-	-	-	x	-
afirmación	-	x	-	-	-	-	x	-
encaminamiento	x	x	x	-	-	-	x	-

+ - Leyenda ----- +
 | M mensaje x permitido |
 | P sonda |
 | R informe |
 +-----+

Los tipos de eventos de transmisión, resumidos en el cuadro 6 son definidos y descritos separadamente en las subcláusulas que siguen.

9.4.1 División

En un evento de división, un MTA duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus destinatarios inmediatos. Este evento permite de manera efectiva a un MTA transportar independientemente un objeto a varios destinatarios potenciales.

Un MTA efectúa una división cuando el siguiente paso o evento, necesario para el transporte de una sonda o mensaje a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros.

9.4.2 Combinación

En un evento de combinación, un MTA combina varios casos del mismo mensaje o sonda, o dos o más informes, de entrega y/o no entrega para el mismo mensaje o sonda objeto.

Un MTA puede, aunque no necesariamente, efectuar una combinación cuando determine que, para transportar a sus destinos varios objetos de información muy relacionados, hacen falta los mismos eventos y el mismo paso siguiente.

9.4.3 Resolución de nombre

En un evento de resolución de nombre, un MTA agrega la *dirección OR* correspondiente al *nombre OR* que identifica a uno de los destinatarios inmediatos de un mensaje o una sonda.

9.4.4 Ampliación de DL

En un evento de ampliación de DL, un MTA reemplaza a un destinatario inmediato que denota a una DL por los miembros de dicha DL, que de este modo se convierten en destinatarios miembros. El evento de ampliación de DL sólo se produce para los mensajes, no para las sondas.

A una DL determinada se le somete a ampliación siempre en una localización preestablecida, dentro del MTS. Esta localización se llama punto de ampliación de la DL, y viene identificada por una *dirección OR*.

El MTA puede generar, como parte de este evento, un informe de entrega.

La ampliación de la DL está sujeta al permiso de depósito. En el caso de una DL jerarquizada, ese permiso debe haber sido concedido a la DL de la que aquélla es miembro. De lo contrario, el permiso debe haber sido concedido al originador.

9.4.5 Redireccionamiento

En un evento de redireccionamiento, un MTA sustituye a un usuario o a una DL entre los destinatarios inmediatos de un mensaje o de una sonda, por un destinatario alternativo, especificado por el originador o asignado por el destinatario.

9.4.6 Conversión

En un evento de conversión, un MTA transforma partes del contenido de un mensaje de un EIT en otro, o altera una sonda de modo que parezca que los mensajes descritos fueron igualmente modificados. Este evento aumenta la probabilidad de que un objeto de información pueda ser entregado o afirmado, adaptándolo a sus destinatarios inmediatos.

Se distinguen los dos tipos de conversión que se indican a continuación, y que difieren en cómo se eligen el EIT de la información a convertir y el EIT resultante de la conversión:

- a) conversión explícita: conversión en la que el originador elige tanto el EIT inicial como el final;
- b) conversión implícita: conversión en la que el MTA elige los EIT finales, en función de los EIT iniciales y de las capacidades del UA.

9.4.7 No entrega

En un evento de no entrega, un MTA establece que el MTS no puede entregar un mensaje a sus destinatarios inmediatos, o no puede entregar un informe al originador de su mensaje o sonda objeto. Este evento detiene el transporte de un objeto al que el MTS considere intransportable.

En el caso de mensaje, el MTA genera, como parte de este evento, un informe de no entrega.

Un MTA efectúa una no entrega cuando, por ejemplo, determina que los destinatarios inmediatos no están especificados adecuadamente, que no aceptan la entrega de mensajes como el mensaje de que se trate, o que no se les ha entregado dentro de los límites de tiempo preestablecidos.

9.4.8 No afirmación

En un evento de no afirmación, un MTA establece que el MTS no puede entregar un mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda.

El MTA genera, como parte de ese evento, un informe de no entrega.

Un MTA produce una no afirmación cuando, por ejemplo, encuentra que los destinatarios inmediatos no están especificados adecuadamente o que no aceptarían la entrega de un mensaje descrito.

9.4.9 Afirmación

En un evento de afirmación, un MTA establece que el MTS puede entregar cualquier mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda y eleva a los destinatarios inmediatos a la categoría de destinatarios efectivos.

El MTA puede generar, como parte de este evento, un informe de entrega.

Un MTA produce una afirmación una vez que ha constatado que los destinatarios inmediatos están especificados adecuadamente y, si esos destinatarios son usuarios (pero no DL), que aceptarían la entrega de cualquier mensaje descrito. Si los destinatarios inmediatos son DL, el MTA producirá una afirmación si existe la DL y si el originador tiene el permiso de presentación pertinente.

9.4.10 Encaminamiento

En un evento de encaminamiento, un MTA selecciona el MTA "adyacente" al que transferirá un mensaje, sonda o informe. Este evento determina, de manera incremental, el camino de un objeto de información a través del MTS y, obviamente, sólo puede producirse si el MTS consta de varios MTA.

Hay dos tipos de encaminamiento, que difieren entre sí por la clase de transferencia para la que preparan:

- a) encaminamiento interno: encaminamiento que prepara para una transferencia interna (es decir, una transferencia dentro de un MD);
- b) encaminamiento externo: encaminamiento que prepara para una transferencia externa (es decir, una transferencia entre distintos MD).

Un MTA realiza un encaminamiento cuando determina que no puede efectuar ningún otro evento ni dar ningún paso con respecto a un objeto.

10 Modelo de seguridad

En esta cláusula se presenta un modelo de seguridad abstracto para la transferencia de mensajes. La realización concreta del modelo es tema de otras Especificaciones del MHS. El modelo de seguridad proporciona un marco para la descripción de los servicios de seguridad que contrarrestan los riesgos potenciales (véase el anexo D) del MTS, y de los elementos de seguridad que facilitan estos servicios.

Las características de seguridad constituyen una ampliación facultativa del MHS, que pueden emplearse para minimizar el riesgo de exposición de bienes de capital y recursos a las infracciones de una política de seguridad (riesgos). Su objetivo es proporcionar seguridad con independencia de los servicios de comunicaciones proporcionados por otras entidades, de nivel superior o inferior. Los riesgos pueden combatirse mediante el recurso a la seguridad de tipo físico, la seguridad de los computadores (COMPUSEC, *computer security*) o los servicios de seguridad proporcionados por el MHS. Según cuáles sean los riesgos que se contemplen, se seleccionarán unos u otros servicios de seguridad de MHS en combinación con adecuadas medidas de seguridad física y de COMPUSEC. Los servicios de seguridad facilitados por el MHS se describen más adelante. La denominación y la estructuración de los servicios se basan en ISO 7498-2.

NOTA 1 – A pesar de estas características de seguridad, pueden producirse ciertas agresiones contra las comunicaciones entre un usuario y el MHS o contra las comunicaciones de usuario a usuario (por ejemplo, en el caso de usuarios que acceden al MHS a través de una unidad de acceso, o de usuarios con acceso a distancia a sus UA). Para contrarrestar esas agresiones es preciso ampliar los servicios y modelos actuales de seguridad, lo que requiere normalización en el futuro.

En muchos casos, la amplitud de los tipos de riesgos queda cubierta por varios de los servicios anotados.

Los servicios de seguridad se facilitan mediante el uso de elementos de servicio del sobre de mensajes del MTS. El sobre contiene argumentos propios de la seguridad, tal como se describe en la Rec. UIT-T X.411 | ISO/CEI 10021-4. La descripción de los servicios de seguridad, se hace de la siguiente manera: en 10.2 se da una relación de los servicios con su definición e indicación, en cada caso, de cómo pueden ser proporcionados empleando los elementos de seguridad de la Rec. UIT-T X.411 | ISO/CEI 10021-4 y en 10.3 se describen uno a uno los elementos de seguridad con definición, en cada caso, del elemento de servicio, y referencias a sus argumentos constituyentes, según la Rec. UIT-T X.411 | ISO/CEI 10021-4.

Muchas de las técnicas empleadas se basan en mecanismos de criptación. Los servicios de seguridad del MHS permiten elegir los algoritmos con flexibilidad. Sin embargo, en algunos casos, sólo se ha definido totalmente en esta Especificación la utilización de la criptación asimétrica. En una futura versión o suplemento a la Especificación se podrán utilizar mecanismos alternativos de cifrado simétrico.

NOTA 2 – Las expresiones "servicio de seguridad" y "elemento de seguridad" que se emplean en esta cláusula no deben confundirse con las expresiones "servicio" y "elemento de servicio" empleadas en la Rec. UIT-T X.400 | ISO/CEI 10021-1. Las primeras expresiones se utilizan en esta cláusula para mantener la armonía con ISO 7498-2.

10.1 Políticas de seguridad

Los servicios de seguridad del MHS deben poder facilitar una amplia gama de políticas de seguridad, que va más allá de los límites del propio MHS. Los servicios seleccionados y los riesgos contra los que se pretende asegurarse dependerán de la aplicación concreta y de los niveles de confianza que se tenga en las distintas partes del sistema.

La política de seguridad define cómo reducir a un nivel aceptable el riesgo de exposición al peligro de los bienes de capital.

Además será preciso el funcionamiento entre dominios diferentes, cada uno de ellos con su propia política de seguridad. Se deberán establecer acuerdos bilaterales sobre ese interfuncionamiento, ya que las políticas globales de seguridad, más amplias que la del mero MHS, a que esos dominios estén sujetos, diferirán de todos modos entre sí. Debe definirse esto de tal manera que no se entre en conflicto con la política de seguridad de ninguno de los dos dominios y que el acuerdo llegue efectivamente a formar parte de la política de seguridad global de ambos.

10.2 Servicios de seguridad

En esta cláusula se definen los servicios de seguridad de la transferencia de mensajes. La denominación y la estructura de los mismos se basa en la ISO 7498-2.

Los servicios de seguridad de la transferencia de mensajes son de amplias y variadas clases. Esas clases, y los servicios correspondientes a cada una de ellas, aparecen relacionadas en el cuadro 7. Un asterisco (*) debajo del encabezamiento del tipo *X/Y* significa que el servicio puede ser proporcionado desde un objeto funcional de tipo *X* a uno de tipo *Y*.

Cuadro 7 – Servicios de seguridad de la transferencia de mensajes

SERVICIO	UA/UA	MS/MTA	MTA/MS	MTA/UA			
	UA/MS	UA/MTA	MTA/MTA	MS/UA			
+ AUTENTICACIÓN DE ORIGEN							
Autenticación de origen de mensajes	*	*	-	*	-	-	-
Autenticación de origen de sondas	-	-	*	*	-	-	-
Autenticación de origen de informes	-	-	-	*	*	*	-
Prueba de depósito	-	-	-	-	-	*	-
Prueba de entrega	*	-	-	-	-	-	Nota
+ GESTIÓN DE ACCESO SEGURO							
Autenticación de entidades pares	-	*	*	*	*	*	*
Contexto de seguridad	-	*	*	*	*	*	*
+ CONFIDENCIALIDAD DE DATOS							
Confidencialidad de conexiones	-	*	*	*	*	*	*
Confidencialidad de contenidos	*	-	-	-	-	-	-
Confidencialidad de flujo de mensajes	*	-	-	-	-	-	-
+ SERVICIOS DE INTEGRIDAD DE DATOS							
Integridad de conexiones	-	*	*	*	*	*	*
Integridad de contenidos	*	-	-	-	-	-	-
Integridad de secuencia de mensajes	*	-	-	-	-	-	-
+ NO RECHAZO							
No rechazo de origen	*	-	-	*	-	-	-
No rechazo de depósito	-	-	-	-	-	*	-
No rechazo de entrega	*	-	-	-	-	-	Nota
+ ETIQUETADO DE MENSAJES DE SEGURIDAD							
Etiquetado de mensajes de seguridad	*	*	*	*	*	*	*
+ SERVICIOS DE GESTIÓN DE LA SEGURIDAD							
Cambio de credenciales	-	*	-	*	*	*	-
Registros	-	*	-	*	-	-	-
Registros de la MS	-	*	-	-	-	-	-

NOTA - Este servicio lo proporciona la MS del destinatario al UA del originador.

A lo largo de la serie de definiciones de servicios de seguridad que viene a continuación se hace referencia a la figura 6, que representa el modelo funcional del MHS de forma simplificada. En el texto se hace referencia en varias ocasiones a las etiquetas numeradas.

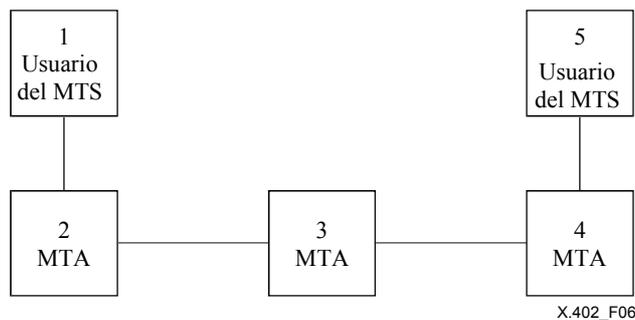


Figura 6 – Modelo funcional de MHS simplificado

10.2.1 Servicios de seguridad de autenticación de origen

Estos servicios de seguridad facilitan la autenticación de la identidad de entidades pares comunicantes y de fuentes de datos.

10.2.1.1 Servicios de seguridad de autenticación de origen de datos

Estos servicios de seguridad permiten la confirmación del origen de un mensaje, una sonda o un informe a todas las entidades afectadas (es decir, los MTA o los usuarios del MTS destinatarios). No pueden proteger contra la duplicación de mensajes, sondas e informes.

10.2.1.1.1 Servicio de seguridad de autenticación de origen de mensajes

Este servicio de seguridad permite la confirmación del origen de un mensaje.

El servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de mensajes o el de integridad de argumento de mensajes. El primero se puede emplear para dar servicio de seguridad a cualquiera de las partes afectadas (1 a 5 inclusive, en la figura 6), mientras que el segundo sólo puede utilizarse para proporcionar servicio de seguridad a los usuarios del MTS (1 ó 5 en la figura 6). El elemento de seguridad elegido depende de la política de seguridad que prevalezca.

10.2.1.1.2 Servicio de seguridad de autenticación de origen de sondas

El servicio de seguridad de autenticación de origen de sondas permite la confirmación del origen de una sonda.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de sondas. Puede emplearse el elemento de seguridad para dar el servicio a cualquiera de los MTA a través de los cuales se transfiere la sonda (2 a 4 inclusive, en la figura 6).

10.2.1.1.3 Servicio de seguridad de autenticación de origen de informes

El servicio de seguridad de autenticación de origen de informes permite la confirmación del origen de un informe.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de informes. El elemento de seguridad se emplea para dar servicio de seguridad al originador del mensaje o de la sonda objeto, así como a cualquiera de los MTA a través de los cuales se transfiere el informe (1 a 5 inclusive, en la figura 6).

10.2.1.2 Servicio de seguridad de prueba de depósito

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido recibido por el MTS para su entrega al destinatario o destinatarios especificados originalmente.

El servicio puede proporcionarse utilizando el elemento de seguridad de prueba de depósito.

10.2.1.3 Servicio de seguridad de prueba de entrega

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido entregado por el MTS al destinatario o destinatarios deseados.

El servicio puede proporcionarse utilizando el elemento de seguridad de prueba de entrega.

10.2.2 Servicio de seguridad de gestión de acceso seguro

El servicio de seguridad de gestión de acceso seguro se ocupa de la protección de los recursos contra su utilización no autorizada. Puede dividirse en dos componentes: servicio de autenticación de entidades pares y servicio de contexto de seguridad.

10.2.2.1 Servicio de seguridad de autenticación de entidades pares

Este servicio de seguridad se proporciona al establecer una conexión, para confirmar la identidad de la entidad que se conecta. Puede utilizarse en los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6 y asegura, únicamente al ser empleado, contra los intentos de suplantación o de reactivación no autorizada de una conexión previa, por parte de una entidad.

El elemento de seguridad de intercambio de autenticación facilita este servicio. Téngase en cuenta que como consecuencia de la utilización de este elemento de seguridad, pueden liberarse otros datos, que en determinadas circunstancias podrían emplearse para facilitar un servicio de seguridad de confidencialidad de conexión y/o de integridad de conexión.

10.2.2.2 Servicio de seguridad de contexto de seguridad

Este servicio de seguridad se utiliza para limitar el alcance del paso de mensajes entre entidades, por referencia a las etiquetas de seguridad asociadas a los mensajes. Es un servicio que está, por tanto, en estrecha relación con el de seguridad de etiquetado de seguridad de mensajes, que permite la asociación de mensajes y etiquetas de seguridad.

Los elementos de seguridad de contexto de seguridad y registro facilitan el servicio de contexto de seguridad.

10.2.3 Servicios de seguridad de confidencialidad de datos

Estos servicios de seguridad protegen los datos contra su revelación no autorizada.

10.2.3.1 Servicio de seguridad de confidencialidad de conexión

El MHS no presta un servicio de seguridad de confidencialidad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, como resultado del empleo del elemento de seguridad de intercambio de autenticación, para proporcionar el servicio de seguridad de autenticación de entidades pares. Este servicio de seguridad puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6.

10.2.3.2 Servicio de seguridad de confidencialidad de contenido

El servicio de seguridad de confidencialidad de contenido garantiza que el contenido de un mensaje sólo sea conocido por su emisor y su destinatario.

Es posible proporcionar este servicio mediante una combinación de los elementos de seguridad de confidencialidad de contenido y de confidencialidad de argumento de mensajes. Este último se puede emplear para transferir una clave secreta, utilizada con el primero en el cifrado del contenido del mensaje. Con estos elementos de seguridad, se proporciona el servicio desde el usuario 1 al usuario 5 del MTS, de la figura 6, siendo el mensaje ininteligible para los MTA.

10.2.3.3 Servicio de seguridad de confidencialidad de flujo de mensajes

Este servicio de seguridad protege contra la extracción de información que podría lograrse mediante la observación del flujo de mensajes. El MHS proporciona este servicio sólo de forma limitada.

La técnica del sobre doble permite que un mensaje completo se convierta en contenido de otro mensaje. Esta técnica puede emplearse para ocultar la información de direccionamiento en determinados tramos del MTS. Junto con el relleno de tráfico (que queda fuera del objeto actual de esta Especificación) podría utilizarse para lograr la confidencialidad del flujo de mensajes. Otros elementos de este servicio, tales como el control del encaminamiento o los seudónimos, quedan también fuera del objeto de esta Especificación.

10.2.4 Servicios de seguridad de integridad de datos

Estos servicios de seguridad se proporcionan para contrarrestar riesgos activos contra el MHS.

10.2.4.1 Servicio de seguridad de integridad de conexión

El MHS no presta un servicio de seguridad de integridad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, utilizando el elemento de seguridad de intercambio de autenticación en la prestación del servicio de seguridad de autenticación de entidades pares. El servicio puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6.

10.2.4.2 Servicio de seguridad de integridad de contenido

Este servicio de seguridad garantiza la integridad del contenido de un mensaje. Para ello, se habilita la determinación de si el contenido del mensaje ha sido o no modificado. El servicio no permite detectar reactuaciones de mensajes, lo que sí es facilitado, en cambio, por el servicio de seguridad de integridad de secuencia de mensajes.

El servicio puede proporcionarse de dos modos diferentes, utilizando dos diferentes combinaciones de elementos de seguridad.

El elemento de seguridad de integridad de contenido junto con el de integridad de argumento de mensajes y, en algunos casos, el de confidencialidad de argumento de mensajes, pueden utilizarse para prestar servicio de seguridad a un destinatario de mensajes, es decir, para la comunicación del usuario 1 al usuario 5 del MTS, de la figura 6. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cuál sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de argumento de mensajes se protege la verificación de integridad del contenido contra posibles cambios. La integridad de cualquier argumento de mensaje confidencial se garantiza utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

También puede emplearse el elemento de seguridad de autenticación de origen de mensajes para prestar este servicio de seguridad.

10.2.4.3 Servicio de seguridad de integridad de secuencia de mensajes

Este servicio de seguridad protege al originador y al destinatario de una secuencia de mensajes, contra el reordenamiento de la secuencia. Al mismo tiempo, protege contra la reactuación de mensajes.

Puede proporcionarse el servicio haciendo uso de una combinación de los elementos de seguridad de integridad de secuencia de mensajes y de integridad de argumento de mensajes. El primero da a cada mensaje un número de secuencia que puede protegerse contra posibles cambios mediante el segundo elemento. Es posible proporcionar simultáneamente confidencialidad e integridad del número de secuencia de mensajes, empleando el elemento de seguridad de confidencialidad de argumento de mensajes.

Estos elementos de seguridad facilitan el servicio para la comunicación del usuario 1 al usuario 5 del MTS, de la figura 6, y no a los MTA intermedios.

10.2.5 Servicio de seguridad de no rechazo

Estos servicios de seguridad dan garantía absoluta a un tercero, después de que el mensaje ha sido depositado, enviado o entregado, de que el depósito, el envío o la recepción se han producido tal como se dice. Téngase en cuenta que, para que esto funcione correctamente, la política de seguridad debe abarcar de manera explícita la gestión de claves asimétricas, a efectos de servicios de no rechazo, si se utilizan algoritmos asimétricos.

10.2.5.1 Servicio de seguridad de no rechazo de origen

Este servicio de seguridad da al destinatario o destinatarios de un mensaje garantía absoluta del origen del mismo, de su contenido y de su etiqueta de seguridad de mensaje asociada.

El servicio puede proporcionarse de dos modos diferentes, utilizando dos combinaciones distintas de elementos de seguridad. Téngase en cuenta que la prestación de este servicio es muy similar a la del servicio de seguridad de integridad de contenido (más débil).

El elemento de seguridad de integridad de contenido junto con el de integridad de argumento de mensajes y, en algunos casos, el de confidencialidad de argumento de mensajes, pueden utilizarse para prestar servicio de seguridad a un destinatario de mensajes, es decir, para la comunicación del usuario 1 al usuario 5 del MTS, de la figura 6. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cuál sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de argumento de mensajes se protege la verificación y, si hace falta, la etiqueta de seguridad de mensajes, contra un posible cambio y/o rechazo. Cualquier argumento de mensaje confidencial queda protegido contra cambio y/o rechazo utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

Si no se requiere el servicio de seguridad de confidencialidad de contenido, también es posible emplear, como base de este servicio de seguridad, el elemento de seguridad de autenticación de origen de mensajes. En este caso puede proporcionarse el servicio de seguridad a todos los elementos del MHS, es decir, a todos los usuarios del 1 al 5 de la figura 6.

10.2.5.2 Servicio de seguridad de no rechazo de depósito

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido depositado en el MTS para su entrega al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de depósito, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de depósito (más débil).

10.2.5.3 Servicio de seguridad de no rechazo de entrega

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido entregado al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de entrega, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de entrega (más débil).

10.2.6 Servicio de seguridad del etiquetado de seguridad de mensajes

Este servicio de seguridad permite asociar etiquetas de seguridad a todas las entidades del MHS, es decir, los MTA y los usuarios del MTS. Conjuntamente con el servicio de seguridad de contexto de seguridad, facilita la ejecución de políticas de seguridad que precisen qué partes del MHS pueden tratar mensajes, mediante las etiquetas de seguridad asociadas especificadas.

El servicio lo proporciona el elemento de seguridad de la etiqueta de seguridad de mensajes. Los elementos de seguridad de integridad de argumento de mensajes y de confidencialidad de argumento de mensajes aseguran la integridad y confidencialidad de la etiqueta.

10.2.7 Servicios de gestión de la seguridad

El MHS necesita cierto número de servicios de gestión de seguridad. Los únicos servicios de gestión previstos en la Rec. UIT-T X.411 | ISO/CEI 10021-4 tratan del cambio de credenciales y del registro de etiquetas de seguridad de usuario del MTS.

10.2.7.1 Servicio de seguridad de cambio de credenciales

Este servicio de seguridad permite a una entidad del MHS cambiar las credenciales que le afectan, contenidas en otra entidad del MHS. Puede proporcionarse utilizando el elemento de seguridad de cambio de credenciales.

10.2.7.2 Servicio de seguridad de registros

Este servicio de seguridad permite el establecimiento en un MTA, de las etiquetas de seguridad autorizadas para un determinado usuario del MTS. Puede proporcionarse utilizando el elemento de seguridad de registros.

10.2.7.3 Servicio de seguridad de registro de la MS

Este servicio de seguridad permite el establecimiento de las etiquetas de seguridad que son admisibles para el usuario de la MS.

10.3 Elementos de seguridad

En las subcláusulas que siguen se describen los elementos de seguridad, disponibles en los protocolos de la Rec. UIT-T X.411 | ISO/CEI 10021-4, para facilitar los servicios de seguridad en el MHS. Esos elementos están relacionados directamente con los argumentos de varios servicios descritos en la Rec. UIT-T X.411 | ISO/CEI 10021-4. Esta subcláusula tiene por objeto extraer los elementos de las definiciones de servicios de la Rec. UIT-T X.411 | ISO/CEI 10021-4 que tienen relación con la seguridad, y definir la función de cada uno de esos elementos de seguridad identificados.

10.3.1 Elementos de seguridad de autenticación

Estos elementos de seguridad se definen para facilitar los servicios de seguridad de autenticación e integridad.

10.3.1.1 Elementos de seguridad de intercambio de autenticación

El elemento de seguridad de intercambio de autenticación está concebido para autenticar, posiblemente de manera mutua, la identidad de un usuario del MTS a un MTA, de un MTA a un MTA, de un MTA a un usuario del MTS, de una MS a un UA o de un UA a una MS. Se basa en la utilización o el intercambio de datos secretos, tales como contraseñas o testigos criptados asimétricamente o simétricamente. El resultado del intercambio es la confirmación de la identidad de la otra parte y, facultativamente, la transferencia de datos confidenciales que pueden utilizarse para la provisión del servicio de seguridad de confidencialidad de conexiones y/o de integridad de conexiones, en capas

subyacentes. Dicha autenticación sólo es válida en el instante en que se produce, dependiendo la continuidad de la validez de la identidad autenticada de si se utiliza o no intercambio de datos confidenciales, o algún otro mecanismo, para establecer un trayecto de comunicación seguro. El establecimiento y uso de un trayecto de comunicación seguro está fuera del alcance de la presente Especificación.

Este elemento de seguridad emplea el argumento de credenciales de iniciador y el resultado de credenciales de contestador de los servicios vinculados al MTS, a la MS y a un MTA. Las credenciales transferidas son contraseñas o testigos.

Cuando se utilizan contraseñas para la autenticación, puede haber contraseñas simples o contraseñas protegidas. La utilización de contraseñas protegidas para la autenticación entre el agente usuario (UA) y el almacenamiento de mensajes (MS) se describe detalladamente en el anexo H.

NOTA – Aunque el anexo H describe la autenticación entre el UA y el MS, aparte del mecanismo protegido para cambiar la contraseña, se aplica igualmente a la autenticación entre el UA y el MTA.

10.3.1.2 Elementos de seguridad de autenticación de origen de datos

Estos elementos de seguridad están concebidos de manera específica para facilitar los servicios de autenticación de origen de datos, aunque también se les puede emplear para proporcionar determinados servicios de integridad de datos.

10.3.1.2.1 Elemento de seguridad de autenticación de origen de mensajes

El elemento de seguridad de autenticación de origen de mensajes permite, a cualquiera que reciba o transfiera un mensaje, autenticar la identidad del usuario del MTS que originó el mensaje. Esto puede significar la prestación del servicio de seguridad de autenticación de origen de mensajes o del de no rechazo de origen.

El elemento de seguridad implica la transmisión, como parte del mensaje, de una verificación de autenticación de origen de mensajes, computada como una función del contenido del mensaje, del identificador de contenido de mensajes y de la etiqueta de seguridad de mensajes. Si también hace falta el servicio de seguridad de confidencialidad de contenido, el control de verificación se computa como una función del contenido del mensaje cifrado, en vez de una función del no cifrado. Actuando sobre el contenido del mensaje según es transportado en el mensaje global (es decir, después del elemento de seguridad facultativo de confidencialidad de contenido), cualquier entidad del MHS puede verificar la integridad del mensaje global sin necesidad de ver el texto en claro del contenido del mensaje. No obstante, si se hace uso del servicio de seguridad de confidencialidad de contenido, no puede emplearse el elemento de seguridad de autenticación de origen de mensajes para proporcionar el servicio de seguridad de no rechazo de origen.

El elemento de seguridad utiliza la verificación de autenticación de origen de mensajes, que es uno de los argumentos de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.1.2.2 Elemento de seguridad de autenticación de origen de sondas

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de sondas permite a cualquier MTA autenticar la identidad del usuario del MTS que originó una determinada sonda.

Este elemento de seguridad utiliza la verificación de autenticación de origen de sondas, que es uno de los argumentos del servicio de depósito de sondas.

10.3.1.2.3 Elemento de seguridad de autenticación de origen de informes

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de informes permite, a cualquier MTA o usuario del MTS que recibe un informe, autenticar la identidad del MTA que lo originó.

Este elemento de seguridad utiliza la verificación de autenticación de origen de informes, que es uno de los argumentos del servicio de entrega de informes.

10.3.1.3 Elemento de seguridad de prueba de depósito

Este elemento de seguridad proporciona al originador de un mensaje los medios para establecer que el mensaje fue aceptado por el MHS para su transmisión.

El elemento de seguridad está constituido por dos argumentos: una petición de prueba de depósito enviada con un mensaje en el momento del depósito, y la prueba de depósito devuelta al usuario del MTS como parte de los resultados del depósito de mensajes. El MTS genera la prueba de depósito, que es computada como una función de todos los argumentos del mensaje depositado, del identificador de depósito de mensajes y del momento en que se produce el depósito de mensajes.

Puede utilizarse el argumento de prueba de depósito para facilitar el servicio de seguridad de prueba de depósitos. Dependiendo de cuál sea la política de seguridad en vigor, puede también facilitar el servicio de seguridad de no rechazo de depósito (más fuerte).

La petición de prueba de depósito es un argumento del servicio de depósito de mensajes. La prueba de depósito es uno de los resultados del servicio de depósito de mensajes.

10.3.1.4 Elemento de seguridad de prueba de entrega

Este elemento de seguridad proporciona al originador de un mensaje medios para establecer que el mensaje fue entregado en destino por el MHS.

El elemento de seguridad está constituido por varios argumentos. El originador del mensaje incluye una petición de prueba de entrega en el mensaje depositado, y esta petición se entrega a cada destinatario con el mensaje. Un destinatario puede entonces computar la prueba de entrega como una función de un cierto número de argumentos asociados al mensaje. El MTS devuelve la prueba de entrega al originador del mensaje, como parte de un informe sobre los resultados del depósito de mensajes original.

Es posible utilizar la prueba de entrega para facilitar el servicio de seguridad de prueba de entrega. Dependiendo de cuál sea la política de seguridad en vigor, podría también facilitar el servicio de seguridad de no rechazo de entrega (más fuerte).

La petición de prueba de entrega es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes. La prueba de entrega es a la vez uno de los resultados del servicio de entrega de mensajes y uno de los argumentos de los servicios de transferencia de informes y de entrega de informes.

NOTA – La no recepción de una prueba de entrega no implica la no entrega.

10.3.2 Elementos de seguridad de gestión de acceso seguro

Estos elementos de seguridad se definen para facilitar el servicio de seguridad de gestión de acceso seguro y los servicios de gestión de la seguridad.

10.3.2.1 Elemento de seguridad de contexto de seguridad

Cuando un usuario del MTS o un MTA se vincula a un MTA o a un usuario del MTS, la operación de vinculación especifica el contexto de seguridad de la conexión. Esto limita el alcance del paso de mensajes por referencia a las etiquetas asociadas a los mensajes. Además, el contexto de seguridad de la conexión puede ser alterado temporalmente para mensajes depositados o entregados.

El propio contexto de seguridad consta de una o más etiquetas de seguridad, que definen la sensibilidad de interacciones que pueden producirse, en línea con la política de seguridad en vigor.

El contexto de seguridad es un argumento de los servicios vinculados al MTS y a un MTA.

10.3.2.2 Elemento de seguridad de registros

El elemento de seguridad de registros permite el establecimiento en un MTA de etiquetas de seguridad autorizadas de un usuario del MTS.

El servicio de registros proporciona este elemento. Dicho servicio permite a un usuario del MTS cambiar los argumentos, contenidos en el MTS, relativos a la entrega de mensajes a ese usuario del MTS.

10.3.2.3 Elemento de seguridad de registro de la MS

El elemento de seguridad de registro de la MS permite el establecimiento de las etiquetas de seguridad admisibles del usuario de la MS.

El servicio de registro de la MS proporciona este elemento. Dicho servicio permite a un usuario de la MS cambiar los argumentos, contenidos en la MS, relativos a la recuperación de mensajes dirigidos a ese usuario de la MS.

10.3.3 Elementos de seguridad de confidencialidad de datos

A todos estos elementos de seguridad, basados en la utilización del cifrado, les afecta la provisión de la confidencialidad de los datos que pasan de una entidad del MHS a otra.

10.3.3.1 Elemento de seguridad de confidencialidad de contenidos

El elemento de seguridad de confidencialidad de contenidos garantiza la protección del contenido del mensaje contra indiscreciones durante la transmisión, mediante un elemento de seguridad cifrado. El elemento de seguridad funciona de modo tal que sólo el destinatario y el emisor del mensaje pueden conocer el texto en claro del contenido del mensaje.

La especificación del algoritmo de cifrado, la clave empleada y cualquier otro dato de inicialización, se transportan utilizando los elementos de seguridad de confidencialidad de argumento de mensajes y de integridad de argumento de mensajes. El algoritmo y la clave se emplean después para cifrar o descifrar los contenidos de los mensajes.

ISO/CEI 10021-2:2004 (S)

Este elemento de seguridad hace uso del identificador de algoritmo de confidencialidad de contenidos, que es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.3.2 Elemento de seguridad de confidencialidad de argumento de mensajes

El elemento de seguridad de confidencialidad de argumento de mensajes proporciona la confidencialidad, la integridad y, si hace falta, la irrevocabilidad de los datos de destinatario asociados a un mensaje. De manera específica, estos datos incluirán cuantas claves criptográficas y datos conexos hagan falta para el funcionamiento adecuado de los elementos de seguridad de confidencialidad e integridad, caso de que se invoquen esos elementos.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de confidencialidad de argumento de mensajes constituyen los datos cifrados comprendidos en el testigo de mensajes. Los datos cifrados del testigo de mensajes resultan ininteligibles para todos los MTA.

El testigo de mensajes es un argumento de los servicios de depósito de mensajes, de transferencia de mensajes y de entrega de mensajes.

10.3.4 Elementos de seguridad de integridad de datos

Estos elementos se proporcionan para facilitar la prestación de los servicios de integridad de datos, autenticación de datos y no rechazo.

10.3.4.1 Elemento de seguridad de integridad de contenidos

El elemento de seguridad de integridad de contenidos protege el contenido de un mensaje contra posibles modificaciones durante la transmisión.

Este elemento emplea uno o más algoritmos de criptografía. La especificación del algoritmo o algoritmos, la clave o claves utilizadas y cualquier otro dato de inicialización se transportan utilizando los elementos de seguridad de confidencialidad e integridad de argumento de mensajes. El resultado de la aplicación de los algoritmos y de la clave es la verificación de integridad de contenidos, que se envía en el sobre del mensaje. El elemento de seguridad sólo está disponible para el destinatario o destinatarios del mensaje, puesto que actúa en el texto en claro de los contenidos de los mensajes.

Si se protegiera el control de verificación de integridad de contenidos utilizando el elemento de seguridad de integridad de argumentos de mensajes, se le podría emplear, dependiendo de cuál fuese la política de seguridad en vigor, para facilitar la prestación del servicio de seguridad de no rechazo de origen.

El control de verificación de integridad de contenido es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.4.2 Elemento de seguridad de integridad de argumento de mensajes

El elemento de seguridad de integridad de argumento de mensajes proporciona la integridad y, si hace falta, la irrevocabilidad de determinados argumentos asociados a un mensaje. De manera específica, estos argumentos pueden comprender cualquier selección del identificador de algoritmo de confidencialidad de contenidos, del control de verificación de integridad de contenidos, de la etiqueta de seguridad de mensajes, de la petición de prueba de entrega y del número de secuencia de mensajes.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de integridad de argumento de mensajes constituyen los datos firmados contenidos en el testigo de mensajes.

El testigo de mensajes es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.4.3 Elemento de seguridad de integridad de secuencia de mensajes

El elemento de seguridad de integridad de secuencia de mensajes protege al emisor y al destinatario de un mensaje contra la recepción de mensajes desordenados o duplicados.

Cada mensaje tiene asociado un número de secuencia de mensajes. Este número identifica la posición de un mensaje en una secuencia, desde el originador al destinatario. Así pues, cada pareja originador-destinatario que necesite utilizar este elemento de seguridad deberá mantener una secuencia precisa de números de mensajes. Este elemento de seguridad no facilita la inicialización o sincronización de números de secuencia de mensajes.

10.3.5 Elementos de seguridad de no rechazo

En la Rec. UIT-T X.411 | ISO/CEI 10021-4 no se definen, de manera específica, los elementos de seguridad de no rechazo. Los servicios de no rechazo pueden proporcionarse mediante una combinación de otros elementos de seguridad.

10.3.6 Elementos de seguridad de la etiqueta de seguridad

La finalidad de estos elementos de seguridad es facilitar el etiquetado de seguridad en el MHS.

10.3.6.1 Elemento de seguridad de etiqueta de seguridad de mensajes

Se pueden etiquetar los mensajes con datos según se especifique en la política de seguridad vigente. La etiqueta de seguridad de mensajes está a disposición de los MTA intermedios, como parte de la política de seguridad global del sistema.

Es posible enviar una etiqueta de seguridad de mensajes como un argumento de mensajes y que sea protegida por el elemento de seguridad de integridad de argumento de mensajes o el de autenticación de origen de mensajes, del mismo modo que otros argumentos de mensajes.

Como alternativa, tanto la confidencialidad como la integridad son necesarias, se puede proteger la etiqueta de seguridad de mensajes, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. En este caso, la etiqueta así protegida es un argumento de originador-destinatario, y puede diferir de la etiqueta de seguridad de mensajes en la envolvente del mensaje.

10.3.7 Elementos de seguridad de gestión de la seguridad

10.3.7.1 Elemento de seguridad de cambio de credenciales

El elemento de seguridad de cambio de credenciales permite actualizar las credenciales de un usuario del MTS o de un MTA.

El elemento de seguridad lo proporciona el servicio de cambio de credenciales del MTS.

10.3.8 Técnica del sobre doble

Es posible dar protección adicional a un mensaje completo, incluidos los parámetros del sobre, especificando que el contenido de un mensaje es, en sí mismo, un mensaje completo, es decir, que se dispone de una técnica de doble sobre.

Se puede aplicar esta técnica utilizando el argumento del tipo de contenido, que permite especificar que el contenido de un mensaje es un sobre interno. Ese tipo de contenido significa que el contenido es, por sí mismo, un mensaje (sobre y contenido). Una vez entregado al destinatario indicado en el sobre externo, el sobre externo se suprime y se descifra el contenido si es necesario, lo que da lugar a un sobre interno y a su contenido. La información contenida en el sobre interno se utiliza para transferir el contenido del sobre interno a los destinatarios indicados en el sobre interno.

El tipo de contenido es un argumento de los servicios de depósito, transferencia y entrega de mensajes.

10.3.9 Codificación para criptación y troceado (hashing)

Cada parámetro MTS que se someta a algoritmos de criptación o troceado se codificará utilizando las reglas de codificación ASN.1 especificadas a los fines de esa criptación o troceado.

NOTA 1 – No puede suponerse que la codificación de los parámetros MTS utilizados en los pasos de depósito, transferencia o entrega utilizará las reglas de codificación especificadas en el identificador de algoritmo.

NOTA 2 – En el caso del contenido deben aplicarse las reglas de codificación especificadas en el identificador de algoritmo sólo a la codificación de los octetos del contenido dentro de la cadena de octetos, y no a la codificación del protocolo de contenido (que permanece invariable).

SECCIÓN 3 – CONFIGURACIONES

11 Visión de conjunto

En esta sección se especifica cómo configurar el MHS para satisfacer cualquiera de los diversos requisitos de tipo funcional, físico y organizativo.

La sección abarca los siguientes temas:

- a) configuraciones funcionales;
- b) configuraciones físicas;
- c) configuraciones organizativas;
- d) el *MHS global*.

Los sistemas de mensajería son de los tipos que se representan de manera esquemática en la figura 8.

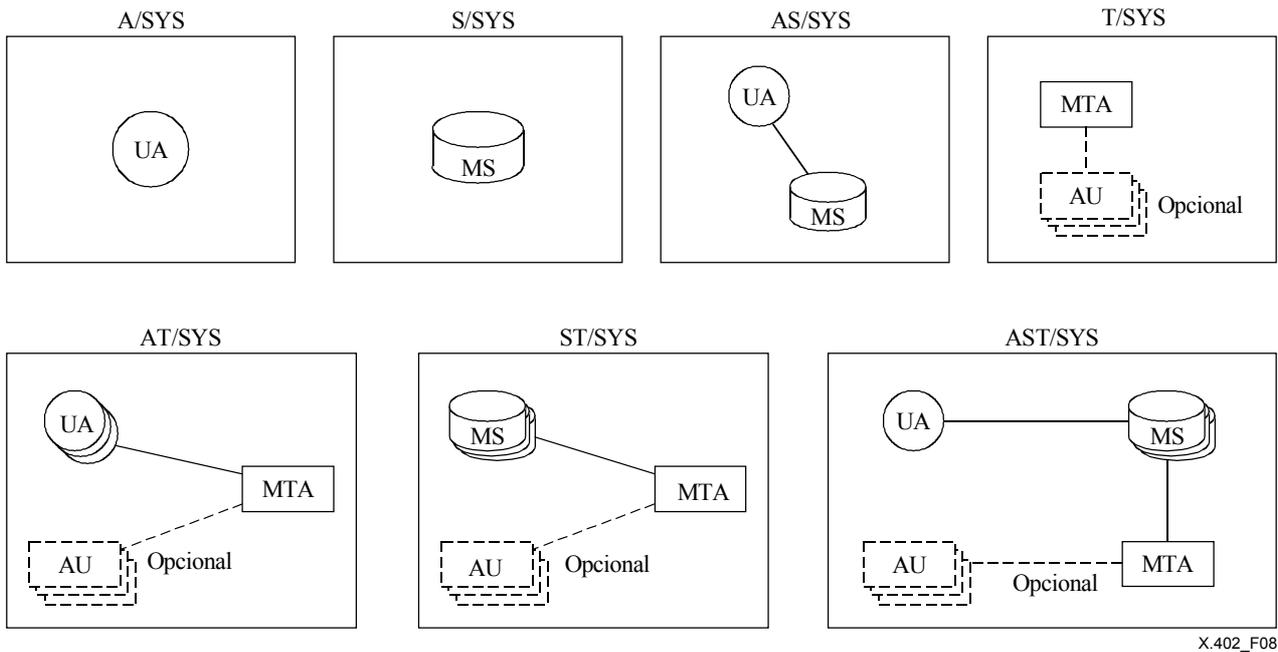


Figura 8 – Tipos de sistemas de mensajería

En la primera columna del cuadro 8 se da una relación de los tipos de sistemas de mensajería representados en la figura. Para cada tipo de esa relación, la segunda columna indica las clases de objetos funcionales –UA, MS, MTA y AU– que pueden estar presentes en dicho sistema de mensajería, si su presencia es obligatoria o facultativa y si el sistema de mensajería consta simplemente de uno o posiblemente de varios de esos objetos.

El cuadro 8 está dividido en dos secciones. Los sistemas de mensajería de los tipos de la primera sección prestan servicio a un solo usuario, mientras que los de la segunda pueden prestar servicio a un solo usuario o a varios usuarios.

Cuadro 8 – Sistemas de mensajería

Sistema de mensajería	Objetos funcionales			
	UA	MS	MTA	AU
A/SYS	1	-	-	-
S/SYS	-	1	-	-
AS/SYS	1	1	-	-
T/SYS	-	-	1	[M]
AT/SYS	M	-	1	[M]
ST/SYS	-	M	1	[M]
AST/SYS	M	M	1	[M]

+- Leyenda -----+
 | M múltiple [...] opcional |
 +-----+

Los tipos de sistemas de mensajería, expuestos de manera resumida en el cuadro 8, se definen y describen en las subcláusulas siguientes.

NOTA – Para la admisión de tipos de sistemas de mensajería se han tenido en cuenta los siguientes principios fundamentales:

- Una AU y el MTA con el que interactúa se hallan típicamente ubicados en la misma posición, puesto que no se ha normalizado ningún protocolo que gobierne su interacción.
- Un MTA se halla típicamente ubicado con múltiples UA o MS, porque, de los protocolos normalizados, sólo el de transferencia lleva un mensaje simultáneamente a destinatarios múltiples. La entrega en serie de un mensaje a destinatarios múltiples servidos por un sistema de mensajería, tal como exigiría el protocolo de entrega, resultaría ineficaz.

ISO/CEI 10021-2:2004 (S)

- c) Nada se consigue ubicando varios MTA en el mismo emplazamiento, en un sistema de mensajería, puesto que un solo MTA presta servicio a múltiples usuarios, y la finalidad de un MTA es transportar objetos funcionales entre sistemas y no dentro de tales sistemas (con esto no se pretende excluir la posibilidad de que varios procesos relacionados con un MTA coexistan en un único sistema por computador).
- d) La coubicación de una AU con un MTA no afecta al comportamiento del sistema con respecto al resto del MHS. Un solo tipo de sistema de mensajería abarca, por tanto, la presencia y la ausencia de la AU.

13.1.1 Sistemas de acceso

Un sistema de acceso (A/SYS, *access system*) contiene un UA, pero no una MS ni un MTA ni una AU.

Un A/SYS se dedica a un único usuario.

13.1.2 Sistemas de almacenamiento

Un sistema de almacenamiento (S/SYS, *storage system*) contiene una MS, pero no un UA ni un MTA ni una AU.

Un S/SYS se dedica a un único usuario.

13.1.3 Sistemas de acceso y almacenamiento

Un sistema de acceso y almacenamiento (AS/SYS, *access and storage system*) contiene un UA, y una MS, pero no un MTA ni una AU.

Un AS/SYS se dedica a un único usuario.

13.1.4 Sistemas de transferencia

Un sistema de transferencia (T/SYS, *transfer system*) contiene un MTA, facultativamente, una o más AU, pero no un UA ni una MS.

Un T/SYS puede prestar servicio a múltiples usuarios.

13.1.5 Sistemas de acceso y transferencia

Un sistema de acceso y transferencia (AT/SYS, *access and transfer system*) contiene uno o más UA, un MTA y, facultativamente, una o más AU, pero no una MS.

Un AT/SYS puede prestar servicio a múltiples usuarios.

13.1.6 Sistemas de almacenamiento y transferencia

Un sistema de almacenamiento y transferencia (ST/SYS, *storage and transfer system*) contiene una o más MS, un MTA y facultativamente, una o más AU, pero no UA.

Un ST/SYS puede prestar servicio a múltiples usuarios.

13.1.7 Sistema de acceso, almacenamiento y transferencia

Un sistema de acceso, almacenamiento y transferencia (AST/SYS, *access, storage and transfer system*) contiene uno o más UA, una o más MS, un MTA y facultativamente, una o más AU.

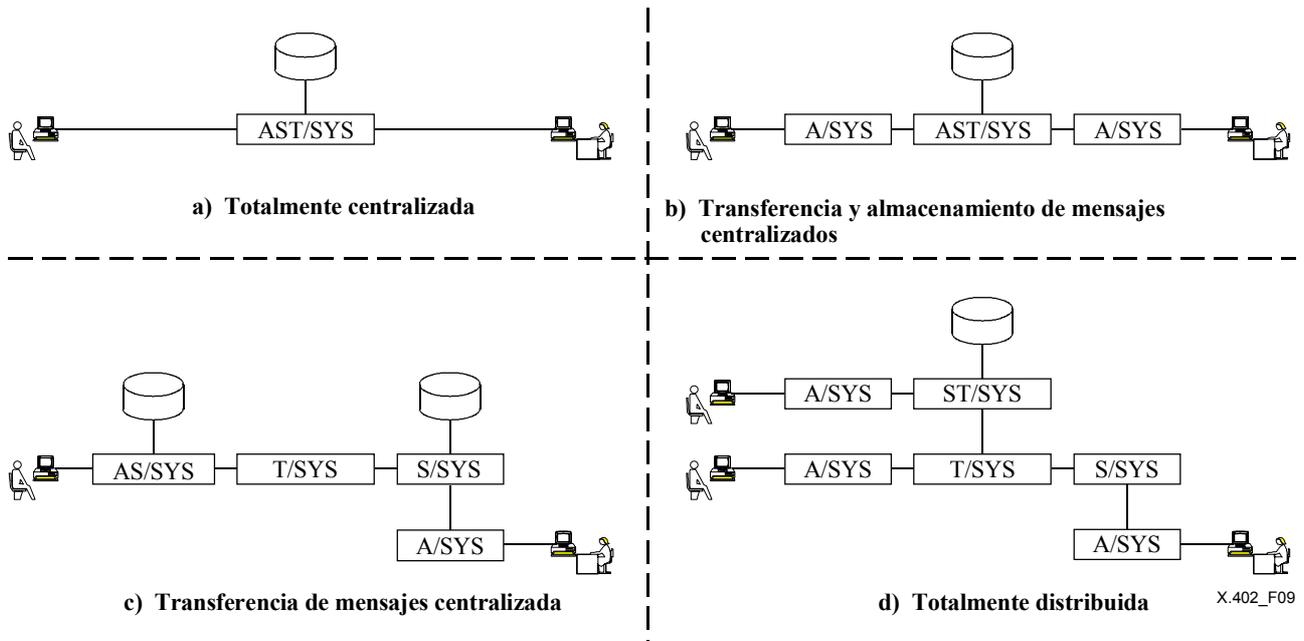
Un AST/SYS puede prestar servicio a múltiples usuarios.

13.2 Configuraciones representativas

Los sistemas de mensajería pueden combinarse de diversas maneras para constituir el MHS. Las configuraciones físicas posibles son ilimitadas, y por ello no pueden ser enumeradas. De todos modos, en la figura 9 y en los puntos que siguen, se describen varias configuraciones representativas importantes.

13.2.1 Totalmente centralizada

El MHS puede estar totalmente centralizado (caso *a* de la figura). Este diseño se realiza mediante un único AST/SYS que contiene objetos funcionales de todas clases y que puede prestar servicio a múltiples usuarios.



NOTA 1 – Aunque los usuarios representados en esta figura son personas, ésta es igualmente aplicable y válida a otras clases de usuarios

NOTA 2 – Además de las configuraciones físicas resultantes de los planteamientos "puros" que a continuación se indican, pueden construirse muchas configuraciones de carácter "híbrido".

Figura 9 – Configuraciones físicas representativas

13.2.2 Transferencia y almacenamiento de mensajes centralizados

El MHS puede proporcionar transferencia y almacenamiento de mensajes centralmente, pero distribuye el acceso de los usuarios (caso *b* de la figura). Este diseño se realiza mediante un único ST/SYS y, por cada usuario, un A/SYS.

13.2.3 Transferencia de mensajes centralizada

El MHS puede proporcionar transferencia de mensajes centralmente, pero distribuye el almacenamiento de mensajes y acceso de usuarios (caso *c* de la figura). Este diseño se realiza mediante un único T/SYS y, por cada usuario, un AS/SYS sólo o un S/SYS con un A/SYS asociado.

13.2.4 Totalmente distribuida

El MHS puede distribuir la transferencia de mensajes (caso *d* de la figura). Este diseño implica múltiples ST/SYS o T/SYS.

14 Configuraciones organizativas

En esta cláusula se especifican las configuraciones organizativas posibles del MHS, es decir, cómo puede realizarse el MHS en forma de conjuntos de sistemas de mensajería interconectados, pero gestionados independientemente (estando los propios sistemas conectados entre sí). Como el número de configuraciones es ilimitado, se describen los tipos de *dominios de gestión* a partir de los cuales se construye el MHS, y se identifican unas cuantas configuraciones representativas importantes.

14.1 Dominios de gestión

A los bloques primarios, utilizados en la construcción de MHS, se les denomina *dominios de gestión*. Un dominio de gestión (MD, *management domain*) (o dominio) es un conjunto de sistemas de mensajería –uno de los cuales por lo menos contenga o realice un MTA– gestionado por una única organización.

Lo anterior no excluye que una organización gestione un conjunto de sistemas de mensajería (por ejemplo, un solo A/SYS) que no tiene categoría de MD por falta de un MTA. Ese grupo de sistemas de mensajería, bloque secundario utilizado en la construcción del MHS, se "adscribe" a un MD.

Los MD son de varios tipos, cada uno de los cuales se define y describe en las subcláusulas que siguen.

14.1.1 Dominio de gestión de administración

Un dominio de gestión de administración (ADMD, *administration management domain*) ofrece servicios públicos de tratamiento de mensajes a una pluralidad de PRMD y/o usuarios individuales. El ADMD tiene la responsabilidad propia de una Administración en cuanto a garantizar que sus usuarios puedan comunicarse con cualquier otro MD adscrito al *MHS global*.

14.1.2 Dominio de gestión privado

Un dominio de gestión privado (PRMD, *private management domain*) comprende sistemas de mensajería gestionados por una organización privada. Si bien no existe restricción alguna en cuanto a la oferta de servicios públicos por el PRMD, éste no ha aceptado las responsabilidades que recaen sobre una Administración en cuanto a garantizar que sus usuarios puedan comunicarse con cualquier otro MD adscrito al *MHS global*.

14.2 Configuraciones representativas

Los MD pueden combinarse de diversas maneras para constituir el MHS. Las configuraciones organizativas posibles son ilimitadas, y por ello no pueden enumerarse. De todos modos, en la figura 10 y en los puntos que siguen se describen varias configuraciones representativas importantes.

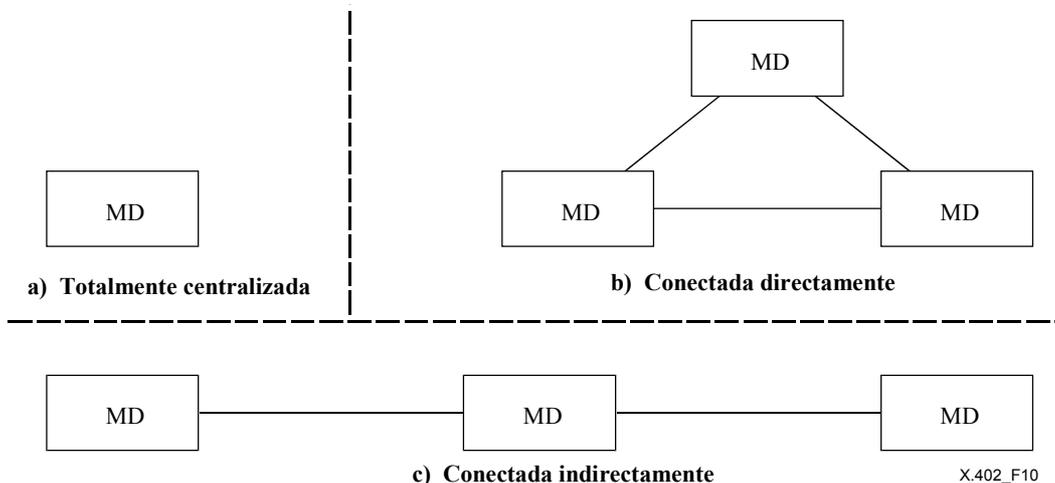


Figura 10 – Configuraciones organizativas representativas

NOTA – Además de las configuraciones organizativas resultantes de los planteamientos "puros" que a continuación se indican, pueden construirse muchas otras organizaciones de carácter "híbrido".

14.2.1 Totalmente centralizada

Todo el MHS puede ser gestionado por una organización (caso *a* de la figura). Este diseño se realiza mediante un único MD.

14.2.2 Conectada directamente

El MHS puede ser gestionado por varias organizaciones, estando los sistemas de mensajería de cada una de ellas conectados a los sistemas de mensajería de todas las demás (caso *b* de la figura). Este diseño se realiza mediante múltiples MD interconectados por pares.

14.2.3 Conectada indirectamente

El MHS puede ser gestionado por varias organizaciones, actuando los sistemas de mensajería de una como intermediarios entre los sistemas de mensajería de las otras (caso *c* de la figura). Este diseño se realiza mediante múltiples MD uno de los cuales está interconectado con todos los demás.

15 El MHS global

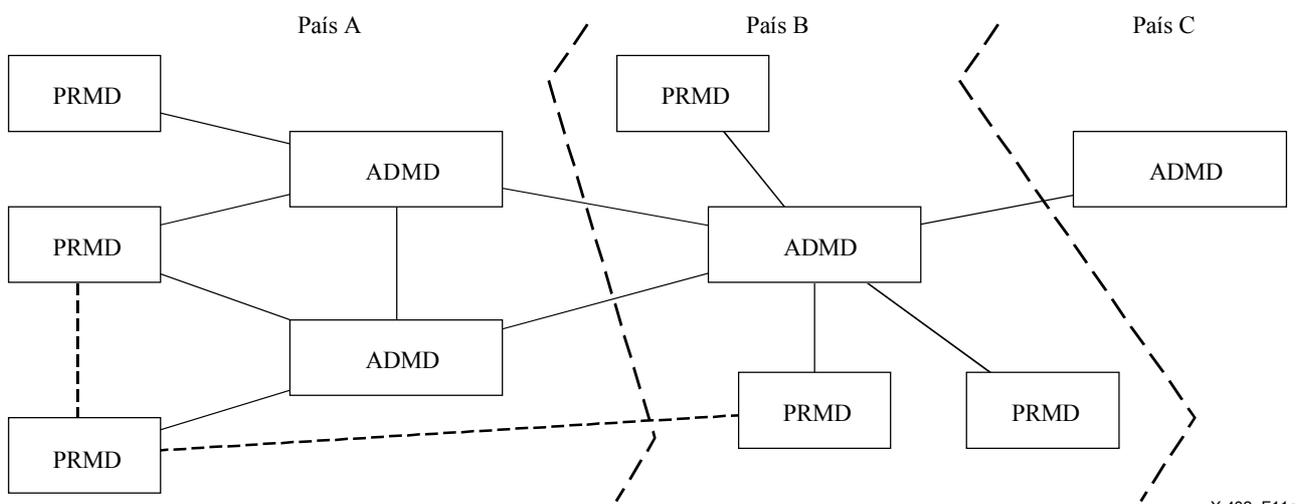
Uno de los principales objetivos de las Especificaciones del MHS es facilitar la construcción del MHS global, un MHS que permita el tratamiento de mensajes intra e interorganizativo, y también intra e internacional, a escala mundial.

El MHS global abarca, casi con toda seguridad, la gama completa de configuraciones funcionales especificadas en la cláusula 12.

La configuración física del MHS global es un híbrido de las configuraciones puras especificadas en la cláusula 13, sumamente complejo y con un alto grado de distribución física.

La configuración organizativa del MHS global es una combinación híbrida de las configuraciones puras especificadas en la cláusula 14, sumamente compleja y con un alto grado de distribución organizativa.

En la figura 11 se da un ejemplo de posibles interconexiones, que no pretende identificar todas las configuraciones posibles. Tal como se indica en la figura, los ADMD juegan un papel central en el MHS global. Mediante su interconexión internacional se constituye la columna vertebral de la transferencia de mensajes. Interconectándolos a nivel nacional, y dependiendo de cuáles sean los reglamentos nacionales, pueden también proporcionar entramados básicos, a ese mismo nivel, unidos al entramado internacional.



NOTA – La existencia de interconexiones representadas por líneas de puntos entre los MTA puede resultar afectada por la reglamentación.

X.402_F11a

Figura 11 – El MHS global

SECCIÓN 4 – DENOMINACIÓN, DIRECCIONAMIENTO Y ENCAMINAMIENTO

16 Visión de conjunto

En esta cláusula se describen la denominación y el direccionamiento de usuarios y DL, y el encaminamiento hacia ellos de objetos de información.

La sección comprende los siguientes temas:

- a) denominación;
- b) direccionamiento;
- c) encaminamiento.

17 Denominación

En este punto se especifica cómo se denomina a los usuarios y DL a efectos de tratamiento de mensajes en general y transferencia de mensajes en particular. Se definen los *nombres OR* y se describe el papel que desempeñan en ellos los nombres de directorio.

ISO/CEI 10021-2:2004 (S)

Cuando un UA o una MS depositan directamente un mensaje o una sonda, identifican al MTS los destinatarios potenciales. Cuando el MTS entrega un mensaje, identifica el originador a cada UA o MS del destinatario potencial. Los *nombres OR* son las estructuras de datos por medio de las cuales se realiza esa identificación.

17.1 Nombres de directorio

Un nombre de directorio es un componente de un *nombre OR*. El nombre de directorio identifica un objeto al directorio. Presentando ese nombre al directorio, el MHS puede acceder la inscripción en el directorio de un usuario o una DL. El MTS obtiene de esa inscripción, por ejemplo, la *dirección OR* del usuario o de la DL.

No todos los usuarios o DL están inscritos en el directorio y, por consiguiente, no todos ellos tienen un nombre de directorio.

NOTA 1 – Muchos usuarios y DL carecerán de nombre de directorio mientras no se generalice la difusión de ésta, como elemento auxiliar del MHS. Gran número de usuarios indirectos (por ejemplo, autoridades postales) no tendrán tales nombres mientras no se disponga ampliamente del directorio, como un adjunto a otros sistemas de comunicación.

NOTA 2 – A los usuarios y a las DL se les puede asignar nombres de directorio incluso antes de que se ponga en marcha un directorio interconectado y distribuido, preestableciendo las autoridades de denominación, de las que dependerá el directorio en su momento.

NOTA 3 – El nombre de directorio típico le resulta más cómodo y estable al usuario que la *dirección OR* típica porque la segunda está expresada necesariamente desde el punto de vista de la estructura organizativa o física del MHS, mientras que el primero no lo está. Se pretende por ello que, con el tiempo, los nombres de directorio se conviertan necesariamente en el principal medio de identificación de los usuarios y las DL fuera del MHS (es decir, por otros usuarios), y que el empleo de las *direcciones OR* se limite en gran medida al MTS (es decir, al uso por los MTA).

17.2 Nombres OR

Cada usuario o DL tiene uno o más *nombres OR*. Un nombre OR es un identificador por medio del cual puede un usuario ser designado como originador, o un usuario o una DL ser designados como destinatario potencial de un mensaje o sonda. El nombre OR distingue a un usuario o una DL de otro, y puede identificar además su punto de acceso al MHS.

Un nombre OR incluye un nombre de directorio, una *dirección OR* o ambas cosas. Si está presente y es válido, el nombre de directorio identifica de manera inequívoca al usuario o a la DL (aunque no es necesariamente el único nombre que podrá hacerlo). La *dirección OR*, cuando existe, hace eso mismo y más (véase 18.5).

En depósito directo, el UA o la MS del originador de un mensaje o sonda pueden incluir cualquiera de los dos componentes, o ambos, en cada nombre OR que suministren. Si se omite la *dirección OR*, el MTS la obtiene a partir del directorio, utilizando el nombre de directorio. Si se omite el nombre de directorio, el MTS prescinde de él. Si se incluyen ambos, el MTS confía en primer lugar en la *dirección OR*. Si constatará que la *dirección OR* era no válida (por ejemplo, porque se hubiera quedado obsoleta), procedería como si la *dirección OR* hubiera sido omitida, confiando en el nombre de directorio.

En entrega, el MTS incluye una *dirección OR* y posiblemente un nombre de directorio en cada nombre OR que suministra al destinatario de un mensaje o al originador de un mensaje o sonda objeto de un informe. El nombre de directorio se incluye si el originador lo ha suministrado, o si se identificó como miembro de una DL ampliada.

NOTA – La redirección o la ampliación de DL pueden dar lugar a que el MTS lleve a un UA o a una MS en entrega, nombres OR que el UA o la MS no suministraron en depósito directo.

Para información sobre las organizaciones que funcionan en varios países, véase el anexo G. Véase asimismo 7.3.2 de la Rec. UIT-T X.400 | ISO/CEI 10021-1.

18 Direccionamiento

En esta cláusula se especifica la manera de direccionar a usuarios y DL. Se definen las *direcciones OR*, se describe la estructura de las *listas de atributos* a partir de las que se elaboran, se examinan los conjuntos de caracteres con los que se componen los *atributos* individuales, se dan reglas para determinar si dos *listas de atributos* son equivalentes y para la inclusión de *atributos* condicionales en tales listas y se definen los *atributos normalizados* que pueden figurar en ellas.

Para transportar un mensaje, una sonda o un informe a un usuario, o para ampliar una DL especificada como destinatario potencial de un mensaje o una sonda, el MTS debe localizar el usuario o la DL relativos a sus propias estructuras física y organizativa. Las *direcciones OR* son las estructuras de datos mediante las cuales se realizan todas estas localizaciones.

18.1 Lista de atributos

Las *direcciones OR* de usuarios y DL son listas de atributos. Una lista de atributos es un conjunto ordenado de *atributos*.

Un atributo es un elemento de información que describe a un usuario o DL y que puede también ubicarlo en relación con la estructura física y organizativa del MHS (o la red inherente al mismo).

Un atributo consta de las siguientes partes:

- a) tipo de atributo (o tipo): Identificador que indica una clase de información (por ejemplo, nombres personales).
- b) valor de atributo (o valor): Ejemplo de la clase de información indicada por el tipo de atributo (por ejemplo, un nombre personal).

Los atributos son de las dos clases siguientes:

- a) atributo normalizado: Atributo cuyo tipo está vinculado a una clase de información por esta Especificación.
El valor de cada atributo normalizado, excepto el del *tipo-terminal*, es una cadena o bien un grupo de cadenas.
- b) atributo definido por el dominio: Atributo cuyo tipo está vinculado a una clase de información por un MD. Por tanto, el tipo y valor de un atributo-definido-por-el dominio son definidos por un MD: el MD es identificado por un *nombre-de-dominio-privado*, por un *nombre-de-dominio-de-administración*, o por ambos.

Tanto el tipo como el valor de cada atributo definido por el dominio son cadenas o grupos de cadenas.

NOTA – El uso generalizado de atributos normalizados genera direcciones OR más uniformes y por tanto más cómodas para el usuario. No obstante, es de prever que no todos los MD serán capaces de emplear tales atributos inmediatamente. La finalidad de los atributos definidos por el dominio es permitir a un MD que retenga durante cierto tiempo los convenios primitivos de direccionamiento existentes. Se pretende sin embargo, que todos los MD tiendan al empleo de atributos normalizados, y que los atributos definidos por el dominio se utilicen sólo con carácter provisional.

18.2 Juegos de caracteres

Los valores de atributos normalizados y los tipos y valores de atributos definidos por el dominio se elaboran a partir de cadenas numéricas, imprimibles, teletex y universal, según los siguientes criterios:

- a) El tipo o valor de un determinado atributo definido por el dominio puede ser una cadena imprimible, una cadena teletex una cadena universal o cualquier combinación de éstas. Se hará idéntica elección (o elecciones) para el tipo y para el valor.
- b) Las clases de cadenas con las que pueden elaborarse valores de atributos normalizados y la manera de elaborarlos (por ejemplo, como una sola cadena o varias) difiere de un atributo a otro (véase 18.3).

El valor de un atributo consta de cadenas de una de las siguientes variedades, dependiendo de su tipo: numérico sólo; imprimible sólo; numérico e imprimible; e imprimible; teletex y universal. En relación con esto, las siguientes reglas gobiernan cada caso de comunicación:

- a) En el caso del *nombre-de-dominio-administración*, *nombre-de-dominio-privado* y *código-postal*, el mismo valor numérico puede representarse como una cadena numérica o imprimible.
- b) Donde se permitan cadenas tanto imprimibles como teletex, podrán suministrarse cadenas de una u otra variedad. Si se suministran cadenas tanto imprimibles como teletex, ambas deberán identificar sin ambigüedad al mismo usuario.
- c) Donde se permitan cadenas imprimible, teletex y universal, podrán suministrarse una, dos o las tres variantes. Cuando se suministra más de una variedad para un atributo, cada valor debe identificar inequívocamente al mismo usuario. Muchos sistemas no podrán reproducir todos los caracteres posibles que pueden ser representados por cadenas universales (por ejemplo, estando restringidos al subconjunto de cadena universal que admite requisitos nacionales), y algunos sistemas no podrán reproducir cadenas universales. En consecuencia, las cadenas universales solas se deben utilizar únicamente cuando se sabe que todos los destinatarios probables pueden tratar los caracteres en cuestión (por ejemplo, dentro de una comunidad de usuarios nacional o regional).

Cuando se suministra una cadena universal, se puede añadir un código de idioma definido en ISO 639 para facilitar la reproducción de la cadena universal; por ejemplo, cuando un carácter se reproduce diferentemente en diferentes idiomas, esto puede originar la selección de un tipo de carácter apropiado. El código de idioma comprende un código de dos caracteres especificado por ISO 639, seguido facultativamente por un espacio y un indicativo de país de dos

ISO/CEI 10021-2:2004 (S)

caracteres de ISO 3166 (véase 4.4 de ISO 639), si es necesario para identificar una utilización nacional específica del idioma (por ejemplo, "en" identifica al idioma inglés, "en GB" identifica al idioma inglés utilizado en el Reino Unido, y "en US" identifica al idioma inglés utilizado en Estados Unidos de América.

Cuando una cadena universal sólo contiene caracteres del plano multilingüe básico (véase ISO/CEI 10646-1), pueden estar codificados en ASN.1 como una cadena universal o como una cadena BMP.

Cuando se comparan valores de dirección OR, se despreciarán los códigos de idioma presentes.

Solamente para UIT-T:

La longitud de cada cadena y de cada secuencia de cadenas en un atributo se limitará tal como se indica en la especificación más detallada de atributos (la ASN.1) de la Rec. UIT-T X.411.

NOTA 1 – Se permiten las cadenas universal y teletex en valores de atributos para facilitar la inclusión, por ejemplo, de caracteres acentuados, utilizados normalmente en muchos países.

NOTA 2 – Las reglas de paso a un grado inferior que figuran en el anexo B de la Rec. UIT-T X.419 | ISO/CEI 10021-6 estipulan que una dirección OR no puede pasarse a un grado inferior si sólo se ha suministrado una cadena universal o una cadena teletex (o ambas) que contienen caracteres que están situados fuera del repertorio de la cadena imprimible.

NOTA 3 – La ASN.1 permite la codificación de cadenas teletex utilizando (entre otros) los repertorios de caracteres 102, 103, 6 y 156, que ofrecen dos posibilidades de codificación de numerosos caracteres latinos. A efectos de compatibilidad con los sistemas anteriores se recomienda que cualquier carácter de los repertorios 102 y 103 se codifique siempre utilizando estos repertorios y que no se utilicen los repertorios 6 y 156 cuando se codifique una cadena que contenga sólo caracteres disponibles en los repertorios 102 y 103. Esta misma condición se aplica a todos los casos de cadena teletex en los protocolos del MHS.

18.3 Atributos normalizados

En la primera columna del cuadro 9 figura la lista de tipos de atributos normalizados. Para cada tipo enumerado se indican en la segunda columna los conjuntos de caracteres –numéricos, imprimibles, teletex y universal– con los que está permitido elaborar valores de atributos.

El cuadro tiene tres secciones. Los tipos de atributos de la primera son de naturaleza general, los de la segunda están relacionados con el *encaminamiento a* un PDS y los de la tercera, con el *direccionamiento dentro de* un PDS.

Cuadro 9 – Atributos normalizados

Tipo de atributo normalizado	Juego de caracteres		
	Númérico	Imprimible	Universal o Teletex
General			
Nombre-dominio-administración	x	x	–
Nombre-común	–	x	x
Nombre-país	x	x	–
Dirección-red	x*	–	–
Identificador-usuario-numérico	x	–	–
Nombre-organización	–	x	x
Nombre-unidades-organización	–	x	x
Nombre-personal	–	x	x
Nombre-dominio-privado	x	x	–
Identificador-terminal	–	x	–
Tipo-terminal	–	–	–
Encaminamiento postal			
Nombre-servicio-entrega-física	–	x	–
Nombre-país-entrega-física	x	x	–
Código-postal	x	x	–
Direccionamiento postal			
Componentes-ampliación-dirección-OR postal	–	x	x
Componentes-ampliación-dirección-entrega-física	–	x	x
Atributos-postales-locales	–	x	x

Tipo de atributo normalizado	Juego de caracteres		
	Numérico	Imprimible	Universal o Teletex
Nombre-oficina-entrega-física	–	x	x
Número-oficina-entrega-física	–	x	x
Nombre-organización-entrega-física	–	x	x
Nombre-personal-entrega-física	–	x	x
Dirección-apartado-correos	–	x	x
Dirección-lista-correos	–	x	x
Dirección-calle	–	x	x
Dirección-postal-no-formatada	–	x	x
Nombre-postal-exclusivo	–	x	x
Leyenda			
X permitido			
* En determinadas circunstancias, una secuencia de cadenas de octetos			

Los tipos de atributos normalizados, resumidos en el cuadro 9, se definen y describen individualmente en las subcláusulas que siguen.

18.3.1 Nombre-dominio-administración

Nombre-dominio-administración es un atributo normalizado que identifica un ADMD relativo al país indicado por un *nombre-país*.

El valor de este atributo es una cadena numérica o imprimible, elegida de entre un conjunto de tales cadenas administrado para este fin por el país aludido anteriormente.

NOTA 1 – El valor de atributo que consta de un único espacio (" ") se reservará para los siguientes fines. Si lo permite el país indicado por el atributo de nombre-país, un único espacio designará cualquiera (es decir, todos) los ADMD dentro del país. Esto afecta tanto a la identificación de usuarios dentro del país como al encaminamiento de mensajes, sondas e informaciones hacia y entre los ADMD de ese país. En relación con lo primero, es preciso que las direcciones OR de los usuarios dentro del país se elijan de tal modo que se asegure su carácter inequívoco, incluso en ausencia de los nombres verdaderos de los ADMD de usuarios. En relación con lo segundo, ello permite que los PRMD de dentro y los ADMD de fuera del país encaminen mensajes, sondas e informes a cualquiera de los ADMD de dentro del país, y exige que estos últimos se interconecten de manera tal que los mensajes, las sondas y los informes sean llevados a sus destinos.

El valor de atributo que consta de un único cero ("0"), codificado como cadena imprimible o numérica, se reservará para la utilización por los PRMD que no estén conectados a ningún ADMD y que no sean alcanzables desde ningún ADMD. El valor cero único no será utilizado por un PRMD que esté conectado a uno o a varios ADMD. El valor cero único no será utilizado por un PRMD indirectamente conectado a un ADMD (es decir, cuando existan acuerdos establecidos tanto con un ADMD como con PRMD intermedios para encaminar mensajes indirectamente entre el ADMD y el PRMD objeto). Además de proporcionar una parte apropiada del espacio de dirección OR para tales PRMD, el valor cero único capacita a los ADMD y a otros PRMD (sin establecer acuerdos de encaminamiento con el PRMD objeto) para determinar que los mensajes, sondas e informes no pueden ser encaminados al PRMD objeto. La presencia de una dirección OR con un único nombre-dominio-administración en destinatarios cuya responsabilidad se haya fijado en no responsable, o en el originador de un mensaje o informe que haya sido ampliado en DL o redirigido, o sufrido alguna otra incidencia, es legítima y no debe causar la no entrega.

NOTA 2 – El nombre-dominio-administración único no requiere una implementación concreta para ejercer ninguna acción especial, pero tal realización permitirá economizar costos de transmisión al detectar la imposibilidad de la entrega en una fase anterior a la que de otro modo podía conseguirse.

18.3.2 Nombre-común

Nombre-común es un atributo normalizado que identifica a una DL o a un usuario relativo a la entidad indicada por otro atributo (por ejemplo, un *nombre-organización*).

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos. Cualquier tipo de cadena que se utilice, el valor se elige de un conjunto de estas cadenas que es administrado para este fin (y quizás para otros) por la entidad mencionada anteriormente.

NOTA – Entre otras muchas posibilidades, un nombre-común podría identificar un cometido organizativo (por ejemplo, "director de mercadotecnia").

ISO/CEI 10021-2:2004 (S)

18.3.3 Nombre-país

El nombre-país es un atributo normalizado que identifica a un país (o, excepcionalmente, a una autoridad de registro MD internacional).

El valor de este atributo es una cadena imprimible que da el par de caracteres asignados al país por ISO 3166, o una cadena numérica que da uno de los números asignados al país (o zona geográfica, o servicio no organizado por zonas) por la Rec. CCITT X.121.

El valor del atributo cadena imprimible que comprende los caracteres "XX" se reservará para indicar la autoridad de registro internacional para nombres de dominio de gestión utilizados de acuerdo con la Rec. UIT-T X.666 | ISO/CEI 9834-7.

NOTA 1 – El valor "XX" está entre los reservados en ISO 3166 para ser empleado por los usuarios de esa Norma; por consiguiente, no existe la posibilidad de un conflicto futuro entre un nuevo distintivo de país asignado en ISO 3166 y este valor reservado.

NOTA 2 – Hay algunos usuarios que han empleado el valor "WW" como nombre de país para lograr un efecto similar al del valor "XX" antes de la existencia de un proceso de registro formal. Sin embargo, ISO 3166 no ha asignado actualmente el valor "WW" para este fin.

18.3.4 Componentes-ampliación-dirección-OR-postal

Componentes-ampliación-dirección-OR-postal es un atributo normalizado que proporciona, en una dirección postal, información adicional necesaria para identificar al destinatario (por ejemplo, una unidad organizativa).

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.5 Componentes-ampliación-dirección-entrega-física

Componentes-ampliación-dirección-entrega-física es un atributo normalizado que especifica, en una dirección postal, información adicional necesaria para identificar el punto exacto de entrega (por ejemplo, número de piso y despacho en un gran edificio).

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.6 Atributos-postales-locales

Atributos-postales-locales es un atributo normalizado que especifica el lugar de distribución, distinto del indicado por un atributo de nombre-oficina-entrega-física (por ejemplo, una zona geográfica) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.7 Dirección-red

Dirección-red es un atributo normalizado que da la dirección de red de un terminal.

Este atributo tiene algunos de los siguientes valores:

- a) una cadena numérica de conformidad con la Rec. CCITT X.121;
- b) dos cadenas numéricas tal como se especifica en la Rec. CCITT E.164;
- c) una dirección de punto de acceso al servicio de presentación (PSAP).

NOTA 1 – Entre las cadenas admitidas por la Rec. CCITT X.121 se encuentran números télex y de teléfono precedidos por una cifra de escape.

NOTA 2 – Los protocolos del MHS permiten llevar 16 cifras en el componente dirección X.121 de la dirección de red. De esta manera se puede utilizar una cifra de escape más un número telefónico o de RDSI completo de 15 cifras. Otros protocolos pueden tener un límite de 14 cifras, o un mecanismo diferente para codificar números de 15 cifras; el establecimiento de la correspondencia entre el MHS y esos protocolos, si se necesita, es un asunto local.

18.3.8 Identificador-usuario-numérico

Identificador-usuario-numérico es un atributo normalizado que identifica numéricamente a un usuario relativo al MD, indicado por un *nombre-dominio-privado* o un *nombre-dominio-administración*; o ambos.

El valor de este atributo es una cadena numérica elegida entre un conjunto de tales cadenas, administrado para este fin por el MD aludido anteriormente.

18.3.9 Nombre-organización

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

Cuando se utiliza en una *dirección OR nemotécnica* (véase 18.5.1), como asunto nacional, las organizaciones pueden identificarse con referencia al país indicado por un nombre-país (de tal modo que cada nombre-organización identifique una única entidad dentro del país) o al MD indicado por un *nombre-dominio-privado*, por un nombre-dominio-administración, o por ambos. Cualquiera que sea el tipo de cadena que se utilice, la cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por el país o el MD aludido anteriormente.

NOTA – En los países en que cada atributo nombre-organización deba corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos atributos.

Cuando se utiliza en una *dirección OR terminal* (véase 18.5.4) el nombre-organización es un valor de forma flexible, sin ningún requisito de registro.

18.3.10 Nombres-unidades-organizativas

Nombre-unidades-organizativas es un atributo normalizado que identifica una o más unidades (por ejemplo, divisiones o departamentos) de la organización indicada por un nombre-organización, siendo cada unidad, excepto la primera, una subunidad de las unidades cuyos nombres le preceden en el atributo.

El valor de este atributo es una secuencia ordenada de cadenas imprimibles, una secuencia ordenada de cadenas teletex, una secuencia ordenada de cadenas universales, o cualquier combinación de estas tres opciones. Cualquiera que sea el tipo de cadena que se utilice, cada cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por la organización (o unidad abarcadora) aludida anteriormente.

18.3.11 Nombre-servicio-entrega-física

Nombre-servicio-entrega-física es un atributo normalizado que identifica a un servicio de entrega física relativo al MD indicado por un *nombre-dominio-privado* o un nombre-dominio-administración, o ambos.

El valor de este atributo es una cadena imprimible elegida de entre un conjunto de tales cadenas, administrado para este fin por el MD aludido anteriormente.

18.3.12 Nombre-personal

Nombre-personal es un atributo normalizado que identifica una persona con respecto a la entidad indicada por otro atributo (por ejemplo, un nombre-organización).

El valor de este atributo comprende los siguientes cuatro elementos de información, de los que el primero es obligatoria y los otros facultativos:

- a) el apellido de la persona;
- b) el nombre de la persona;
- c) las iniciales de todos sus apelativos, excepto la del apellido;
- d) su generación (por ejemplo "hijo").

La información anterior se suministra como cadenas imprimibles, cadenas teletex, cadenas universales o cualquier combinación de estos tipos.

18.3.13 Nombre-país-entrega-física

Nombre-país-entrega-física es un atributo normalizado que identifica el país en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo está sometido a las mismas limitaciones que el de un nombre-país.

18.3.14 Nombre-oficina-entrega-física

Nombre-oficina-entrega-física es un atributo normalizado que identifica la ciudad, el pueblo, etc., en el que se halla la oficina postal a través de la cual un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.15 Número-oficina-entrega-física

Número-oficina-entrega-física es un atributo normalizado que distingue entre varias oficinas postales indicadas por un único nombre-oficina-entrega-física.

ISO/CEI 10021-2:2004 (S)

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.16 Nombre-organización-entrega-física

Nombre-organización-entrega-física es un atributo normalizado que identifica una organización de la autoridad postal.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.17 Nombre-personal-entrega-física

Nombre-personal-entrega-física es un atributo normalizado que identifica una autoridad postal.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.18 Dirección-apartado-correos

Dirección-apartado-correos es un atributo normalizado que especifica el número del casillero de la oficina postal en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal, o una combinación de estos tipos, a elegir entre el conjunto de tales cadenas asignadas para este fin por la oficina postal indicada por un atributo de nombre-oficina-entrega-física.

18.3.19 Código-postal

Código-postal es un atributo normalizado que especifica el código postal para la zona geográfica en la que el usuario recibe la entrega de los mensajes físicos.

El valor de este atributo es una cadena imprimible o numérica, elegida entre el conjunto de tales cadenas, mantenido y normalizado para este fin por la administración postal del país identificado por un atributo de nombre-país-entrega-física.

18.3.20 Dirección-lista-correos

Dirección-lista-correos es un atributo normalizado que identifica el código que un usuario da a la oficina postal para que acopie los mensajes físicos que se le deben entregar.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.3.21 Nombre-dominio-privado

Nombre-dominio-privado es un atributo normalizado que identifica un PRMD. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre de PRMD identifique una única entidad dentro del país) o referirse al ADMD identificado por un nombre-dominio-administración.

El valor de este atributo es una cadena numérica o imprimible elegida entre un conjunto de tales cadenas administradas para este fin por el país o el ADMD aludido anteriormente.

NOTA – En los países en que cada nombre de PRMD deba corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos nombres.

18.3.22 Dirección-calle

Dirección-calle es un atributo normalizado que especifica la dirección de calle [por ejemplo, número de la casa y nombre de la calle y tipo (por ejemplo, "camino")] en la que el usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.23 Identificador-terminal

Identificador-terminal es un atributo normalizado que da el identificador terminal de un terminal (por ejemplo, un distintivo télex o un identificador de terminal de teletex).

El valor de este atributo es una cadena imprimible.

18.3.24 Tipo-terminal

Tipo-terminal es un atributo normalizado que da el tipo de un terminal.

El valor de este atributo es uno cualquiera de los siguientes: *télex*, *teletex*, *facsimil G3*, *facsimil G4*, *terminal IA5* o *videotex*.

18.3.25 Dirección-postal-no-formatada

Dirección-postal-no-formatada es un atributo normalizado que especifica una dirección postal de usuario de forma flexible.

El valor de este atributo es una secuencia de cadenas imprimibles, representando una línea de texto, o bien una única cadena universal o una cadena teletex, estando las líneas separadas por CR LF o LF CR (se permiten hasta cinco apariciones del separador, o bien ambos).

18.3.26 Nombre-postal-exclusivo

Nombre-postal-exclusivo es un atributo normalizado que identifica el punto de entrega, distinto del indicado por un dirección-calle, un dirección-apartado-correos o un dirección-lista-correos (por ejemplo, un edificio o un caserío) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos.

18.4 Equivalencia de listas de atributos

Varias direcciones OR, y por tanto varias listas de atributos, pueden indicar el mismo usuario o la misma DL. Esta multiplicidad de direcciones OR se debe en parte (pero sólo en parte) a las siguientes reglas de equivalencia de listas de atributos:

- a) El orden relativo de atributos normalizados es intrascendente.
- b) Cuando el valor de un atributo normalizado pueda ser una cadena numérica o una cadena imprimible equivalente, la elección entre ellas se considerará intrascendente.

NOTA 1 – Esta regla se aplica incluso al atributo normalizado nombre-país cuando la elección entre las formas X.121 o ISO 3166 se considere irrelevante. Cuando en X.121 se asignen a un país más de un número, la relevancia del número utilizado no ha sido normalizada en esta Especificación.

- c) Cuando el valor de un atributo normalizado puede ser una cadena imprimible, una cadena teletex, una cadena universal o una combinación de estos tipos, la elección entre las siete posibilidades se considerará intrascendente.
- d) Cuando el tipo o valor de un atributo definido por el dominio, o el valor de un atributo normalizado conste de caracteres del repertorio de cadena imprimible, la elección que se permita entre su codificación en una cadena universal o una cadena teletex y una cadena imprimible se considerará intrascendente.
- e) Cuando el tipo o valor de un atributo definido por el dominio o el valor de un atributo normalizado comprende caracteres del repertorio de cadena teletex, la elección que se permita entre su codificación en una cadena teletex y en una cadena universal se considerará intrascendente.
- f) Cuando el valor de un atributo normalizado pueda contener letras, los tipos de esas letras se considerarán intrascendentes.
- g) En un tipo o valor de atributo definido por el dominio o en un valor de atributo normalizado, todos los espacios precedentes, todos los espacios subsiguientes y todos los intermedios consecutivos menos uno, se considerarán intrascendentes.
- h) En una cadena teletex el carácter gráfico de subrayado no espaciador se considerará intrascendente, así como todas las funciones de control excepto el espacio y las utilizadas para los procedimientos de ampliación de código.
- i) En una cadena teletex, la elección entre diferentes codificaciones del mismo carácter se considerará intrascendente.
- j) En una cadena universal, la elección entre diferentes codificaciones del mismo carácter (por ejemplo, el orden en el cual se codifican los componentes de los caracteres compuestos) se considerará intrascendente.

NOTA 2 – Un MD puede imponer reglas de equivalencia adicionales a los atributos que asigna a sus propios usuarios y DL. Podría definir, por ejemplo, reglas relativas a los caracteres de puntuación en los valores de atributos, el tipo de las letras de tales atributos o el orden relativo de los atributos definidos por el dominio.

18.5 Formas de direcciones OR

Todo usuario o DL tiene asignadas una o más direcciones OR. Una dirección OR es una lista de atributos que distingue a un usuario de otro e identifica el punto de acceso del usuario al MHS o al punto de ampliación de la DL.

Una dirección OR puede tomar alguna de las formas que, de manera resumida, se indican en el cuadro 10. En la primera columna de este cuadro se da una relación de los atributos disponibles para la elaboración de direcciones OR. Para cada forma de dirección OR, la segunda columna indica los atributos que pueden aparecer en estas direcciones OR y sus grados (véase también 18.6).

El cuadro tiene cuatro secciones. Los tipos de atributos de la primera son los de carácter general, los de la segunda y la tercera son específicos de la entrega física, pero una dirección postal no formatada puede utilizarse como ampliación de la dirección terminal. La cuarta sección comprende los atributos definidos por el dominio.

Cuadro 10 – Formas de direcciones OR

Tipo de atributo	Formas de direcciones-OR				
	MNEM	NUMR	POSTAL		
			F	U	TERM
+- General -----+					
nombre-dominio-administración	M	M	M	M	C
nombre-común	C	-	-	-	C*
nombre-país	M	M	M	M	C
dirección-red	-	-	-	-	M
identificador-usuario-numérico	-	M	-	-	-
nombre-organización	C	-	-	-	C*
nombres-unidades-organizativas	C	-	-	-	C*
nombre-personal	C	-	-	-	C*
nombre-dominio-privado	C	C	C	C	C
identificador-terminal	-	-	-	-	C
tipo-terminal	-	-	-	-	C
+- Encaminamiento postal -----+					
nombre-servicio-entrega-física	-	-	C	C	-
nombre-país-entrega-física	-	-	M	M	-
código-postal	-	-	M	M	-
+- Direccionamiento postal -----+					
componentes-ampliación	-	-	C	-	-
-dirección-OR-postal	-	-	C	-	-
componentes-ampliación	-	-	C	-	-
-dirección-entrega-física	-	-	C	-	-
atributos-postales-locales	-	-	C	-	-
nombre-oficina-entrega-física	-	-	C	-	-
número-oficina-entrega-física	-	-	C	-	-
nombre-organización-entrega-física	-	-	C	-	-
nombre-personal-entrega-física	-	-	C	-	-
dirección-apartado-correos	-	-	C	-	-
dirección-lista-correos	-	-	C	-	-
dirección-calle	-	-	C	-	-
dirección-postal-no-formatada	-	-	-	M	C*
nombre-postal-exclusivo	-	-	C	-	-
+- Definido por el dominio -----+					
definido-por-dominio (uno o más)	C	C	-	-	C
+- Leyenda -----+					
MNEM	nemotécnica	NUMR	numérica	POST	postal
F	formatada	U	no formatada	M	obligatoria
C*	Condicionales, pero concebidas para utilizarse con fines de reproducción y no para el direccionamiento o el encaminamiento del MHS				

Las formas de direcciones OR, expuestas de manera resumida en el cuadro, se definen y describen individualmente en los puntos que siguen. En el anexo F se describe la representación de direcciones OR para utilización humana.

18.5.1 Dirección OR nemotécnica

Dirección OR nemotécnica es la que proporciona una identificación memorable de un usuario o una DL. Identifica a un MD y a un usuario o una DL relativos a éste.

Una dirección OR nemotécnica consta de los siguientes atributos:

- a) un nombre-país, un nombre-dominio-administración, y de manera condicional, un nombre-dominio-privado, que juntos identifican a un MD;
- b) un nombre-organización, o un nombres-unidades-organizativas, o un nombre-personal o nombre-común, o uno o más atributos definidos por el dominio, o una combinación de los anteriores que, conjuntamente, identifican a un usuario o una DL relativos al MD mencionado en el apartado a). Si hay presentes nombres-unidades-organizativas, estará entonces presente el nombre-organización.

18.5.2 Dirección OR numérica

Dirección OR numérica es una dirección que identifica numéricamente a un usuario relativo a un MD.

Una dirección OR numérica consta de los siguientes atributos:

- a) un nombre-país, un nombre-dominio-administración y, de manera condicional, un nombre-dominio-privado, que conjuntamente identifican a un MD;
- b) un identificador-usuario-numérico, que identifica al usuario relativo al MD mencionado en el apartado a);
- c) de manera condicional, uno o más atributos definidos por el dominio que proporcionan información adicional a la de identificación del usuario.

NOTA – Sólo el identificador-usuario-numérico está obligado a ser numérico.

18.5.3 Dirección OR postal

Dirección OR postal es una dirección que identifica a un usuario por su dirección postal. Identifica al servicio de entrega física a través del cual ha de accederse al usuario y da la dirección postal del mismo.

Se distinguen las siguientes clases de direcciones OR postales:

- a) *formatada*: dirección OR postal que especifica la dirección postal de un usuario mediante varios atributos. Para esta forma de dirección OR postal, la presente Especificación prescribe, con cierto detalle, la estructura de direcciones postales;
- b) *no formatada*: dirección OR postal que especifica una dirección postal de un usuario en un solo atributo. Para esta forma de dirección OR postal, la presente Especificación no prescribe mayormente la estructura de las direcciones postales.

Una dirección OR postal, tanto si es *formatada* como si no lo es, consta de los siguientes atributos:

- a) un nombre-país, un nombre-dominio-administración y de manera condicional, un nombre-dominio-privado, que juntos identifican a un MD;
- b) de manera condicional, un nombre-servicio-entrega-física, que identifica al servicio de entrega física mediante el cual se accede al usuario;
- c) un nombre-país-entrega-física y un código-postal que juntos identifican la zona geográfica en la que el usuario recibe la entrega de mensajes físicos.

Una dirección OR postal *formatada* comprende, además, un ejemplar de cada uno de los atributos de direccionamiento postal condicionales que necesita el PDS y cuya relación figura en el cuadro 10.

Una dirección OR postal *formatada* no contiene el atributo de dirección-postal-no-formatada.

NOTA – El número total de caracteres de los valores de todos los atributos, excepto nombre-país, nombre-dominio-administración y nombre-servicio-entrega-física, en una dirección OR postal, deberá ser lo bastante reducido para permitir su reproducción en seis líneas de 30 caracteres, que es el tamaño de una ventanilla de sobre típica. El algoritmo de reproducción es específico de la PDAU, pero es probable que incluya delimitadores de inserción (por ejemplo, espacios) entre algunos de los valores de atributos.

18.5.4 Dirección OR terminal

Dirección OR terminal es una dirección que identifica un usuario mediante la dirección de red y, si es preciso, el tipo de su terminal. También puede identificar el MD a través del cual se accede a ese terminal. En el caso de un terminal telemático, da la dirección de red del terminal y, posiblemente, su identificador y tipo de terminal. En el caso de un terminal télex, da su número de télex.

Una dirección OR terminal consta de los siguientes atributos:

- a) una dirección-red;
- b) de manera condicional, un identificador-terminal;
- c) de manera condicional, un tipo-terminal;

ISO/CEI 10021-2:2004 (S)

- d) de manera condicional, un nombre-país y un nombre-dominio-administración y en ciertas condiciones un nombre-dominio-privado que juntos identifican un MD;
- e) de manera condicional, uno o más atributos elegidos del nombre-organización, nombres-unidades-organizativas, nombre-personal, dirección postal no formatada y nombre-común y, condicionalmente asimismo, uno o más atributos definidos por el dominio, todos los cuales proporcionan información adicional para identificar al usuario.

Los atributos de nombre-dominio-privado y definido por el dominio sólo estarán presentes si también lo están los de nombre-dominio-administración y nombre-país.

18.5.5 Determinación de las formas de dirección

La forma de una dirección OR se determinará de la manera siguiente:

- si contiene un identificador-usuario-numérico, es una dirección OR numérica;
- si contiene una dirección-red, es una dirección OR terminal;
- si contiene un país-entrega-física, es una dirección OR postal;
- cualquier otra dirección OR es una dirección OR nemotécnica.

Si una dirección OR postal contiene una dirección-postal-no formatada, es una dirección OR postal no formatada, y en todos los demás casos es una dirección OR postal formatada.

18.6 Atributos condicionales

La presencia o ausencia en una dirección OR particular, de los atributos señalados como condicionales en el cuadro 10, se determina según los criterios que a continuación se exponen.

Todos los atributos condicionales, excepto los específicos de las direcciones OR postales, figuran en una dirección OR a discreción del MD indicado por los atributos nombre-país, nombre-dominio-administración y, si estuviera presente, nombre-dominio-privado, y de acuerdo con las reglas establecidas por él.

Todos los atributos condicionales específicos de las direcciones OR postales están presentes o ausentes en tales direcciones OR, de modo que se satisfagan las exigencias de direccionamiento postal de los usuarios a los que identifican.

19 Encaminamiento

Versión UIT-T:

Para transportar un mensaje, sonda o informe a un usuario o al punto de ampliación de una DL, un MTA debe, no sólo localizar el usuario o la DL (es decir obtener su dirección OR), sino también seleccionar un encaminamiento hacia esa ubicación.

El encaminamiento externo es un proceso incremental y sólo vagamente normalizado. A continuación se sugieren algunos principios para el encaminamiento externo. El interno queda fuera del alcance de esta Recomendación.

Estos principios son ilustrativos, y no son definitivos:

- a) En un MHS que conste de un único MD, la cuestión del encaminamiento, naturalmente, no se plantea.
- b) Un PRMD puede estar conectado a un único ADMD. Cuando esto ocurre, el encaminamiento implica necesariamente al ADMD.
- c) Un ADMD puede estar conectado a múltiples PRMD. Si éste es el caso, el encaminamiento puede basarse en atributos de dirección OR condicionales, incluyendo el de nombre-dominio-privado, pero sin limitarse a él.
- d) Un MD puede estar conectado directamente a algunos otros MD, pero no a todos. Cuando la dirección OR identifica a un MD con el que no existe conexión directa, el encaminamiento se puede basar en un acuerdo bilateral con los MD con los que sí existen conexiones directas, y en otras reglas locales.
- e) Cuando el MD está conectado directamente al MD identificado por la dirección OR, el objeto es encaminado, por sistema, directamente a ese MD.
- f) Por acuerdo bilateral, un MD podría encaminar un objeto a otro MD a efectos de, por ejemplo, conversión.

- g) Un MD puede encaminar a una dirección OR mal formada siempre que, naturalmente, contenga por lo menos los atributos requeridos para ello.

NOTA – Los acuerdos bilaterales y las reglas locales a que se ha aludido anteriormente, quedan fuera del alcance de esta Recomendación, y pueden estar basados en consideraciones de tipo técnico, político o económico, o de otra clase.

Versión ISO/CEI:

Para transportar un mensaje, sonda o informe hacia un usuario o hacia el punto de ampliación de una DL, un MTA no solamente debe localizar dicho usuario o DL (es decir, obtener su dirección OR) sino también debe seleccionar una ruta hacia esa localización. El encaminamiento es pues el proceso de seleccionar, conocida una dirección OR, el MTA al cual debe transferirse el mensaje, sonda o informe.

Esta cláusula tiene un carácter instructivo: Rec. UIT-T X.412 |ISO/CEI 10021-10 normaliza los mecanismos para la distribución y el empleo de la información requerida para las decisiones que afectan al encaminamiento. La Rec. UIT-T X.404 | ISO/IEC TR 10021-11 se dan indicaciones a los gestores de sistemas de mensajería sobre la utilización de estos mecanismos de encaminamiento.

Cuando no haya que atender a otras condiciones, el encaminamiento óptimo consistirá en transferir el mensaje lo más directamente posible al MTA al cual se conecta el UA del destinatario. No obstante, pueden darse factores en favor del empleo de una ruta indirecta, tales como la existencia de rutas menos directas que utilicen enlaces de mayor anchura de banda entre los MTA, o el empleo de una ramificación tardía para lograr la optimización de los costos de la transmisión, o la necesidad de acceder a un MTA intermedio para un servicio de conversión, por ejemplo. El coste que conlleva la distribución y el almacenamiento de la información de encaminamiento, combinado posiblemente con el hecho de que la estructura interna de algunos dominios no debe descubrirse, determina que, con frecuencia, el encaminamiento directo al MTA final no sea posible, aun cuando pudiera ser deseable.

La primera parte de la decisión de encaminamiento que compete al MTA determina si el destinatario está o no en su propio MD. Para realizarlo, el MTA debe conocer todas las combinaciones de los atributos nombre-país, nombre-dominio-administración y nombre-dominio-privado que identifican su propio dominio. Un PRMD puede poseer tantas de estas combinaciones como puntos de entrada desde los ADMD haya en ese PRMD, si bien para los PRMD comprendidos enteramente en países que adopten nombres-dominio-privado exclusivos de la nación bastará un único par de valores de nombre-país y nombre-dominio-privado para identificar el PRMD en cuestión de manera interna, con independencia de que se permita o no la ausencia semántica del nombre-dominio-administración en los puntos de entrada de los ADMD.

Si el destinatario se identifica como comprendido en el mismo MD, se examinan los valores de otros atributos de la dirección OR del destinatario para determinar si éste es un UA servido por ese MTA, en cuyo caso se produciría una entrega local, o bien si puede identificarse dentro del MD un MTA apropiado al cual pueda retransmitirse el mensaje. Si una y otra posibilidad fallan, se producirá un evento de no entrega.

No todos los MTA comprendidos en un MD han de ser necesariamente configurados con la capacidad de retransmitir o recibir desde otros MD, pero por lo menos uno de los MTA del MD deberá poseer tales capacidades con el fin de que el MD no se quede aislado de los demás MD. Todo MTA comprendido en un MD (no aislado) ha de poder realizar el encaminamiento hacia un MTA de ese mismo MD que sea capaz de retransmitir hacia otros MD, en caso de que él mismo carezca de tal capacidad. De este modo, aun cuando el destinatario se identifique como exterior al MD, puede todavía necesitarse la retransmisión a otro MTA del mismo MD.

Si una vez identificado el MD exterior se encuentra que existe conexión directa al mismo, se utilizará entonces con frecuencia esa conexión directa. También puede resultar que el MD exterior se alcance mediante la retransmisión a través de uno o varios MD intermedios. Si estos MD intermedios fueran PRMD, la opción solamente podría llevarse a cabo mediante un acuerdo bilateral. Otra posibilidad es que el MD exterior sea desconocido, en cuyo caso se requerirán los servicios de un ADMD.

El papel de un ADMD dentro del MHS es el de proporcionar, directa o indirectamente, retransmisión a todos los demás ADMD, y retransmitir mensajes a todos los PRMD conectados directamente a ese ADMD. De este modo un PRMD siempre tiene la facultad de elegir el uso de los servicios de un ADMD para el encaminamiento hacia otros PRMD.

Cuando se identifique más de un punto de entrada a un MD exterior, es posible valerse de atributos de dirección OR adicionales o de otras consideraciones para determinar cuál sea el punto de entrada más apropiado. En el caso extremo de que el MD originador tenga información completa acerca del MD del destinatario, ello permitiría la comunicación directa entre el MTA del originador y el MTA del destinatario.

SECCIÓN 5 – USO DEL DIRECTORIO

20 Visión de conjunto

En esta sección se describen los usos que el MHS puede hacer del directorio, cuando se dispone de él. Si el MHS no dispone de directorio, la manera según la cual realiza las mismas tareas, si es que las realiza, es un asunto local.

La sección comprende los siguientes temas:

- a) autenticación;
- b) resolución de nombres;
- c) ampliación de DL;
- d) evaluación de capacidades.

21 Autenticación

Un objeto funcional puede efectuar la autenticación utilizando información almacenada en el directorio.

22 Resolución de nombres

Un objeto funcional puede llevar a cabo la resolución de nombres utilizando el directorio.

Un objeto que posee el nombre de directorio de un usuario o de una DL y cuya dirección o direcciones OR desea obtener, presenta ese nombre al directorio y pide los siguientes atributos de la inscripción en el directorio del objeto:

- a) *direcciones OR del MHS;*
- b) *métodos de entrega preferidos.*

Para hacerlo de manera satisfactoria, el objeto debe primero autenticarse él mismo al directorio, y tener derechos de acceso a la información solicitada.

El objeto funcional intenta seguidamente determinar una dirección OR que satisfaga a un método de entrega preferido. Para otros métodos que no sean la entrega-MHS, el objeto funcional tal vez necesite construir una dirección utilizando otros atributos obtenidos de la información de inscripción en el directorio y de configuración local.

23 Ampliación de DL

Un objeto funcional puede llevar a cabo la ampliación de una DL utilizando el directorio, previa verificación de que existen los permisos de depósitos necesarios.

El objeto presenta el nombre de directorio de una DL al directorio y solicita los siguientes atributos de la inscripción en el directorio del objeto:

- a) *miembros de DL del MHS;*
- b) *política de DL del MHS;*
- c) *permisos de depósito de DL del MHS.*

Para hacerlo de manera satisfactoria, el MTA debe primero autenticarse él mismo al directorio, y tener derechos de acceso a la información solicitada.

24 Evaluación de capacidades

Un objeto funcional puede evaluar las capacidades de un usuario de DL o MS utilizando el directorio.

Los atributos de directorio siguientes representan capacidades de usuario de posible importancia en el tratamiento de mensajes:

- a) *tipos de contenido entregables del MHS;*
- b) *EIT entregables del MHS;*
- c) *longitud de contenido máximo del MHS;*

- d) *direcciones OR del MHS con capacidades;*
- e) *EIT no entregables del MHS;*
- f) *métodos de entrega preferidos.*

Los atributos de directorio siguientes representan capacidades de MS de posible importancia en el tratamiento de mensajes:

- a) *atributos soportados por el MHS;*
- b) *acciones automáticas soportadas por el MHS;*
- c) *tipos de contenido soportados por el MHS;*
- d) *reglas de concordancia soportadas por el MHS.*

Para evaluar determinada capacidad de un usuario de DL o MS cuyo nombre de directorio posee, el objeto presenta ese nombre al directorio y pide los atributos asociados a esa capacidad, que figuran en la inscripción en el directorio del objeto.

Para hacerlo de manera satisfactoria, el MTA debe primero autenticarse él mismo al directorio y tener derechos de acceso a la información solicitada.

SECCIÓN 6 – REALIZACIÓN POR OSI

25 Visión de conjunto

En esta sección se describe cómo se realiza el MHS por medio de la OSI.

La sección comprende los siguientes temas:

- a) elementos de servicio de aplicación;
- b) contextos de aplicación.

26 Elementos de servicio de aplicación

En esta cláusula se identifican los elementos de servicio de aplicación (ASE) que figuran en la realización mediante OSI del tratamiento de mensajes.

En la OSI, las capacidades de comunicación de sistemas abiertos se organizan en grupos de capacidades relacionadas, llamados ASE. En la presente cláusula, se examina este concepto, a partir del modelo de referencia OSI, se establece una distinción entre ASE *simétricos* y *asimétricos* y se presentan los ASE definidos para el tratamiento de mensajes o que le sirven de soporte.

NOTA – El MHS depende no sólo de los ASE examinados, sino también del elemento de servicio de acceso al directorio, definido en la Rec. UIT-T X.519 | ISO/CEI 9594-5. Sin embargo, como este ASE no figura en los AC para tratamiento de mensajes (véase la Rec. UIT-T X.419 | ISO/CEI 10021-6), no se analiza aquí.

26.1 El concepto de ASE

La figura 12 ilustra el concepto de ASE. En ella se representan de manera esquemática dos sistemas abiertos en comunicación. Sólo se muestran las partes de los sistemas abiertos relacionados con la OSI, a las que se llama entidades de aplicación (AE). Cada AE consta de un UE y de uno o más ASE. El UE representa la parte organizativa o de control de una AE, que define el cometido del sistema abierto (por ejemplo, el de un MTA). Por su parte, un ASE representa uno de los conjuntos de capacidad de comunicaciones, o servicios (por ejemplo, depósito o transferencia de mensajes), que el UE necesita para desempeñar su cometido.

A la relación entre dos AE en sistemas abiertos diferentes se le llama asociación de aplicación. Los ASE de un sistema abierto se comunican con sus ASE pares del otro a través de una conexión de presentación entre ellos. Esa comunicación es la que crea y mantiene la relación inherente a la asociación de aplicación. Para que varios ASE se combinen de manera satisfactoria en una única AE, deben estar diseñados de manera que coordinen su utilización de la asociación de aplicación.

Un ASE desempeña el papel, en gran medida mecánico, de trasladar las peticiones formuladas por su UE, y las respuestas, a y desde la forma dictada por el protocolo de aplicación que gobierna la interacción del ASE con su ASE par del sistema abierto al que la asociación le conecta. El ASE efectúa un servicio, o una parte del mismo, abstracto, a efectos de comunicación de la OSI (véanse las cláusulas 28-30).

NOTA – En sentido estricto, el papel de un sistema abierto viene determinado por el comportamiento de sus procesos de aplicación. En el contexto del tratamiento de mensajes, un proceso de aplicación realiza un objeto funcional de uno de los tipos definidos en la cláusula 7. A su vez, un UE es una parte de un proceso de aplicación.

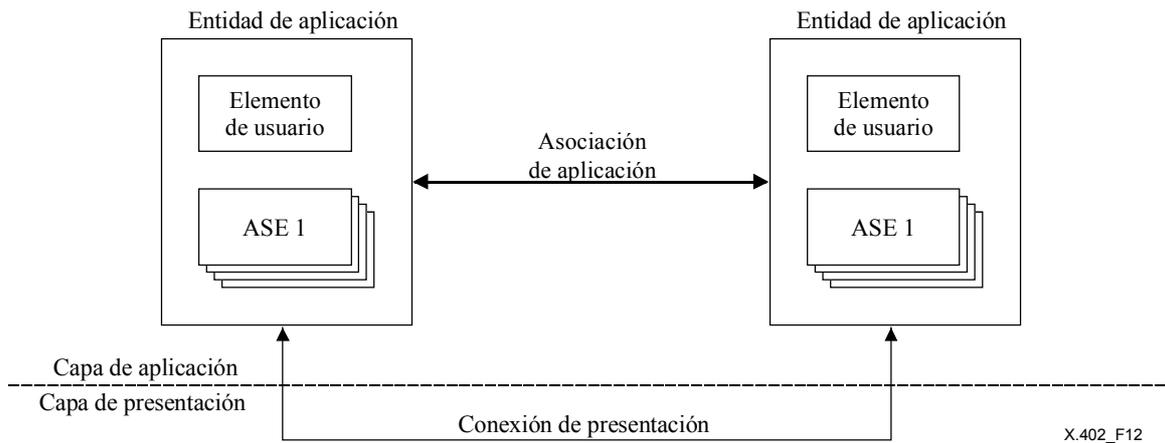


Figura 12 – El concepto de ASE

26.2 ASE simétricos y asimétricos

Cabe distinguir los siguientes dos tipos de ASE, ilustrados en la figura 13:

- a) **simétrico**: ASE por medio del cual un UE suministra y consume un servicio. El ASE para transferencia de mensajes, por ejemplo, es simétrico, porque ambos sistemas abiertos, cada uno de los cuales incorpora un MTA, ofrece y puede consumir por medio de él el servicio de transferencia de mensajes;
- b) **asimétrico**: ASE por medio del cual un UE suministra o consume un servicio, pero no ambas cosas, dependiendo de cómo esté configurado el ASE. El ASE para entrega de mensajes, por ejemplo, es asimétrico, porque sólo el sistema abierto que incorpora un MTA ofrece el servicio asociado, y sólo el otro sistema abierto, que incorpora un AU o una MS, lo consume.

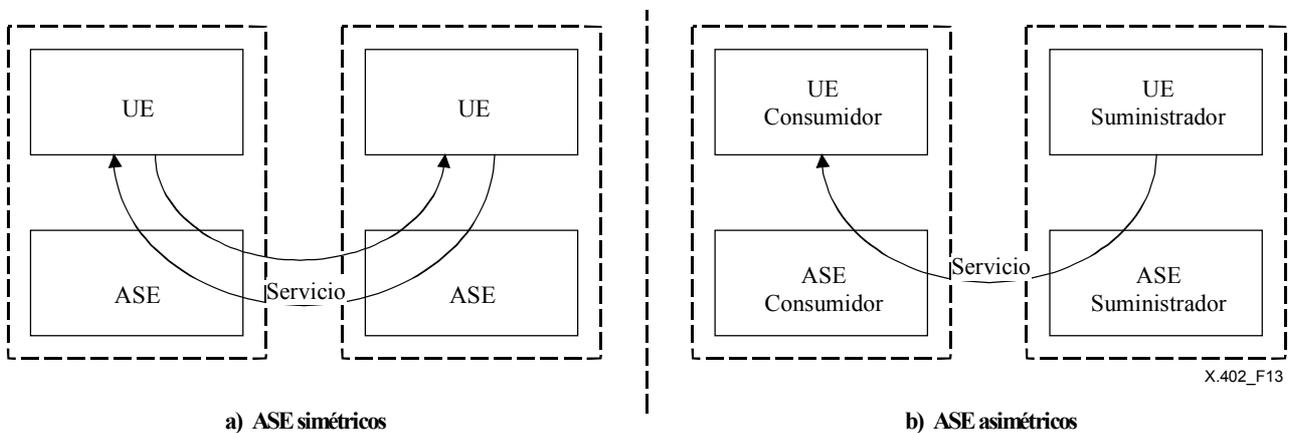


Figura 13 – ASE simétricos y asimétricos

Con respecto a un determinado ASE asimétrico, un UE suministra un servicio que el otro consume. Los ASE, coubicados con los UE, ayudan en el suministro y consumo del servicio. Los cuatro papeles resultantes se muestran en la figura 14, con la siguiente terminología:

- a) UE suministrador de *x*: Proceso de aplicación que suministra el servicio representado por el ASE asimétrico *x*.
- b) ASE suministrador de *x*: ASE asimétrico *x* configurado para combinación con un UE suministrador de *x*.
- c) UE consumidor de *x*: Proceso de aplicación que consume el servicio representado por el ASE asimétrico *x*.
- d) ASE consumidor de *x*: ASE asimétrico *x* configurado para coubicación con un UE consumidor de *x*.

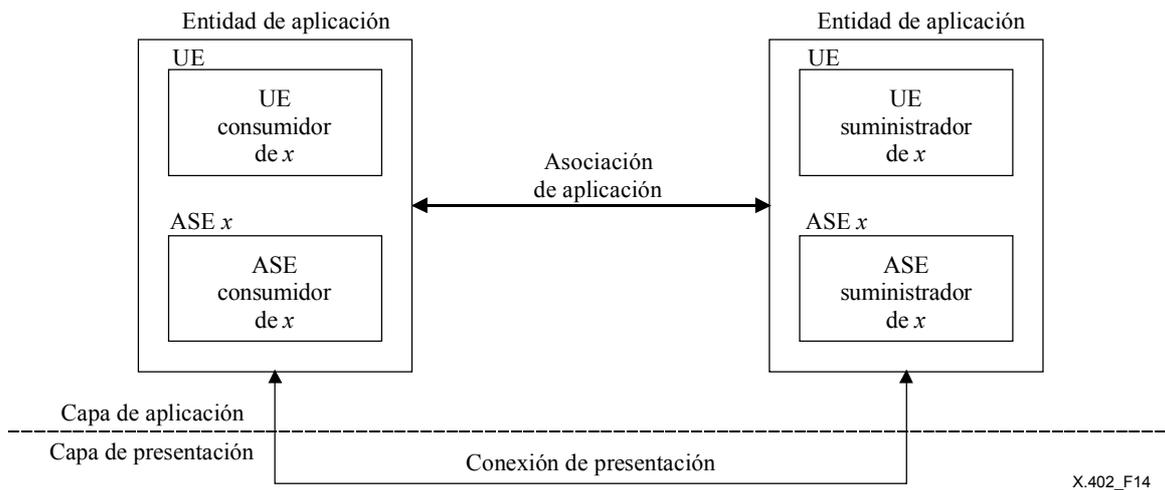


Figura 14 – Terminología para ASE asimétricos

Como se ha indicado, los cuatro papeles descritos anteriormente están definidos en relación con un determinado ASE. Cuando una AE consta de varios ASE asimétricos, estos papeles se asignan independientemente a cada ASE. Así, tal como se muestra en la figura 15, un único UE podría servir como consumidor con respecto a un ASE y como proveedor con respecto a otro.

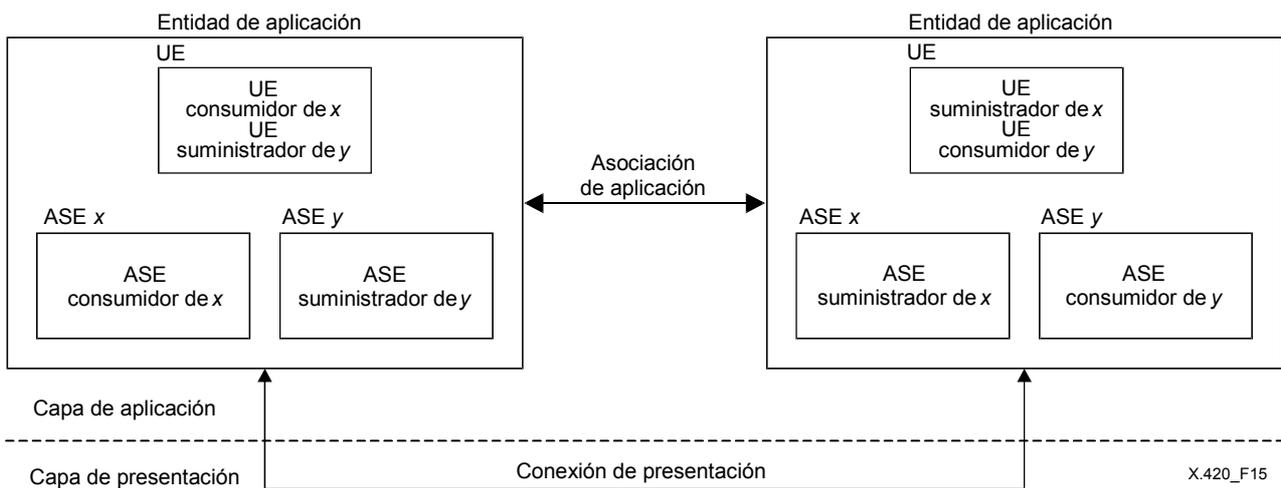


Figura 15 – ASE asimétricos múltiples

26.3 ASE de tratamiento de mensajes

En la primera columna del cuadro 11 figura la lista de los ASE que proporcionan los diversos servicios del tratamiento de mensajes. Para cada ASE de la primera columna, se indica en la segunda si es simétrico o asimétrico. La tercera columna identifica los objetos funcionales –UA, MS, MTA y AU– que están asociados al ASE, como consumidores o como proveedores.

Cuadro 11 – ASE de tratamiento de mensajes

		Objetos funcionales			
ASE	Forme	UA	MS	MTA	AU
MTSE	SY	-	-	CS	-
MSSE	ASY	C	CS	S	-
MDSE	ASY	C	C	S	-
MRSE	ASY	C	S	-	-
MASE	ASY	C	CS	S	-

Legend	
SY	symmetric C consumer
ASY	asymmetric S supplier

Los ASE de tratamiento de mensajes, resumidos en el cuadro, se presentan por separado en las subcláusulas que siguen. En la Rec. UIT-T X.419 | ISO/CEI 10021-6 figuran sus definiciones.

26.3.1 Transferencia de mensajes

El elemento de servicio transferencia de mensajes (MTSE, *message transfer service element*) es el medio por el cual se efectúa el paso de transmisión de transferencia.

26.3.2 Depósito de mensajes

El elemento de servicio depósito de mensajes (MSSE, *message submission service element*) es el medio por el cual se efectúa el paso de transmisión de depósito.

26.3.3 Entrega de mensajes

El elemento de servicio entrega de mensajes (MDSE, *message delivery service element*) es el medio por el cual se efectúa el paso de transmisión de entrega.

26.3.4 Recuperación de mensajes

El elemento de servicio recuperación de mensajes (MRSE, *message retrieval service element*) es el medio por el cual se efectúa el paso de transmisión de extracción.

26.3.5 Administración de mensajes

El elemento de servicio de administración de mensajes (MASE, *message administration service element*) es el medio por el cual un UA, una MS o MTA archiva, en cada uno de los otros dos, la información que facilita y controla su interacción subsiguiente, mediante el MSSE, el MDSE, el MRSE y el MASE.

26.4 ASE de soporte

En la primera columna del cuadro 12 figura la lista de los ASE de uso general, de los que dependen los ASE de tratamiento de mensajes. Para cada ASE de la primera columna, se indica en la segunda si es simétrico o asimétrico.

Cuadro 12 – ASE de soporte

ASE	Forma
ROSE	SY
RTSE	SY
ACSE	SY

Leyenda	
SY	simétrico
ASY	asimétrico

Los ASE de soporte, resumidos en el cuadro 12, se presentan por separado en las subcláusulas que siguen.

26.4.1 Operaciones distantes

El elemento de servicio de operaciones a distancia (ROSE, *remote operations service element*) es el medio por el cual, los ASE asimétricos de tratamiento de mensajes, estructuran sus interacciones de petición-respuesta, entre sistemas abiertos consumidores y suministradores.

El ROSE se define en la Rec. UIT-T X.880 | ISO/CEI 13712-1.

26.4.2 Transferencia fiable

El elemento de servicio transferencia fiable (RTSE, *reliable transfer service element*) es el medio por el cual diversos ASE de tratamiento de mensajes, simétricos y asimétricos, transportan objetos de información –especialmente grandes (por ejemplo, mensajes facsimil)– entre sistemas abiertos, de modo que se garantice su almacenamiento seguro en sus destinos.

El RTSE se define en la Rec. UIT-T X.218 e ISO/CEI 9066-1.

26.4.3 Control de asociación

El elemento de servicio control de asociación (ACSE, *association control service element*) es el medio por el cual se establecen, se liberan y, en otros aspectos, se gestionan todas las asociaciones de aplicación entre sistemas abiertos.

El ACSE se define en la Rec. UIT-T X.217 | ISO/CEI 8649.

27 Contextos de aplicación

En la OSI, las capacidades de comunicación (es decir, los ASE) de dos sistemas abiertos son gobernados, para un fin determinado, mediante contextos de aplicación (AC). Un AC es una especificación detallada del empleo de una asociación entre dos sistemas abiertos, es decir, un protocolo.

Un AC especifica cómo debe establecerse la asociación (por ejemplo, qué parámetros de inicialización se deben intercambiar), qué ASE deben participar en una comunicación entre pares a través de la asociación, qué limitaciones han de imponerse (si es que se impone alguna) a su utilización individual de la asociación, si el consumidor de cada ASE asimétrico es el iniciador o el contestador y cómo ha de liberarse la asociación (por ejemplo, qué parámetros de finalización se deben intercambiar).

Todo AC tiene asignado un nombre (un identificador de objeto ASN.1). El iniciador de una asociación indica al contestador cuál es el AC que dirigirá el uso de la asociación, haciéndole llegar el nombre del AC por medio del ACSE.

Un AC identifica también con un nombre (un identificador de objeto ASN.1) las sintaxis abstractas de las APDU que puede llevar una asociación, como resultado de su utilización por los ASE del AC. De manera convencional, se asigna un nombre bien al conjunto de las APDU asociadas a cada ASE individual o bien al AC como un todo. El iniciador de una asociación indica al contestador la o las sintaxis abstractas, enviándole sus nombres por medio del ACSE.

La sintaxis abstracta de una APDU es su estructura como objeto de información (por ejemplo, un conjunto ASN.1 que comprenda un código de instrucción entero y un argumento de instrucción cadena IA5). Se diferencia de la sintaxis de transferencia de la APDU, que es como se representa el objeto de información para transmisión entre dos sistemas abiertos (por ejemplo, un octeto indicando un conjunto ASN.1, seguido por un octeto que dé la longitud del conjunto, etc.).

Los AC, por medio de los cuales se proporcionan los diversos servicios de tratamiento de mensajes, se especifican en la Rec. UIT-T X.419 | ISO/CEI 10021-6. A estos protocolos (P, *protocols*) se les conoce por P1, P3 y P7.

NOTA – La naturaleza del contenido de un mensaje no entra en la definición del AC de tratamiento de mensajes, porque el contenido queda englobado (como una cadena de octetos) en los protocolos que lo transportan.

SECCIÓN 7 – CONVENIOS SOBRE DEFINICIÓN DEL SERVICIO ABSTRACTO

28 Visión de conjunto

Al describir una tarea compleja de tratamiento de información distribuida, hay ciertas ventajas en especificar la tarea de una manera abstracta en lugar de recurrir a términos concretos. Este planteamiento garantiza que los requisitos funcionales de la tarea se enuncian con independencia de la realización concreta. Además de permitir que la especificación se prepare a través de un proceso de refinamiento escalonado, esta separación es importante ya que cada aspecto de la tarea puede admitir varias realizaciones concretas. Por ejemplo, en un sistema de transferencia de mensajes que comprenda tres agentes de transferencia de mensajes, el primero y el segundo podrían interactuar mediante comunicación OSI, y el segundo y el tercero hacerlo por medios de carácter propio.

En esta sección se especifican los convenios para efectuar la descripción abstracta de los servicios que proporciona una tarea de tratamiento de información distribuida, es decir, el servicio abstracto, mediante el empleo de un modelo abstracto. Se describe también la realización del servicio abstracto por medio de los servicios de comunicación OSI.

NOTA – Esta sección sustituye y anula la sección relativa a convenios para la definición del servicio abstracto de la Rec. CCITT X.407 (1988) | ISO/CEI 10021-3:1990.

La Rec. UIT-T X.880 | ISO/CEI 13712-1 define varias clases de objetos de información que son de utilidad en la especificación de protocolos de aplicación basados en el servicio de operaciones a distancia (ROS, *remote operation service*), tales como los que se han definido para el MHS.

29 Componentes del modelo abstracto**29.1 Objetos abstractos**

Un objeto abstracto (objeto MHS) es una entidad funcional, posiblemente una entre varias que interactúan entre sí. Un objeto abstracto de un tipo podría representar un sistema, cuyos usuarios vendrían representados por múltiples objetos abstractos de otro tipo. Los objetos abstractos sólo interactúan cuando están vinculados conjuntamente en una asociación que define los servicios ofrecidos y el contexto de su interacción en términos de un contrato abstracto.

Un objeto MHS se especifica como un caso de la clase de objeto de información MHS-object. Su definición es idéntica a la de clase de objeto de información ROS-OBJECT-CLASS de operaciones a distancia (ROS). Las capacidades de un objeto abstracto se definen con respecto a los contratos (de asociación) a los que presta apoyo como iniciador, contestador o en uno y otro papel.

MHS-OBJECT ::= ROS-OBJECT-CLASS

29.2 Contratos abstractos

Un contrato abstracto (en adelante, contrato) define un contexto dentro del cual pueden interactuar un par de objetos abstractos. Incluye una especificación de la manera en que dos objetos abstractos establecen una asociación (vinculan), liberan la asociación (desvinculan), e identifica los puertos abstractos vinculados entre sí mientras perdura la asociación. Al especificar un contrato, se identifican los puertos en los que el iniciador de la asociación asume el papel de "consumidor", los puertos en los que dicho iniciador asume el papel de "suministrador" y los puertos que, o bien son simétricos o en los cuales el iniciador de la asociación puede desempeñar tanto el papel de "consumidor" como el de "suministrador".

Un contrato se define como un caso de la clase de objeto de información CONTRACT de operaciones a distancia.

29.3 Paquetes de conexión

Un paquete de conexión especifica la parte del contrato que se refiere al establecimiento y liberación dinámica de una asociación. Especifica la operación de vinculación abstracta que sirve para establecer la asociación y la operación de desvinculación abstracta utilizada para liberarla.

Un paquete de conexión se define como un caso de la clase de objeto de información CONNECTION-PACKAGE de operaciones a distancia.

29.4 Puertos abstractos

Un puerto abstracto (en adelante, puerto) es un punto en el cual un objeto abstracto interactúa con otro objeto abstracto cuando se encuentran vinculados según los términos de un contrato. Define el conjunto de operaciones que pueden ser invocadas por un objeto abstracto que asume el papel de "consumidor", las operaciones que pueden ser invocadas por un objeto abstracto que asume el papel de "suministrador" y las operaciones que pueden ser invocadas por uno y otro objeto abstracto.

Se define un puerto como simétrico si todos los casos posibles del puerto son idénticos (es decir, cuando no cabe distinción entre los papeles de consumidor y suministrador). Un puerto se define como asimétrico si cada caso de puerto es de uno de los dos tipos, suministrador o consumidor, esto es, si hay distinción entre los papeles.

Un puerto se especifica como un caso de la clase de objeto de información PORT. Su definición es idéntica a la clase de objeto de información OPERATION-PACKAGE de operaciones a distancia.

```
PORT ::= OPERATION-PACKAGE
```

29.5 Operaciones abstractas y errores abstractos

Una operación abstracta es un procedimiento que un objeto abstracto (el invocador) puede solicitar de otro (el ejecutor) en un par de puertos vinculados según los términos de un contrato. Si los puertos son simétricos, uno u otro objeto abstracto puede invocar la operación. Pero si los puertos son asimétricos, la definición del puerto prescribirá qué operaciones pueden ser invocadas por el objeto abstracto que actúe como consumidor del puerto, y cuáles pueden ser invocadas por el objeto abstracto que actúe como suministrador.

Un error abstracto es una condición excepcional que puede ocurrir durante la ejecución de una operación abstracta, causando el fallo de la misma. Cuando se notifica un error abstracto, el ejecutor transporta al invocador la identidad del error abstracto y posiblemente un único objeto de información llamado parámetro del mismo.

Las operaciones abstractas y los errores abstractos se especifican como casos de las clases de objetos de información ABSTRACT-OPERATION y ABSTRACT-ERROR.

Sus definiciones son, respectivamente, idénticas a las de las clases de objetos de información OPERATION y ERROR de operaciones a distancia.

```
ABSTRACT-OPERATION ::= OPERATION
```

```
ABSTRACT-ERROR ::= ERROR
```

30 Realización de ROS (servicio de operaciones a distancia)

Una vez que se ha descrito y especificado en términos abstractos una tarea de tratamiento de información distribuida, debe prescribirse la manera en la que debe realizarse concretamente cada aspecto de la tarea. Cada uno de tales aspectos puede admitir varias realizaciones concretas.

La realización concreta de los componentes del servicio abstracto MHS suele carecer de importancia cuando se ejecuta por medio de las operaciones a distancia. Esto se debe a que, para un servicio abstracto determinado, existe un protocolo de aplicación basado en operaciones a distancia (ROS) que es funcionalmente idéntico a él. Ello es consecuencia de que el marco que encuadra las especificaciones de los servicios abstractos es isomorfo con el de las especificaciones de protocolos de aplicación ROS. Las correspondencias que soportan este isomorfismo se señalan en el cuadro 13.

Cuadro 13 – Correspondencia entre componentes de servicio abstracto y clases de objetos de información ROS

Componente de servicio abstracto	Clase de objeto de información ROS
MHS-object	ROS-OBJECT-CLASS
Port	OPERATION-PACKAGE
Abstract-operation	OPERATION
Abstract-error	ERROR

Las clases de objeto de información ROS CONTRACT y CONNECTION-PACKAGE se utilizan directamente en el modelo abstracto MHS.

Anexo A

Clases de objetos de directorio y atributos

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

Varias clases de objetos de directorio, atributos, sintaxis de atributos, contextos y nombres alternativos de sujeto de certificado son específicos del tratamiento de mensajes. Se definen en el presente anexo utilizando las clases de objetos de información OBJECT-CLASS, ATTRIBUTE y CONTEXT de la Rec. UIT-T X.501 | ISO/CEI 9594-2 las clases de objeto de información OTHER-NAME de la Rec. UIT-T X.509 | ISO/CEI 9594-8, respectivamente.

A.1 Clases de objetos

A continuación se especifican las clases de objetos del tratamiento de mensajes.

NOTA – Las clases de objetos de directorio descritos en este anexo pueden combinarse con otras clases de objetos, por ejemplo, los definidos en la Rec. UIT-T X.521 | ISO/CEI 9594-7. En la cláusula 12 de la Rec. UIT-T X.501 | ISO/CEI 9594-2 figura una explicación del modo en que pueden combinarse las clases de objetos de directorio en una inscripción de directorio. El anexo B de la Rec. UIT-T X.521 | ISO/CEI 9594-7 da más información sobre las formas de nombres de directorio y posibles estructuras de árboles de informaciones de directorio.

A.1.1 Lista de distribución del MHS

Un objeto **lista de distribución del MHS** es una DL. Los atributos de su inscripción identifican su nombre común, permisos de depósito y direcciones OR y, en la medida en que están presentes los atributos, describen la DL, identifican a su organización, sus unidades organizativas y su propietario, mencionan objetos conexos, identifican su longitud de contenido máxima, tipos de contenido entregable y EIT aceptables, exclusivamente aceptables e inaceptables; e identifican su política de expansión, direcciones de suscripción, direcciones de archivo, listas conexas y miembros.

```

mhs-distribution-list OBJECT-CLASS ::= {
  SUBCLASS OF { top }
  MUST CONTAIN { commonName |
                mhs-dl-submit-permissions |
                mhs-or-addresses }
  MAY CONTAIN { description |
               organizationName |
               organizationalUnitName |
               owner |
               seeAlso |
               mhs-maximum-content-length |
               mhs-deliverable-content-types |
               mhs-acceptable-eits |
               mhs-exclusively-acceptable-eits |
               mhs-unacceptable-eits |
               mhs-dl-policy |
               mhs-dl-subscription-service |
               mhs-dl-archive-service |
               mhs-dl-related-lists |
               mhs-dl-members }
  ID id-oc-mhs-distribution-list }

```

A.1.2 Memoria de mensajes del MHS

Un objeto **memoria de mensajes del MHS** es una AE que realiza una MS. Los atributos de su inscripción, en la medida en que estén presentes, describen la MS, identifican a su propietario y enumeran los atributos, las acciones automáticas, las reglas de concordancia, los tipos de contenido y la información de protocolo que facilita.

```

mhs-message-store OBJECT-CLASS ::= {
  SUBCLASS OF { applicationEntity }
  MAY CONTAIN { owner |
               mhs-supported-attributes |
               mhs-supported-automatic-actions |
               mhs-supported-matching-rules |
               mhs-supported-content-types |
               protocolInformation }
  ID id-oc-mhs-message-store }

```

A.1.3 Agente de transferencia de mensajes del MHS

Un objeto **agente de transferencia de mensajes del MHS** es una AE que pone en ejecución un MTA. Los atributos de su inscripción, en la medida que estén presentes, describen el MTA e identifican a su propietario, la longitud de contenido máxima y la información de protocolo.

```
mhs-message-transfer-agent OBJECT-CLASS ::= {
    SUBCLASS OF    { applicationEntity }
    MAY CONTAIN    { owner |
                    mhs-maximum-content-length |
                    protocolInformation }
    ID             id-oc-mhs-message-transfer-agent }
```

A.1.4 Usuario del MHS

Un objeto **usuario del MHS** es un usuario genérico del MHS. (El usuario genérico del MHS puede tener, por ejemplo, una dirección comercial, o una dirección privada, o ambas.) Los atributos de su inscripción identifican la dirección OR del usuario y, en la medida en que están presentes, los atributos pertinentes identifican la longitud del contenido entregable del usuario, tipos de contenido EIT, su MS y sus métodos de entrega preferidos.

```
mhs-user OBJECT-CLASS ::= {
    SUBCLASS OF    { top }
    KIND           auxiliary
    MUST CONTAIN   { mhs-or-addresses }
    MAY CONTAIN    { mhs-maximum-content-length |
                    mhs-deliverable-content-types |
                    mhs-acceptable-eits |
                    mhs-exclusively-acceptable-eits |
                    mhs-unacceptable-eits |
                    mhs-or-addresses-with-capabilities |
                    mhs-message-store-dn }
    ID             id-oc-mhs-user }
```

Si el usuario del MHS posee más de una dirección OR, que tienen diferentes capacidades de entregabilidad, los atributos tipos de contenido entregable del MHS, EIT entregables del MHS y EIT no entregable de MHS, deberían representar la unión de las capacidades de entregabilidad; el atributo longitud de contenido máximo del MHS debería contener los valores mayores de este atributo. La capacidad de cada dirección OR se puede determinar entonces cuando sea necesario a partir del atributo direcciones OR con capacidades del MHS.

NOTA – La información de método de entrega preferido (preferredDeliveryMethod) del usuario del MHS es heredada en el juego de atributos de telecomunicaciones (telecommunicationAttributeSet) de la clase de objeto denominación del usuario del directorio.

A.1.5 Agente de usuario del MHS

Un objeto **agente de usuario del MHS** es una AE que realiza un UA. Los atributos de su inscripción, en la medida en que están presentes, identifican al propietario del UA, su longitud de contenido máxima, tipos de contenido y EIT; sus clases entregables; su dirección OR; y los protocolos de red soportados.

```
mhs-user-agent OBJECT-CLASS ::= {
    SUBCLASS OF    { applicationEntity }
    MAY CONTAIN    { owner |
                    mhs-maximum-content-length |
                    mhs-deliverable-content-types |
                    mhs-acceptable-eits |
                    mhs-exclusively-acceptable-eits |
                    mhs-unacceptable-eits |
                    mhs-deliverable-classes |
                    mhs-or-addresses |
                    protocolInformation }
    ID             id-oc-mhs-user-agent }
```

A.2 Atributos

Los atributos específicos del tratamiento de mensajes son los que se indican a continuación.

A.2.1 EIT aceptables del MHS

El atributo **EIT aceptables del MHS** identifica un conjunto de EIT; la presencia de cualquiera de estos EIT en un mensaje compone un mensaje cuya entrega aceptará un usuario, o que ampliará una DL, como se define en 8.4.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. El orden de precedencia entre este atributo y los indicados en A.2.10 y A.2.19 se define en 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

ISO/CEI 10021-2:2004 (S)

Un valor de este atributo es un identificador de objeto.

```
mhs-acceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedEncodedInformationType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-acceptable-eits }
```

A.2.2 Clases entregables del MHS

El atributo **clases entregables del MHS** identifica las clases de mensajes cuya entrega aceptará un UA (véase 8.4.1.1.3 en la Rec. UIT-T X.411 | ISO/CEI 10021-4).

Un valor de este atributo es una capacidad (véase A.3.4).

```
mhs-deliverable-classes ATTRIBUTE ::= {
    WITH SYNTAX                Capability
    EQUALITY MATCHING RULE     capabilityMatch
    ID                          id-at-mhs-deliverable-classes }
```

A.2.3 Tipos de contenido entregable del MHS

El atributo **tipos de contenido entregable del MHS** identifica los tipos de contenido de los mensajes cuya entrega aceptará un usuario, o que ampliará una DL. La ausencia de este atributo indica que cualquier tipo de contenido puede ser entregado (o ampliado).

Un valor de este atributo es un identificador de objeto.

```
mhs-deliverable-content-types ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedContentType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-deliverable-content-types }
```

A.2.4 Servicio de archivo de DL del MHS

El atributo **servicio de archivo de DL del MHS** identifica un servicio al cual puede solicitar un usuario copias de los mensajes que hayan sido distribuidos anteriormente por esa DL. Una especificación más detallada de un servicio de este tipo (por ejemplo, el formato de las peticiones) queda fuera del alcance de esta Norma Internacional.

Un valor de este atributo es un nombre OR.

```
mhs-dl-archive-service ATTRIBUTE ::= {
    WITH SYNTAX                ORName
    EQUALITY MATCHING RULE     ORNameExactMatch
    -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
    --                            ORNameSubstringElementsMatch |
    --                            ORNameSingleElementMatch }--
    ID                          id-at-mhs-dl-archive-service }
```

A.2.5 Miembros del DL del MHS

El atributo **miembros del DL del MHS** identifica los miembros de una DL. Cuando una DL se amplía, cada uno de los valores de este atributo se convertirá en destinatario del mensaje.

Un valor de este atributo es un nombre OR.

```
mhs-dl-members ATTRIBUTE ::= {
    WITH SYNTAX                ORName
    EQUALITY MATCHING RULE     ORNameExactMatch
    -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
    --                            ORNameSubstringElementsMatch |
    --                            ORNameSingleElementMatch }--
    ID                          id-at-mhs-dl-members }
```

Un valor de este atributo puede tener una anotación adjunta para proporcionar información para la utilización en la administración de DL (véase A.4.1), o puede tener una indicación adjunta de que este miembro es él mismo una DL para permitir una evaluación eficiente del permiso de depósito de DL (véase A.4.2), o puede tener una indicación adjunta de que este miembro utiliza un sistema no normalizado (véase A.4.3).

A.2.6 Política de DL del MHS

El atributo **política de DL del MHS** identifica las diversas opciones de política que pueden aplicarse para ampliar una DL.

Un valor de este atributo es una política de DL.

```

mhs-dl-policy ATTRIBUTE ::= {
    WITH SYNTAX                DLPolicy
    SINGLE VALUE                TRUE
    ID                          id-at-mhs-dl-policy }

```

A.2.7 Listas relacionadas con DL del MHS

El atributo **listas relacionadas con DL del MHS** identifica otras listas de distribución que, de algún modo no especificado, se relacionan con esta DL.

Un valor de este atributo es un nombre distinguido.

```

mhs-dl-related-lists ATTRIBUTE ::= {
    SUBTYPE OF                distinguishedName
    EQUALITY MATCHING RULE    distinguishedNameMatch
    ID                          id-at-mhs-dl-related-lists }

```

A.2.8 Permisos de depósito de DL del MHS

El atributo **permisos de depósito de DL del MHS** identifica los usuarios y las DL que pueden depositar mensajes (o sondas) a una DL. No afecta al tratamiento de informes en los puntos de ampliación de la DL.

Un valor de este atributo es un permiso de depósito de DL.

```

mhs-dl-submit-permissions ATTRIBUTE ::= {
    WITH SYNTAX                DLSubmitPermission
    ID                          id-at-mhs-dl-submit-permissions }

```

A.2.9 Servicio de suscripción a DL del MHS

El atributo **servicio de suscripción a DL del MHS** identifica un servicio al cual un usuario puede solicitar la suscripción a una DL (es decir, pasar a ser miembro de la misma). Una especificación más detallada de un servicio de este tipo (por ejemplo, el formato de las peticiones) cae fuera del ámbito de esta Norma Internacional.

Un valor de este atributo es un nombre OR.

```

mhs-dl-subscription-service ATTRIBUTE ::= {
    WITH SYNTAX                ORName
    EQUALITY MATCHING RULE    oRNameExactMatch
    -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
    --                            oRNameSubstringElementsMatch |
    --                            oRNameSingleElementMatch }--
    ID                          id-at-mhs-dl-subscription-service }

```

A.2.10 EIT exclusivamente aceptables del MHS

Los atributos **EIT exclusivamente aceptables del MHS** identifican un conjunto de EIT; la presencia de todos los EIT de un mensaje dentro de este conjunto conforman un mensaje cuya entrega aceptará un usuario, o que ampliará una DL, como se define en 8.4.1.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. El orden de precedencia entre este atributo y los indicados en A.2.1 y A.2.19 se define en 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

NOTA – Se puede efectuar conversión implícita en el MTS antes de la entrega de un mensaje, de modo tal que cualquier EIT presentado finalmente en el mensaje, pero no entre los EIT exclusivamente aceptables, puede ser convertido en un EIT exclusivamente aceptable, permitiendo así la entrega (o ampliación de la DL).

Un valor de este atributo es un identificador de objeto.

```

mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedEncodedInformationType
    EQUALITY MATCHING RULE    objectIdentifierMatch
    ID                          id-at-mhs-exclusively-acceptable-eits }

```

A.2.11 Longitud de contenido máxima del MHS

El atributo **longitud de contenido máxima del MHS** identifica la longitud máxima del contenido de los mensajes cuya entrega aceptará un usuario, ampliará una DL o aceptará un MTA.

ISO/CEI 10021-2:2004 (S)

Un valor de este atributo es un entero.

```
mhs-maximum-content-length ATTRIBUTE ::= {
    WITH SYNTAX                ContentLength
    EQUALITY MATCHING RULE     integerMatch
    SINGLE VALUE               TRUE
    ID                          id-at-mhs-maximum-content-length }
```

A.2.12 Nombre de directorio memoria de mensajes del MHS

El atributo **nombre de directorio memoria de mensajes del MHS** identifica una MS de usuario por nombre.

El valor de este atributo es un nombre distinguido de directorio.

```
mhs-message-store-dn ATTRIBUTE ::= {
    SUBTYPE OF                 distinguishedName
    EQUALITY MATCHING RULE     distinguishedNameMatch
    SINGLE VALUE               TRUE
    ID                          id-at-mhs-message-store-dn }
```

A.2.13 Direcciones OR del MHS

El atributo **direcciones OR del MHS** especifica las direcciones OR de un usuario o de una DL. El usuario del directorio puede elegir cualquiera de los valores para utilizarlo como la dirección OR de este usuario.

Un valor de este atributo es una dirección OR.

```
mhs-or-addresses ATTRIBUTE ::= {
    WITH SYNTAX                ORAddress
    EQUALITY MATCHING RULE     oRAddressMatch
    -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch |
    --                           oRAddressSubstringElementsMatch |
    --                           oRNameSingleElementMatch } --
    ID                          id-at-mhs-or-addresses }
```

Cuando en una inscripción está presente el atributo direcciones OR del MHS con capacidades, el atributo direcciones OR del MHS deberá contener la dirección preferida del usuario.

A.2.14 Direcciones OR con capacidades del MHS

El atributo **direcciones OR con capacidades del MHS** identifica la capacidad de entregabilidad de cada una de las direcciones OR de un usuario.

Un valor de este atributo es una dirección OR con capacidades.

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
    WITH SYNTAX                AddressCapabilities
    EQUALITY MATCHING RULE     addressCapabilitiesMatch
    ID                          id-at-mhs-or-addresses-with-capabilities }
```

Ese atributo se puede utilizar para indicar las capacidades individuales de cada dirección OR de usuario cuando direcciones diferentes tienen capacidades que difieren. Se puede utilizar también cuando una misma dirección tiene, por ejemplo, capacidades que difieren para diferentes tipos de contenido. Cuando no hay capacidades que difieren de las que el usuario requiere distinguir, es suficiente el atributo direcciones OR del MHS solamente.

A.2.15 Atributos permitidos por el MHS

El atributo **atributos permitidos por el MHS** identifica los atributos que permite totalmente una MS.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-attributes ATTRIBUTE ::= {
    WITH SYNTAX                ATTRIBUTE.&id({AttributeTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-attributes
}
```

A.2.16 Acciones automáticas permitidas por el MHS

El atributo **acciones automáticas permitidas por el MHS** identifica las acciones automáticas que una MS soporta totalmente.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
    WITH SYNTAX                AUTO-ACTION.&id ({AutoActionTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-automatic-actions }
```

A.2.17 Tipos de contenido soportados por el MHS

El atributo **tipos de contenido soportados por el MHS** identifica los tipos de contenido de los mensajes cuya sintaxis y semántica soporta totalmente una MS.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-content-types ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedContentType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-content-types }
```

A.2.18 Reglas de concordancia soportadas por el MHS

El atributo **reglas de concordancia soportadas por el MHS** identifica las reglas de concordancia que una MS soporta totalmente.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-matching-rules ATTRIBUTE ::= {
    WITH SYNTAX                MATCHING-RULE.&id ({MatchingRuleTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-matching-rules }
```

A.2.19 EIT no aceptables del MHS

El atributo **EIT no aceptable del MHS** identifica un conjunto de EIT; la presencia de cualquiera de estos EIT en un mensaje conforma un mensaje cuya entrega no aceptará un usuario o no ampliará una DL, como se define en 8.4.1.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. El orden de precedencia entre este atributo y los indicados en A.2.1 y A.2.10 se define en 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

NOTA – Se puede efectuar conversión implícita en el MTS antes de la entrega de un mensaje, de modo tal que cualquier EIT originalmente presente en el mensaje, pero entre los EIT no aceptables, puede ser convertido en un EIT aceptable, permitiendo así la entrega (o ampliación de la DL).

Un valor de este atributo es un identificador de objeto.

```
mhs-unacceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedEncodedInformationType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-unacceptable-eits }
```

A.3 Sintaxis de atributos

Las sintaxis de atributos específicos del tratamiento de mensajes son las que se indican a continuación.

A.3.1 Permiso de depósito de DL

La sintaxis de atributo **permiso de depósito de DL del MHS** caracteriza un atributo, cada uno de cuyos valores es un permiso de depósito.

```
DLSubmitPermission ::= CHOICE {
    individual          [0] ORName,
    member-of-dl       [1] ORName,
    pattern-match      [2] ORNamePattern,
    member-of-group    [3] Name }
```

ISO/CEI 10021-2:2004 (S)

Un permiso de depósito de DL concede, dependiendo de su tipo, acceso de presentación a los cero o más usuarios y listas de distribución siguientes:

- a) *Individual*: Usuario o DL (no ampliada) alguno de cuyos nombres OR es igual al nombre OR especificado.
- b) *Miembro-de-dl*: Cada miembro de la DL, o de cada DL jerarquizada de manera recurrente, alguno de cuyos nombres OR es igual al nombre OR especificado.
- c) *Concordancia-de-esquemas*: Cada usuario o DL (no ampliada) alguno de cuyos nombres OR satisface el esquema de nombres OR especificado.

ORNamePattern ::= ORName

La presencia de un esquema de nombres OR vacío (es decir, un ORName que contenga una secuencia vacía de atributos normalizados incorporados) indica que cualquier usuario tiene permiso de depósito.

```
any-user-may-submit DLSubmitPermission ::=  
    pattern-match: { built-in-standard-attributes { } }
```

- d) *Miembro-de-grupo*: Cada miembro de grupo-de-nombres, o de cada grupo-de-nombres jerarquizado, de manera recurrente, cuyo nombre está especificado.

Se considera que un valor presentado es igual a un valor objetivo de este tipo si los dos son idénticos, atributo por atributo. Además, se puede declarar igualado en otras condiciones, que son asunto local.

A.3.1.1 Procedimiento para evaluar el permiso de depósito de DL

Cuando se utiliza el atributo permiso de depósito de DL del MHS para determinar si un determinado mensaje puede ser ampliado por una DL, se aplica el procedimiento que se expone a continuación. Si el mensaje contiene una historia de ampliaciones en DL, el nombre OR de la última DL que figura en la historia de ampliaciones se compara con los valores del atributo permiso de depósito, y en todos los demás casos es el nombre OR del originador del mensaje el que se compara.

La comparación se realiza sucesivamente con cada valor del atributo hasta que se produce la primera concordancia, mediante la cual el mensaje ha obtenido permiso de depósito, o hasta haber agotado los valores del atributo con los que se compara, sin haber logrado el mensaje obtener permiso de depósito.

NOTA – El directorio no mantiene ninguna ordenación de los valores del atributo. Se conseguirá habitualmente una mayor eficiencia considerando los valores *concordancia-de-esquemas*, más cortos, al principio, y seguidamente los valores *individual*.

Para cada valor del atributo se aplica el procedimiento apropiado que seguidamente se indica:

- a) *Individual*
El nombre OR procedente del mensaje se compara con el nombre OR de este valor del atributo mediante el procedimiento especificado en A.3.1.2.
- b) *Miembro-de-dl*
Este valor del atributo es el nombre OR de una DL. Se obtienen los miembros de la DL del MHS de esa DL. Si algún nombre OR de un miembro carece de un componente de dirección OR, se obtiene éste del atributo direcciones OR del MHS procedente de la inscripción de ese miembro en el directorio. El nombre OR procedente del mensaje se compara sucesivamente con el nombre OR de cada uno de los miembros aplicando el procedimiento especificado en A.3.1.2 hasta que se produce una concordancia.
Si no se encuentra ninguna concordancia se realiza una revisión del directorio en el nombre OR de cada miembro para determinar si es en sí mismo otra DL. Para cada DL jerarquizada que se encuentre se aplica repetidamente el procedimiento señalado para *miembro-de-dl*.
- c) *Concordancia-de-esquemas*
Este valor del atributo contiene elementos de un nombre OR: puede contener algunos componentes de dirección OR, o algunos componentes RDN de un nombre de directorio, o componentes de ambas clases. Si el valor del atributo es un esquema de nombre OR vacío, existe permiso de depósito para cualquier usuario.
Se construye un nombre OR que no contiene ningún tipo de atributos que estén ausentes del esquema mediante la eliminación de otros atributos del nombre OR procedente del mensaje. Este nombre OR así construido se compara con el nombre OR del esquema obtenido de este valor del atributo por medio del procedimiento especificado en la regla de concordancia-de-elementos-de-nombre-OR en 12.4.5 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

d) *Miembro-de-grupo*

Este valor del atributo es el nombre de directorio de un grupo de nombres (véase 6.10 en ISO/CEI 9594-7). Se obtienen los miembros de ese grupo de nombres y se construye un nombre OR para cada dirección OR de cada uno de los miembros a partir del nombre de directorio de ese miembro más el atributo direcciones OR del MHS del mismo miembro. Se compara sucesivamente el nombre OR procedente del mensaje con el nombre OR de cada miembro siguiendo el procedimiento señalado en A.3.1.2 hasta que se produce una concordancia.

Si no se encuentra concordancia, se realiza una revisión del directorio en el nombre de directorio de cada miembro para determinar si es en sí mismo otro grupo de nombres. Para cada grupo de nombres jerarquizado que se encuentre se aplica repetidamente el procedimiento indicado para *miembro-de-grupo*.

En el caso de que un miembro de una DL o un grupo tenga más de un valor presente en el atributo direcciones OR del MHS de ese miembro, se construye un nombre OR separado para cada dirección OR.

A.3.1.2 Procedimiento para determinar la equivalencia de nombres OR

El nombre OR procedente del mensaje contiene siempre una dirección OR y puede contener además un nombre de directorio. El nombre OR obtenido del atributo puede incluir un nombre de directorio, una dirección OR, o ambos a la vez; la dirección OR estará presente si también lo está en el valor del atributo o si puede obtenerse del directorio para miembros de DL o grupos.

Los nombres OR se comparan utilizando la regla de concordancia-de-nombres-OR definida en 12.4.4 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

A.3.2 Política de DL

La sintaxis del atributo **política de DL** caracteriza un atributo cuyo valor expresa una política.

```
DLPolicy ::= SET {
    report-propagation [0] INTEGER {
        previous-dl-or-originator (0),
        dl-owner (1),
        both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,
    report-from-dl [1] INTEGER {
        whenever-requested (0),
        when-no-propagation (1) } DEFAULT whenever-requested,
    originating-MTA-report [2] INTEGER {
        unchanged (0),
        report (2),
        non-delivery-report (3),
        audited-report (4) } DEFAULT unchanged,
    originator-report [3] INTEGER {
        unchanged (0),
        no-report (1),
        report (2),
        non-delivery-report (3) } DEFAULT unchanged,
    return-of-content [4] ENUMERATED {
        unchanged (0),
        content-return-not-requested (1),
        content-return-requested (2) } DEFAULT unchanged,
    priority [5] INTEGER {
        unchanged (0),
        normal (1),
        non-urgent (2),
        urgent (3) } DEFAULT unchanged,
    disclosure-of-other-recipients [6] ENUMERATED {
        unchanged (0),
        disclosure-of-other-recipients-prohibited (1),
        disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,
    implicit-conversion-prohibited [7] ENUMERATED {
        unchanged (0),
        implicit-conversion-allowed (1),
        implicit-conversion-prohibited (2) } DEFAULT unchanged,
    conversion-with-loss-prohibited [8] ENUMERATED {
        unchanged (0),
        conversion-with-loss-allowed (1),
        conversion-with-loss-prohibited (2) } DEFAULT unchanged,
    further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,
    originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,
    proof-of-delivery [11] INTEGER {
        dl-expansion-point (0),
        dl-members (1),
        both (2),
        neither (3) } DEFAULT dl-members,
```

```

requested-delivery-method [12] CHOICE {
    unchanged [0] NULL,
    removed [1] NULL,
    replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,
token-encryption-algorithm-preference [13] SEQUENCE OF
    AlgorithmInformation OPTIONAL,
token-signature-algorithm-preference [14] SEQUENCE OF
    AlgorithmInformation OPTIONAL,
... }
AlgorithmInformation ::= SEQUENCE {
    algorithm-identifier [0] AlgorithmIdentifier,
    originator-certificate-selector [1] CertificateAssertion OPTIONAL,
    recipient-certificate-selector [2] CertificateAssertion OPTIONAL}

```

Una política de DL puede especificar valores para las opciones siguientes:

- a) *Propagación de informe*: Decide si los informes recibidos en el punto de ampliación de la DL han de ser enviados a la DL precedente (o al originador si no hubiera DL precedente), o al propietario de la DL, o a los dos.
- b) *Informe procedente de DL*: Decide si el punto de ampliación de la DL envía un informe confirmativo de la entrega siempre que amplíe un mensaje que solicite tal informe, o si los informes de este tipo únicamente son enviados cuando la propagación del informe es propietario-de-dl o cuando el informe-del-originador es la ausencia de informe (no-informe) o informe-de-no-entrega.
- c) *Informe del MTA de origen*: Decide si la petición de informe del MTA no se modifica, o si se solicitan sendos informes de entrega y de no entrega, o se solicitan informes de no entrega únicamente, o informes de entrega verificados.
- d) *Informe del originador*: Decide si la petición de informe del originador no se modifica, o si no se solicita informe alguno o se solicitan sendos informes de entrega y de no entrega o se solicitan únicamente informes de no entrega.
- e) *Devolución de contenido*: Decide si la petición de devolución de contenido del originador no se modifica, o si no se solicita devolución, o si se solicita devolución con los informes de no entrega.
- f) *Prioridad*: Decide si el tipo de prioridad establecido por el originador no se modifica, o si se fija en normal, en no urgente o en urgente.
- g) *Divulgación de otros destinatarios*: Decide si no se modifica lo establecido por el originador, o se fija en prohibir la divulgación o en permitir la divulgación.
- h) *Conversión implícita prohibida*: Decide si no se modifica lo establecido por el originador, o se fija en permitir la conversión implícita o en prohibir la conversión implícita.
- i) *Conversión con pérdida prohibida*: Decide si no se modifica lo establecido por el originador o se fija en permitir la conversión con pérdida o en prohibir la conversión con pérdida.
- j) *Nueva ampliación de DL permitida*: Decide si se permite o prohíbe la ampliación mediante cualquier DL jerarquizada.
- k) *Supresión de destinatario alternativo solicitado por el originador*: Decide si la designación de destinatario alternativo por el originador no se modifica o se suprime.
- l) *Generación de prueba de entrega*: Decide si la prueba de entrega, en caso de ser solicitada, es generada en el punto de ampliación de la DL o si lo es por los miembros de la DL, o por unos y otros, o si no es generada.
- m) *Método de entrega solicitado*: Decide si no se modifica lo establecido por el originador, o si se suprime o reemplaza por un valor especificado.
- n) *Preferencia de algoritmo de criptación de testigo*: Especifica el orden de preferencia de los algoritmos de criptación asimétricos a utilizar para recriptar datos para cada miembro de DL en un testigo, en el que el mensaje que se amplía contiene datos criptados en un testigo para el destinatario de DL;
- o) *Preferencia de algoritmo de signatura de testigo*: Especifica el orden de preferencia de los algoritmos de signatura a utilizar para signar datos cuando esto es necesario para crear un nuevo testigo para cada miembro de DL, por ejemplo, cuando el mensaje que se amplía contiene datos encriptados en un testigo-mensaje para el destinatario de DL.

En 14.3.10 de la Rec. UIT-T X.411 | ISO/CEI 10021-4 se dan más detalles de estas opciones de política.

A.3.3 Dirección OR

La sintaxis de una dirección OR se define en la Rec. UIT-T X.411 | ISO/CEI 10021-4, y su semántica en la cláusula 18 de esta Especificación.

Un valor de dirección OR presentado es igual a un valor de dirección OR objetivo en las condiciones especificadas en 18.4. Las reglas de concordancia para concordancia-de-direcciones-OR, concordancia-de-elementos-de-dirección-OR, concordancia-de-elementos-de-subcadenas-de-dirección-OR y concordancia de elementos-aislados-de-nombre-OR se definen en 12.4.1, 12.4.2, 12.4.3 y 12.4.7 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

A.3.4 Dirección OR con capacidades

La sintaxis del atributo dirección OR con capacidades caracteriza un atributo cuyo valor identifica la capacidad de entregabilidad de cada una de las direcciones OR de un usuario. Cuando una dirección ha de ser elegida automáticamente, la selección entre las direcciones que tienen las capacidades apropiadas es un asunto local. Cuando la selección la hace un usuario humano, la descripción puede permitir una elección más apropiada.

Un valor de este atributo es una dirección OR con capacidades.

```
AddressCapabilities ::= SEQUENCE {
    description GeneralString,
    address ORAddress,
    capabilities SET OF Capability }
Capability ::= SET {
    content-types [0] SET OF ExtendedContentType OPTIONAL,
    maximum-content-length [1] ContentLength OPTIONAL,
    encoded-information-types-constraints [2] EncodedInformationTypesConstraints
                                                OPTIONAL,
    security-labels [3] SecurityContext OPTIONAL,
    ... }
```

La regla de concordancia de capacidades de dirección determina si un valor presentado es idéntico a un valor de atributo de dirección OR con capacidades. Esta regla de concordancia es utilizada solamente para el mantenimiento del directorio.

```
addressCapabilitiesMatch MATCHING-RULE ::= {
    SYNTAX AddressCapabilities
    ID id-mr-address-capabilities-match }
```

La regla devuelve un valor *verdadero* si, y solamente si:

- a) los elementos de descripción contienen cadenas equivalentes;
- b) los elementos de dirección concuerdan según la regla concordancia-de-direcciones-OR definida en 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5; y
- c) los elementos de capacidad contienen componentes idénticos.

Teniendo en cuenta el carácter complejo del componente de capacidades, no se puede esperar que el directorio determine si un requisito de capacidad presentado podría ser satisfecho por un valor de atributo cualquiera. Se prevé, en consecuencia, que, todo los valores se obtengan a partir del directorio y que la evaluación la efectúe el usuario del directorio (por ejemplo, el MTA).

La regla concordancia de capacidades determina si un valor presentado es idéntico a un valor de atributo de clases entregables del MHS. Esta regla de concordancia sólo se utiliza para mantenimiento del directorio.

```
capabilityMatch MATCHING-RULE ::= {
    SYNTAX Capability
    ID id-mr-capability-match }
```

La regla devuelve un valor *verdadero* solamente si las capacidades contienen componentes equivalentes.

A.3.5 Nombre OR

La sintaxis de un nombre OR se define en la Rec. UIT-T X.411 | ISO/CEI 10021-4, y su semántica en la cláusula 17 de esta Especificación.

La regla concordancia-exacta-de-nombres-OR determina si tanto el nombre de directorio como las componentes de dirección OR de un nombre OR concuerdan. Cada componente debe concordar si está presente en el valor presentado o en el valor objetivo. Un valor de nombre OR presentado es igual a un valor de nombre OR objetivo si los componentes de dirección OR son equivalentes al aplicar las reglas especificadas en 18.4, y si los componentes de nombre de directorio son equivalentes en aplicación de las reglas especificadas en las Recomendaciones UIT-T de la serie X.500 | ISO/CEI 9594. Por añadidura, puede declararse la igualdad en otras condiciones que son un asunto local.

ISO/CEI 10021-2:2004 (S)

```
oRNameExactMatch MATCHING-RULE ::= {  
    SYNTAX    ORName  
    ID        id-mr-orname-exact-match }
```

La regla devuelve un valor *verdadero* únicamente en las condiciones siguientes:

- si el valor presentado no contiene más que una dirección OR, la regla sólo establece la concordancia con un valor de atributo sin nombre de directorio cuando la concordancia de dirección OR sigue la regla definida en 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5;
- si el valor presentado no contiene más que un nombre de directorio, la regla sólo establece la concordancia con un valor de atributo sin dirección OR cuando la concordancia de nombre de directorio sigue la regla de concordancia de nombre distinguido definida en 12.5.2 de la Rec. UIT-T X.501 | ISO/CEI 9594-2;
- si el valor presentado contiene a la vez una dirección OR y un nombre de directorio, la regla sólo establece la concordancia con un valor de atributo que contiene estos dos componentes cuando la concordancia de la dirección OR sigue la regla definida en 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5 y la concordancia del nombre de directorio sigue la regla definida en 12.5.2 de la Rec. UIT-T X.501 | ISO/CEI 9594-2.

NOTA – La regla concordancia-exacta-de-nombres-OR no exige una codificación idéntica de los valores presentado y objetivo.

Las reglas de concordancia para concordancia-de-nombres-OR, concordancia-de-elementos-de-nombre-OR, concordancia-de-elementos-de-subcadena-de-nombres-OR y concordancia-de-elementos-aislados-de-nombre-OR se definen en 12.4.4, 12.4.5, 12.4.6 y 12.4.7 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

A.4 Contextos

A continuación se describen los contextos específicos del tratamiento de mensajes.

A.4.1 Anotación de administrador DL

El contexto de anotación de administrador DL asocia un valor del atributo miembros de DL del MHS con una anotación textual asignada por el administrador DL y para uso de éste.

```
dl-administrator-annotation CONTEXT ::= {  
    WITH SYNTAX CHOICE{  
        bmpstring                BMPString,  
        universalstring           UniversalString}  
    ID id-con-dl-administrator-annotation
```

Se considera que un valor presentado concuerda con un valor almacenado si el valor presentado es una subcadena del valor almacenado.

```
    }  
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE                mhs-dl-members.&id OPTIONAL  
    CONTEXTS                      {dl-administrator-annotation} }
```

Se puede asociar una anotación textual con cada miembro del DL, y se utiliza solamente para que el administrador DL pueda asociar información con el miembro con el fin de asistir al administrador en la administración de DL. Esto puede ser útil, por ejemplo, cuando un valor de atributo miembros DL MSH omite el componente nombre de directorio y comprende solamente una dirección OR numérica.

A.4.2 DL anidada de DL

El contexto DL anidada de DL asocia un valor del atributo miembros MHS DL con una indicación de que este miembro es él mismo una DL.

```
dl-nested-dl CONTEXT ::= {  
    WITH SYNTAX                NULL  
    ID                          id-con-dl-nested-dl }  
  
dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE                mhs-dl-members.&id OPTIONAL  
    CONTEXTS                      {dl-nested-dl} }
```

Cuando este contexto está asociado con un valor de atributo miembros MHS DL, indica que el miembro es él mismo una DL (anidada). Este contexto puede ser añadido por un DUA administrativo para facilitar una evaluación eficiente de la opción permiso de depósito de DL miembro-de-DL.

A.4.3 Reiniciación de originador DL

El contexto reiniciación de originador DL asocia un valor del atributo miembros DL MSH con una indicación de que este miembro utiliza, o es alcanzado a través de, un sistema que no envía informes de entrega (no entrega) al último DL identificado en la historia de ampliación de DL (requerido de conformidad con X.400 ISO/CEI 10021).

```
dl-reset-originator CONTEXT ::= {
    WITH SYNTAX          NULL
    ID                   id-con-dl-reset-originator }

dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE      mhs-dl-members.&id
    OPTIONAL CONTEXTS  {dl-reset-originator} }
```

Cuando este contexto está asociado con un valor de atributo miembros DL MSH, si el elemento de propagación de informe de la política DL es propietario DL (solamente), cuando el punto de ampliación DL sustituye al originador en el sobre de la copia del mensaje para este miembro DL por el nombre OR del propietario DL. Esto puede ser útil, por ejemplo cuando este miembro DL utiliza un sistema conforme a X.400 (1984), o un sistema que utilice un protocolo que no sea X.400 | ISO/CEI 10021.

A.5 Nombres alternativos de sujeto de certificado

Las otras formas de nombre específicos del tratamiento de mensajes para su utilización en un campo de nombre alternativo de sujeto de certificado (véase 12.3.2.1 en la Rec. UIT-T X.509 | ISO/CEI 9594-8) son los que se especifican a continuación.

A.5.1 Nombre de MTA

El nombre alternativo nombre de MTA para un sujeto de certificado permite a una autoridad de certificación emitir certificados que contienen una vinculación certificada entre el nombre de MTA y la clave pública.

```
mta-name OTHER-NAME ::= { SEQUENCE {
    domain          GlobalDomainIdentifier,
    mta-name       MTAName }
    IDENTIFIED BY  id-san-mta-name }
```

Anexo B

Definición de referencia de identificadores de objetos

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

En este anexo se definen, a efectos de referencia, diversos identificadores de objetos mencionados en el módulo ASN.1 del anexo C. Se utiliza la ASN.1.

Todos los identificadores de objetos asignados por esta Especificación están asignados en el presente anexo. Este anexo es definitivo para todos, excepto para los de los módulos del ASN.1 y del propio MHS. Las asignaciones definitivas para el primero se producen en los mismos módulos; en las cláusulas IMPORT aparecen otras referencias a los mismos. El segundo es hijo.

```
MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0) object-identifiers(0)
                        version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
-- Prologue
```

```
-- Exports everything.
```

```
IMPORTS -- nothing -- ;
```

```
ID ::= OBJECT IDENTIFIER
```

```
-- MHS Aspects
```

```
id-mhs-protocols ID ::= {joint-iso-itu-t mhs(6) protocols (0)}
-- MHS Application Contexts and Protocols
-- See ITU-T Rec. X.419 | ISO/IEC 10021-6.
id-ipms ID ::= {joint-iso-itu-t mhs(6) ipms (1)}
-- Interpersonal Messaging
-- See ITU-T Rec. X.420 | ISO/IEC 10021-7.
-- Value {joint-iso-itu-t mhs(6) 2} is no longer defined
id-mts ID ::= {joint-iso-itu-t mhs(6) mts (3)}
-- Message Transfer System
-- See ITU-T Rec. X.411 | ISO/IEC 10021-4.
id-ms ID ::= {joint-iso-itu-t mhs(6) ms (4)}
-- Message Store
-- See ITU-T Rec. X.413 | ISO/IEC 10021-5.
id-arch ID ::= {joint-iso-itu-t mhs(6) arch (5)}
-- Overall Architecture
-- See this Specification.
id-group ID ::= {joint-iso-itu-t mhs(6) group (6)}
-- Reserved.
id-edims ID ::= {joint-iso-itu-t mhs(6) edims (7)}
-- EDI Messaging
-- See ITU-T Rec. X.435 | ISO/IEC 10021-9.
id-management ID ::= {joint-iso-itu-t mhs(6) management (9)}
-- MHS Management
-- See ITU-T Recs. X.460 — X.467 | ISO/IEC 11588.
id-routing ID ::= {joint-iso-itu-t mhs(6) routing (10)}
-- MHS Routing
-- See ITU-T Rec. X.412 | ISO/IEC 10021-10.
```

```
-- Categories
```

```
id-mod ID ::= {id-arch 0} -- modules; not definitive
id-oc ID ::= {id-arch 1} -- object classes
id-at ID ::= {id-arch 2} -- attribute types
-- Value {id-arch 3} is no longer defined
id-mr ID ::= {id-arch 4} -- matching rules
id-con ID ::= {id-arch 5} -- contexts
id-san ID ::= {id-arch 6} -- certificate subject alternative names
```

```
-- Modules
```

```
id-object-identifiers          ID ::= {id-mod 0} -- not definitive
id-directory-objects-and-attributes ID ::= {id-mod 1} -- not definitive
```

-- Object classes

```
id-oc-mhs-distribution-list      ID ::= {id-oc 0}
id-oc-mhs-message-store         ID ::= {id-oc 1}
id-oc-mhs-message-transfer-agent ID ::= {id-oc 2}
id-oc-mhs-user                  ID ::= {id-oc 3}
id-oc-mhs-user-agent            ID ::= {id-oc 4}
```

-- Attributes

```
id-at-mhs-maximum-content-length ID ::= {id-at 0}
id-at-mhs-deliverable-content-types ID ::= {id-at 1}
id-at-mhs-exclusively-acceptable-eits ID ::= {id-at 2}
id-at-mhs-dl-members             ID ::= {id-at 3}
id-at-mhs-dl-submit-permissions ID ::= {id-at 4}
id-at-mhs-message-store-dn       ID ::= {id-at 5}
id-at-mhs-or-addresses           ID ::= {id-at 6}
-- Value {id-at 7} is no longer defined
id-at-mhs-supported-automatic-actions ID ::= {id-at 8}
id-at-mhs-supported-content-types ID ::= {id-at 9}
id-at-mhs-supported-attributes ID ::= {id-at 10}
id-at-mhs-supported-matching-rules ID ::= {id-at 11}
id-at-mhs-dl-archive-service ID ::= {id-at 12}
id-at-mhs-dl-policy ID ::= {id-at 13}
id-at-mhs-dl-related-lists ID ::= {id-at 14}
id-at-mhs-dl-subscription-service ID ::= {id-at 15}
id-at-mhs-or-addresses-with-capabilities ID ::= {id-at 16}
id-at-mhs-acceptable-eits ID ::= {id-at 17}
id-at-mhs-unacceptable-eits ID ::= {id-at 18}
id-at-mhs-deliverable-classes ID ::= {id-at 19}
id-at-encrypted-mhs-maximum-content-length ID ::= {id-at 0 2}
id-at-encrypted-mhs-deliverable-content-types ID ::= {id-at 1 2}
id-at-encrypted-mhs-exclusively-acceptable-eits ID ::= {id-at 2 2}
id-at-encrypted-mhs-dl-members ID ::= {id-at 3 2}
id-at-encrypted-mhs-dl-submit-permissions ID ::= {id-at 4 2}
id-at-encrypted-mhs-message-store-dn ID ::= {id-at 5 2}
id-at-encrypted-mhs-or-addresses ID ::= {id-at 6 2}
id-at-encrypted-mhs-supported-automatic-actions ID ::= {id-at 8 2}
id-at-encrypted-mhs-supported-content-types ID ::= {id-at 9 2}
id-at-encrypted-mhs-supported-attributes ID ::= {id-at 10 2}
id-at-encrypted-mhs-supported-matching-rules ID ::= {id-at 11 2}
id-at-encrypted-mhs-dl-archive-service ID ::= {id-at 12 2}
id-at-encrypted-mhs-dl-policy ID ::= {id-at 13 2}
id-at-encrypted-mhs-dl-related-lists ID ::= {id-at 14 2}
id-at-encrypted-mhs-dl-subscription-service ID ::= {id-at 15 2}
id-at-encrypted-mhs-or-addresses-with-capabilities ID ::= {id-at 16 2}
id-at-encrypted-mhs-acceptable-eits ID ::= {id-at 17 2}
id-at-encrypted-mhs-unacceptable-eits ID ::= {id-at 18 2}
id-at-encrypted-mhs-deliverable-classes ID ::= {id-at 19 2}
```

-- Matching Rules

```
id-mr-orname-exact-match      ID ::= {id-mr 0}
id-mr-address-capabilities-match ID ::= {id-mr 1}
id-mr-capability-match        ID ::= {id-mr 2}
```

-- Contexts

```
id-con-dl-administrator-annotation ID ::= {id-con 0}
id-con-dl-nested-dl ID ::= {id-con 1}
id-con-dl-reset-originator ID ::= {id-con 2}
```

-- Certificate subject alternative names

```
id-san-mta-name ID ::= {id-san 0}
```

END -- of MHSObjectIdentifiers

Anexo C

Definición de referencia de clases de objetos y atributos de directorio

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

Este anexo, que complementa el anexo A, define a efectos de referencia las clases de objetos, los atributos y las sintaxis de atributos específicos del tratamiento de mensajes. Para ello, se hace uso de las clases de objetos de información OBJECT-CLASS y ATTRIBUTE de la Rec. UIT-T X.501 | ISO/CEI 9594-2.

```
MHSDirectoryObjectsAndAttributes { joint-iso-itu-t mhs(6) arch(5) modules(0) directory(1)
    version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

*-- Prologue**-- Exports everything.*

IMPORTS

-- MHS Object Identifiers

```
id-at-mhs-acceptable-eits, id-at-mhs-deliverable-classes,
id-at-mhs-deliverable-content-types, id-at-mhs-dl-archive-service,
id-at-mhs-dl-members, id-at-mhs-dl-policy, id-at-mhs-dl-related-lists,
id-at-mhs-dl-submit-permissions, id-at-mhs-dl-subscription-service,
id-at-mhs-exclusively-acceptable-eits, id-at-mhs-maximum-content-length,
id-at-mhs-message-store-dn, id-at-mhs-or-addresses,
id-at-mhs-or-addresses-with-capabilities, id-at-mhs-supported-attributes,
id-at-mhs-supported-automatic-actions, id-at-mhs-supported-content-types,
id-at-mhs-supported-matching-rules, id-at-mhs-unacceptable-eits,
id-con-dl-administrator-annotation, id-con-dl-nested-dl, id-con-dl-reset-originator,
id-mr-address-capabilities-match, id-mr-capability-match, id-mr-orname-exact-match,
id-oc-mhs-distribution-list, id-oc-mhs-message-store, id-oc-mhs-message-transfer-agent,
id-oc-mhs-user, id-oc-mhs-user-agent, id-san-mta-name
```

```
-----
FROM MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0)
    object-identifiers(0) version-1999(1) }
```

-- MTS Abstract Service

```
ContentLength, EncodedInformationTypesConstraints, ExtendedContentType,
ExtendedEncodedInformationType, GlobalDomainIdentifier, MTAName, ORAddress, ORName,
RequestedDeliveryMethod, SecurityContext
```

```
-----
FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
    mts-abstract-service(1) version-1999(1) }
```

-- MS Abstract Service

ATTRIBUTE, AUTO-ACTION

```
-----
FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
    abstract-service(1) version-1999(1) }
```

-- MS General Attribute Types

AttributeTable

```
-----
FROM MSGeneralAttributeTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
    general-attribute-types(2) version-1999(1) }
```

-- MS General Auto Action Types

AutoActionTable

```
-----
FROM MSGeneralAutoActionTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
    general-auto-action-types(3) version-1994(0) }
```

-- MS Matching Rules

```

MatchingRuleTable, oRAddressMatch, oRAddressElementsMatch,
oRAddressSubstringElementsMatch, oRNameMatch, oRNameElementsMatch,
oRNameSingleElementMatch, oRNameSubstringElementsMatch
-----
FROM MSMatchingRules { joint-iso-itu-t mhs(6) ms(4) modules(0)
                       general-matching-rules(5) version-1999(1) }

```

-- Information Framework

```

ATTRIBUTE, CONTEXT, distinguishedNameMatch, DIT-CONTEXT-USE-RULE,
objectIdentifierMatch, MATCHING-RULE, Name, OBJECT-CLASS, top
-----
FROM InformationFramework { joint-iso-itu-t ds(5) module(1)
                            informationFramework(1) 3 }

```

-- Selected Object Classes

```

applicationEntity
-----
FROM SelectedObjectClasses { joint-iso-itu-t ds(5) module(1)
                             selectedObjectClasses(6) 3 }

```

-- Selected Attribute Types

```

commonName, description, distinguishedName, integerMatch, organizationName,
organizationalUnitName, owner, protocolInformation, seeAlso
-----
FROM SelectedAttributeTypes { joint-iso-itu-t ds(5) module(1)
                              selectedAttributeTypes(5) 3 }

```

-- Authentication Framework

```

AlgorithmIdentifier
-----
FROM AuthenticationFramework { joint-iso-itu-t ds(5) module(1)
                               authenticationFramework(7) 3 }

```

-- Certificate Extensions

```

CertificateAssertion, OTHER-NAME
-----
FROM CertificateExtensions { joint-iso-itu-t ds(5) module(1)
                             certificateExtensions(26) 0 };

```

*-- OBJECT CLASSES**-- MHS Distribution List*

```

mhs-distribution-list OBJECT-CLASS ::= {
  SUBCLASS OF { top }
  MUST CONTAIN { commonName |
                mhs-dl-submit-permissions |
                mhs-or-addresses }
  MAY CONTAIN { description |
               organizationName |
               organizationalUnitName |
               owner |
               seeAlso |
               mhs-maximum-content-length |
               mhs-deliverable-content-types |
               mhs-acceptable-eits |
               mhs-exclusively-acceptable-eits |
               mhs-unacceptable-eits |
               mhs-dl-policy |
               mhs-dl-subscription-service |
               mhs-dl-archive-service |
               mhs-dl-related-lists |
               mhs-dl-members }
  ID          id-oc-mhs-distribution-list }

```

-- MHS Message Store

```
mhs-message-store OBJECT-CLASS ::= {
    SUBCLASS OF { applicationEntity }
    MAY CONTAIN { owner |
                mhs-supported-attributes |
                mhs-supported-automatic-actions |
                mhs-supported-matching-rules |
                mhs-supported-content-types |
                protocolInformation }
    ID          id-oc-mhs-message-store }
```

-- MHS Message Transfer Agent

```
mhs-message-transfer-agent OBJECT-CLASS ::= {
    SUBCLASS OF { applicationEntity }
    MAY CONTAIN { owner |
                mhs-maximum-content-length |
                protocolInformation }
    ID          id-oc-mhs-message-transfer-agent }
```

-- MHS User

```
mhs-user OBJECT-CLASS ::= {
    SUBCLASS OF { top }
    KIND        auxiliary
    MUST CONTAIN { mhs-or-addresses }
    MAY CONTAIN { mhs-maximum-content-length |
                mhs-deliverable-content-types |
                mhs-acceptable-eits |
                mhs-exclusively-acceptable-eits |
                mhs-unacceptable-eits |
                mhs-or-addresses-with-capabilities |
                mhs-message-store-dn }
    ID          id-oc-mhs-user }
```

-- MHS User Agent

```
mhs-user-agent OBJECT-CLASS ::= {
    SUBCLASS OF { applicationEntity }
    MAY CONTAIN { owner |
                mhs-maximum-content-length |
                mhs-deliverable-content-types |
                mhs-acceptable-eits |
                mhs-exclusively-acceptable-eits |
                mhs-unacceptable-eits |
                mhs-deliverable-classes |
                mhs-or-addresses |
                protocolInformation }
    ID          id-oc-mhs-user-agent }
```

-- ATTRIBUTES

-- MHS Acceptable EITs

```
mhs-acceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX          ExtendedEncodedInformationType
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                   id-at-mhs-acceptable-eits }
```

-- MHS Deliverable Classes

```
mhs-deliverable-classes ATTRIBUTE ::= {
    WITH SYNTAX          Capability
    EQUALITY MATCHING RULE capabilityMatch
    ID                   id-at-mhs-deliverable-classes }
```

-- MHS Deliverable Content Types

```
mhs-deliverable-content-types ATTRIBUTE ::= {
    WITH SYNTAX          ExtendedContentType
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                   id-at-mhs-deliverable-content-types }
```

-- MHS DL Archive Service

```

mhs-dl-archive-service ATTRIBUTE ::= {
  WITH SYNTAX                ORName
  EQUALITY MATCHING RULE     oRNameExactMatch
  -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
  --                            oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
  ID                          id-at-mhs-dl-archive-service }

```

-- MHS DL Members

```

mhs-dl-members ATTRIBUTE ::= {
  WITH SYNTAX                ORName
  EQUALITY MATCHING RULE     oRNameExactMatch
  -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
  --                            oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
  ID                          id-at-mhs-dl-members }

```

-- MHS DL Policy

```

mhs-dl-policy ATTRIBUTE ::= {
  WITH SYNTAX                DLPolicy
  SINGLE VALUE               TRUE
  ID                          id-at-mhs-dl-policy }

```

-- MHS DL Related Lists

```

mhs-dl-related-lists ATTRIBUTE ::= {
  SUBTYPE OF                 distinguishedName
  EQUALITY MATCHING RULE     distinguishedNameMatch
  ID                          id-at-mhs-dl-related-lists }

```

-- MHS DL Submit Permissions

```

mhs-dl-submit-permissions ATTRIBUTE ::= {
  WITH SYNTAX                DLSubmitPermission
  ID                          id-at-mhs-dl-submit-permissions }

```

-- MHS DL Subscription Service

```

mhs-dl-subscription-service ATTRIBUTE ::= {
  WITH SYNTAX                ORName
  EQUALITY MATCHING RULE     oRNameExactMatch
  -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
  --                            oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
  ID                          id-at-mhs-dl-subscription-service }

```

-- MHS Exclusively Acceptable EITs

```

mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
  WITH SYNTAX                ExtendedEncodedInformationType
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-exclusively-acceptable-eits }

```

-- MHS Maximum Content Length

```

mhs-maximum-content-length ATTRIBUTE ::= {
  WITH SYNTAX                ContentLength
  EQUALITY MATCHING RULE     integerMatch
  SINGLE VALUE               TRUE
  ID                          id-at-mhs-maximum-content-length }

```

-- MHS Message Store Directory Name

```

mhs-message-store-dn ATTRIBUTE ::= {
  SUBTYPE OF                 distinguishedName
  EQUALITY MATCHING RULE     distinguishedNameMatch
  SINGLE VALUE               TRUE
  ID                          id-at-mhs-message-store-dn }

```

ISO/CEI 10021-2:2004 (S)

-- MHS OR-Addresses

```
mhs-or-addresses ATTRIBUTE ::= {
  WITH SYNTAX                ORAddress
  EQUALITY MATCHING RULE     oRAddressMatch
  -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch | oRNameSingleElementMatch |
  --                          oRAddressSubstringElementsMatch } --
  ID                          id-at-mhs-or-addresses }
```

-- MHS OR-Addresses with Capabilities

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
  WITH SYNTAX                AddressCapabilities
  EQUALITY MATCHING RULE     addressCapabilitiesMatch
  ID                          id-at-mhs-or-addresses-with-capabilities }
```

-- MHS Supported Attributes

```
mhs-supported-attributes ATTRIBUTE ::= {
  WITH SYNTAX                ATTRIBUTE.&id({AttributeTable})
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-supported-attributes
  }
```

-- MHS Supported Automatic Actions

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
  WITH SYNTAX                AUTO-ACTION.&id ({AutoActionTable})
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-supported-automatic-actions }
```

-- MHS Supported Content Types

```
mhs-supported-content-types ATTRIBUTE ::= {
  WITH SYNTAX                ExtendedContentType
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-supported-content-types }
```

-- MHS Supported Matching Rules

```
mhs-supported-matching-rules ATTRIBUTE ::= {
  WITH SYNTAX                MATCHING-RULE.&id ({MatchingRuleTable})
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-supported-matching-rules }
```

-- MHS Unacceptable EITs

```
mhs-unacceptable-eits ATTRIBUTE ::= {
  WITH SYNTAX                ExtendedEncodedInformationType
  EQUALITY MATCHING RULE     objectIdentifierMatch
  ID                          id-at-mhs-unacceptable-eits }
```

-- ATTRIBUTE SYNTAXES

-- DL Submit Permission

```
DLSubmitPermission ::= CHOICE {
  individual          [0] ORName,
  member-of-dl       [1] ORName,
  pattern-match      [2] ORNamePattern,
  member-of-group    [3] Name }
```

```
ORNamePattern ::= ORName
```

```
any-user-may-submit DLSubmitPermission ::= pattern-match: { built-in-standard-attributes { } }
```

-- DL Policy

```

DLPolicy ::= SET {
  report-propagation [0] INTEGER {
    previous-dl-or-originator (0),
    dl-owner (1),
    both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,
  report-from-dl [1] INTEGER {
    whenever-requested (0),
    when-no-propagation (1) } DEFAULT whenever-requested,
  originating-MTA-report [2] INTEGER {
    unchanged (0),
    report (2),
    non-delivery-report (3),
    audited-report (4) } DEFAULT unchanged,
  originator-report [3] INTEGER {
    unchanged (0),
    no-report (1),
    report (2),
    non-delivery-report (3) } DEFAULT unchanged,
  return-of-content [4] ENUMERATED {
    unchanged (0),
    content-return-not-requested (1),
    content-return-requested (2) } DEFAULT unchanged,
  priority [5] INTEGER {
    unchanged (0),
    normal (1),
    non-urgent (2),
    urgent (3) } DEFAULT unchanged,
  disclosure-of-other-recipients [6] ENUMERATED {
    unchanged (0),
    disclosure-of-other-recipients-prohibited (1),
    disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,
  implicit-conversion-prohibited [7] ENUMERATED {
    unchanged (0),
    implicit-conversion-allowed (1),
    implicit-conversion-prohibited (2) } DEFAULT unchanged,
  conversion-with-loss-prohibited [8] ENUMERATED {
    unchanged (0),
    conversion-with-loss-allowed (1),
    conversion-with-loss-prohibited (2) } DEFAULT unchanged,
  further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,
  originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,
  proof-of-delivery [11] INTEGER {
    dl-expansion-point (0),
    dl-members (1),
    both (2),
    neither (3) } DEFAULT dl-members,
  requested-delivery-method [12] CHOICE {
    unchanged [0] NULL,
    removed [1] NULL,
    replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,
  token-encryption-algorithm-preference [13] SEQUENCE OF AlgorithmInformation OPTIONAL,
  token-signature-algorithm-preference [14] SEQUENCE OF AlgorithmInformation OPTIONAL,
  ... }

```

```

AlgorithmInformation ::= SEQUENCE {
  algorithm-identifier [0] AlgorithmIdentifier,
  originator-certificate-selector [1] CertificateAssertion OPTIONAL,
  recipient-certificate-selector [2] CertificateAssertion OPTIONAL}

```

-- OR-Address with Capabilities

```

AddressCapabilities ::= SEQUENCE {
  description GeneralString OPTIONAL,
  address ORAddress,
  capabilities SET OF Capability }

```

```

Capability ::= SET {
  content-types [0] SET OF ExtendedContentType OPTIONAL,
  maximum-content-length [1] ContentLength OPTIONAL,
  encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,
  security-labels [3] SecurityContext OPTIONAL,
  ... }

```

ISO/CEI 10021-2:2004 (S)

-- MATCHING RULES

-- OR-Address with Capabilities Match

```
addressCapabilitiesMatch MATCHING-RULE ::= {  
    SYNTAX    AddressCapabilities  
    ID        id-mr-address-capabilities-match }
```

-- Capability Match

```
capabilityMatch MATCHING-RULE ::= {  
    SYNTAX    Capability  
    ID        id-mr-capability-match }
```

-- OR-Name Exact Match

```
ORNameExactMatch MATCHING-RULE ::= {  
    SYNTAX    ORName  
    ID        id-mr-orname-exact-match }
```

-- CONTEXTS

-- DL Administrator Annotation

```
dl-administrator-annotation CONTEXT ::= {  
    WITH SYNTAX CHOICE{  
        bmpstring      BMPString,  
        universalstring UniversalString  
    }  
    ID id-con-dl-administrator-annotation  
}  
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE          mhs-dl-members.&id OPTIONAL  
    CONTEXTS                {dl-administrator-annotation} }
```

-- DL Nested DL

```
dl-nested-dl CONTEXT ::= {  
    WITH SYNTAX          NULL  
    ID                   id-con-dl-nested-dl }  
dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE          mhs-dl-members.&id OPTIONAL  
    CONTEXTS                {dl-nested-dl} }
```

-- DL Reset Originator

```
dl-reset-originator CONTEXT ::= {  
    WITH SYNTAX          NULL  
    ID                   id-con-dl-reset-originator }  
dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE          mhs-dl-members.&id  
    OPTIONAL CONTEXTS      {dl-reset-originator} }
```

-- CERTIFICATE SUBJECT ALTERNATIVE NAMES

-- MTA Name

```
mta-name OTHER-NAME ::= { SEQUENCE {  
                                domain      GlobalDomainIdentifier,  
                                mta-name    MTAName }  
    IDENTIFIED BY id-san-mta-name }
```

END -- of MHSDirectory

Anexo D

Amenazas contra la seguridad

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

En 15.1 de la Rec. UIT-T X.400 | ISO/CEI 10021-1 se da una visión general de las amenazas contra la seguridad del MHS. En esta Recomendación se consideran las amenazas tal como se plantean en el MHS: amenazas en el acceso, amenazas entre mensajes, amenazas en los propios mensajes y amenazas en su almacenamiento. Todas estas amenazas pueden aparecer en las diversas formas siguientes:

- a) suplantación;
- b) secuenciamiento de mensajes;
- c) modificación de información;
- d) denegación de servicio;
- e) fuga de información;
- f) rechazo;
- g) otras amenazas del MHS.

Además, las amenazas pueden surgir por accidente o intento doloso, y pueden tener un carácter activo o pasivo. Las agresiones al MHS se dirigirán hacia sus debilidades potenciales, y pueden comprender un cierto número de amenazas. Este anexo se ocupa de amenazas individuales, examinándose varios tipos amplios de amenazas, que de todos modos no constituyen una relación exhaustiva de las mismas.

En el cuadro D.1 se indica cómo hacer frente a esas amenazas utilizando los servicios de seguridad del MHS. La lista de amenazas que aquí se da es indicativa, no definitiva.

D.1 Suplantación

El fenómeno llamado suplantación ocurre cuando una entidad finge, con éxito, ser una entidad distinta de la que es, y puede tener lugar de diferentes maneras. Un usuario no autorizado del MTS puede simular a otro para acceder sin permiso a las facilidades del MTS, o actuar en detrimento de un usuario válido, por ejemplo, desechando sus mensajes. Un usuario del MTS puede suplantar a otro y acusar recibo, falsamente, de un mensaje en nombre del receptor "válido". Un mensaje puede ser introducido en el MTS por un usuario que utilice falsamente la identidad de otro. Un usuario del MTS, un MS o un MTA se pueden enmascarar como si fuesen un usuario, un MS o un MTA distintos.

Entre las amenazas de tipo suplantación figuran las siguientes:

- a) simulación y mal uso del MTS;
- b) falso acuse de recibo;
- c) falsa originación de un mensaje;
- d) simulación de un MTA a un usuario del MTS;
- e) simulación de un MTA a otro MTA.

Una suplantación incluye normalmente otras formas de agresión y, en un sistema seguro, puede implicar series de autenticaciones de usuarios válidos, por ejemplo, en la reactuación o modificación de mensajes.

D.2 Secuenciamiento de mensajes

Las amenazas contra la secuenciación de mensajes se producen cuando un mensaje se repite, entero o en parte, se le desplaza en el tiempo o se reordena. Puede recurrirse a esto para aprovecharse de la información de autenticación de un mensaje válido o reordenar o desplazar en el tiempo mensajes válidos. Si bien con los servicios de seguridad del MHS es imposible evitar la reactuación de mensajes, sí cabe detectarlas y eliminar los efectos de esa amenaza.

Entre las amenazas a la secuenciación de mensajes figuran las siguientes:

- a) reactuación de mensajes;
- b) reordenación de mensajes;
- c) adelanto de mensajes;
- d) retraso de mensajes.

Cuadro D.1 – Utilización de los servicios de seguridad del MHS

AMENAZA	SERVICIOS
SUPLANTACIÓN	
Simulación y mal uso del MTS	Autenticación de origen de mensajes Autenticación de origen de sondas Gestión de acceso seguro Prueba de entrega
Falso acuse de recibo	Autenticación de origen de mensajes
Falsa originación de un mensaje	Prueba de depósito
Simulación de un MTA a un usuario del MTS	Autenticación de origen de informes Gestión de acceso seguro
Simulación de un MTA a otro MTA	Autenticación de origen de informes Gestión de acceso seguro
SECUENCIACIÓN DE MENSAJES	
Reactuación de mensajes	Integridad de secuencia de mensajes
Reordenación de mensajes	Integridad de secuencia de mensajes
Adelanto de mensajes	
Retraso de mensajes	
MODIFICACIÓN DE INFORMACIÓN	
Modificación de mensajes	Integridad de conexión Integridad de contenido Integridad de secuencia de mensajes
Destrucción de mensajes	
Degradación del encaminamiento y de otra información de gestión	
DENEGACIÓN DE SERVICIO	
Denegación de comunicaciones	
Saturación de MTA	
Saturación del MTS	
RECHAZO	
Denegación de origen	No rechazo de origen
Denegación de depósito	No rechazo de depósito
Denegación de entrega	No rechazo de entrega
FUGA DE INFORMACIÓN	
Pérdida de confidencialidad	Confidencialidad de conexión Confidencialidad de contenido Confidencialidad de flujo de mensajes
Pérdida de anonimato	Gestión de acceso seguro
Apropiación indebida de mensajes	Confidencialidad de flujo de mensajes
Análisis del tráfico	
OTRAS AMENAZAS	
Originador no autorizado para etiqueta de seguridad de mensajes	Gestión de acceso seguro Etiquetado de seguridad de mensajes
Usuario MTA/MTS no autorizado para el contexto de seguridad	Gestión de acceso seguro
Encaminamiento erróneo	Gestión de acceso seguro Etiquetado de seguridad de mensajes
Procedimientos de etiquetado diferentes	

D.3 Modificación de información

La información para un destinatario deseado, la información de encaminamiento y otros datos relativos a la gestión pueden perderse o modificarse sin que ello se detecte. Es algo que puede ocurrir con cualquier elemento del mensaje, por ejemplo, su etiquetado, el contenido, los atributos, el destinatario o el originador. La degradación de la información de encaminamiento o de otro tipo de información de la gestión, almacenada en los MTA o utilizada por ellos, puede dar lugar a que el MTS pierda mensajes o bien a que funcione de manera incorrecta.

Entre las amenazas de modificación de información figuran las siguientes:

- modificación de mensajes;
- destrucción de mensajes;
- degradación del encaminamiento y de otra información de gestión.

D.4 Denegación de servicio

La denegación de servicio se produce cuando una entidad deja de realizar su cometido o evita que otras realicen los suyos. Puede tratarse de una denegación de acceso o de comunicaciones (que da lugar a otros problemas, como los de sobrecarga), una eliminación deliberada de mensajes dirigidos a un determinado destinatario, o una invención de tráfico extra. Se denegará el MTS si se ha provocado el fallo o el funcionamiento incorrecto de un MTA. Además, un usuario del MTS puede dar lugar a que dicho servicio se deniegue a otro usuario, saturándolo con mensajes que podrían sobrecargar la capacidad de conmutación de un MTA o llenar el espacio de almacenamiento de mensajes de que se disponga.

Entre las amenazas de denegación de servicio figuran las siguientes:

- a) denegación de comunicaciones;
- b) fallo del MTA;
- c) saturación del MTS.

D.5 Rechazo

El rechazo tiene lugar cuando un usuario del MTS o el propio MTS pueden negar a posteriori el depósito, la recepción o la originación de un mensaje.

Entre las amenazas de rechazo figuran las siguientes:

- a) denegación de origen;
- b) denegación de depósito;
- c) denegación de entrega.

D.6 Fuga de información

Un usuario no autorizado puede captar información vigilando las transmisiones o accediendo sin permiso a la información almacenada en alguna entidad del MHS o por suplantación. En algunos casos, la presencia en el sistema de un usuario del MTS puede ser un asunto delicado y debe preservarse su anonimato. También es posible que un usuario del MTS distinto del destinatario deseado se haga con un mensaje enviado al segundo. Éste podría ser el resultado de la simulación y del mal uso del MTS, o de haber provocado el funcionamiento incorrecto de un MTA. Además, observando el tráfico se pueden obtener otros detalles sobre la información que fluye por un MTS.

Entre las amenazas de fuga de información, figuran las siguientes:

- a) pérdida de confidencialidad;
- b) pérdida de anonimato;
- c) apropiación indebida de mensajes;
- d) análisis de tráfico.

D.7 Otras amenazas

En un sistema de seguridad de nivel único o de nivel múltiple, puede haber cierto número de amenazas relativas al etiquetado de seguridad, por ejemplo, el encaminamiento a través de un nodo al que no se le puede confiar información particularmente valiosa o en donde los sistemas utilizan procedimientos de etiquetado diferentes. Pueden existir amenazas a la implantación de una política de seguridad basada en la separación lógica utilizando etiquetas de seguridad. Es posible que un usuario del MTS origine un mensaje y le asigne una etiqueta para la que no está autorizado. Cabe también que un usuario del MTS o un MTA establezcan o acepten una asociación con un contexto de seguridad, para el que no tienen autorización.

Entre las "otras amenazas" aludidas en el epígrafe, figuran las siguientes:

- a) originador no autorizado para etiqueta de seguridad de mensajes (depósito inadecuado);
- b) usuario del MTA/MTS no autorizado para el contexto;
- c) encaminamiento erróneo;
- d) procedimientos de etiquetado diferentes.

Anexo E

**Prestación de servicios de seguridad en la
Rec. UIT-T X.411 | ISO/CEI 10021-4**

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

En el cuadro E.1 se indica qué elementos de servicio de la Rec. UIT-T X.411 | ISO/CEI 10021-4 pueden utilizarse para soportar los servicios de seguridad descritos en 10.2.

Cuadro E.1 – Prestación de servicios de seguridad del MHS

SERVICIO	ARGUMENTOS/SERVICIOS DEL MTS
+ - SERVICIOS DE SEGURIDAD DE AUTENTICACIÓN DE ORIGEN -----	
Autenticación de origen de mensajes	Verificación de autorización de origen de mensajes Testigo de mensajes
Autenticación de origen de sondas	Verificación de autorización de origen de sondas
Autenticación de origen de informes	Verificación de autorización de origen de informes
Prueba de depósito	Petición de prueba de depósito Prueba de depósito
Prueba de entrega	Petición de prueba de entrega Prueba de entrega
+ - SERVICIOS DE SEGURIDAD DE GESTIÓN DE ACCESO SEGURO -----	
Autenticación de entidades pares	Credenciales de iniciador Credenciales de respondedor
Contexto de seguridad	Contexto de seguridad
+ - SERVICIOS DE SEGURIDAD DE CONFIDENCIALIDAD DE DATOS -----	
Confidencialidad de conexiones	No proporcionado
Confidencialidad de contenidos	Identificador del algoritmo de confidencialidad de contenidos Testigo de mensajes
Confidencialidad del flujo de mensajes	Tipo de contenido
+ - SERVICIOS DE SEGURIDAD DE INTEGRIDAD DE DATOS -----	
Integridad de conexiones	No proporcionado
Integridad de contenido	Verificación de integridad de contenido Testigo de mensajes
Integridad de secuencia de mensajes	Verificación de autorización de origen de mensajes Número de secuencia de mensajes Testigo de mensajes
+ - SERVICIOS DE SEGURIDAD DE NO RECHAZO -----	
No rechazo de origen	Verificación de integridad de contenido Testigo de mensajes
No rechazo de depósito	Verificación de autorización de origen de mensajes Petición de prueba de depósito Prueba de depósito
No rechazo de entrega	Petición de prueba de entrega Prueba de entrega
Etiquetado de seguridad de mensajes	Etiqueta de seguridad de mensajes Testigo de mensajes Verificación de autorización de origen de mensajes
+ - SERVICIOS DE SEGURIDAD DE GESTIÓN DE LA SEGURIDAD -----	
Cambio de credenciales	Cambio de credenciales
Registros	Registros

Anexo F

Representación de las direcciones OR para su utilización por el hombre

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

Este material constituye el anexo B a la Rec. F.401 y no es parte de esta Recomendación UIT-T.

F.1 Finalidad

Una dirección OR (especificada en la cláusula 18) consta de un conjunto de valores de atributos tomados de la lista que se expone en el cuadro F.1. Con el fin de representar visualmente una dirección a un usuario humano y permitirle que introduzca la dirección en una interfaz de usuario, cada valor de atributo tiene que estar asociado con el tipo de atributo correcto. Muchos de los nombres de los tipos de atributo ilustrados en el cuadro F.1 son demasiado largos para ser utilizados cómodamente sobre el papel o la pantalla. Se necesita un formato que permita una representación concisa de los atributos, en una tarjeta comercial, por ejemplo.

En este anexo se indica cómo pueden expresarse de manera concisa las direcciones por medio de etiquetas que representen los tipos de atributos. Existen tres categorías de atributos: los atributos nemotécnicos normalizados, que con mayores probabilidades van a encontrarse en direcciones OR representadas para utilización por el hombre (en tarjetas, por ejemplo), los utilizados en direcciones de entrega física y otros atributos especializados (en los que se incluyen los atributos definidos por el dominio). Con el fin de proporcionar un formato lo más conciso posible, muchas de las etiquetas son de un solo carácter, lo que disminuye su dependencia del idioma.

En F.3 se especifica el formato para la representación de las direcciones, y en F.4, las características exigidas a los interfaces de usuario que se pretende utilizar conjuntamente con este formato.

F.2 Objeto

Para la comunicación de direcciones OR a usuarios humanos se especifica un formato etiquetado. Dicho formato consiste en un conjunto de pares de etiquetas y valores de atributo. También se especifican las características de la interfaz de usuario que son necesarias para aceptar las direcciones dadas en este formato.

Se especifica además un formato autoexplicativo cuya utilización es apropiada cuando se dispone de más espacio, por ejemplo, en material impreso y en la interfaz de usuario.

F.3 Formato

F.3.1 Generalidades

El objetivo del formato etiquetado es permitir la representación de las direcciones OR en un formato conciso y que pueda ser transmitido con exactitud a los usuarios humanos. Esto puede conseguirse examinando detenidamente qué atributos y valores se utilizan para formar una dirección OR.

Si los atributos de una dirección OR comprenden caracteres procedentes de un juego de caracteres ampliado, las personas que no utilicen normalmente el mismo juego de caracteres pueden experimentar dificultades para representar la dirección OR o para introducirla en su sistema de mensajería. En tal situación, debería disponerse de un seudónimo de la dirección OR que estuviera compuesto únicamente de caracteres de la cadena imprimible.

NOTA 1 – Es preciso examinar detenidamente la política de estructuración de las direcciones OR. Para que la probabilidad de que dos usuarios se encuentren con la misma dirección OR se reduzca a un nivel aceptable, las direcciones OR individuales deberán asignarse dentro de una división del espacio de direcciones apropiada. Habitualmente basta con utilizar el nombre de la persona o las iniciales para distinguir entre los usuarios. Tal vez no sea apropiado descender a demasiado detalle en los nombres-unidades-organizativas, particularmente si la estructura organizativa está sujeta a cambios frecuentes o los usuarios se desplazan de una unidad-organizativa a otra.

NOTA 2 – Las ventajas de utilizar valores largos para los atributos, que sean autoexplicativos (como el nombre completo de una organización), pueden estar reñidas con la comodidad de utilizar valores más cortos, que puedan caber en una pequeña tarjeta. Una solución a este conflicto consiste en utilizar un valor de atributo corto (por ejemplo, las iniciales de la organización) a modo de seudónimo alternativo del valor largo.

NOTA 3 – En el caso de que el usuario humano dude de la existencia de un espacio en un valor de atributo (en particular cuando está tipografiado) podrían proporcionarse seudónimos que comprendan el espacio y que carezcan del mismo (por ejemplo, "SNOMAIL400" como seudónimo de "SNOMAIL 400" y "Mac Donald" como seudónimo de "MacDonald").

NOTA 4 – Si se establece un seudónimo para una dirección OR, es de desear que se genere una forma coherente (preferida) de dirección OR para todos los mensajes originados por el usuario.

ISO/CEI 10021-2:2004 (S)

Cuando los usos nacionales permitan el valor de un solo espacio para el nombre-dominio-administración de una dirección, esto se representará en la dirección omitiendo el atributo nombre-dominio-administración, o bien mostrando dicho atributo con ningún valor o el valor de un espacio. El valor "XX" de nombre de país puede ser representado en una dirección omitiendo el atributo nombre de país.

F.3.2 Formato etiquetado

F.3.2.1 Sintaxis

En el formato etiquetado las direcciones OR constan de pares delimitados de una etiqueta (*label*) y un valor (*value*) con la sintaxis <label>="<value>. Las etiquetas que corresponden a cada atributo se indican en los cuadros F.1, F.2 y F.3. (Para completar la exposición se incluyen los atributos de entrega física en el cuadro F.2.) La etiqueta y su valor están separadas por el carácter "=" o por el espacio que media entre las dos columnas de un cuadro. Las etiquetas pueden ser representadas en tipos mayúsculos o minúsculos, pero se recomienda el empleo de las mayúsculas para distinguirse más fácilmente a la vista.

Las parejas etiqueta/valor consecutivas que aparezcan en una línea estarán separadas por delimitadores. Facultativamente los delimitadores podrán ir seguidos por uno o más espacios. El carácter delimitador puede ser ";" o "/" pero solamente uno de ellos podrá utilizarse en una misma dirección OR. Cuando el delimitador es "/" la primera etiqueta viene precedida por "/". El uso de delimitador al final de una línea es facultativo. Si el valor de un atributo contiene el carácter delimitador, éste deberá estar representado por un par de caracteres delimitadores.

Si se requiere que un identificador anteceda a una dirección etiquetada, se recomienda utilizar "X.400" para ese fin.

Cuando una dirección se compone enteramente de los atributos contenidos en el cuadro F.1, se recomienda que la ordenación de los atributos en la dirección sea la señalada en el cuadro F.1. Si dicha ordenación fuera incompatible con los hábitos culturales normales, podría adoptarse una ordenación para la representación de las direcciones concebida primordialmente para utilizarse en esa determinada cultura.

Cuadro F.1 – Atributos normalizados de la forma de dirección nemotécnica

Tipo de atributo	Definido en subcláusula	Abreviatura (si se precisa)	Etiqueta
Nombre personal	18.3.12	Nombre	G
Iniciales	18.3.12	Iniciales	I
Apellido	18.3.12	Apellido	S
Calificador generacional	18.3.12	Generación	Q
Nombre común	18.3.2	Nombre común	CN
Organización	18.3.9	Organización	O
Unidad organizativa 1	18.3.10	Unid.org.1	OU1
Unidad organizativa 2	18.3.10	Unid.org.2	OU2
Unidad organizativa 3	18.3.10	Unid.org.3	OU3
Unidad organizativa 4	18.3.10	Unid.org.4	OU4
Nombre dominio privado	18.3.21	PRMD	P
Nombre dominio administración	18.3.1	ADMD	A
País	18.3.3	País	C

Cuadro F.2 – Atributos de entrega física

Tipo de atributo	Definido en subcláusula	Abreviatura (si se precisa)	Etiqueta
Nombre personal entrega física	18.3.17	PD-persona	PD-PN
Componentes ampliación dirección OR postal	18.3.4	PD-dir.ext.	PD-EA
Componentes ampliación dirección entrega física	18.3.5	PD-ext.ent.	PD-ED
Número oficina entrega física	18.3.15	PD-num.ofic.	PD-OFN
Nombre oficina entrega física	18.3.14	PD-oficina	PD-OF
Nombre organización entrega física	18.3.16	PD-organiz.	PD-O
Dirección calle	18.3.22	PD-calle	PD-S
Dirección postal no formatada	18.3.25	PD-dir.	PD-A1
			PD-A2
			PD-A3
(hay etiquetas individuales para cada línea de dirección)			PD-A4
			PD-A5
			PD-A6
Nombre postal exclusivo	18.3.26	PD-excl.	PD-U
Atributos postales locales	18.3.6	PD-local	PD-L
Dirección lista correos	18.3.20	PD-lista	PD-R
Dirección apartado correos	18.3.18	PD-apart.	PD-B
Código postal	18.3.19	PD-código	PD-PC
Nombre servicio entrega física	18.3.11	PD-servicio	PD-SN
Nombre país entrega física	18.3.13	PD-país	PD-C

Cuadro F.3 – Otros atributos

Tipo de atributo	Definido en subcláusula	Abreviatura (si se precisa)	Etiqueta
Dirección red X.121	18.3.7	X.121	X.121
Dirección red E.164	18.3.7	ISDN	ISDN
Dirección red PSAP	18.3.7	PSAP	PSAP
Identificador usuario numérico	18.3.8	N-ID	N-ID
Identificador terminal	18.3.23	T-ID	T-ID
Tipo terminal	18.3.24	T-TY	T-TY
Atributo definido por el dominio	18.1	DDA:<type>	DDA:<type>
La notación <type> identifica el tipo de atributo definido por el dominio.			

EJEMPLO

X.400: G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

La dirección anterior puede también disponerse en forma de cuadro:

```
G  John
S  Smith
O  A Bank Ltd
P  ABL
A  Snomail
C  AQ
```

F.3.2.2 Tipo-terminal

Existen actualmente seis tipos-terminal definidos en 18.3.24, y por razones de uniformidad internacional deberían utilizarse las siguientes abreviaturas para representar los valores correspondientes a dichos tipos: tlx, ttx, g3fax, g4fax, ia5 y vtx.

F.3.2.3 Atributo definido por el dominio

La etiqueta de un atributo definido por el dominio se compone de "DDA: " seguida por el tipo de atributo definido por el dominio. Si la dirección incluye más de un atributo definido por el dominio del mismo tipo, se da por sentado que se desea procesar dichos atributos en el mismo orden en el que se representan.

EJEMPLO

DDA:RFC-822=fred(a)widget.co.uk; O=gateway; P=abc; C=gb

Si el tipo de atributo definido por el dominio incluye el carácter "=", éste se representa por "\=". Si el tipo de atributo definido por el dominio incluye el carácter "\", éste se representa por "\\ ". No se requiere representación especial si el tipo de atributo definido por el dominio incluye el carácter delimitador ";" o "/".

F.3.3 Formato autoexplicativo

Cuando hay espacio disponible puede utilizarse el formato autoexplicativo. Este formato consta de una lista de los tipos de atributo, ya sea completos o abreviados. Los tipos de atributo o las abreviaturas pueden estar en cualquier idioma, pero cada tipo de atributo o abreviatura va seguido por la etiqueta especificada en los cuadros F.1, F.2 o F.3. Si se utilizan abreviaturas en lengua inglesa, deberán ser las indicadas en los cuadros F.1, F.2 y F.3.

Si una dirección se compone íntegramente de los atributos contenidos en el cuadro F.1, se recomienda que la ordenación de los atributos sea la indicada en ese cuadro. Si dicha ordenación fuera incompatible con los hábitos culturales normales, podría adoptarse una ordenación para la representación de las direcciones concebida primordialmente para utilizarse en esa determinada cultura.

EJEMPLO 1 – Utilización de tipos de atributo en lengua noruega:

Fornavn (G)	Per
Etternavn (S)	Hansen
Organisasjon (O)	Teledir
Organisasjonsenhet (OU1)	Forskning
Privat domene (P)	Tele
Administrasjonsdomene (A)	Telemax
Land (C) NO	

EJEMPLO 2 – Utilización de tipos de atributo en lengua inglesa:

Given name (G)	John
Surname (S)	Smith
Organisation (O)	A Bank Ltd
Org. Unit (OU1)	IT Dept
Org. Unit (OU2)	MSG Group
PRMD (P)	ABL
ADMD (A)	Snomail
Country (C)	AQ

F.4 Interfaz del usuario

Se especifican en esta cláusula las características que debe tener una interfaz del usuario para que el usuario pueda introducir las direcciones OR representadas en uno u otro de los formatos especificados en la cláusula F.3.

Es necesario que la interfaz del usuario sea capaz de aceptar la introducción de cualquier combinación de atributos válida obtenida de los cuadros F.1, F.2 y F.3.

Si la interfaz del usuario contiene los atributos señalados en el cuadro F.1, se recomienda utilizar la ordenación del mismo cuadro, o en el caso de que ésta fuera incompatible con los hábitos culturales normales, la ordenación alternativa adoptada para una determinada cultura.

Si el usuario suministra un valor para el atributo nombre-dominio-privado pero omite el atributo nombre-dominio-administración, o bien omite el valor de este último atributo, el valor de nombre-dominio-administración que ha de utilizarse será un espacio único.

Si el usuario suministra un valor para el atributo nombre de dominio privado o el atributo nombre de dominio de administración pero omite el atributo nombre de país, el valor de nombre de país que se ha de utilizar es "XX".

Cuando se introduce una dirección OR en forma de cadena única (por ejemplo, una interfaz de línea de instrucción), es necesario aceptar cualquier dirección en formato etiquetado válido que permita al usuario introducir uno u otro delimitador. La interfaz no deberá exigir que los atributos se especifiquen en ningún orden particular. Asimismo deberá aceptar las etiquetas en tipos mayúsculos o minúsculos.

NOTA 1 – En algunas interfaces de línea de instrucción existentes, puede ser necesario encerrar entre comillas la dirección entera en formato etiquetado.

Si la interfaz es de cualquier otro tipo (por ejemplo, uno interactivo o de relleno de formularios), será preciso proveer medios para que el usuario pueda asociar fácilmente la identidad de cada atributo con las etiquetas especificadas en los cuadros F.1, F.2 y F.3.

NOTA 2 – Un modo de asociar la identidad de cada atributo con las etiquetas consiste en hacer seguir el tipo de atributo (o su abreviatura) de cada atributo por la etiqueta entre paréntesis, por ejemplo:

Given name (G)
 Initials (I)
 Surname (S)
 Generation Qualifier (Q)
 Common Name (CN)
 Organisation (O)
 Organisational Unit 1 (OU1)
 Organisational Unit 2 (OU2)
 Organisational Unit 3 (OU3)
 Organisational Unit 4 (OU4)
 Private Management Domain Name (P)
 Administration Management Domain Name (A)
 Country (C)

NOTA 3 – Numerosos usuarios pueden encontrar dificultades en copiar una dirección presentada en forma de cuadro (en formato etiquetado o en formato autoexplicativo) en una interfaz de línea de instrucción que utiliza delimitadores.

NOTA 4 – Para las interfaces de tipo formulario, la calidad de operación del usuario se optimizará cuando la interfaz más estrechamente se asemeje al formato de la dirección suministrada con la misma ordenación de atributos que utilizan los tipos o etiquetas de atributo.

EJEMPLOS DE APLICACIÓN

1 – El usuario noruego de una interfaz de línea de instrucción recibe una tarjeta comercial que contiene la siguiente dirección OR:

G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

La interfaz de línea de instrucción faculta al usuario para teclear la dirección exactamente como viene presentada en la tarjeta.

2 – El usuario noruego de una interfaz de formulario recibe la misma tarjeta comercial. El formulario que aparece en pantalla incluye los siguientes campos:

Fornavn (G)
 Etternavn (S)
 Organisasjon (O)
 Privat domene (P)
 Administrasjonsdomene (A)
 Land (C)

El usuario puede rellenar el formulario asociando las etiquetas de una sola letra contenidas en la tarjeta con las mismas etiquetas que figuran entre paréntesis a continuación de los nombres noruegos de los atributos presentados en la pantalla. (No se utilizan delimitadores para rellenar el formulario.)

3 – El usuario anglófono de una interfaz de línea de instrucción recibe un documento citando la siguiente dirección OR:

Fornavn (G)
 Etternavn (S)
 Organisasjon (O)
 Privat domene (P)
 Administrasjonsdomene (A)
 Land (C)

El usuario sabe cómo transformar la dirección de formato autoexplicativo a etiquetado. Puede elegir uno u otro delimitador para introducir la dirección, a saber:

g=per;s=hansen;o=teledir;ou1=forskning;p=tele;a=telemax;c=no

o bien:

/g=per/s=hansen/o=teledir/ou1=forskning/p=tele/a=telemax/c=no

Anexo G

La utilización de direcciones OR por parte de las organizaciones multinacionales

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

Véase asimismo el anexo E de la Rec. UIT-T F.400.

Está permitido que, cuando las reglamentaciones lo permiten, muchas organizaciones pueden desear explotar sistemas de tratamiento de mensajes que están situados en más de un país. Estas organizaciones pueden ser organizaciones privadas y proveedores del servicio MH de carácter público. Las políticas de direccionamiento y encaminamiento de los mencionados sistemas deben ser compatibles con el modelo general MHS, para asegurar el interfuncionamiento con el resto del sistema.

La existencia de servicios de directorio puede influir considerablemente en las políticas de direccionamiento que las organizaciones decidan adoptar. Si se dispone de un servicio de directorio universal, es posible referirse a los originadores y destinatarios de los mensajes mediante un nombre de directorio sencillo; el sistema de tratamiento de mensaje permite obtener las direcciones OR en el directorio. En este caso los usuarios humanos no necesitan recurrir a los valores de dirección OR utilizados, y la política de direccionamiento puede decidirse con arreglo a criterios puramente técnicos. Si no se dispone de un servicio de directorio de este tipo, será necesario que los usuarios traten las direcciones OR de forma manual. En este caso, las consideraciones estéticas y otros factores humanos han de influir igualmente en la selección de la política de direccionamiento.

G.1 Principios de direccionamiento

Es posible obtener que los nombres de MHS tengan un carácter inequívoco, a nivel mundial, mediante una estructura de registro jerárquica y la aplicación coherente de convenios sobre denominación. Ello implica que, cada vez que se use una dirección OR, es necesario registrar los valores de atributo de dirección con arreglo a los procedimientos aplicables para el país indicado por el valor del atributo nombre-país. En el caso del nombre-dominio-privado y nombre-dominio-administración, ello exige el registro ante las autoridades de registro competentes en ese país o dominio. Estos principios sientan la base de la mensajería mundial.

La interconexión de dominios (PRMD a ADMD, ADMD a ADMD, PRMD a PRMD) está sujeta a acuerdos bilaterales. Dichos acuerdos dependen de criterios comerciales y técnicos; entre otras cuestiones, estos convenios pueden especificar la gama de valores de dirección OR que están aceptados.

Cuando una organización exige nombres de dominios con más de un código de país, es necesario registrar los nombres de conformidad con los procedimientos en cada país. Con frecuencia será posible registrar el mismo valor de nombre-dominio-privado (o nombre-dominio-administración, según corresponda) en cada país; con todo, por factores ajenos al alcance del MHS (como la propiedad jurídica del nombre) a veces será necesario que una organización multinacional utilice valores diferentes para su nombre-dominio, con arreglo al código de país utilizado.

Lo ideal para los usuarios de MHS sería tener una dirección que pudieran utilizar en la mensajería mundial y que estuviera consignada en los membretes y tarjetas comerciales (indicando el país en que está situado el usuario), y que sus potenciales asociados pudieran utilizar en sus comunicaciones por conducto de los sistemas MHS. La posibilidad de llegar a interlocutores distantes a través de un proveedor de servicios depende de las posibilidades de conexión que existan.

G.2 Ejemplos de configuraciones

Las organizaciones multinacionales pueden optar por organizar sus sistemas de mensajería en cualquier forma que sea compatible con estos principios básicos. Entre los ejemplos de configuraciones posibles de un PRMD multinacional pueden citarse:

G.2.1 PRMD independientes múltiples

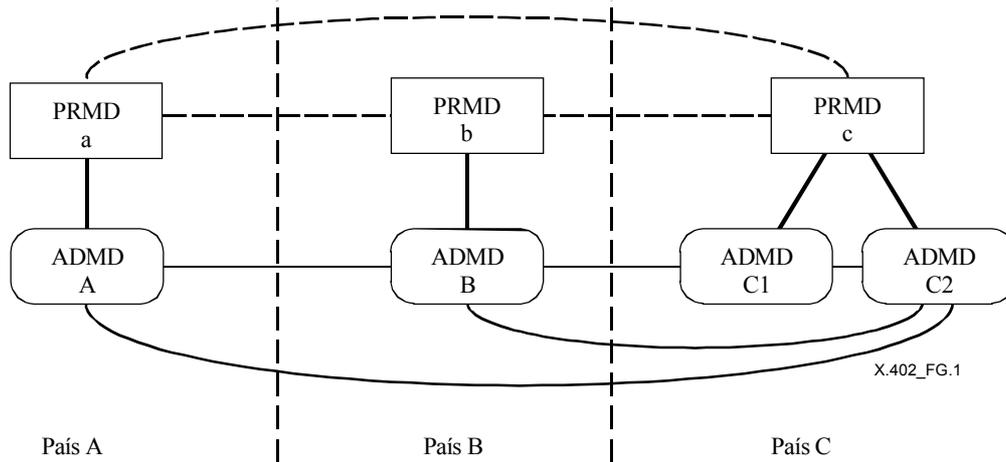


Figura G.1 – PRMD independientes múltiples

La organización multinacional puede dividir su sistema de mensajería de forma lógica en porciones que estén contenidas íntegramente en un solo país. Cada porción funciona como un PRMD distinto y utiliza direcciones registradas en su propio país.

Cada PRMD puede conectar con uno o más ADMD de su propio país. En el caso de que el PRMD esté conectado a más de un ADMD, y que no se utilice el nombre de ADMD de espacio único, cada usuario (o DL) tendrá múltiples direcciones OR (seudónimos) con diferentes valores para el atributo nombre-dominio-administración. Algunos de los valores de estos seudónimos pueden utilizarse como el valor de la dirección OR del originador. Si el propio país permite la utilización del nombre ADMD de espacio único y el PRMD opta por utilizarlo, cada usuario (o DL) puede tener un valor único de dirección OR, independientemente del número de ADMD a los que esté conectado el PRMD, suponiendo que se han preparado mecanismos para tratar este convenio.

NOTA 1 – La elección de un seudónimo tiene una serie de consecuencias, véase G.3.

NOTA 2 – Los procedimientos MTS pueden tener que revisarse para admitir PRMD multinacionales en un entorno de mensajería mundial.

Este caso no es específico de las organizaciones multinacionales; no puede distinguirse de los múltiples PRMD empleados por organizaciones distintas.

Esta configuración permite reglamentaciones diferentes en diversos países y además prevé la asignación de direcciones OR únicas.

G.2.2 Un PRMD único, nombrado a partir del país de origen

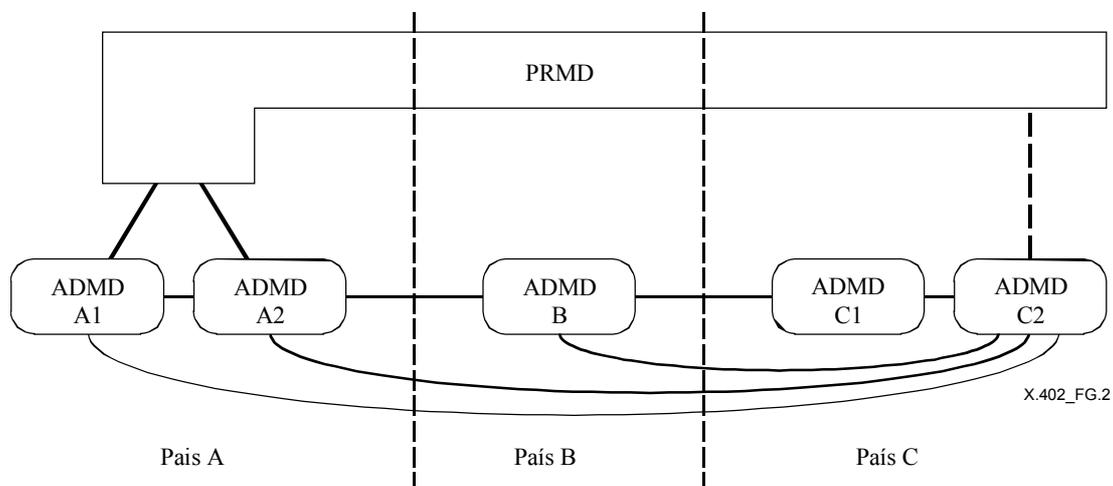


Figura G.2 – PRMD único con nombre único

La organización multinacional puede utilizar un dominio de gestión único que esté situado físicamente en más de un país. Un solo país se selecciona como país de origen a los efectos del direccionamiento. En este caso, todos los UA dentro del MD están direccionados con los mismos valores para nombre-país, nombre-dominio-administración y nombre-dominio-privado. Esta serie de valores de atributos se registra con arreglo a las exigencias del país elegido.

El PRMD puede conectarse con uno o más ADMD del país de origen y además (con sujeción a la reglamentación nacional y los criterios comerciales) a los ADMD de otros países. La conexión a los ADMD situados fuera del país de origen exige que esos ADMD tengan la capacidad y voluntad de encaminar mensajes directamente a un PRMD cuando el nombre-país utilizado en la dirección OR es diferente de la utilizada por el ADMD.

Puede ser que los usuarios de este PRMD no estén satisfechos con la consiguiente utilización de un nombre-país en la dirección OR a la que no pertenezcan.

NOTA – Tal vez sea preciso revisar los procedimientos MTS para soportar los PRMD multinacionales en un entorno de mensajería mundial.

G.2.3 Un PRMD único con múltiples nombres de dominio y de país

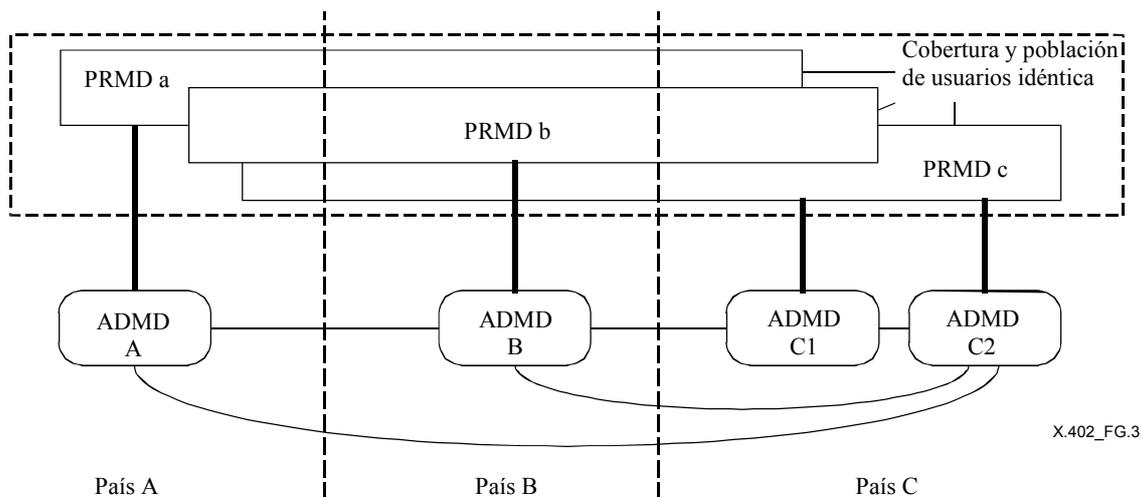


Figura G.3 – PRMD único con múltiples nombres de dominio y de país

La organización multinacional puede utilizar un sistema único de mensajería, pero utilizar nombres PRMD registrados en más de un país. Al formar las direcciones OR, el nombre-dominio-administración debe corresponder a uno de los valores autorizados por el país indicado en el valor del nombre-país. El valor nombre-dominio-privado utilizado en una dirección OR en particular debe ser uno registrado de forma compatible con el nombre de país y el nombre-dominio-administración siguiendo los procedimientos del país o el ADMD de que se trate.

El PRMD multinacional puede conectarse a uno o más ADMD. Cada usuario (o DL) tiene actualmente múltiples seudónimos de direcciones OR, con diferentes valores para el nombre-país, el nombre-dominio-administración y el nombre-dominio-privado. Cualquiera de estos seudónimos puede ser utilizado como el valor de la dirección OR del originador; los usuarios pueden optar por utilizar una dirección que identifica el país en el que están situados físicamente, pero no están obligados a hacerlo, siempre que el ADMD de que se trata acepte la dirección OR del originador.

Si aparecen múltiples (seudónimos de) direcciones OR para el mismo usuario, el interlocutor de este usuario puede no saber cómo resolver la situación. El emisor y el destinatario deben entender cuál de las diversas direcciones OR es necesario utilizar en los diferentes casos. Si no lo entienden, ello obstaculizará una buena comunicación abierta. Además, los costos de un determinado mensaje pueden variar con arreglo al punto de acceso elegido para el primer ADMD.

NOTA 1 – La elección del seudónimo presenta diversas consecuencias, véase G.3.

Los acuerdos bilaterales entre el PRMD y cada ADMD a los cuales se conecta identificarán el criterio utilizado por el ADMD para encaminar mensajes dentro del PRMD. Con arreglo a estos acuerdos, se puede optar por encaminar directamente mensajes dirigidos a cualquiera de los seudónimos que identifican el PRMD o encaminar directamente sólo los mensajes direccionados utilizando el código de país local, encaminando los demás por conducto de un ADMD del país, especificado en la dirección OR del destinatario, en la medida en que los proveedores del servicio de que se trata puedan aplicar los principios de tasación y contabilidad.

NOTA 2 – Puede ser necesario revisar los procedimientos MTS para soportar los PRMD multinacionales en un entorno de mensajería mundial.

G.3 Seudónimos de direcciones OR

Los casos mencionados a continuación muestran que pueden aparecer seudónimos de los nombres de dominio de gestión. La presencia de dichos seudónimos tiene diversas consecuencias, tanto para los usuarios como para los explotadores del sistema.

NOTA – Pueden también presentarse seudónimos de direcciones para los usuarios dentro de un dominio; el tratamiento de éstos suele ser independiente de los seudónimos del dominio de gestión.

Cada usuario puede seleccionar un ADMD preferido entre los disponibles y citar el nombre-país, nombre-dominio-administración y nombre-dominio-privado correspondientes cuando comunique su dirección OR, ya sea en una tarjeta comercial o en la dirección OR de mensajes del originador.

Si el usuario desea asimismo utilizar los servicios de otros ADMD a los que esté conectado el PRMD, pueden plantearse algunas dificultades. En algunos pocos casos el usuario (o agente del usuario) puede seleccionar otra combinación del nombre ADMD y el nombre del PRMD correspondiente al ADMD que ha de utilizarse, y cambiar la dirección OR del originador en consecuencia. Sin embargo, esto es sólo posible en el caso de que llegue a todos los destinatarios del mensaje por conducto del mismo ADMD, y que se conozca el ADMD elegido en el momento del depósito. No es posible cambiar la dirección OR después del depósito, pues está en pugna con los servicios de seguridad. Además, puede ser confuso para los usuarios recibir mensajes del mismo originador pero con direcciones OR diferentes.

Por estos motivos sería más satisfactorio que el usuario utilizara sólo una dirección OR, y que algunos ADMD aceptaran los mensajes en los que la dirección OR del originador no corresponda a ese nombre-país y ese nombre-dominio-administración. Puede suceder que direcciones OR del originador no correspondan al PRMD local si se utilizan los servicios listas de distribución y redireccionamientos (por ejemplo, el servicio destinatario-alternativo-asignado-destinatario). Los acuerdos bilaterales entre operadores de ADMD deberán tener en cuenta la utilización de estas posibilidades (entre otras) en el caso de tránsito a través de más de un dominio. El alcance mundial es factible, al menos en principio.

La dirección OR del originador utilizada al enviar mensajes puede afectar el encaminamiento seguido por los mensajes que se envíen como respuesta. En el caso general, los mensajes de respuesta se encaminarán por conducto del país y el ADMD especificados en la dirección OR. Los acuerdos bilaterales entre los PRMD o entre el PRMD y los ADMD pueden permitir la utilización de otros caminos. Estos factores ejercerán influencia en el usuario al seleccionar el nombre de dominio adecuado que utilizará en la dirección OR. Debe tenerse presente que la utilización de múltiples direcciones OR para el mismo usuario puede también tener consecuencias sobre los potenciales destinatarios. Esta situación confusa no favorecería una buena comunicación abierta.

Anexo H

Utilización de contraseñas protegidas para el acceso a almacenamiento de mensajes

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

La finalidad del mecanismo de contraseña protegida en la vinculación MS es que los usuarios puedan autenticarse por sí mismos ante un almacenamiento de mensajes cuando utilizan una red insegura, sin correr el riesgo de que la contraseña utilizada pueda ser obtenida por alguien que supervisa el tráfico de la red. Este problema se plantea en entornos de redes de zona local (tales como Ethernet), donde cualquier estación conectada a la red puede supervisar todo el tráfico que pasa a través de la misma. De manera similar, los administradores de redes públicas de zona amplia pueden no ser fiables.

La solución obvia es criptar todo el tráfico que pasa por redes que no son fiables, pero se puede considerar que no es rentable el tiempo de procesamiento o la administración adicionales requeridos por este sistema. Asimismo, la utilización de una criptación fuerte está restringida jurídicamente en muchas zonas. El mecanismo de contraseña protegida se puede implementar con un costo mínimo, y la utilización de algoritmos de troceado en vez de una criptación completa evita la mayoría de los aspectos jurídicos. Aunque los datos no están aún protegidos, el posible riesgo se limita a la cantidad de datos extraídos de la MS durante una sesión, mientras que la obtención de la contraseña permitiría a un intruso acceder a todo el contenido de la MS y también efectuar ataques de negación de servicio o mascarada. La contraseña protegida es, por consiguiente, un compromiso útil, que ofrece un aumento notable de seguridad a bajo costo.

La base del esquema de contraseña protegida es la utilización de algoritmos de troceado criptográfico, que son algoritmos matemáticos que producen una salida relacionada con sus datos de entrada, pero con la propiedad de que no es factible computacionalmente determinar qué valor de entrada produce una salida dada, ni determinar cualquier otro valor de entrada que produciría la misma salida.

El algoritmo de contraseña protegida posible más sencillo sería tomar la contraseña introducida por el usuario, pasarla a través de un algoritmo de troceado y transmitir el resultado. El intruso sólo podría ver el valor troceado, y no sería capaz de extraer la contraseña original. Lamentablemente, esto no proporciona mucha seguridad suplementaria, porque el intruso no necesita saber el texto claro de la contraseña: como la contraseña estará troceada siempre al mismo valor, el intruso sólo tiene que construir un agente usuario que pueda reproducir el valor registrado de la contraseña troceada y la MS lo aceptará.

La solución a este problema es añadir un número aleatorio a la contraseña antes de calcular el valor de troceado. El UA envía entonces la contraseña troceada a la MS, acompañada por el valor elegido de número aleatorio. La MS conocerá la contraseña real y puede realizar el mismo cálculo utilizando el valor aleatorio suministrado por el UA: si el cálculo de troceado da el mismo resultado que el suministrado por el UA, el usuario debe haber pasado la contraseña correcta. Éste se puede representar matemáticamente como sigue:

Definición: $\text{protected} = F(\text{password} + \text{random})$

El UA envía a la MS: $\text{protected}, \text{random}$

La MS almacena: $\text{protected}, \text{ todos los valores utilizados de random}$

El intruso puede obtener el valor de protected y también el valor de random utilizados, pero no puede extraer el valor original de la contraseña. Además, si la MS sigue la pista de todos los valores de número aleatorio que han sido utilizados en el pasado y no permite que se utilice de nuevo el mismo valor, el intruso no puede acceder reenviando los mismos datos que, según se había observado, funcionaban en el pasado.

Como es bastante improbable que la MS mantengan una lista de todos los valores de `random` que han sido utilizados en el pasado (puede haber un gran número de éstos), es preferible utilizar la fecha y hora actuales en lugar (o además) del número aleatorio. La MS registra simplemente la hora más reciente que ha sido utilizada, y requiere que cada nuevo intento de conexión utilice una hora ulterior que la registrada¹⁾. Esto asegura de nuevo que cada conexión utilizará un nuevo valor de `protected` e impide el acceso del intruso. Esta versión se convierte en:

Definición: `protected = F (password + random + time)`

El UA envía a la MS: `protected, random, time`

La MS almacena: `password`, último valor de `time`

Esta versión proporciona una protección adecuada contra ataques externos, pero tiene el inconveniente de que la MS debe almacenar la versión en claro de la contraseña del usuario. Esto se considera indeseable, pues las contraseñas pueden ser reveladas inadvertidamente durante el mantenimiento del sistema, y porque es extremadamente fácil que un administrador de sistema corrompido revele las contraseñas. El esquema de contraseña protegido especificado para el sistema de tratamiento de mensajes añade una capa suplementario de troceado, de modo que la MS no almacene las contraseñas en claro²⁾:

Definición: `protected1 = F1(password + random1 + time1)`

Definición: `protected2 = F2(protected1 + time2 + random2)`

El UA almacena: `time1, random1`

El UA envía a la MS: `protected2, time2, y/o random2, facultativamente time1 y/o random1`

La MS almacena: `protected1`, utilizado por última vez en `time2`, facultativamente `time1, random1`

En este esquema, el UA calcula primero `protected1` utilizando un valor conocido (preconfigurado) de `time1` y `random1` más la contraseña del usuario. Elige después `random2`, lee el reloj para `time2` y calcula `protected2`. Los datos enviados a la MS incluyen por lo menos `protected2, time2` y `random2`. La MS toma el valor almacenado de `protected1` más `time2` y `random2` suministrados para calcular otra versión de `protected2`, si esto concuerda con `protected2` del UA, el usuario es autenticado.

El protocolo permite una amplia elección de algoritmo, permitiendo diferentes algoritmos para `F1()` y `F2()` y permitiendo que se omita cualquiera de `time1, time2, random1, random2`. El uso exacto de los parámetros tiempo (`time`) y aleatorio (`random`) dependerá de los algoritmos utilizados y de la política de seguridad. Sin embargo, normalmente será necesario utilizar por lo menos uno de `time2/random2` para asegurar que el valor de troceado es diferente cada vez. La MS debe almacenar información suficiente sobre los valores previos de `time2/random2` para impedir que se utilice la misma combinación de nuevo en el futuro (la hora es particularmente conveniente para esto). La protección de contraseña básica sólo utiliza `time1/random1` para asegurar que dos usuarios que han elegido la misma contraseña tienen valores diferentes de `protected1` (lo que hace menos efectivos los ataques de "diccionario"); sin embargo, las políticas de seguridad pueden utilizar estos campos para fines adicionales, tales como envejecimiento/expiración de la contraseña o para seleccionar entre múltiples contraseñas diferentes.

La gama de posibilidades se puede ilustrar mediante tres ejemplos:

- Si la MS acepta contraseñas en claro, `F1()` puede ser una función nula (que devuelve su entrada inalterada) y se puede omitir `time1, random1`, lo que da un solo nivel de troceado. Se puede omitir también `random2`.
- Una implementación típica pudiera utilizar la misma función de troceado para `F1()` y `F2()` y pasar por alto `random2` y `time1`, transmitiendo solamente `protected2` y `time2` en el argumento de vinculación y tomando `random1` de la configuración.
- Una implementación más compleja requeriría que la MS almacenase más de una contraseña (es decir, el valor `protected1`) para cada usuario, y transmitiría así los valores `time1/random1` para indicar cuál está utilizando el UA.

1) La MS puede validar también que la hora es aproximadamente correcta de acuerdo con la hora del día mundial real. Esto no se requiere para los efectos de autenticación, pero impide que un usuario sea dejado fuera inadvertidamente utilizando una máquina cuyo reloj es más rápido o más lento.

2) Cabe señalar que si bien la protección contra ataques externos es muy fuerte, la protección contra ataques internos (es decir, administradores del sistema que leen los ficheros cuando la MS almacena las contraseñas) es de carácter más aparente. Aunque las contraseñas ya no son almacenadas en claro, la `protected1` almacenada es todo lo que se necesita teóricamente para acceder a la MS, dado un UA adecuadamente adaptado. Sin embargo, es muy probable que un intruso que puede leer el fichero de contraseñas de la MS pueda leer también los ficheros de buzones, de modo que la protección sólo necesita impedir la revelación inadvertida más bien que los ataques deliberados.

ISO/CEI 10021-2:2004 (S)

La MS no tiene que almacenar `time1/random1` si se utilizan contraseñas protegidas para cada conexión. Sin embargo, el esquema de contraseña protegida puede interfuncionar con la autenticación de contraseña simple normal si la MS almacena también `time1/random1`. Cuando un UA ha suministrado una contraseña simple a una MS que está diseñada para contraseña protegida, la MS sencillamente calcula un valor de `protected1` de la contraseña suministrada y `time1, random1` almacenados y compara el resultado con `protected1` almacenado. De manera similar, si el usuario cambia la contraseña con el cambio de credenciales normalizado, la MS puede calcular un `protected1` nuevo a partir de la contraseña nueva suministrada y `time1/random1` almacenados.

La prestación de un mecanismo protegido para cambiar la contraseña es más difícil. No es útil suministrar la nueva contraseña en forma de un valor `protected2`, pues la MS tiene que almacenar `protected1` y es fundamental para todo el esquema que no se pueda calcular `protected1` a partir de `protected2`. Tampoco se puede enviar directamente el nuevo `protected1`, porque exponer el nuevo `protected1` a un intruso es casi tan nocivo como revelar la contraseña clara. Sin embargo, la MS y el UA sí tienen un secreto compartido en forma del antiguo valor de `protected1`. El nuevo `protected1` puede ser expresado como un cambio que se debe aplicar al `protected1` antiguo para obtener el nuevo `protected1`. Como sólo se transmite el cambio de información, el intruso que no conocía el `protected1` antiguo no conocerá el nuevo `protected1`. Si el algoritmo de troceado `F1()` tiene la característica de que produce un resultado de tamaño fijo (como la mayoría de estos algoritmos), el cambio se puede especificar como una cadena de bits que ha de ser puesta a OR exclusiva con el antiguo `protected1` para dar el nuevo `protected1`. El número de bits que cambia no da al intruso ninguna información útil, puesto que un algoritmo de troceado adecuado tendrá las características de que un pequeño cambio en la entrada puede originar un gran cambio en la salida. Para los algoritmos de troceado con salida de longitud variable, se requerirá una descripción de cambio más compleja, pero se aplican los mismos principios.

Anexo I

Diferencias entre ISO/CEI 10021-2 y la Rec. UIT-T X.402

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

El presente anexo identifica las diferencias técnicas entre la Rec. UIT-T X.402 e ISO/CEI 10021-2.

Entre ambas especificaciones hay las diferencias siguientes:

- a) La Recomendación UIT-T sugiere que la interconexión directa de los PRMD puede ser "afectada por la reglamentación", mas no así la norma ISO/CEI. (Véase la figura 11.)
- b) Tanto en esta Norma ISO/CEI como en la Recomendación UIT-T correspondiente, las direcciones OR están estructuradas jerárquicamente, pero la Recomendación UIT-T confía a los ADMD la responsabilidad de la administración de esta jerarquía, mientras que la Norma ISO/CEI permite que la jerarquía sea gestionada de un modo independiente (por las autoridades de registro nacional, por ejemplo). (Véanse las cláusulas 14.1.1, 14.1.2 y 15.)
 La Recomendación UIT-T requiere que el encaminamiento entre dominios respete esta jerarquía (de manera que todo encaminamiento de mensajes entre los PRMD haga que intervengan uno o más ADMD); en cambio la Norma ISO/CEI permite además la conexión directa de los PRMD (mediante acuerdo bilateral, por ejemplo). (Véase la cláusula 19.)
- c) En 18.3.1, el párrafo que define al nombre-dominio-administración de espacio único es una parte normativa de la Norma ISO/CEI, mientras que en la Recomendación UIT-T es una nota. El párrafo que define al nombre-dominio-administración de cero único es una parte normativa de la Norma ISO/CEI, mientras que está omitido en la Recomendación UIT-T.
- d) La representación de direcciones OR para utilización por personas (véase el anexo F) es un anexo informativo a la Norma Internacional ISO/CEI, pero corresponde al anexo B de la Rec. UIT-T F.401 informativo y no forma parte de la Rec. UIT-T X.402.

Anexo J

Resumen de los cambios con respecto a ediciones anteriores

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

J.1 Diferencias entre ISO/CEI 10021-2:1990 y la Rec. CCITT X.402 (1992)

Las diferencias técnicas son las siguientes:

- a) incorporación del anexo G sobre utilización de las direcciones OR por parte de las organizaciones multinacionales;
- b) empleo de atributos normalizados suplementarios en direcciones OR terminales.

J.2 Diferencias entre la Rec. CCITT X.402 (1992) y la Rec. UIT-T X.402 (1995) | ISO/CEI 10021-2:1996

Las diferencias técnicas son las siguientes:

- a) incorporación del anexo F sobre representación de las direcciones OR para su utilización por el hombre;
- b) nueve nuevas definiciones de atributos de directorio (véanse A.2.1, A.2.2, A.2.4, A.2.6, A.2.7, A.2.9, A.2.14, A.2.18 y A.2.19);
- c) una nueva sección 7 relativa a convenios sobre definición del servicio abstracto (véanse las cláusulas 28-30).

Otros cambios son de tipo editorial y están relacionados con el empleo de la notación ASN.1 revisada, definida en las Recomendaciones UIT-T X.680-684 (1994) | ISO/CEI 8824:1994 y utilizada en las Recomendaciones UIT-T X.500-X.525 (1993) | ISO/CEI 9596:1994.

J.3 Diferencias entre la Rec. UIT-T X.402 (1995) | ISO/CEI 10021-2:1996 y la Rec. UIT-T X.402 (1999) | ISO/CEI 10021-2:1999

Las diferencias técnicas son las siguientes:

- a) la utilización del juego de caracteres multiocteto universales en los atributos de direcciones-OR (véase 18.2-18.4);
- b) las definiciones de nuevo contexto de directorio (véase A.4), y un nombre alternativo de sujeto de certificado para los MTA (véase A.5);
- c) el nuevo anexo H sobre la utilización de contraseñas protegidas para el acceso a almacenamiento de mensajes.

Anexo K

Índice

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

Este anexo contiene un índice de esta Especificación, 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. La lista de cada categoría es exhaustiva.

El índice se divide en las siguientes categorías:

- a) Abreviaturas;
- b) Términos;
- c) Elementos de información;
- d) Módulos ASN.1;
- e) Clases de objetos de información ASN.1;
- f) Tipos ASN.1;
- g) Valores ASN.1.

Abreviaturas

A/SYS
AC
ACs
ACSE
ADMD
AE
APDU
AS/SYS
ASE
ASEs
ASN.1
AST/SYS
AT/SYS
AU
C
COMPUSEC
D
DL
DSA
EIT
M
MASE
MD
MDSE
MHE
MHS
MRSE
MS
MSSE
MTA
MTS
MTSE
O
OSI
PI

P3

P7
PDAU
PDS
PRMD
RO
ROSE
RT
RTSE
S/SYS
ST/SYS
T/SYS
UA
UE

Términos

sistemas de acceso y almacenamiento
sistemas de acceso y transferencia
sistema de acceso
unidad de acceso
sistema de acceso, almacenamiento y transferencia
destinatario efectivo
dominio de gestión de administración
nombre-dominio-administración
afirmación
asimétrico
atributo
lista de atributos
tipo de atributo
valor del atributo
nombre-común
condicional
ASE consumidor
UE consumidor
contenido
tipo de contenido

conversión
nombre-país
defectible
entrega
agente de entrega
informe de entrega
mensaje descrito
depósito directo
usuario directo
lista de distribución
ampliación de DL
dominio
atributo definido por el dominio
tipo de información codificada
sobre
evento
punto de ampliación
conversión explícita
exportación
componentes-ampliación-dirección-entrega-física
encaminamiento externo
transferencia externa
formatada
MHS Global
grado
destinatario inmediato
conversión implícita
importación
depósito indirecto
usuario indirecto
destinatario deseado
encaminamiento interno
transferencia interna
combinación
atributos-postales-locales
dominio de gestión
obligatorio
destinatario miembro
miembros
mensaje
tratamiento de mensajes
entorno de tratamiento de mensajes
sistema de tratamiento de mensajes
almacenamiento de mensajes
almacenamiento de mensajes
transferencia de mensajes
agente de transferencia de mensajes
sistema de transferencia de mensajes
sistema de mensajería
dirección-OR nemotécnica
resolución de nombre
jerarquizado
dirección-red
no afirmación
no entrega
informe de no entrega
dirección-OR numérica
identificador-usuario-numérico
opcional
dirección-OR
nombre-unidades-organización
nombre-organización
origen

originador
destinatario alternativo especificado por el originador
nombre-OR
nombre-pds
nombre-personal
entrega física
unidad de acceso de entrega física
sistema de entrega física
mensaje físico
reproducción física
nombre-país-entrega-física
nombre-oficina-entrega-física
número-oficina-entrega-física
nombre-organización-entrega-física
nombre-personal-entrega-física
dirección-OR postal
código-postal
dirección-lista-correos
dirección- apartado-correos
destinatario potencial
dominio de gestión privado
nombre-dominio-privado
sonda
recepción
destinatario
destinatario alternativo designado por el
destinatario
redireccionamiento
informe
recuperación
encaminamiento
política de seguridad
división
atributo normalizado
paso
sistema de almacenamiento y transferencia
sistema de almacenamiento
dirección-calle
mensaje objeto
sonda objeto
depósito
agente de depósito
permiso de depósito
ASE suministrador
UE suministrador
simétrico
dirección OR terminal
identificador-terminal
tipo-terminal
transferencia
sistema de transferencia
transmisión
evento transmisión
paso transmisión
tipo
no formatado
dirección-postal-no formatada
nombre-postal-exclusivo
usuario
agente de usuario
valor
Elementos de información
concordancia de capacidades de dirección

concordancia de capacidades
 anotación de administrador DL
 DL anida de DL
 política DL
 reiniciación de originador DL
 permiso de depósito de DL
 EIT aceptables del MHS
 clases entregables del MHS
 tipos de contenido entregable del MHS
 lista de distribución del MHS
 servicio de archivo de DL del MHS
 miembros del DL del MHS
 política de DL del MHS
 listas relacionadas con DL del MHS
 permisos de depósito de DL del MHS
 servicio de suscripción a DL del MHS
 EIT exclusivamente aceptables del MHS
 longitud de contenido máxima del MHS
 almacenamiento de mensajes del MHS
 nombre de directorio memoria de mensajes del MHS
 agente de transferencia de mensajes del MHS
 direcciones OR del MHS
 direcciones OR con capacidades del MHS
 atributos permitidos por el MHS
 acciones automáticas permitidas por el MHS
 tipos de contenido permitidos por el MHS
 reglas de concordancia permitidas por el MHS
 EIT no aceptable del MHS
 usuario del MHS
 agente de usuario de MHS
 nombre de MTA
 dirección-OR
 dirección OR con capacidades
 nombre-OR

Módulos ASN.1

MHSDirectoryObjectsAndAttributes
 MHSObjectIdentifiers

Clases de objetos de información ASN.1

ABSTRACT-ERROR
 ABSTRACT-OPERATION
 ATTRIBUTE
 ATTRIBUTE (Directory) - véase ISO/CEI 9594-2
 ATTRIBUTE (MS) - véase ISO/CEI 10021-5
 AUTO-ACTION - véase ISO/CEI 10021-5
 CONTEXT - véase ISO/CEI 9594-2
 DIT-CONTEXT-USE-RULE - véase ISO/CEI 9594-2
 MATCHING-RULE - véase ISO/CEI 9594-2
 MHS-OBJECT
 MS-ATTRIBUTE
 OBJECT-CLASS - véase ISO/CEI 9594-2
 OTHER-NAME - véase ISO/CEI 9594-8
 PORT
 ASN.1 types
 AddressCapabilities
 AlgorithmIdentifier - véase ISO/CEI 9594-8
 AlgorithmInformation
 AttributeTable - véase ISO/CEI 10021-5
 AutoActionTable - véase ISO/CEI 10021-5
 Capability
 CertificateAssertion - véase ISO/CEI 9594-8
 ContentLength - véase ISO/CEI 10021-4

DLPolicy
 DLSubmitPermission
 EncodedInformationTypesConstraints
 ExtendedContentType - véase ISO/CEI 10021-4
 ExtendedEncodedInformationType - véase ISO/CEI 10021-4
 GlobalDomainIdentifier - véase ISO/CEI 10021-4
 ID
 MatchingRuleTable - véase ISO/CEI 10021-5
 MTAName - véase ISO/CEI 10021-4
 Name - véase ISO/CEI 9594-2
 ORAddress - véase ISO/CEI 10021-4
 ORName - véase ISO/CEI 10021-4
 ORNamePattern
 RequestedDeliveryMethod - véase ISO/CEI 10021-4
 SecurityContext - véase ISO/CEI 10021-4

Valores ASN.1

addressCapabilitiesMatch
 any-user-may-submit
 applicationEntity - véase ISO/CEI 9594-7
 capabilityMatch
 commonName - véase ISO/CEI 9594-6
 description - véase ISO/CEI 9594-6
 distinguishedName - véase ISO/CEI 9594-6
 distinguishedNameMatch - véase ISO/CEI 9594-2
 dl-administrator-annotation
 dl-administrator-annotation-use-rule
 dl-nested-dl
 dl-nested-dl-use-rule
 dl-reset-originator
 dl-reset-originator-use-rule
 id-arch
 id-at
 id-at-encrypted-mhs-acceptable-eits
 id-at-encrypted-mhs-deliverable-classes
 id-at-encrypted-mhs-deliverable-content-types
 id-at-encrypted-mhs-dl-archive-service
 id-at-encrypted-mhs-dl-members
 id-at-encrypted-mhs-dl-policy
 id-at-encrypted-mhs-dl-related-lists
 id-at-encrypted-mhs-dl-submit-permissions
 id-at-encrypted-mhs-dl-subscription-service
 id-at-encrypted-mhs-exclusively-acceptable-eits
 id-at-encrypted-mhs-maximum-content-length
 id-at-encrypted-mhs-message-store-dn
 id-at-encrypted-mhs-or-addresses
 id-at-encrypted-mhs-or-addresses-with-capabilities
 id-at-encrypted-mhs-supported-attributes
 id-at-encrypted-mhs-supported-automatic-actions
 id-at-encrypted-mhs-supported-content-types
 id-at-encrypted-mhs-supported-matching-rules
 id-at-encrypted-mhs-unacceptable-eits
 id-at-mhs-acceptable-eits
 id-at-mhs-deliverable-classes
 id-at-mhs-deliverable-content-types
 id-at-mhs-dl-archive-service
 id-at-mhs-dl-members
 id-at-mhs-dl-policy
 id-at-mhs-dl-related-lists
 id-at-mhs-dl-submit-permissions
 id-at-mhs-dl-subscription-service

ISO/CEI 10021-2:2004 (S)

<i>id-at-mhs-exclusively-acceptable-eits</i>	<i>objectIdentifierMatch</i>	- véase ISO/CEI 9594-2
<i>id-at-mhs-maximum-content-length</i>	<i>oRAddressElementsMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-message-store-dn</i>	<i>oRAddressMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-or-addresses</i>	<i>oRAddressSubstringElementsMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-or-addresses-with-capabilities</i>	<i>organizationalUnitName</i>	- véase ISO/CEI 9594-6
<i>id-at-mhs-supported-attributes</i>	<i>organizationName</i>	- véase ISO/CEI 9594-6
<i>id-at-mhs-supported-automatic-actions</i>	<i>oRNameElementsMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-supported-content-types</i>	<i>oRNameExactMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-supported-matching-rules</i>	<i>oRNameMatch</i>	- véase ISO/CEI 10021-5
<i>id-at-mhs-unacceptable-eits</i>	<i>oRNameSingleElementMatch</i>	- véase ISO/CEI 10021-5
<i>id-con</i>	<i>oRNameSubstringElementsMatch</i>	- véase ISO/CEI 10021-5
<i>id-con-dl-administrator-annotation</i>	<i>owner</i>	- véase ISO/CEI 9594-6
<i>id-con-dl-nested-dl</i>	<i>protocolInformation</i>	- véase ISO/CEI 9594-6
<i>id-con-dl-reset-originator</i>	<i>seeAlso</i>	- véase ISO/CEI 9594-6
<i>id-directory-objects-and-attributes</i>	<i>top</i>	- véase ISO/CEI 9594-2
<i>id-edims</i>		
<i>id-group</i>		
<i>id-ipms</i>		
<i>id-management</i>		
<i>id-mhs-protocols</i>		
<i>id-mod</i>		
<i>id-mr</i>		
<i>id-mr-address-capabilities-match</i>		
<i>id-mr-capability-match</i>		
<i>id-mr-orname-exact-match</i>		
<i>id-ms</i>		
<i>id-mts</i>		
<i>id-object-identifiers</i>		
<i>id-oc</i>		
<i>id-oc-mhs-distribution-list</i>		
<i>id-oc-mhs-message-store</i>		
<i>id-oc-mhs-message-transfer-agent</i>		
<i>id-oc-mhs-user</i>		
<i>id-oc-mhs-user-agent</i>		
<i>id-routing</i>		
<i>id-san</i>		
<i>id-san-mta-name</i>		
<i>integerMatch</i>	- véase ISO/CEI 9594-6	
<i>mhs-acceptable-eits</i>		
<i>mhs-deliverable-classes</i>		
<i>mhs-deliverable-content-types</i>		
<i>mhs-distribution-list</i>		
<i>mhs-dl-archive-service</i>		
<i>mhs-dl-members</i>		
<i>mhs-dl-policy</i>		
<i>mhs-dl-related-lists</i>		
<i>mhs-dl-submit-permissions</i>		
<i>mhs-dl-subscription-service</i>		
<i>mhs-exclusively-acceptable-eits</i>		
<i>mhs-maximum-content-length</i>		
<i>mhs-message-store</i>		
<i>mhs-message-store-dn</i>		
<i>mhs-message-transfer-agent</i>		
<i>mhs-or-addresses</i>		
<i>mhs-or-addresses-with-capabilities</i>		
<i>mhs-supported-attributes</i>		
<i>mhs-supported-automatic-actions</i>		
<i>mhs-supported-content-types</i>		
<i>mhs-supported-matching-rules</i>		
<i>mhs-unacceptable-eits</i>		
<i>mhs-user</i>		
<i>mhs-user-agent</i>		
<i>mta-name</i>		

<i>Abbreviations</i>			
A/SYS	30	asymmetric	48
AC	6	attribute	35
ACs	51	attribute list	35
ACSE	6, 51	attribute type	35
ADMD	32	attribute value	35
AE	5	common-name	37
APDU	5	conditional	7
AS/SYS	30	consuming ASE	48
ASE	5	consuming UE	48
ASEs	47	content	12
ASN.1	6	content type	12
AST/SYS	30	conversion	18
AT/SYS	30	country-name	37
AU	10	defaultable	7
C	7	delivery	16
COMPUSEC	19	delivery agent	16
D	7	delivery report	13
DL	9	described message	12
DSA	5	direct submission	16
EIT	13	direct user	9
M	7	distribution list	9
MASE	50	DL expansion	18
MD	31	domain	31
MDSE	50	domain-defined attribute	35
MHE	8	encoded information type	12
MHS	9	envelope	12
MRSE	49	event	14
MS	10	expansion point	18
MSSE	49	explicit conversion	18
MTA	11	export	16
MTS	10	extension-physical-delivery-address-components	38
MTSE	49	external routing	19
O	7	external transfer	16
OSI	5	formatted	43
P1	51	Global MHS	32
P3	51	grade	7
P7	51	immediate recipient	14
PDAU	11	implicit conversion	18
PDS	11	import	16
PRMD	32	indirect submission	16
RO	6	indirect user	9
ROSE	6, 50	intended recipient	15
RT	6	internal routing	19
RTSE	6, 51	internal transfer	16
S/SYS	30	joining	17
ST/SYS	30	local-postal-attributes	38
T/SYS	30	management domain	31
UA	10	mandatory	7
UE	5	member recipient	15
		members	9
		message	12
		Message Handling	8
		Message Handling Environment	8
		Message Handling System	9
		Message Storage	8
		message store	10
		Message Transfer	8
		message transfer agent	11
		Message Transfer System	10
		messaging system	29
		mnemonic OR-address	42
<i>Terms</i>			
access and storage system	30		
access and transfer system	30		
access system	30		
access unit	10		
access, storage, and transfer system	30		
actual recipient	15		
administration management domain	32		
administration-domain-name	37		
affirmation	18		

ISO/CEI 10021-2:2004 (S)

name resolution	18	transmittal	13
nested	9	transmittal event	14
network-address	38	transmittal step	14
non-affirmation	18	type	35
non-delivery	18	unformatted	43
non-delivery report	13	unformatted-postal-address	40
numeric OR-address	42	unique-postal-name	41
numeric-user-identifier	38	user	9
optional	7	user agent	10
OR-address	41	value	35
organizational-unit-names	39	Information items	
organization-name	38	address-capabilities-match	62
origination	15	capability-match	63
originator	14	DL Administrator Annotation	63
originator-specified alternate recipient	15	DL Nested DL	64
OR-name	34	DL Policy	60
pds-name	39	DL Reset Originator	64
personal-name	39	DL Submit Permission	59
Physical delivery	11	MHS Acceptable EITs	55
physical delivery access unit	11	MHS Deliverable Classes	56
physical delivery system	11	MHS Deliverable Content Types	56
physical message	11	MHS Distribution List	54
physical rendition	11	MHS DL Archive Service	56
physical-delivery-country-name	39	MHS DL Members	56
physical-delivery-office-name	39	MHS DL Policy	56
physical-delivery-office-number	39	MHS DL Related Lists	57
physical-delivery-organization-name	39	MHS DL Submit Permissions	57
physical-delivery-personal-name	39	MHS DL Subscription Service	57
postal OR-address	43	MHS Exclusively Acceptable EITs	57
postal-code	40	MHS Maximum Content Length	57
poste-restante-address	40	MHS Message Store	54
post-office-box-address	40	MHS Message Store Directory Name	57
potential recipient	15	MHS Message Transfer Agent	54
private management domain	32	MHS OR-Addresses	58
private-domain-name	40	MHS OR-Addresses with Capabilities	58
probe	12	MHS Supported Attributes	58
receipt	17	MHS Supported Automatic Actions	58
recipient	15	MHS Supported Content Types	58
recipient-assigned alternate recipient	15	MHS Supported Matching Rules	59
redirection	18	MHS Unacceptable EITs	59
report	13	MHS User	55
retrieval	16	MHS User Agent	55
routing	19	MTA Name	54
security policy	19	OR-Address	62
splitting	17	OR-Address with Capabilities	62
standard attribute	35	OR-name	63
step	14		
storage and transfer system	30	ASN.1 modules	
storage system	30	MHSDirectoryObjectsAndAttributes	67
street-address	40	MHSObjectIdentifiers	65
subject message	13		
subject probe	13	ASN.1 information object classes	
submission	16	ABSTRACT-ERROR	52
submission agent	16	ABSTRACT-OPERATION	52
submit permission	9	ATTRIBUTE	67
supplying ASE	48	ATTRIBUTE (Directory)	- see ISO/IEC 9594-2
supplying UE	48	ATTRIBUTE (MS)	- see ISO/IEC 10021-5
symmetric	48	AUTO-ACTION	- see ISO/IEC 10021-5
terminal OR-address	43	CONTEXT	- see ISO/IEC 9594-2
terminal-identifier	40	DIT-CONTEXT-USE-RULE	- see ISO/IEC 9594-2
terminal-type	40	MATCHING-RULE	- see ISO/IEC 9594-2
transfer	16	MHS-OBJECT	51
transfer system	30	MS-ATTRIBUTE	67

OBJECT-CLASS	- see ISO/IEC 9594-2	id-at-encrypted-mhs-supported-content-types	66
OTHER-NAME	- see ISO/IEC 9594-8	id-at-encrypted-mhs-supported-matching-rules	66
PORT	52	id-at-encrypted-mhs-unacceptable-eits	66
ASN.1 types		id-at-mhs-acceptable-eits	66
AddressCapabilities	62, 72	id-at-mhs-deliverable-classes	66
AlgorithmIdentifier	- see ISO/IEC 9594-8	id-at-mhs-deliverable-content-types	66
AlgorithmInformation	61, 72	id-at-mhs-dl-archive-service	66
AttributeTable	- see ISO/IEC 10021-5	id-at-mhs-dl-members	66
AutoActionTable	- see ISO/IEC 10021-5	id-at-mhs-dl-policy	66
Capability	62, 72	id-at-mhs-dl-related-lists	66
CertificateAssertion	- see ISO/IEC 9594-8	id-at-mhs-dl-submit-permissions	66
ContentLength	- see ISO/IEC 10021-4	id-at-mhs-dl-subscription-service	66
DLPolicy	61, 72	id-at-mhs-exclusively-acceptable-eits	66
DLSubmitPermission	59, 71	id-at-mhs-maximum-content-length	66
EncodedInformationTypesConstraints		id-at-mhs-message-store-dn	66
	- see ISO/IEC 10021-4	id-at-mhs-or-addresses	66
ExtendedContentType	- see ISO/IEC 10021-4	id-at-mhs-or-addresses-with-capabilities	66
ExtendedEncodedInformationType		id-at-mhs-supported-attributes	66
	- see ISO/IEC 10021-4	id-at-mhs-supported-automatic-actions	66
GlobalDomainIdentifier	- see ISO/IEC 10021-4	id-at-mhs-supported-content-types	66
ID	65	id-at-mhs-supported-matching-rules	66
MatchingRuleTable	- see ISO/IEC 10021-5	id-at-mhs-unacceptable-eits	66
MTAName	- see ISO/IEC 10021-4	id-con	65
Name	- see ISO/IEC 9594-2	id-con-dl-administrator-annotation	66
ORAddress	- see ISO/IEC 10021-4	id-con-dl-nested-dl	66
ORName	- see ISO/IEC 10021-4	id-con-dl-reset-originator	66
ORNamePattern	59, 71	id-directory-objects-and-attributes	65
RequestedDeliveryMethod	- see ISO/IEC 10021-4	id-edims	65
SecurityContext	- see ISO/IEC 10021-4	id-group	65
		id-ipms	65
ASN.1 values		id-management	65
addressCapabilitiesMatch	62, 73	id-mhs-protocols	65
any-user-may-submit	59, 71	id-mod	65
applicationEntity	- see ISO/IEC 9594-7	id-mr	65
capabilityMatch	63, 73	id-mr-address-capabilities-match	66
commonName	- see ISO/IEC 9594-6	id-mr-capability-match	66
description	- see ISO/IEC 9594-6	id-mr-orname-exact-match	66
distinguishedName	- see ISO/IEC 9594-6	id-ms	65
distinguishedNameMatch	- see ISO/IEC 9594-2	id-mts	65
dl-administrator-annotation	63, 73	id-object-identifiers	65
dl-administrator-annotation-use-rule	63, 73	id-oc	65
dl-nested-dl	64, 73	id-oc-mhs-distribution-list	66
dl-nested-dl-use-rule	64, 73	id-oc-mhs-message-store	66
dl-reset-originator	64, 73	id-oc-mhs-message-transfer-agent	66
dl-reset-originator-use-rule	64, 73	id-oc-mhs-user	66
id-arch	65	id-oc-mhs-user-agent	66
id-at	65	id-routing	65
id-at-encrypted-mhs-acceptable-eits	66	id-san	65
id-at-encrypted-mhs-deliverable-classes	66	id-san-mta-name	66
id-at-encrypted-mhs-deliverable-content-types	66	integerMatch	- see ISO/IEC 9594-6
id-at-encrypted-mhs-dl-archive-service	66	mhs-acceptable-eits	55, 69
id-at-encrypted-mhs-dl-members	66	mhs-deliverable-classes	56, 69
id-at-encrypted-mhs-dl-policy	66	mhs-deliverable-content-types	56, 69
id-at-encrypted-mhs-dl-related-lists	66	mhs-distribution-list	54, 68
id-at-encrypted-mhs-dl-submit-permissions	66	mhs-dl-archive-service	56, 70
id-at-encrypted-mhs-dl-subscription-service	66	mhs-dl-members	56, 70
id-at-encrypted-mhs-exclusively-acceptable-eits	66	mhs-dl-policy	56, 70
id-at-encrypted-mhs-maximum-content-length	66	mhs-dl-related-lists	57, 70
id-at-encrypted-mhs-message-store-dn	66	mhs-dl-submit-permissions	57, 70
id-at-encrypted-mhs-or-addresses	66	mhs-dl-subscription-service	57, 70
id-at-encrypted-mhs-or-addresses-with-capabilities	66	mhs-exclusively-acceptable-eits	57, 70
id-at-encrypted-mhs-supported-attributes	66	mhs-maximum-content-length	57, 70
id-at-encrypted-mhs-supported-automatic-actions	66	mhs-message-store	54, 69

ISO/CEI 10021-2:2004 (S)

mhs-message-store-dn	58, 70	oRAddressSubstringElementsMatch	- see ISO/IEC 10021-5
mhs-message-transfer-agent	55, 69	organizationalUnitName	- see ISO/IEC 9594-6
mhs-or-addresses	58, 71	organizationName	- see ISO/IEC 9594-6
mhs-or-addresses-with-capabilities	58, 71	oRNameElementsMatch	- see ISO/IEC 10021-5
mhs-supported-attributes	58, 71	oRNameExactMatch	63, 73
mhs-supported-automatic-actions	58, 71	oRNameMatch	- see ISO/IEC 10021-5
mhs-supported-content-types	58, 71	oRNameSingleElementMatch	- see ISO/IEC 10021-5
mhs-supported-matching-rules	59, 71	oRNameSubstringElementsMatch	- see ISO/IEC 10021-5
mhs-unacceptable-eits	59, 71	owner	- see ISO/IEC 9594-6
mhs-user	55, 69	protocolInformation	- see ISO/IEC 9594-6
mhs-user-agent	55, 69	seeAlso	- see ISO/IEC 9594-6
mta-name	64, 73	top	- see ISO/IEC 9594-2
objectIdentifierMatch	- see ISO/IEC 9594-2		
oRAddressElementsMatch	- see ISO/IEC 10021-5		
oRAddressMatch	- see ISO/IEC 10021-5		

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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
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

