UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

F.440

(08/92)

SERVICIO DE TRATAMIENTO DE MENSAJES

EXPLOTACIÓN Y DEFINICIÓN DEL SERVICIO

SERVICIOS DE TRATAMIENTO DE MENSAJES: SERVICIO DE MENSAJERÍA VOCAL

Recomendación F.440

PREFACIO

El CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) es un órgano permanente de la Unión Internacional de Telecomunicaciones (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 Asamblea Plenaria del CCITT, que se celebra cada cuatro años, establece los temas que han de estudiarse y aprueba las Recomendaciones preparadas por sus Comisiones de Estudio. La aprobación de Recomendaciones por los miembros del CCITT entre las Asambleas Plenarias de éste es el objeto del procedimiento establecido en la Resolución N.º 2 del CCITT (Melbourne, 1988).

La Recomendación F.440 ha sido preparada por la Comisión de Estudio I y fue aprobada por el procedimiento de la Resolución N.º 2 el 4 de agosto de 1992.

NOTA DEL CCITT

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una Administración de telecomunicaciones como una empresa privada de explotación reconocida de telecomu-nicaciones.

Recomendación F.440

SERVICIOS DE TRATAMIENTO DE MENSAJES: SERVICIO DE MENSAJERÍA VOCAL

(1992)

ÍNDICE

1 Finalidad y alcance

1.1 *Generalidades*

Esta Recomendación especifica los aspectos generales, operacionales y de calidad de servicio del servicio público internacional de mensajería vocal. Los servicios de mensajería vocal prestados por las Administraciones pertenecen al grupo de servicios telemáticos definidos en las Recomendaciones de la serie F.

Este tipo de servicio de tratamiento de mensajes (MH, *message handling*) es un servicio internacional de telecomunicación ofrecido por las Administraciones, que permite a los abonados enviar mensajes a uno o más recibientes y recibir mensajes por redes de telecomunicación, utilizando una combinación de técnicas de almacenamiento y retransmisión y de almacenamiento y extracción.

Las funciones proporcionadas localmente, para las que no se requiere la comunicación con otros abonados, no se tratan en las Recomendaciones del CCITT.

El servicio de mensajería vocal (VM, *voice messaging*) permite a los abonados solicitar que se emplee una diversidad de características durante el tratamiento e intercambio de mensajes vocales codificados.

Algunas características son inherentes al servicio VM básico. Otras características no básicas pueden ser seleccionadas por el abonado, mensaje por mensaje o durante un periodo de tiempo acordado por contrato, si son proporcionadas por las Administraciones.

Con el servicio VM puede proporcionarse, opcionalmente, la intercomunicación con el de mensajería interpersonal (IPM, *interpersonal messaging*).

Las características básicas tienen que ser facilitadas internacionalmente por las Administraciones. Las no básicas, visibles para el abonado, se clasifican en esenciales o adicionales.

Las características opcionales esenciales deben ser facilitadas internacionalmente por las Administraciones. Las características opcionales adicionales pueden ser facilitadas por algunas Administraciones para uso nacional, e internacionalmente por acuerdo bilateral. Las características no básicas se llaman facilidades facultativas de usuario.

La prestación del servicio VM se efectúa utilizando cualquier red de comunicaciones. Este servicio puede ofrecerse por separado o en combinación con diversos servicios telemáticos o de comunicación de datos. Puede obtenerse adoptando las disposiciones pertinentes.

Las especificaciones técnicas y los protocolos que han de utilizarse en el servicio VM se definen en las Recomendaciones de la serie X.400.

La definición del servicio figura en el § 2. Los § 3 y 4 describen los requisitos para la intercomunicación entre abonados. El § 5 describe la denominación y el direccionamiento, mientras que los § 6, 7 y 8 describen el funcionamiento del servicio, la calidad de servicio y los principios de tarificación y contabilidad. En el § 9 se dan los requisitos de red. La provisión de información al usuario figura en el § 10, y en el § 11 se informa sobre cómo utilizar la VM en el marco de los servicios telemáticos definidos por el CCITT.

1.2 *Sistemas de tratamiento de mensajes utilizados en la prestación del servicio de mensajería vocal*

1.2.1 *Realizaciones conformes a la versión de 1984*

Esta Recomendación supone que los sistemas de tratamiento de mensajes realizados para prestar el servicio en ella descrito se basan en la versión de 1988 de las Recomendaciones de la serie X.400. Se reconoce, sin embargo, que durante algún tiempo tras la publicación de esta Recomendación, la mayoría de las realizaciones del servicio VM se basarán en la versión de 1984 de las Recomendaciones de la serie X.400. Se alienta a las Administraciones a adoptar las Recomendaciones más recientes del CCITT; no obstante, en el periodo de transición podrán aplicar esta Recomendación a las realizaciones conformes con la versión de 1984, como se indica más adelante.

1.2.2 *Elementos de servicio*

Los elementos de servicio disponibles para los servicios de tratamiento de mensajes se enumeran y clasifican en la Recomendación F.400. El anexo C a la presente Recomendación establece una lista de los elementos de servicio utilizados en el servicio VM, según la Recomendación X.400 (versión de 1984), que se basan en los elementos de servicio IPM. El anexo C a la presente Recomendación (versión 1988) enumera tanto los elementos de servicio de 1988 como los de 1984 cuya clasificación cambió. El anexo D a la presente Recomendación enumera los elementos de servicio específicos del servicio VM. En el anexo E se dan las definiciones de los elementos de servicio para VM adicionales a los descritos en la Recomendación F.400 (1988). En todos los casos pueden utilizarse los elementos de servicio de 1984 para la prestación del servicio VM, tal como se describen en esta Recomendación, durante un periodo de gracia que concluye en 1996.

Se insta a las Administraciones a que actualicen sus realizaciones a este respecto conforme a las Recomendaciones de 1988.

1.2.3 *Formas de nombre*

Las formas de nombre que se han de utilizar en el servicio VM son coherentes con las especificadas en las Recomendaciones F.400 (1988) y X.400 (1988).

1.2.4 *Interfuncionamiento*

Para proteger las inversiones de las Administraciones que ya han realizado sistemas de la versión 1984 para la prestación del servicio VM, las realizaciones de dominios de gestión de Administración conformes a la versión de 1988 deben poder interfuncionar con los dominios de gestión de Administración (ADMD, *Administration management domain*) de 1984 como se indica en el anexo B de la Recomendación X.419.

El interfuncionamiento de las realizaciones ADMD de 1988 con los dominios de gestión privados (PRMD, *private management domains*) de 1984 es un asunto nacional.

2 Servicio de mensajería vocal

2.1 *Requisitos generales del servicio*

2.1.1 El servicio VM tiene por objeto fundamentalmente facilitar un interfaz público entre originadores y recibientes de comunicaciones vocales para mejorar sus medios de comunicación, especialmente cuando no se dispone de un servicio inmediato o adecuado de telecomunicación directa entre equipos de abonados o los servicios de telecomunicación de que se dispone son incompatibles. Este servicio puede proporcionar también características para la preparación y presentación de los mensajes.

2.1.2 Las Administraciones prestarán el servicio VM utilizando el servicio de transferencia de mensajes definido en la Recomendación F.410, y por sistemas conformes con las Recomendaciones de la serie X.400.

Los dominios de gestión (MD, *management domain*) se definen con el propósito de delimitar las responsabilidades. El MD regido por una Administración se denomina dominio de gestión de Administración (ADMD). El MD regido por una organización se denomina dominio de gestión privado (PRMD).

2.1.3 El intercambio internacional de mensajes se realiza entre dominios de gestión de Administración a través de servicios públicos de transmisión de datos normalizados por el CCITT.

2.1.4 A través de este servicio pueden intercambiarse diferentes tipos de partes del cuerpo de los mensajes. En el § 3 se enumeran los diferentes tipos de partes del cuerpo.

2.1.5 Una Administración puede proporcionar a los abonados diferentes métodos de acceso al servicio VM. Los métodos posibles son:

1) directamente desde el terminal del usuario, por ejemplo, un aparato telefónico;

2) a través de un sistema privado de tratamiento de mensajes.

Nota – El dominio de gestión de mensajería vocal puede residir en una centralita automática privada.

2.1.6 Cada Administración será responsable del acceso nacional a su dominio de gestión.

2.1.7 Las características de las interfaces y los métodos de acceso utilizados entre terminales y el servicio VM son asunto de carácter nacional, si bien pueden seguir las disposiciones del CCITT relativas al servicio telefónico. Se han definido, no obstante, las facilidades facultativas de usuario que ofrece el servicio VM, que son independientes del método de acceso y del terminal del usuario.

2.1.8 Una realización nacional del servicio VM puede proporcionar la intercomunicación con servicios existentes tales como el de IPM, el teletex, el facsímil y el videotex. Cuando se realicen las interfaces entre el servicio VM y otros servicios deberán cumplir las Recomendaciones pertinentes del CCITT.

2.1.9 Como el servicio proporciona comunicación indirecta, pueden producirse casos de no entrega del mensaje al recibiente deseado. El servicio VM provee la notificación de no entrega y, como facilidades facultativas de usuario, las notificaciones de entrega, de recepción y de no recepción.

2.1.10 Debido al almacenamiento intermedio del mensaje, el servicio puede proporcionar facilidades facultativas de usuario de conversión con respecto a: la velocidad, los procedimientos de acceso, las redes y la codificación del contenido del mensaje.

2.1.11 El mensaje pertenece al originador hasta que se haya realizado la entrega. Después de la entrega, el mensaje pertenece al recibiente.

2.1.12 Cuando el expedidor y el recibiente tengan necesidades diferentes y contrapuestas, tendrán precedencia las del expedidor (por ejemplo, conversión del tipo de cuerpo o control de redireccionamiento).

2.2 *Características del servicio de mensajería vocal*

2.2.1 *Introducción*

En el § 19 de la Recomendación F.400, se definen los elementos de servicio disponibles en el servicio VM y se clasifican como pertenecientes al servicio básico o como facilidades facultativas de usuario VM. Los elementos de servicio del servicio VM básico son parte integrante del servicio y siempre se proporcionan y están disponibles. Las facilidades facultativas de usuario que se clasifican como esenciales siempre estarán presentes y las clasificadas como adicionales pueden estar disponibles a nivel nacional, o a nivel internacional sobre la base de acuerdos bilaterales.

2.2.2 *Servicio de mensajería vocal básico*

El servicio VM básico comprende un conjunto de elementos de servicio, que se define en la Recomendación F.400 y se enumeran en el cuadro 10/F.400. El servicio VM básico, construido a partir del servicio de transferencia de mensajes (MT, *message transfer*), permite al usuario enviar y recibir mensajes vocales.

Un usuario prepara mensajes vocales con la ayuda de su agente de usuario (UA, *user agent*). Los agentes de usuario, que son un conjunto de procesos de aplicación de ordenador, cooperan entre sí facilitando la comunicación entre sus respectivos usuarios. Para enviar un mensaje vocal, los usuarios originadores efectúan una petición de sus UA, especificando el nombre o la dirección del recibiente que debe recibir el mensaje vocal. El mensaje vocal, que lleva consigo un identificador, es enviado a continuación por el UA del originador al UA del recibiente mediante el servicio de transferencia de mensajes.

Una vez lograda su entrega al UA del recibiente, el mensaje vocal puede ser recibido por el recibiente. Para facilitar una comunicación significativa, un usuario receptor puede especificar el (o los) tipos de información codificada que podrán contener los mensajes vocales entregados al usuario, así como la longitud máxima de los mismos. Cada mensaje vocal entregado va acompañado de la indicación del (o de los) tipos de información codificada originales, de cualquier conversión o conversiones que puedan haberse realizado, y del (o de los) tipos de información codificada resultante. Además, en cada mensaje vocal se especifican la hora de depósito, la hora de entrega y otras posibilidades. En el servicio básico se proporciona una notificación de no entrega.

2.2.3 *Facilidades facultativas de usuario del servicio de mensajería vocal*

Un conjunto de elementos de servicio del servicio VM son facilidades facultativas de usuario. Estas facilidades pueden seleccionarse mensaje por mensaje o por un periodo de tiempo convenido, y se enumeran en los cuadros 11/F.400 y 12/F.400, respectivamente. Las facilidades de usuario locales pueden ser proporcionadas convenientemente junto con algunas de estas facilidades de usuario.

Las facilidades facultativas de usuario del servicio VM seleccionadas mensaje por mensaje son clasificadas tanto para el origen como para el destino por los UA. Si una Administración proporciona el servicio VM y ofrece estas facilidades facultativas de usuario para ser originadas por los UA, el usuario puede crear y enviar mensajes vocales de acuerdo con los procedimientos definidos para el elemento de servicio asociado. Si una Administración presta el servicio VM y ofrece estas facilidades facultativas de usuario para la recepción por los UA, el UA receptor podrá recibir y reconocer la indicación asociada con el elemento de servicio correspondiente, e informar al usuario de la facilidad facultativa de usuario solicitada. Cada facilidad de usuario se clasifica como adicional o esencial para los UA desde estas dos perspectivas.

2.2.4 *Funciones locales*

El sistema de tratamiento de mensajes (MHS, *message handling system*) puede efectuar muchas funciones locales para sus abonados y facilitar además características de VM. Puede, por ejemplo, ayudar a los abonados a preparar y editar mensajes vocales proporcionándoles una capacidad de edición. El MHS podría avisar a los abonados cuando llegaran nuevos mensajes (por ejemplo, con un aviso lumínico de mensaje en sus teléfonos o visualizando en sus terminales el nombre del originador y el tema de todos los mensajes no leídos, o por indicación vocal iniciada por ordenador).

Si no se dispone de un medio de aviso, es posible que el abonado tenga que acceder frecuentemente al MHS para saber si han llegado nuevos mensajes.

El MHS puede proporcionar controles de bases de datos locales que ayuden al abonado a encontrar mensajes vocales recibidos y archivados con anterioridad (a encontrar, por ejemplo, el mensaje de la Sra. García entregado un día del mes de agosto). Un abonado que esté de vacaciones puede pedir que el MHS reenvíe automáticamente todos los mensajes vocales a un delegado, o fijar las reglas para que no se reenvíen automáticamente algunos mensajes vocales (por ejemplo, los mensajes personales).

Los servicios locales como los arriba indicados no requieren la coordinación o cooperación con otros abonados, aunque utilicen quizás algunas de las características VM. No influyen, por tanto, en los protocolos de comunicación asociados al MHS. Las funciones locales que puedan prestar las Administraciones quedan, por tanto, fuera del alcance del CCITT.

2.3 *Delimitación de las responsabilidades*

El objetivo del MHS es facilitar el depósito de los mensajes para su transferencia al destino y su entrega a un UA/MS cuya dirección haya especificado el originador.

El usuario interactúa, utilizando un terminal de acceso, con un UA en los lados emisión y recepción. A petición, se deposita el mensaje en el sistema de transferencia de mensajes (MTS, *message transfer system*). También puede extraer un mensaje recibido de un UA o una memoria de mensajes (MS, *message store*).

La responsabilidad del mensaje sigue siendo del MHS cuando el usuario de origen da la orden de enviarlo. Una vez lograda la entrega, la responsabilidad del mensaje se transfiere al UA/MS receptor. Si el UA o la MS lo proporciona la Administración, el usuario asume la responsabilidad del mensaje cuando éste se reproduce. Como característica básica, el MHS crea una notificación de no entrega, cuando no es posible la entrega al UA/MS receptor.

Las condiciones aplicadas a este criterio pueden depender además de las facilidades facultativas de usuario, por ejemplo, de la prohibición de conversión. Un usuario de origen puede solicitar de manera específica, para un determinado mensaje, una notificación de entrega y/o una notificación de recepción y/o una notificación de no recepción. En el caso de direcciones telemáticas, la entrega se produce automáticamente cuando se transmite el mensaje al servicio telemático. Tras su entrega a una memoria de documentos o a una memoria de mensajes, la responsabilidad del mensaje vuelve a ser del usuario, en cuanto lo haya leído una vez. Si el mensaje se deja en la memoria, la responsabilidad será definida por el proveedor del servicio.

Puede producirse una pérdida de información en el proceso de conversión, siempre que ésta no haya sido prohibida explícitamente por el usuario de origen.

La responsabilidad de los mensajes transferidos a través de dominios de gestión (MD) comienza cuando entran en el dominio y termina cuando lo abandonan, pero debe ser posible una auditoría posterior.

Cuando un ADMD interactúa con un PRMD, el ADMD asume la responsabilidad de las acciones del PRMD relacionadas con la interacción. Además de asegurar que el PRMD proporciona debidamente el servicio MT, el ADMD debe garantizar que se realicen correctamente las funciones de contabilidad, inscripción en fichero registro cronológico, calidad de servicio y otras operaciones conexas del PRMD. El ADMD actúa a modo de autoridad de denominación para los PRMD asociados, de conformidad con las directrices nacionales.

2.4 *Memoria de mensajes*

Las Administraciones pueden proporcionar opcionalmente una memoria de mensajes (MS) para facilitar la entrega de mensajes sin que el UA del recibiente tenga que estar en línea continuamente. En el § 7.4 de la Recomendación F.400 hay una descripción de lo indicado. Se considera que la entrega de un mensaje a una MS, la efectúa el MHS. Los mensajes entregados a una MS pueden ser recuperados por el recibiente a su conveniencia, y pueden proporcionarse diferentes facilidades facultativas de usuario que permitan el listado, la búsqueda y la supresión de mensajes. En caso de abono a un MS, todos los mensajes destinados al UA son entregados a la MS, enviándose al UA un aviso (desde la MS) para informar al usuario de que acaba de llegar un mensaje.

2.5 *Unidad de acceso al servicio telefónico*

La unidad de acceso al servicio telefónico (TSUA, *telephone service access unit*) es una unidad de acceso que proporciona interfuncionamiento entre un usuario del servicio de mensajería vocal (servicio VM) o del servicio de mensajería interpersonal (servicio IPM) y usuarios del servicio telefónico. Los usuarios del servicio VM pueden solicitar la entrega de un mensaje vocal a cualquier usuario del servicio telefónico que puede ser direccionado por medio de una dirección de red telefónica (número telefónico). Los usuarios del servicio telefónico pueden hacer que un mensaje vocal sea grabado y entregado a usuarios del servicio VM y del servicio IPM por medio de la TSAU.

2.5.1 *Descripción de las funciones de la TSAU*

En el entorno del MHS, el agente de usuario del servicio IPM o del servicio VM puede acceder a la red telefónica a través de la TSAU. El usuario del MHS compone el mensaje vocal mientras interactúa con el UA y lo designa para su entrega a un usuario de la red telefónica. El usuario del MHS especifica también el número telefónico del recibiente utilizando una dirección O/R numérica. La parte del cuerpo vocal del MHS es enviada en un sobre F.400 a la TSAU, que extrae la parte del cuerpo vocal del sobre MHS y llama al recibiente por la red telefónica para entregarle el mensaje vocal. Cuando el mensaje vocal se pasa a la TSAU, se envía una notificación de entrega al originador. Los algoritmos que controlan el comportamiento llamante de la TSAU son un asunto de carácter local.

Un usuario de la red telefónica puede llamar a la TSAU, grabar un mensaje, proporcionar una dirección de entrega (restringida a los caracteres numéricos previstos en el teclado telefónico) y solicitar la entrega del mensaje a un usuario del servicio VM o del servicio IPM.

2.5.2 *Entrega asistida*

La TSAU entregará normalmente el mensaje a cualquiera que conteste al teléfono en la dirección del recibiente. La entrega asistida permite a un asistente (telefonista) ayudar en la entrega del mensaje. Cuando se selecciona, el usuario del servicio VM puede especificar que el mensaje sólo puede ser entregado a un recibiente

designado. El asistente indagará si el recibiente está disponible antes de entregar el mensaje vocal y sólo lo entregará si dicho recibiente designado está disponible para recibirlo. El asistente puede utilizar el indicador de recibiente para indagar si el recibiente está presente.

2.5.3 *Notificaciones de la TSAU*

La TSAU que sirve a usuarios del servicio telefónico utiliza informes de entrega del MTS para indicar la transferencia del mensaje del MTS a la TSAU y notificaciones vocales (de recepción y de no recepción) para indicar la recepción satisfactoria en el terminal telefónico.

2.6 *Utilización de directorios*

Mediante los sistemas de directorio, los usuarios del servicio VM podrán direccionar a los recibientes, utilizando los nombres de directorio o los nombres de listas de distribución, cuyo empleo es más cómodo que las direcciones O/R. El MHS podrá acceder a un sistema de directorio, y encontrar la dirección o direcciones O/R correspondientes a un determinado nombre de directorio o de lista de distribución, para entregar un mensaje. Un número telefónico internacional tiene todas las propiedades de un nombre de directorio. En el § 14 de la Recomendación F.400 se describe esta capacidad.

2.7 *Seguridad*

Las Administraciones pueden proporcionar, opcionalmente, los mecanismos de seguridad descritos en el § 15 de la Recomendación F.400, para hacer frente a las diferentes amenazas a la seguridad mencionadas. Esta capacidad puede utilizar un sistema de directorio para almacenar copias certificadas de claves públicas de usuarios del MHS.

2.8 *Listas de distribución*

Un grupo de usuarios, cuya condición de miembro esté almacenada en el directorio, puede utilizarse como lista de distribución (DL, *distribution list*). El originador suministra simplemente el nombre de la lista al depositar un mensaje y el MHS obtiene los nombres de directorio (y a continuación las direcciones O/R) de los distintos recibientes, consultando el directorio. Al recibir un mensaje dirigido a una lista de distribución, el recibiente puede determinar a través de qué DL ha llegado. Un originador puede prohibir la expansión de la distribución si uno de los recibientes especificados se refiere a una lista de distribución. En el § 14 de la Recomendación F.400 se describen todas las capacidades de que disponen los usuarios de DL.

Si un usuario envía inadvertidamente un mensaje a una DL, quizás se le carguen múltiples entregas que no esperaba. Por ello, los nombres de las listas de distribución deberán indicar que lo que se está designando es una DL. Los propietarios de DL deberían garantizar además que respetan el deseo de un miembro potencial de convertirse en miembro así como a las reglas del país de éste, que pueden prohibir su inclusión sin un acuerdo previo.

3 Tipos de partes del cuerpo

Los mensajes enviados y recibidos en el servicio VM pueden estar compuestos por una o más partes del cuerpo.

3.1 *Tipos de partes del cuerpo aplicables*

En la Recomendación X.440 se definen los tipos de partes del cuerpo aplicables, que constan de lo siguiente:

– voz,

– mensaje (por ejemplo, para un mensaje reenviado),

– notificaciones,

– definido externamente.

En principio, la codificación vocal soportada será la MICDA a 32 kbit/s, especificada en la Recomendación G.721 (1988). Es posible que en el futuro se añadan sistemas de codificación a velocidades binarias inferiores.

3.2 *Estructura de los mensajes vocales*

La categoría de agentes de usuario de mensajería vocal (VM-UA, *voice messaging user agent*) crea mensajes con un contenido específico del servicio de mensajería vocal. Dicho contenido, enviado desde un VM-UA a otro, es el resultado de un originador, generalmente una persona que interactúa con un teléfono, que compone y envía un mensaje llamado mensaje vocal. El mensaje vocal llevará el objeto vocal codificado y, opcionalmente, otra información asociada al mismo. Sólo un mensaje vocal estará presente en un objeto vocal codificado y cada mensaje vocal contendrá, al originarse, una parte del cuerpo vocal codificada. En la figura 1/F.440 se muestra la estructura de un mensaje vocal, similar a la de un mensaje básico del MHS. Cuando el mensaje vocal se transfiere a través del MHS, se transmite con un sobre electrónico.

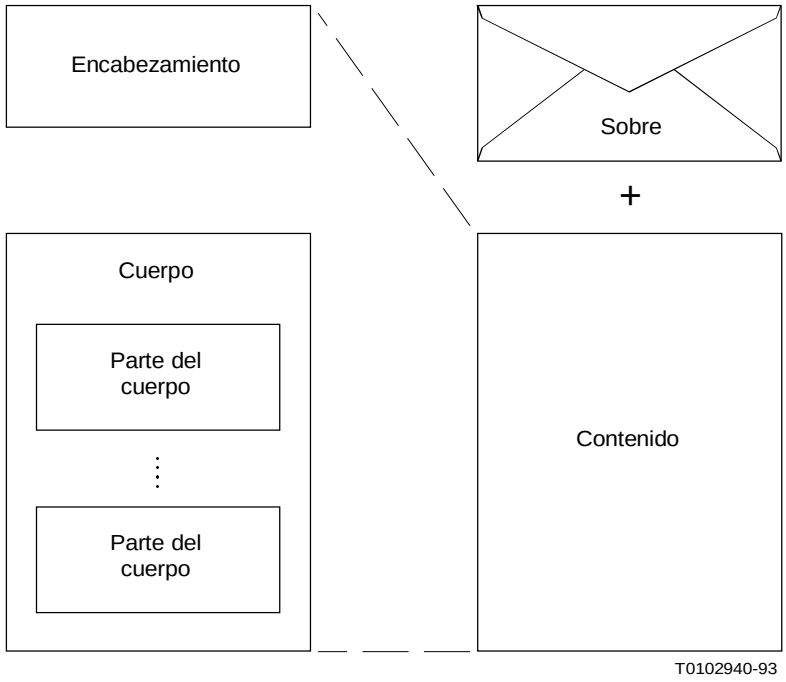


FIGURA 1/F.440
Estructura de mensaje vocal

La figura 2/F.440 muestra la correspondencia entre un objeto vocal codificado típico y la correspondiente estructura de mensaje vocal. El objeto vocal se hace corresponder enteramente con una de las partes del cuerpo, llamada parte del cuerpo primaria, y puede ser un objeto vocal codificado privadamente o según la Recomendación G.721, o bien un mensaje vocal reenviado. A menos que se especifique lo contrario, se supondrá que este objeto vocal está codificado mediante MICDA a 32 kbit/s de la Recomendación G.721. Se dispone de otras partes de cuerpo para transportar información asociada al objeto vocal codificado, tal como dibujos, información de texto adicional, etc. El encabezamiento del mensaje vocal contiene diversos campos de información que transportan peticiones de servicio procedentes del originador. Esto se representa en la figura 2/F.440 como campo-V-C *n*, para información vocal codificada, y campo *n*, para información no vocal codificada.

El encabezamiento y la (o las) partes del cuerpo constituyen el mensaje vocal. Un mensaje vocal puede constar de un sólo objeto vocal codificado, contenido totalmente en una parte del cuerpo.

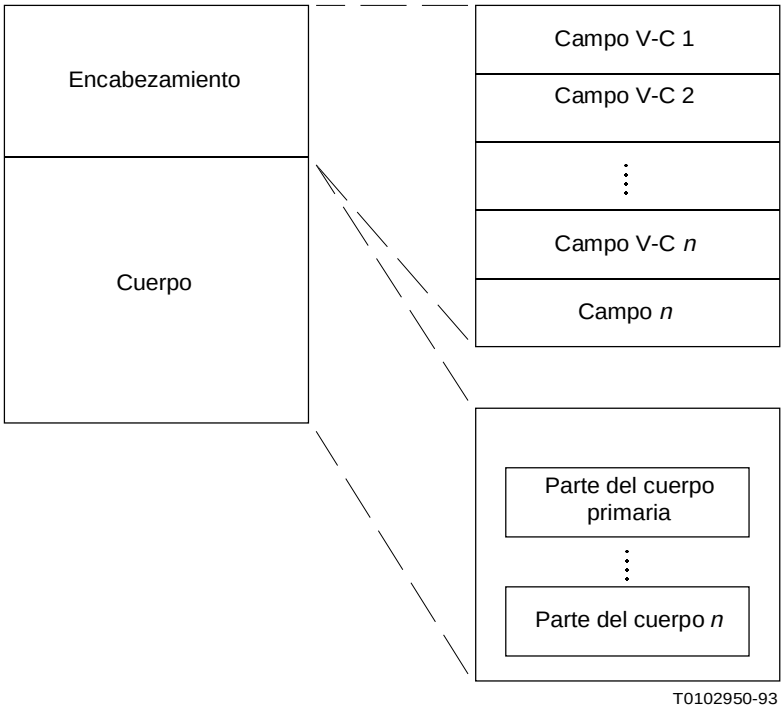


FIGURA 2/F.440
Estructura de mensaje vocal de una transacción de mensajería vocal típica

3.3 *Reenvío de mensajes vocales*

Un usuario del servicio de mensajería vocal puede hacer que los mensajes recibidos sean reenviados con o sin aceptación. La petición de notificaciones puede reenviarse también automáticamente, junto con el mensaje reenviado. Pueden distinguirse tres casos:

a) reenvío del mensaje vocal aceptado con las notificaciones solicitadas,

b) reenvío del mensaje vocal y notificaciones sin aceptación, y

c) reenvío del mensaje vocal cuando no se solicitan notificaciones.

El tercer caso es en realidad idéntico al segundo. Un usuario puede solicitar también que se establezca el reenvío automático.

Si se reenvía un mensaje vocal después de la aceptación, la parte del cuerpo primaria del mensaje reenviado es el contenido del mensaje recibido con o sin modificaciones. Pueden incluirse o suprimirse partes del cuerpo de mensaje vocal adicionales, pero puede no haber más de una parte vocal del cuerpo codificada adicional para cada caso de reenvío. La parte del cuerpo del mensaje vocal reenviado puede no suprimirse. Se emitirán notificaciones de recepción según se soliciten. En el reenvío, no se devolverá al originador del mensaje una notificación de no recepción (NRN, *non receipt notification*). El reenvío de mensajes vocales puede efectuarse a uno o más recibientes, y pueden establecerse peticiones de notificación para cualquiera de estos recibientes.

Las partes del cuerpo pueden no añadirse o suprimirse si se reenvía un mensaje vocal sin aceptación. El reenvío puede hacerse a más de un recibiente. La petición de notificación debe ser igual que para el mensaje original, pero sólo puede enviarse a uno de los recibientes del mensaje reenviado. Esto asegurará que el originador original sólo recibe la notificación que solicitó.

4 Conversión entre diferentes tipos de información codificada

El MTS proporciona funciones de conversión que permiten a los usuarios VM introducir mensajes en un formato codificado, llamado tipo de información codificada (EIT, *encoded information type*), y que su entrega se haga en otro EIT para atender a usuarios con diferentes tipos de terminal. Esta capacidad es inherente al servicio VM y aumenta la posibilidad de entrega conformando el mensaje a las capacidades del terminal del recibiente. Los EIT soportados por el servicio VM se definen en la Recomendación X.440.

El MTS puede proporcionar la conversión automática entre diferentes esquemas de codificación normalizados, cuando así se requiera para la entrega del mensaje.

Los aspectos generales de la conversión y las reglas específicas de conversión entre diferentes EIT en el servicio VM quedan en estudio.

5 Denominación y direccionamiento en general

En un MHS, la principal entidad que requiere denominación es el usuario (originador y recibiente de los mensajes). Además, las listas de distribución (DL) tienen nombres que se emplean en el MHS. Los usuarios del MHS y las DL se identifican mediante nombres O/R. Los nombres O/R están compuestos por nombres de directorio y/o direcciones O/R, cuyas descripciones se ofrecen en este punto. La Recomendación F.401 da más detalles sobre denominación y direccionamiento para los servicios públicos de tratamiento de mensajes, incluidas las restricciones relativas a la denominación y las responsabilidades de las Administraciones.

5.1 *Nombres de directorio*

Los usuarios del servicio MHS, así como las DL, pueden identificarse por un nombre, llamado nombre de directorio. Este nombre debe utilizarse para buscar en el directorio la dirección O/R correspondiente para un servicio determinado. La estructura y los componentes de los nombres de directorio se describen en las Recomendaciones de la serie X.500.

Un usuario puede acceder directamente a un sistema de directorio para encontrar la dirección O/R de otro usuario, o las direcciones O/R de los miembros de una DL (ambos casos caen fuera del alcance de estas Recomendaciones).

Como alternativa, un usuario puede utilizar el nombre de directorio y hacer que el MHS acceda al directorio para encontrar automáticamente la dirección o direcciones O/R correspondientes. No es necesario que cada usuario MHS o cada DL tenga un nombre de directorio, a menos que estén registrados en un directorio. A medida que los directorios se utilicen cada vez más, se prevé que los nombres de directorio serán el método preferido para que los usuarios del MHS se identifiquen entre sí.

5.2 *Nombres O/R*

Cada usuario MHS o cada DL tendrá un nombre O/R. Este comprende un nombre de directorio, una dirección O/R, o ambos. El nombre de directorio identifica sin ambigüedad a un usuario del MHS, pero no necesariamente de forma exclusiva. La dirección O/R identifica exclusivamente al usuario MHS.

Para depositar un mensaje se puede utilizar uno o ambos componentes de un nombre O/R. Si sólo se suministra el nombre de directorio, el MHS tendrá acceso a un directorio para intentar determinar la dirección O/R, que utilizará después para encaminar el mensaje y entregarlo. Si no se indica el nombre de directorio, utilizará la dirección O/R dada. Cuando se indiquen ambos elementos al efectuar el depósito, el MHS utilizará la dirección O/R, pero cursará el nombre de directorio, y presentará ambos al recibiente. Si la dirección O/R es incorrecta, intentará utilizar el nombre de directorio como se indica anteriormente.

5.3 *Direcciones O/R*

Una dirección O/R contiene información que permite al MHS identificar en forma única a un usuario a fin de entregarle un mensaje o devolverle una notificación. (El prefijo «O/R» reconoce el hecho de que el usuario puede actuar como originador o como recibiente del mensaje o de la notificación de que se trata.)

Están definidas actualmente varias formas de direcciones O/R, cada una con su propia finalidad. Esas formas y finalidades son las siguientes:

– *Dirección O/R numérica:* Proporciona un medio de identificar a los usuarios con teclados numéricos.

– *Dirección O/R de terminal:* Proporciona un modo de identificar a los usuarios con terminales pertenecientes a diferentes redes.

– *Dirección O/R nemónica:* Proporciona un medio práctico para el usuario de identificar a otros usuarios en ausencia de un directorio. Se utiliza también para identificar una lista de distribución.

Una dirección O/R está constituida por un conjunto de informaciones denominadas atributos. En la Recomendación F.401 se detallan estos atributos, tal como se utilizan en cada una de las formas de dirección O/R, antes mencionadas.

Los dominios de gestión deben permitir a sus usuarios enviar mensajes utilizando cualesquiera de las formas indicadas. La forma en la que los nombres son introducidos por el abonado o presentados a este, es un asunto de carácter nacional (como por ejemplo, la utilización de listas de distribución o de maneras fáciles y comprensibles de identificar a los agentes de usuario). Se prevé que la dirección O/R numérica será la utilizada más frecuentemente en el servicio VM.

Cada Administración es responsable de la identificación exclusiva de cada agente de usuario de su dominio de gestión.

6 Funcionamiento del servicio

6.1 *Generalidades*

6.1.1 El servicio VM ofrece la posibilidad de enviar, transferir, entregar y recibir mensajes utilizando procedimientos totalmente automáticos.

6.1.2 Los mensajes se preparan en una memoria, se envían desde una memoria y se entregan a una memoria. Estas memorias forman parte de la funcionalidad agente de usuario/memoria de mensajes y están bajo el control del usuario.

6.1.3 La transferencia de mensajes entre dominios de gestión se hará de acuerdo con el servicio de transferencia de mensajes descrito en la Recomendación F.410.

6.1.4 Cada Administración que presta el servicio VM debe validar las identidades de los abonados, en el momento del acceso.

6.1.5 Es un asunto nacional la autorización o prohibición de la conexión de sistemas de mensajería privados con el servicio público de VM a fin de que los usuarios de estos sistemas puedan intercambiar mensajes. Si se proporcionan estas interconexiones, deberán efectuarse entre dominios de gestión de Administración, de acuerdo con las Recomendaciones del CCITT.

6.1.6 Si la Administración proporciona la conversión implícita mediante el servicio de transferencia de mensajes, se convertirá el mensaje si es necesario, a menos que lo prohíba el originador. La conversión se efectuará de acuerdo con las reglas especificadas en la Recomendación X.408. Véase también el § 4 de la presente Recomendación.

6.1.7 La entrega diferida la proporcionará el dominio de gestión del originador, quien es responsable del almacenamiento del mensaje hasta la fecha y hora especificadas para la entrega prevista. Por esta razón, el elemento de servicio entrega diferida no debería utilizarse a través de enlaces internacionales.

6.2 *Fases de tratamiento de los mensajes*

6.2.1 *Generalidades*

El servicio VM tiene diferentes fases de tratamiento de los mensajes que son visibles para el usuario.

6.2.2 *Fase de preparación*

En esta fase se preparan los mensajes utilizando la funcionalidad agente de usuario (por ejemplo, captación, edición y archivo). La manera de realizar estas funciones cae fuera del ámbito de la presente Recomendación.

6.2.3 *Fase de envío*

En esta fase, el originador puede pedir al agente de usuario o a la memoria de mensajes que envíen un mensaje preparado a uno o más recibientes y solicitar ciertas facilidades facultativas de usuario.

6.2.4 *Fase de recepción*

En esta fase, el abonado puede recibir mensajes entregados y notificaciones del agente de usuario o de la memoria de mensajes. La fase de recepción la puede iniciar el servicio (recepción automática) o el abonado para la recepción de mensajes. En la Recomendación X.440 se especifica el funcionamiento de los agentes de usuario que reciben mensajes.

Los abonados que utilicen terminales sin la funcionalidad agente de usuario pueden registrarse por un periodo contractual, durante el cual recibirán automáticamente de su agente de usuario los mensajes entregados a un terminal, si la Administración ofrece esta posibilidad. Para recibir mensajes entrantes se llama, normalmente, al agente de usuario.

En caso de recepción automática, el MHS efectuará una llamada al terminal del abonado. En el otro caso, el abonado efectuará una llamada al MHS en el momento que lo considere adecuado.

Las partes del cuerpo del mensaje serán recibidas por el abonado en la forma en que el originador las ha enviado, a menos que se haya efectuado una conversión.

La indicación de las facilidades facultativas de usuario solicitadas por el originador las presenta el agente de usuario al recibiente en una forma conveniente para el usuario.

Notificaciones: Pueden recibirse cuatro notificaciones:

- notificación de no entrega;
- notificación de entrega;
- notificación de recepción;
- notificación de no recepción.

La notificación de no entrega la origina automáticamente el MTS, mientras que las notificaciones de entrega, recepción y no recepción dependen de la acción del recibiente.

6.2.5 *Notificaciones de servicio*

Las notificaciones de servicio se envían solamente a petición del originador. Se envían inmediatamente después de que el mensaje deja el MTS para el UA o la MS del recibiente. Las notificaciones de servicio las puede generar un UA o una MS o una TSAU cuando se solicita en el indicador de petición de notificación vocal (VN, *voice notification*) por cada recibiente. Los motivos de la notificación de servicio se especifican en el anexo B para el elemento de servicio «petición de notificación de mensaje vocal».

7 Calidad de servicio

7.1 *Situación de los mensajes*

La identificación exclusiva de cada mensaje vocal permite al sistema proporcionar información, por ejemplo, sobre la situación de un mensaje vocal.

En caso de fallo del sistema, deberá poder seguirse el rastro de todos los mensajes aceptados y no entregados. Si los mensajes no pueden entregarse, deberá informarse de ello al originador mediante una notificación de no entrega.

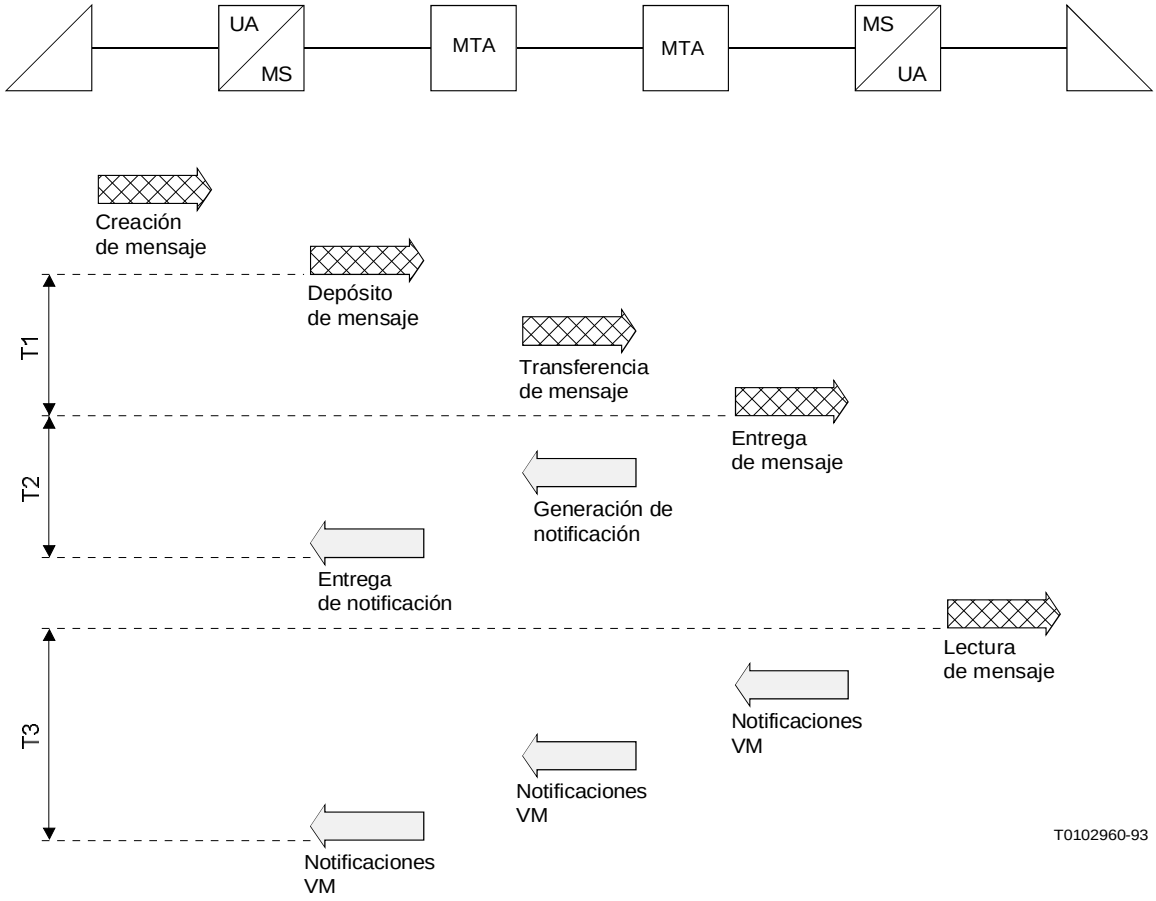
7.2 *Asistencia de las Administraciones*

Las Administraciones deben proporcionar asistencia a sus abonados con respecto a las notificaciones de no entrega que no se reciban oportunamente, en lo que respecta a los componentes del sistema público. Puede suministrarse asimismo bajo la responsabilidad de cada país, asistencia relativa a la situación y al rastreo de los mensajes.

Cuando el agente de usuario lo proporciona una Administración, ésta deberá suministrar funcionalidad adicional para reducir al mínimo los casos en que no se lean los mensajes en un plazo determinado (la definición de dicho plazo queda en estudio). Esta funcionalidad podría ser, por ejemplo, mensajes de alerta enviados a un terminal de recepción automática.

7.3 *Modelo de tiempos de entrega y de notificación*

Véase la figura 3/F.440.



T1 Tiempo de entrega
T2 Tiempo de notificación de entrega
T3 Tiempo de notificaciones VM
} Para más detalles véase la Recomendación

Nota 1 – La hora de comienzo de T3 corresponde a la hora en que el mensaje se presenta visualmente al usuario y éste envía la notificación VM.

Nota 2 – La hora de terminación de T3 es la hora en que la notificación VM se indica al usuario a través del UA o el MS.

Nota 3 – Consideraciones similares son aplicables a las notificaciones de no recepción.

FIGURA 3/F.440

Modelo de tiempo de notificación

7.4 *Objetivos de tiempo de entrega de los mensajes*

El dominio de gestión del UA del recibiente debería forzar la notificación de no entrega si el mensaje no ha sido entregado antes de *x* horas después del depósito (o después de la fecha y hora indicadas para entrega diferida). El valor de *x* depende del grado de clase de entrega solicitado por el originador. (Véase el § 4.4 de la Recomendación F.410.)

7.5 *Objetivos de tiempo de notificación de entrega*

Las notificaciones de no entrega, o las notificaciones de entrega solicitadas, deben devolverse recibiente por recibiente para no retardar las notificaciones relativas a los mensajes a múltiples direcciones que ya hayan sido entregados, y permitir al dominio de gestión de origen devolver una notificación por cada recibiente, o transmitir por lotes las notificaciones a sus abonados. (Véase el § 4.5 de la Recomendación F.410.)

7.6 *Notificaciones de recepción y de no recepción*

Los tiempos de entrega de las notificaciones de recepción, no recepción y de disponibilidad de elementos de servicio dependen, en primer lugar, de los arreglos locales. Cuando son iniciadas por el usuario/UA receptor, tienen los mismos objetivos de tiempo que los mensajes que las provocaron.

CUADRO 1/F.440

Objetivos de tiempo de las notificaciones

Grado de entrega (del mensaje en cuestión)	En el 95%, entregados en un plazo de	No entrega forzada después de
Urgente	0,25 horas	2 horas
Normal	1,0 hora	6 horas
No urgente	4,0 horas	12 horas

Nota – La intercomunicación con los PRMD no se incluye en el cálculo de los objetivos de tiempo.

7.7 *Protección contra errores*

La protección contra errores en la transmisión la proporcionan el MHS y los protocolos subyacentes utilizados en la prestación del servicio VM.

7.8 *Disponibilidad del servicio*

En principio, el servicio VM debe estar permanentemente disponible. El agente de usuario debe estar permanentemente disponible para el depósito o la entrega (a menos que se invoque la retención de entrega). En los casos en que el UA no esté permanentemente disponible para la entrega, deberá utilizarse una memoria de mensajes.

7.9 *Capacidad mínima de almacenamiento*

La capacidad de almacenamiento de un agente de usuario y de una memoria de mensajes deberá ser suficiente para conseguir un elevado grado de servicio.

Nota – Esto queda en estudio.

8 Tariff and accounting principles

See the D-Series Recommendations.

9 Network requirements

The VM-service is network independent, that is, the basic service and the essential optional user facilities are provided independently of the type of network used for service access. Additional optional user facilities chosen by an Administration to offer may vary.

10 User information and support

A directory shall be provided by each Administration for its domain. The directory can be hard copy or preferably electronic form.

The directory shall at least contain the following:

a) how to use the directory and the service;

b) list of O/R addresses of subscribers belonging to the Administrations domain;

c) list of standardized abbreviations for O/R address attributes;

d) list of country and administration management domain names reachable by the public VM-service.

11 Use of the VM-service within CCITT defined telematic services

In the telematic services, intercommunication between the VM-service and the IPM-service is desirable. Intercommunication with other Telematic Services is for further study.

Intercommunication with the telephone service is provided for by means of the optional telephone service access unit.

ANNEX A

(to Recommendation F.440)

Abbreviations

The following abbreviations are used in this Recommendation:

ADMD	Administration management domain
ADPCM	Adaptive differential pulse code modulation
AU	Access unit
DL	Distribution list
EIT	Encoded information type
IP	Interpersonal
IPM	Interpersonal messaging
MD	Management domain
MH	Message handling
MHS	Message handling system
MS	Message store
MT	Message transfer

MTA	Message transfer agent
MTS	Message transfer system
N/A	Not applicable
NRN	Non-receipt notification
O/R	Originator/recipient
PDN	Public data network
PRMD	Private management domain
TS	Telephone service
TSAU	Telephone service access unit
UA	User agent
VM	Voice messaging
VM-MS	Voice messaging store
VM-UA	Voice messaging user agent
VN	Voice notification

Note 1 – For a glossary of terms, see Annex A of Recommendation F.400.

Note 2 – For references, see Recommendations F.400 and F.401.

ANNEX B

(to Recommendation F.440)

Subscriber access and terminal requirements

B.1 *General*

Various types of terminals may be used for accessing the service. These terminals are functionally divided into two categories; those without user agent functionality, and those with user agent functionality. The telematic terminals assume a special user agent.

B.2 *Terminals without UA functionality*

Terminals in this category require additional functions to be provided by MHS to enable their participation in the VM-service.

In this category are voice terminals or telephone subscriber sets as commonly used in telephony.

B.3 *Terminals with UA functionality*

These terminals shall, as a minimum, have the capabilities to:

1) provide the capabilities to subscribers of the basic features defined in § 2;
2) have speech input and output capability;
3) make use of the VM protocol specified in Recommendation X.440;
4) use the submission and delivery protocol specified in Recommendation X.419;
5) use the remote operation procedures specified in Recommendation X.419.

This type of terminal may be configured to access both the IPM-and VM-services.

ANNEX C

(to Recommendation F.440)

VM elements of service for 1984 systems

TABLE C-1/F.440

Elements of service	Classification			
	Basic	Optional		
		Origination	Reception	Contractual
Access management	X			
Alternate recipient allowed		A	A	
Alternate recipient assignment				A
Authorizing users indication		A	E	
Auto-forwarded indication		A	E	
Blind copy recipient indication		A	E	
Body part encryption indication		A	E	
Content type indication	X			
Conversion prohibition		E	E	
Converted indication	X			
Cross referencing indication		A	E	
Deferred delivery		E	N/A	
Deferred delivery cancellation		A	N/A	
Delivery notification		E	N/A	
Delivery time stamp indication	X			
Disclosure of other recipients		A	E	
Expiry date indication		A	E	
Explicit conversion		A	N/A	
Forwarded IP-message indication		A	E	
Grade of delivery selection		E	E	
Hold for delivery				A
Implicit conversion				A
Importance indication		A	E	
IP-message identification	X			
Message identification	X			
Multi-destination delivery		E	N/A	
Multi-part body		A	E	
Non-delivery notification	X			
Non-receipt notification		A	A	
Obsoleting indication		A	E	
Original encoded information types indication	X			
Originator indication		E	E	
Prevention of non-delivery notification		A	N/A	
Primary and copy recipients indication		E	E	
Probe		A	N/A	
Receipt notification		A	A	
Registered encoded information types	X			
Reply request indication		A	E	
Replying IP-message indication		E	E	
Return of contents		A	N/A	
Sensitivity indication		A	E	
Subject indication		E	E	
Submission time stamp indication	X			
Typed body	X			

ANNEX D

(to Recommendation F.440)

Classification of elements of service for Voice Messaging

TABLE D-1/F.440

Elements of service	Origination	Reception	Reference (Note)
Access management	B	B	B.1
Attendant-assisted delivery	A	A	E.1
Auto-forwarding indication	A	A	B.6
Body part encryption indication	A	A	B.9
Content type indication	B	B	B.12
Conversion prohibition	E	E	B.13
Converted indication	B	B	B.15
Deferred delivery	E	N/A	B.19
Deferred delivery cancellation	A	N/A	B.20
Delegation of recipient by directory name	A	N/A	B.24
Delivery notification	E	N/A	B.21
Delivery time stamp indication	B	B	B.22
Disclosure of other recipients	A	E	B.25
DL-Expansion prohibited	A	N/A	B.27
Expiry date (+time) indication	A	A	B.29
Forwarding V-message indication	E	E	E.2
Grade of delivery selection	E	E	B.32
Hold for delivery	A	C	B.33
Implicit conversion	A	C	B.34
Importance indication	E	E	B.35
Language indication	A	A	B.38
Latest delivery designation	A	N/A	B.39
Message identification	B	B	B.41
MS register	A	A	B.95
Multi-destination delivery	E	N/A	B.45
Multi-part body	A	A	B.46
Non receipt notification request indication	E	E	B.48
Non-delivery notification	B	B	B.47
Obsoleting indication	A	A	B.52
Prevention of non-delivery notification	E	N/A	B.61
Receipt notification request indication	E	E	B.67
Redirection disallowed by originator	A	N/A	B.68
Redirection of incoming message	A	C	B.69
Replying V-message indicator	A	E	E.3
Restricted delivery	A	C	B.77
Sensitivity indication	E	E	B.80
Stored message alert	A	C	B.82
Stored message deletion	N/A	E[a)]	B.84
Stored message fetching	N/A	E[a)]	B.85
Stored message listing	N/A	E[a)]	B.86
Stored message summary	N/A	E[a)]	B.87
Stored V-message auto-forward	A	A	E.4
Submission time stamp indication	B	B	B.89
TS-recipient spoken name indicator	A	A	E.5
TSAU-recipient	E	E	E.6
Typed body	B	B	B.90
Use of distribution list	E	N/A	B.92

TABLE D-1/Rec. F.440 (*Cont.*)

Elements of service	Origination	Reception	Reference (Note)
User/UA capability registration	B	B	B.93
V-message creation time	B	B	E.7
V-message duration indicator	B	B	E.8
V-message identification	B	B	E.9
VM-encoding algorithm indicator	B	B	E.10
VM-forwarding	A	A	E.11
VM-multi-part body	A	E	E.12
VM-receiver	A	A	E.13
VM-recipient indicator	E	E	E.14
VM-service status request notification	E	E	E.15
VM-spoken name indication	E	E	E.16
VM-subject indication	E	E	E.17

a) This classification applies if the message store is provided.

A Additional
B Basic
C Contractual
E Essential
N/A Not Applicable

Note – References to B-sections are found in Annex B of Recommendation F.400. References to E-sections are found in Annex E of this Recommendation.

ANNEX E

(to Recommendation F.440)

Definitions of elements of service specific to Voice Messaging

E.1 attendant-assisted delivery

This element of service allows the voice messaging user agent to indicate that a human operator should be used in the delivery of the message by means of the telephone service access unit.

E.2 forwarding voice message indicator

This element of service allows a forwarded voice message or a forwarded voice message plus its "delivery information" to be sent as the body (or as one of the body parts) of a voice message. An indication that the body part is forwarded is conveyed along with the body part. In a multi-part body, forwarded body parts can be included along with the body parts of other types. "Delivery information" is information which is conveyed from the message transfer system when a voice message is delivered (for example, time stamps and indication of conversion.) However, inclusion of this delivery information along with a forwarded voice message, in no way guarantees that this delivery information is validated by the message transfer system.

Note – In the context of voice, the additional body types that may be added during forwarding is still for further study.

E.3 replying voice message indicator

This element of service allows the originator of a voice message to indicate to the recipient(s) that this voice message is being sent in reply to another voice message. A reply can, depending on the wishes of the originator of the replied-to message, and on the final decision of the originator of the reply, be sent to:

a) the recipients specified in the reply request indication of the replied-to message;

b) the originator of the replied-to message;

c) the originator and other recipients;

d) a distribution list in which the originator of the replied-to message can be a receiving member;

e) other recipients as chosen by the originator of the reply.

E.4 **stored VM-auto-forward**

This element of service allows the user of a VM-MS to have the message store automatically perform voice message forwarding, with or without accepting the message. The user of the VM-MS may establish criteria for selecting voice messages through use of the element of service "MS-register". The complete voice message, as received from the originator, is forwarded unchanged, and, if requested, an appropriate voice message notice is generated by the VM-MS. Forwarding is limited to one recipient.

E.5 **TS-recipient spoken name indicator**

This element of service is used to allow the attendant in attendant-assisted delivery to ascertain delivery of the message to the intended recipient.

E.6 **TSAU-recipient**

This element of service specifies the recipient on the telephone service for which the message is intended.

E.7 **voice message creation time**

This element of service enables an originating user agent to convey the message creation time to the recipients user agent. This message creation time can be used for correlation of returning notifications.

E.8 **voice message duration indicator**

This element of service enables an originator's user agent to indicate, to the recipient(s), the duration of a message.

E.9 **voice message identification**

This element of service enables cooperating voice messaging user agents to convey a globally unique identifier to each voice message sent or received. The voice message identifier is composed of an originator/recipient name of the originator and an identifier that is unique with respect to that name. A voice messaging user agent and user use this identifier, optionally together with message creation time, to refer to a previously sent or received voice message (for example, in receipt notifications.)

E.10 **VM-encoding algorithm indicator**

This element of service enables the originating user agent to indicate to the recipient user agents, the voice encoding algorithm used to construct the message.

Note – 32 kbit/s ADPCM defined by Recommendation G.721 is the default encoding algorithm.

E.11 **VM-forwarding**

This element of service enables an voice messaging user agent to forward with or without changes, and a voice messaging store to forward without changes, a received voice message. Support of the element of service voice messaging receiver is also required when forwarding.

E.12 **VM-multi-part body**

This element of service allows an originator to send to a recipient a voice message with a body that is partitioned in several parts. The nature and attributes, or type, of each part are conveyed along with the body part as well as its positional index into the body.

E.13 **VN-receiver**

This element of service allows the originator, or a forwarding voice messaging user agent/message store, to indicate to a recipient the originator/recipient address that requested notifications should be returned to. Notifications should always take the same return path as was used for delivery of the voice message.

E.14 **VM-recipient indicator**

This element of service allows the originator to provide the name of zero, or more users, or distribution list who are the intended recipients of voice message. In addition, it is possible to specify a qualifier for each recipient.

E.15 **VM-service status request notification**

This element of service allows the originator to request notification when any requested service can not be performed by the recipient's user agent.

Note – Qualifier values are for further study.

E.16 **VM-spoken name indication**

This element of service allows the identity of the originator of a voice message to be conveyed in a voice form to the recipient.

E.17 **VM-subject indication**

This element of service allows an originator to indicate in a voice form, the subject of a voice message to the recipient(s). The recipients of the reply receive it as a regular voice message, together with an indication of which voice message it is in reply to.

ANNEX F

(to Recommendation F.440)

Classification of elements of service specific to the telephone service access unit

The classification of the MH elements of service defined in Annex B of Recommendation F.400 that apply to the TSAU is shown in Table F-1/F.440. In addition, since the TSAU is provided as part of the VM service, it may use all elements of service that apply to the VM service listed in the Annex D of this Recommendation.

TABLE F-1/F.440

Elements of service applying when using the telephone service access unit

Elements of service	Origination	Reception	Reference (Note)
Attendant-assisted delivery	A	A	E.1
Conversion prohibition	E	E	B.13
Converted indication	B	B	B.15
Deferred delivery	E	N/A	B.19
Deferred delivery cancellation	A	N/A	B.20
Delivery notification	E	N/A	B.21
DL expansion prohibited	A	A	B.27
Grade of delivery selection	E	E	B.32

TABLE F-1/F.440 (*Cont.*)

Elements of service	Origination	Reception	Reference (Note)
Hold for delivery	A	C	B.33
Implicit conversion	A	C	B.34
Importance indication	A	E	B.35
Language indication	A	A	B.38
Message identification	B	B	B.41
Multi-destination delivery	E	N/A	B.45
Non-delivery notification	B	B	B.47
Non-receipt notification	A	E	B.48
Original encoded information types indication	B	B	B.54
Prevention of non-delivery notification	E	N/A	B.61
Receipt notification request indication	A	E	B.67
Redirection disallowed by originator	A	N/A	B.68
Replying message indicator	A	A	B.73
Submission time stamp indication	B	B	B.89
TS-recipient spoken name indicator	A	A	E.5
TSAU-recipient	E	E	E.6
Typed body	B	B	B.90
Use of distribution list	E	N/A	B.92
User/UA capability registration	B	B	B.93
V-message identification	B	B	B.37

A Additional
B Basic
C Contractual
E Essential
N/A Not Applicable

Note – References to B-sections are found in Annex B of Recommendation F.400. References to E-sections are found in Annex E of this Recommendation.

ANNEX G

(to Recommendation F.440)

Secure voice messaging elements of service

(This annex forms an integral part of this Recommendation)

This Annex defines the secure voice messaging elements of service.

G.1 **non-repudiation of content originated**

This element of service allows an originating VM-UA to provide a recipient VM-UA an irrevocable proof as to the authenticity and integrity of the content of the message as it was submitted into the MHS environment.

The corresponding proof data can be supplied in two ways depending on the security policy in force:

1) by using the non-repudiation of origin security applied to the original message; or

2) by using a notarization mechanism.

Note – At this time, use of a notarization mechanism requires bilateral agreements, protocol is not provided.

G.2 **non-repudiation of content received**

This element of service allows an originating VM-UA to get from a recipient VM-UA an irrevocable proof that the original subject message content was received by the recipient VM-UA and the subject voice message was accepted, forwarded or refused. This service provides irrevocable proof as to the authenticity of the recipient of the message and irrevocable proof as to the integrity of the content of the message. It will protect against any attempt by the recipient(s) to subsequently deny having received the message content.

Note 1 – This service is stronger than the Proof of Content Received service.

The corresponding proof data can be supplied in two ways depending on the security policy in force:

1) by returning a Non-repudiation of Origin of the voice notification which incorporates the following:

   – the originator's Non-repudiation of Origin security arguments (if present); or

   – the complete original message content, if the originators Non-repudiation of Origin arguments are not present;

2) by using a notarization mechanism.

Note 2 – At this time, use of a notarization mechanism requires bilateral agreements, protocol is not provided.

G.3 **non-repudiation of content received request**

This element of service enables an originating VM-UA to request a recipient VM-UA to provide it with an irrevocable proof that the original subject message content was received by means of a receipt or non-receipt notification.

Note – This element of service requires the "receipt notification request indication or non-receipt notification request indication" to also be requested of this recipient.

G.4 **non-repudiation of voice notification**

This element of service provides the originator of a message with irrevocable proof that the subject message was received by the VM-UA and the subject voice message was accepted, forwarded, refused or that certain requested elements of service were not available to the recipient even though the message was accepted.

This shall protect against any attempt by the recipient VM-UA to deny subsequently that the message was received and that the subject voice message was not accepted as indicated. This element of service provides the originator with irrevocable proof of the proof-of-voice message-notification. Such proof may be provided by means of the Non-repudiation of Origin security service, defined in Recommendation X.402 (1988), § 10.2.5.1, being applied to the notification.

Note – This service is stronger than the Proof of Voice Notification service.

G.5 **non-repudiation of voice notification request**

This element of service, used in conjunction with non-receipt notification request indication or receipt notification request indication or voice messaging-service status request notification, enables an originating VM-UA to request the responding VM-UA to provide it with irrevocable proof of origin of the Voice notification.

Note – This element of service supersedes the proof of voice notification request and assumes that a request for at least one of the three voice messaging notifications is always present.

G.6 **proof of content received**

This element of service allows an originating VM-UA to get from a recipient VM-UA proof that the original subject message content was received by the recipient VM-UA and that the subject voice message was accepted, forwarded or refused.

The corresponding proof is obtained by returning a proof of origin of the voice message notification which incorporates the originator's message origin authentication and/or content integrity arguments, if present, or the complete original message content otherwise.

G.7 **proof of content received request**

This element of service allows an originating VM-UA to request the recipient VM-UA to provide it with proof that the original subject message content was received by use of voice messaging receipt or non-receipt Notification.

Note – This element of service requires the "receipt notification request indication or non-receipt notification request indication" to also be requested of this recipient.

G.8 **proof of voice notification**

This element of service allows an originator of a message to obtain the means to corroborate that the subject message was received by the recipient VM-UA and that the voice message was accepted, forwarded or refused. Such corroboration is provided by means of the MTA user-to-message transfer system-user "Message Origin Authentication" security service defined in Recommendation X.402 (1988), § 10.2.1.1.1, being applied to the voice messaging notification.

G.9 **proof of voice notification request**

This element of service, used in conjunction with non-receipt notification request indication or receipt notification request indication or voice messaging service status request notification, enables an originating VM-UA to request the responding VM-UA to provide it with a corroboration of the source voice notification.

Note – This element of service requires the "voice messaging notification request" to also be present.

G.10 *New voice messaging security – optional per recipient user facilities elements of service*

Table G-1/F.440 lists the new secure voice messaging elements of service.

TABLE G-1/F.440

Elements of service	Originator	Recipient	Section reference
Non-repudiation of content originated	A	A	G.1
Non-repudiation of content received	A	A	G.2
Non-repudiation of content received request	A	A	G.3
Non-repudiation of voice notification	A	A	G.4
Non-repudiation of voice notification request	A	A	G.5
Proof of content received	A	A	G.6
Proof of content received request	A	A	G.7
Proof of voice notification	A	A	G.8
Proof of voice notification request	A	A	G.9

G.11 *Voice messaging security – optional per message/recipient user facilities elements of service*

These elements of service originally defined for IPM in Recommendation F.400 (1988), are applicable to voice messaging on a per message level, see Table G-2/F.440.

TABLE G-2/F.440

Element of service	Originator	Recipient	Section reference to F.400
Non-repudiation of delivery	A	A	B.49
Non-repudiation of origin	A	A	B.50
Non-repudiation of submission	A	A	B.51
Proof of delivery	A	A	B.65
Proof of submission	A	A	B.66
Report origin authentication	A	A	B.74

ANNEX H

(to Recommendation F.440)

Voice messaging security overview

(This annex does not form an integral part of this Recommendation)

H.1 *Introduction*

This annex details the vulnerabilities identified within the Voice Messaging-service environment and the resulting security services required to counter those vulnerabilities.

This annex is based on the assumption that a VM-service environment may use the secure messaging services as defined in Recommendation F.400. However, where vulnerabilities are not adequately covered by the existing MHS security services, provision has been made in Recommendation X.440 for additional security services in the VM-service environment.

Some of the security services defined for the VM-service environment are of a generic message handling nature, others are specific to the VME. The security services defined for the VM-service environment are specific to VM and are therefore fully defined in Recommendation X.400.

H.2 *Vulnerabilities*

In most of the areas identified below, there will also be further vulnerabilities and corresponding service considerations at the level of the voice messaging users (VM-users). The security model reflected in this annex assumes that such considerations are outside the scope of this Recommendation. The voice messaging (VM) security model assumes that the VM-user provides adequate security and trusted functionality in the operation of VM sufficient to meet the user's security policy.

Note – In practice this may necessitate co-location of the VM-user and the VM-UA unless a suitably secure environment is established which includes both components.

The following description of vulnerabilities is based on the threat definitions in Annex D of Recommendation X.402. In addition, it has been considered necessary to examine message loss independently of message sequencing and modification of information, and to take account of further vulnerabilities for VM which are not currently identified in Recommendation X.402.

An important aspect of the VM environment which is not recognized within the Recommendation X.402 security model is the concept of VM acceptance for messages at each stage of the message path through the MHS environment.

It is therefore necessary to establish the concept of VM-acceptance domains, which may involve additional consideration of legal issues. One possible division of the VM-service environment into VM acceptance domains is as follows:

1) VM-user environment plus the VM-UA;

2) MTS management domain;

3) VM-message store (if not co-located with either of the above).

H.2.1 *Masquerade*

As defined in Recommendation X.402, Annex D.

H.2.2 *Message sequencing*

As defined in Recommendation X.402, Annex D.

Users should not assume the voice message shall be delivered in correct sequence. Voice messaging users should be able to recover from duplication and out-of-sequence messages, provided the MHS offers protection against the modification of information while messages are within the MHS environment.

H.2.3 *Message loss*

Vulnerability to message loss is considered critical in the VMG environment. Two types of message loss are distinguished:

a) catastrophic failure of a VM-UA, VM-MS or MTA;

b) loss of individual message(s).

VM-users and service providers may need to consider more carefully issues concerning transfer of messages between VM-acceptance domains:

a) from the originating VM-UA user domain;

b) between relaying domains;

c) to the recipient VM-UA user domain.

H.2.4 *Modification of information*

As defined in Recommendation X.402, Annex D.

H.2.5 *Denial of service*

As defined in Recommendation X.402, Annex D.

H.2.6 *Repudiation*

As defined in Recommendation X.402, Annex D.

Furthermore repudiation vulnerability in the VM-service environment is considered to be critical. Such vulnerability may be increased by use of certain MHS services (e.g. auto-forwarding, redirection).

H.2.7 *Leakage of information*

As defined in Recommendation X.402, Annex D.

H.2.8 *Manipulation of information by VM-User*

The VM community has additionally identified a further vulnerability where the integrity of a message content is altered subsequent to creation of the spoken message (i.e., by either or both of the originating VM-UA and recipient VM-UA). This vulnerability includes manipulation of message content in the originator's local store after non-repudiation of submission and/or manipulation of message content in the recipient's store after non-repudiation of delivery.

H.2.9 *Other vulnerabilities*

Other vulnerabilities as defined in Recommendation X.402 are considered important such as:

1) misrouting;

2) misdelivery (especially important in the context of redirection);

3) insider threats;

4) receipt of data that the VM-user is not prepared to accept or process.

H.3 *Vulnerabilities countered*

Recommendation X.402, § 10, provides an abstract security model for message transfer. The security model provides a framework for describing security services that counter potential vulnerabilities within the MTS and between MTS-user to MTS-user. VM vulnerabilities may also be countered by security services which are outside the existing model defined in Recommendation X.402. The following text describes how the VM vulnerabilities are countered using Recommendation X.402 security services, enhanced security services defined in Recommendation X.440 and pervasive mechanisms defined in this Recommendation.

H.3.1 *Masquerade*

The existing MHS-security services which counter this vulnerability are:

a) Message Origin Authentication;

b) Secure Access Management;

c) Security Labeling;

d) Proof of Delivery;

e) Proof of Submission.

Since voice messaging UA/MS is deemed in the MHS architecture as belonging to one user, it is not considered appropriate to provide selective access control for the various operations that may be performed on a VM-MS. However, there is a requirement for security audit trail to record the actions of the VM-user.

In this Recommendation, such security audit trails are expected to be implemented as pervasive mechanisms (the term pervasive mechanism is defined in ISO 7498-2). Protocols to support audit capability may be the subject of future standardization.

H.3.2 *Message sequencing*

The existing MHS-security service which counters this vulnerability is: Message Sequence Integrity. This security service has limited effect as it is based on the provision of an integer by the originating VM-UA with no assurance as to uniqueness or consecutiveness. It is considered that the MHS environment should not be required to ensure message sequence integrity, but should support detection of sequence integrity failure (by additional provision of audit/logging facilities and/or the provision of third party notary services). In this Recommendation it is considered the responsibility of the VM-user to recover from sequence errors and message duplication.

H.3.3 *Message loss*

Message loss could occur potentially over any peer-to-peer communications link (e.g., by deliberate malicious act), or by the failure or incorrect behavior (whether by malicious intent or otherwise) of any MHS component (VM-UA, VM-MS, MTA). The following categories of message loss are distinguished:

1) catastrophic message loss (i.e., failure of a component);

2) malicious loss of individual messages in the VM-MS;

3) accidental loss of individual messages in the VM-MS;

4) MTS-message loss.

H.3.3.1 *Catastrophic failure*

Failure of the VM-UA is outside the scope of this Recommendation.

Failure of the VM-MS is potentially catastrophic and desirably needs some protection, at least in terms of detection. This should be provided by an off-line archive to hold all submitted and delivered messages. In this Recommendation detection and recovery from message loss using such archive mechanisms is a local matter.

Failure of any component in the MTS may similarly be catastrophic and can again be protected by off-line archive of messages. As for the message store, detection and recovery from message loss suing such archive mechanisms in the MTS is a local matter and outside the scope of this Recommendation.

H.3.3.2 *VM-MS specific message loss*

Loss of individual messages in the message store – whether malicious or accidental – shall require the provision of a secure audit trail to enable detection of such loss. Such a service may need to be provided to the VM-user and to VM-MS management. In this Recommendation, secure VM-MS audit trail could be realized as a pervasive mechanism and is a local issue. Protocol to support an audit trail may be the subject of future standardization.

H.3.3.3 *MTS specific message loss*

Loss of individual messages in the MTS (whether malicious or accidental) shall also require the provision of a secure audit trail to enable detection of such loss. Such a mechanism would need to be provided on a per-MTA and a per-MD basis depending on security policy in force. A secure MTA/MTS audit trail could be realized as a pervasive mechanism and is a local issue. The protocol to support an audit trail may be the subject of future standardization.

H.3.3.4 *End-to-end message loss*

The following description assumes that the functionality of the VM-UA (including any associated components to meet such functionality – e.g., encryption devices), is trusted.

The existing “Message Sequence Integrity” service does not guarantee detection of message loss, since it relies on the provision of an integer value by the originating VM-UA. In practice, effective operation of this service may be achieved with a common code of practice between VM users which is outside the scope of this Recommendation.

As a result, MHS services which may provide an indication of message loss are confined to services offered to the originating VM-user. Whereas the existing Proof of Submission and deliver services provide some degree of confidence that the message has not been lost, they do not operate end-to-end. In particular they do not take account of the scenario where the recipient VM-UA and VM-MS are not co-located.

There is, therefore, a requirement for a proof of receipt (i.e., by the recipient VM-UA) service. This capability is realized by the user requesting a voice messaging notification (VN) which may be secured. The VN indicating the status of VM as accepted, forwarded or refused includes elements which associates the notification with the subject message.

In a VM environment, proof of receipt may therefore be provided by signing the VN-service using the existing MTS security elements. In particular, the VM-UA to VM-UA security service of Message Origin Authentication may be used to sign the VN on submission of the VN to the MTS. In this Recommendation the requirement for proof of receipt may be implemented by a trusted form of VN in the VM environment.

Note – This service is called Proof of VM Notification and/or Non-repudiation of VM Notification in VM, depending on the strength of the mechanism provided.

The MTS mechanism used on message submission to provide this service is defined as the MTS submission abstract operation in Recommendation X.411, § 8.2.1.1.1.28 *Content-integrity-check*. In this instance the message content is the VN. Proof of association between the subject message and replying VN is provided by subject message VM identifier and if included in the subject message the message content-integrity-check argument.

H.3.4 *Modification of information*

The existing MHS security services which counter this vulnerability are:

– Connection Integrity;

– Content Integrity.

These security services provide sufficient protection against modification of message content. It is also noted that use of double enveloping (i.e. with encrypted checksum on outer envelope) may provide additional protection.

Note – VM-UAs are trusted entities in terms of content integrity.

H.3.5 *Denial of service*

This is a very important vulnerability for VM-users, but is outside the scope of this Recommendation.

H.3.6 *Repudiation*

Services which offer protection against repudiation in the VM environment are fundamentally concerned with formalizing the forwarding of a VM. The security services as defined in Recommendation X.402 are:

a) Non-repudiation of Origin;

b) Non-repudiation of Submission;

c) Non-repudiation of Delivery.

These security services only cover some areas of transfer between VM-Acceptance domains, which may be of significance in a VM environment. Areas which are not covered by security services provided in 1988 for message handling include:

– between VM-user domains (i.e., end-to-end);

– between MTS management domains;

– between a VM-MS and a recipient VM-UA.

Therefore, services and/or pervasive mechanisms defined in this Recommendation covering the above deficiencies are:

– non-repudiation/Proof of Transfer;

– non-repudiation/Proof of Retrieval;

– non-repudiation/Proof of VM Notification;

– non-repudiation/Proof of Content.

"Non-repudiation/Proof of Transfer" counters the vulnerability of repudiation of responsibility between MTA and/or management domains. VM environments may provide such a service using an additional pervasive mechanisms, such as security logs and archives within MTA and/or MTS boundaries. Such pervasive mechanisms provide a "secure MT audit trail" to record the message details and trace information.

Non-repudiation/Proof of Retrieval counters the vulnerability of repudiation of responsibility of a message between a UA and an MS. VM environments may provide such a service using an additional pervasive mechanisms, such as security logs and archives within VM-MSs. Such pervasive mechanisms provide a "secure VM-MS audit trail" to record VM-user actions in the VM-message store.

Non-repudiation/Proof of VM Notification counters the vulnerability of repudiation of a voice messaging notification for VM-UA to VM-UA. This service is specific to VM and a complete solution is included in this Recommendation. This vulnerability may be especially relevant in the case of VM forwarding, redirection, etc., in addition to the scenario of delivery to an untrusted VM-message store.

Two mechanisms have been defined for non-repudiation of VM notifications: the first uses the trusted VN as described above, the second uses an external notary systems. Only the trusted VN was fully defined in this Recommendation. External notary systems may be the subject of future standardization.

Non-repudiation/Proof of Content counters the vulnerability of manipulation of information by the VM-user after the message has been received by the VM-UA. Although such vulnerability is outside the MHS environment, the MHS environment may provide assistance in terms of trusted return of content and notarization services. There are several ways this requirement may be supported, using the secure messaging environment based on the security services provided in 1988.

Firstly, non-repudiation of content by the originating VM-UA may be provided by the existing Non-repudiation of Origin security service.

Secondly, non-repudiation of content by the recipient VM-UA may be provided by returning the subject content within the VM notification and submitting the voice messaging notification to the MTS using the Non-repudiation of Origin security service.

Thirdly, by notarization services, such services may be achieved by forwarding messages via a mutually trusted third-party notary (i.e., using existing MHS-security services).

All three approaches would thus require no modification to the secure messaging environment based on the existing MHS Recommendations.

Note – Non-repudiation services (which may imply the involvement of a third party) are considered stronger than "proof-of" services.

H.3.7 *Leakage of information*

The existing MHS-security services which counter this vulnerability are:

– Connection Confidentiality;

– Content Confidentiality;

– Secure Access Management;

– Message Flow Confidentiality.

These security services provide sufficient protection against leakage of message content. It is also noted that use of double enveloping could provide some protection against traffic analysis. Traffic padding is outside the scope of this area of work.

Note – UAs are trusted entities in terms of content and message flow confidentiality.

H.3.8 *Manipulation of information by VM-user*

Manipulation of information by the VM-user may be countered by use of the "Non-repudiation of content" security service.

H.3.9 *Other vulnerabilities*

The use of "security access management" and "security labeling" to counter all other vulnerabilities is also applicable in the VM environment. In addition, there is a requirement for auditing and accountability which is likely to require at least a "secure audit trail"; this may be provided by a pervasive mechanism as a local matter.

H.3.10 *Other VM-user vulnerabilities*

Within the VM environment the VM-user may be vulnerable to security threats. To counter these vulnerabilities the VM-user may wish to generate its own security services and mechanisms (such as, signatures from one VM-user to another). These VM-user security services are conveyed in VM security fields as purely information conveying elements of services within the VM environment and may consequently be used for several end-to-end services including message recovery and non-repudiation. It is a local issue to determine how the VM-user security services are used.

H.3.11 *Summary*

This annex identifies VM vulnerabilities and the security services necessary to counter those vulnerabilities using the MHS specification of 1988, then specifies the corresponding security elements required.

VM may provide additional pervasive mechanisms as follows:

– secure VM-MS audit trail;

– secure MT-audit trail;

– VM-MS archive;

– MD archive;

– security of MTA management and routing information.

This Recommendation currently allows the use of both standard symmetric and standard asymmetric tokens. The use of trusted notary systems may be the subject of future standardization.

H.4 *Additional pervasive mechanisms*

H.4.1 *Secure VM-MS audit trail*

This facility would monitor and record VM-UA actions on the message store. It would also provide support for “proof of retrieval”.

It is strongly recommended that “secure VM-MS audit trail” be controlled via a secure link or other secure local means to protect against masquerade. In this Recommendation “secure VM-MS audit trail” may only be realized as a pervasive mechanism. The pervasive mechanisms mentioned may be the subject of future standardization.

H.4.2 *Secure MT-audit trail*

This facility would monitor and record all MTA actions. It would also provide additional support for: “proof of submission”, “proof of transfer”, “proof of delivery”, security of the administration of the MTA. In this Recommendation, secure MT-audit trail may be realized as a pervasive mechanism.

H.4.3 *VM-MS archive*

This mechanism is potentially useful for providing recovery from MS failure, i.e. by providing a secure off-line archive of all submitted and delivered messages. Detection and recovery from message loss using such archive mechanism is a local matter.

H.4.4 *MT archive*

This mechanism is potentially useful for providing recovery from MTA failure, i.e. by providing a secure off-line archive of all messages. Detection and recovery from message loss using such archive mechanism is a local matter.