INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

F.440

(08/92)

MESSAGE HANDLING SERVICE
OPERATIONS AND DEFINITION OF SERVICE

MESSAGE HANDLING SERVICES: THE VOICE MESSAGING SERVICE

Recommendation F.440

FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation F.440 was prepared by Study Group I and was approved under the Resolution No. 2 procedure on the 4th of August 1992.

CCITT NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

© ITU 1993

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

Recommendation F.440

MESSAGE HANDLING SERVICES: THE VOICE MESSAGING SERVICE

(1992)

CONTENTS

1 *Purpose and scope*

1.1 General

1.2 Message handling systems used in the provision of VM-service

2 *VM-service*

2.1 General service requirements

2.2 VM-service features

2.3 Responsibility boundaries

2.4 Message store

2.5 Telephone service access unit

2.6 Use of directory

2.7 Security

2.8 Distribution lists

3 *Types of body parts*

3.1 Applicable body part types

3.2 Structure of voice messages

3.3 VM forwarding

4 *Conversion between different encoded information types*

5 *Naming and addressing in general*

5.1 Directory names

5.2 O/R names

5.3 O/R addresses

6 *Operation of the service*

6.1 General

6.2 Message handling phases

7 *Quality of service*

7.1 Message status

7.2 Support by Administrations

7.3 Model of delivery and notification times

7.4 Message delivery time targets

7.5 Delivery notification time targets

7.6 Receipt notifications and non-receipt notifications

7.7 Error protection

7.8 Availability of service

7.9 Minimum storage capacity

8 *Tariff and accounting principles*

9 *Network requirements*

10 *User information and support*

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

Annex A – Abbreviations

Annex B – Subscriber access and terminal requirements

Annex C – VM elements of service for 1984 systems

Annex D – Classification of elements of service for Voice Messaging

Annex E – Definitions of elements of service specific to Voice Messaging

Annex F – Classification of elements of service specific to the telephone service access unit

Annex G – Secure voice messaging elements of service

Annex H – Voice messaging security overview

1 Purpose and scope

1.1 *General*

This Recommendation specifies the general, operational and quality of service aspects of the public international Voice Messaging service. Voice Messaging services provided by Administrations belong to the group of Telematic Services defined in the F-Series Recommendations.

This type of Message Handling (MH) service is an international telecommunication service offered by Administrations, enabling subscribers to send a message to one or more recipients and to receive messages via telecommunication networks using a combination of store and forward, and store and retrieve techniques.

Locally provided functions, for which communication with other subscribers is not required, are not covered by CCITT Recommendations.

The Voice Messaging (VM) service enables subscribers to request a variety of features to be performed during the handling and exchange of voice encoded messages.

Some features are inherent in the basic VM-service. Other non-basic features may be selected by the subscriber, either on a per-message basis or for an agreed contractual period of time, if they are provided by Administrations.

Intercommunication with the Interpersonal Messaging (IPM) service, may be provided as an option in the VM-service.

Basic features have to be made available internationally by Administrations. Non-basic features, visible to the subscriber, are classified as either essential or additional.

Essential optional features must be made available internationally by Administrations. Additional optional features may be made available by some Administrations for national use and internationally on the basis of bilateral agreement. Non-basic features are called optional user facilities.

VM-service may be provided using any communications network. VM-service may be offered separately or in combination with various telematic or data communication services. It can be obtained by making appropriate arrangements.

Technical specifications and protocols, to be used in the VM-service are defined in the X.400-Series Recommendations.

The service definition is contained in § 2. Requirements for intercommunication between subscribers are described in §§ 3 and 4. Naming and addressing are described in § 5, while §§ 6, 7 and 8 describe the operation of the service, quality of service, tariff and accounting principles. Network requirements are given in § 9. The provision of subscriber information is in §§ 10, and 11 contains information on the use of the VM-service within CCITT defined telematic services.

1.2 *Message handling systems used in the provision of VM-service*

1.2.1 *1984 implementations*

This Recommendation assumes that the message handling systems implemented to provide the service outlined herein are based on the 1988 version of the X.400-Series Recommendations. It is recognized however, that for some time after the publication of this Recommendation, the majority of implementations of the VM-service will be based on the l984 X.400-Series Recommendations. Administrations are encouraged to adopt the latest CCITT Recommendations; however, in the interim, they may make use of this Recommendation with 1984 implementations as outlined below.

1.2.2 *Elements of service*

Elements of service available for message handling services are listed and classified in Recommendation F.400. Annex C of Recommendation F.440 provides a list of all the elements of service (called service elements in 1984) for VM from Recommendation X.400 (version 1984) which are based on the IPM elements of service. Annex C of Recommendation F.400 (version 1988) lists both the elements of service in 1988 as well as changes in classification to any 1984 elements of service. Annex D of Recommendation F.400 lists the elements of service specific to the VM-service. Annex E of Recommendation F.400 provides the definitions for the elements of service for VM additional to those described in Recommendation F.400 (1988). In all cases, 1984 elements of service may be used for the provision of the VM-service as described in this Recommendation, for a grace period ending in 1996.

Administrations are urged to upgrade their implementations in this respect to the 1988 Recommendations.

1.2.3 *Name forms*

The name forms to be used for the VM-service are consistent with those specified in the F.400 (1988) and X.400 (1988) Recommendations.

1.2.4 *Interworking*

In order to protect the investment of Administrations who have implemented 1984 systems for the provision of VM-service, 1988, administration management domain (ADMD) implementations shall be able to interwork to 1984 ADMDs as outlined in Recommendation X.419, Annex B.

Interworking from 1988 ADMDs to 1984 private management domains (PRMDs) is a national matter.

2 VM-service

2.1 *General service requirements*

2.1.1 The fundamental ability of the VM-service is to provide a public interface between originators and recipients of voice communications to enhance their means of communication, especially where there is no immediate or convenient direct telecommunication service available between subscribers' equipment, or the telecommunication services available are incompatible. This service may also provide features available for the preparation and the presentation of the messages.

2.1.2 The VM-service will be provided by Administrations using the Message Transfer service defined in Recommendation F.410, and by systems that conform to the X.400-Series Recommendations.

Management domains (MDs) are defined for the purpose of responsibility boundaries. The MD managed by an Administration is called an administration management domain. The MD managed by an organization is called a private management domain (PRMD).

2.1.3 International exchange of messages are performed between administration management domains through CCITT standardized public data transmission services.

2.1.4 Different body part types of messages may be exchanged through this service. The various body part types are listed in § 3.

2.1.5 An Administration may provide subscribers with different methods of access to the VM-service. The possible methods are:

1) directly from the user's terminal, e.g. telephone set;

2) via a private message handling system.

Note – A voice messaging management domain may be resident in a private automatic branch exchange.

2.1.6 Each Administration is responsible for the national access to its management domain.

2.1.7 The characteristics of the interfaces and access methods used between terminals and the VM-service are a national matter, although they may follow provisions of the CCITT voice telephone service. However, the VM-service optional user facilities offered are defined and are independent of the access method and user's terminal.

2.1.8 The national implementation of the VM-service may provide intercommunication with existing services such as the IPM-service, teletex, facsimile and videotex. When implemented, the interfaces between the VM and the other services shall be according to relevant CCITT Recommendations.

2.1.9 As the service is providing indirect communication, cases of non-delivery of the message to the intended recipient may occur. The VM-service provides for non-delivery notification and, as optional user facilities, for delivery, receipt and non-receipt notifications.

2.1.10 Due to the intermediate storage of the message, the service may provide conversion optional user facilities: speed, access procedures, networks, and coding of message contents.

2.1.11 The message belongs to the originator until delivery has taken place. After delivery, the message belongs to the recipient.

2.1.12 Where sender and recipient have different and conflicting requirements, the sender's requirements shall take precedence (e.g. body type conversion or redirection control).

2.2 *VM-service features*

2.2.1 *Introduction*

Recommendation F.400, § 19, defines elements of service which are available in the VM-service and are classified as either belonging to the basic service or as VM-optional user facilities. Elements of service comprising the basic VM-service are inherently part of the service and are always provided and available. The optional user facilities that are classified as essential are always provided and those classified as additional, may be available nationally, or internationally on the basis of bilateral agreement.

2.2.2 *Basic VM-service*

A set of elements of services comprises the basic VM-service. This set is defined in Recommendation F.400, and listed in Table 10/F.400. The basic VM-service, which is built upon the Message Transfer (MT) service, enables a user to send and receive voice messages.

A user prepares V-messages with the assistance of his user agent (UA). User agents, which are a set of computer application processes, cooperate with each other to facilitate communication between their respective users. To send an V-message, the originating users make a request of their UA, specifying the name or address of the recipient who is to receive the V-message. The V-message, which has an identifier conveyed with it, is then sent by the originator's UA to the recipient's UA via the Message Transfer service.

Following a successful delivery to the recipient's UA, the V-message can be received by the recipient. To facilitate meaningful communication, a receiving user may specify the encoded information type(s) that can be contained in V-messages delivered to the user, as well as the maximum length of a message that may be delivered. The original encoded information type(s) and an indication of any conversions that may have been performed and the resulting encoded information type(s) are supplied with each delivered V-message. In addition, the submission time, delivery time and other capabilities are supplied with each V-message. Non-delivery notification is provided with the basic service.

2.2.3 *VM optional user facilities*

A set of the elements of services of the VM-service are optional user facilities. The optional user facilities of the VM-service, which may be selected on a per-message basis or for an agreed contractual period of time, are listed in Tables 11/F.400 and 12/F.400, respectively. Local user facilities may be usefully provided in conjunction with some of these user facilities.

The optional user facilities of the VM-service that are selected on a per-message basis are classified for both origination and reception by UAs. If an Administration provides the VM-service and offers these optional user facilities for origination by UAs, then a user is able to create and send V-messages according to the procedures defined for the associated element of service. If an Administration provides the VM-service and offers these optional user facilities for reception by UAs, then the receiving UA will be able to receive and recognize the indication associated with the corresponding element of service and to inform the user of the requested optional user facility. Each optional user facility is classified as additional or essential for UAs from these two perspectives.

2.2.4 *Local functions*

The message handling system (MHS) may perform many local functions for its subscribers in addition to providing VM features. For example, to assist subscribers in preparing and editing voice messages, MHS may provide an editing capability. The MHS could alert the subscribers when new messages have arrived (for example, by setting a message light on their telephone, or by displaying on their desktop terminals the originator's name and subject of all unread messages or by computer initiated voice indication).

If alerting is not available, a subscriber may have to access MHS frequently to determine if new messages have arrived.

The MHS may provide local database controls to help the subscriber find previously received and filed voice messages (for example, to find the message from Ms. Smith delivered sometime in August). A subscriber on vacation may request the MHS to automatically forward all voice messages to a delegate, or define rules for which voice messages should not be auto-forwarded (for example, personal messages).

Local services such as those above, while perhaps utilizing some of the VM features, do not require coordination or cooperation with other subscribers. Thus, they do not impact the communication protocols associated with MHS. Therefore, local functions that may be provided by Administrations are outside the scope of CCITT.

2.3 *Responsibility boundaries*

The purpose of the MHS is to allow messages to be submitted for transfer to the destination and to be delivered to a UA/MS whose address is specified by the originator.

A user interacts, using an access terminal, with a UA on the sending and on the receiving side. On request, a message is submitted to the message transfer system (MTS). It is also able to retrieve a received message from a UA or message store (MS).

The responsibility for the message rests in the MHS when the originating user gives the command to send the message. The responsibility for a message is turned over to the receiving UA/MS after successful delivery. If the UA or MS is provided by an Administration, the responsibility for the message is taken over by the user when the message is rendered. As a basic feature, a non-delivery notification is created by the MHS when delivery to the receiving UA/MS is not possible.

The conditions applied to this criterion may also depend on optional user facilities, e.g. conversion prohibition. An originating user may for a particular message specifically request a delivery notification, and/or a receipt notification, and/or a non-receipt notification. In the case of telematic addresses delivery takes place automatically when the message is transmitted to the telematic service. After delivery to a document store, or a message store, responsibility turns over to the user after having read the message once. When leaving the message in the store, the responsibility will be defined by the service provider.

Loss of information may occur through the process of conversion as long as the conversion is not explicitly prohibited by the originating user.

The responsibility of messages transferred through MDs starts at the moment of entering the domain and ends when leaving the domain, however, a later audit must be possible.

When an ADMD interacts with a PRMD, the ADMD takes responsibility for the actions of the PRMD which are related to the interaction. In addition to ensuring that the PRMD properly provides the MT-service, and ADMD is responsible for ensuring that the accounting, logging, quality of service, and other related operations of the PRMD are correctly performed. An ADMD acts as the naming authority for the associated PRMDs, in accordance with national guidelines.

2.4 *Message store*

Administrations may optionally provide a message store (MS) to permit delivery of messages so that the recipient's UA does not have to be on line continuously. This is described in Recommendation F.400, § 7.4. A message delivered to an MS is deemed delivered by MHS. Messages delivered to an MS can be retrieved by the recipient as convenient and various optional user facilities can be provided to allow for retrieval for listing, fetching, and deletion of messages. When subscribing to an MS, all messages destined to the UA are delivered to the MS, an alert will be sent to the UA (from the MS) to inform the user of the fact that a message just arrived.

2.5 *Telephone service access unit*

The telephone service access unit (TSAU) is an access unit which provides for interworking between a Voice or Interpersonal Messaging service (VM-service or IPM-service) user and users of the telephone service. Users of the VM-service may request delivery of a voice message to any user of the telephone service who can be addressed by means of a telephone network address (telephone number). Users of the telephone service can cause a voice message to be recorded and delivered to users of the VM-service and IPM-service by means of the TSAU.

2.5.1 *Description of TSAU functions*

In an MHS environment, the IPM or VM-service user agent (UA) can access the telephone network through the TSAU. The MHS user composes the voice message (V-message) while interacting with the UA and designates it for delivery to a user of the telephone network. The MHS user also specifies the recipient's telephone number using a numeric originator/recipient (O/R) address. The MHS voice body part is sent in an F.400 envelope to the TSAU, which extracts the voice body part from the MHS envelope and calls the recipient on the telephone network to effect delivery of the V-message to the recipient. When the V-message is passed to the TSAU, a delivery notification is sent to the originator. Algorithms which control the calling behavior of the TSAU are a local matter.

A user of the telephone network can call the TSAU, record a message, provide a delivery address (restricted to numeric characters provided on the telephone keypad), and request delivery of the message to a VM-service or IPM-service user.

2.5.2 *Attendant-assisted delivery*

The TSAU will normally deliver the message to anyone answering the telephone at the recipient's address. Attendant-assisted delivery allows a human attendant (telephone operator) to assist in the delivery of the message. When it is selected the VM-service user can specify that the message may only be delivered to a designated recipient.

The attendant will ascertain if the recipient is available before playing the voice message and only deliver it if the designated recipient is available to receive the message. The attendant may use the recipient indicator for querying whether the recipient is present.

2.5.3 *TSAU notifications*

The TSAU servicing users of the telephone service uses MTS delivery reports to indicate transfer of the message from the MTS to the TSAU, and voice notifications (receipt and non-receipt) to indicate successful reception at the telephone terminal.

2.6 *Use of directory*

By making use of directory systems, VM-service users will be able to address recipients by using directory names or distribution list names, which are more user friendly than O/R addresses. The MHS will be able to access a directory systems and find out the O/R address(es) corresponding to a given directory name or distribution list name, for delivery of a message. An international telephone number has all the properties of a directory name. This capability is described in Recommendation F.400, § 14.

2.7 *Security*

Administrations may optional provide security mechanisms as outlined in Recommendation F.400, § 15, to counter the various security threats mentioned. This capability may use a directory system for storing certified copies of public keys for MHS-users.

2.8 *Distribution lists*

A group whose membership is stored in the directory can be used as a distribution list (DL). The originator simply supplies the name of the list on submission of a message, and the MHS can obtain the directory names (and then the O/R addresses) of the individual recipients, by consulting the directory. Upon receipt of a message addressed to a distribution list, the recipient can determine through which DL the message arrived. An originator can prohibit the expansion of the distribution if one of the recipients specified refers to a distribution list. Recommendation F.400, § 14, outlines the full capabilities available to DL-users.

If a user unknowingly sends a message to a DL, charges may be incurred for multiple deliveries that were not expected. Because of this, names of distribution lists should be indicative of the fact that what is being named is a DL. Owners of DLs should also ensure that they respect a potential member's wishes about being a member and the rules of the country of the member that may prohibit inclusion without prior agreement.

3 Types of body parts

Messages sent and received in the VM-service can be composed of one or more body parts.

3.1 *Applicable body part types*

Applicable body part types are defined in Recommendation X.440 and comprise the following:

– voice;

– message (e.g. for a forwarded message);

– notifications;

– externally defined.

Initially, the voice encoding supported will be 32 kbit/s ADPCM as specified in Recommendation G.721(1988). Encoding schemes at lower bit rates may be added in the future.

3.2 *Structure of voice messages*

The voice messaging class of UAs (VM-UA) create messages containing a content specific to the Voice Messaging service. The specific content that is sent from one VM-UA to another is a result of an originator, which is generally a human interacting with a telephone, composing and sending a message, called a voice message. The voice message shall carry the voice-encoded object and optionally other information associated with the voice-encoded object. Only one voice-encoded object shall be present in a voice message, and every voice message shall contain a voice-encoded body part on origination of the voice message. The structure of a voice message as it relates to the basic message structure of MHS is shown in Figure 1/F.440. The voice message is conveyed with an electronic envelope when being transferred through the MTS.

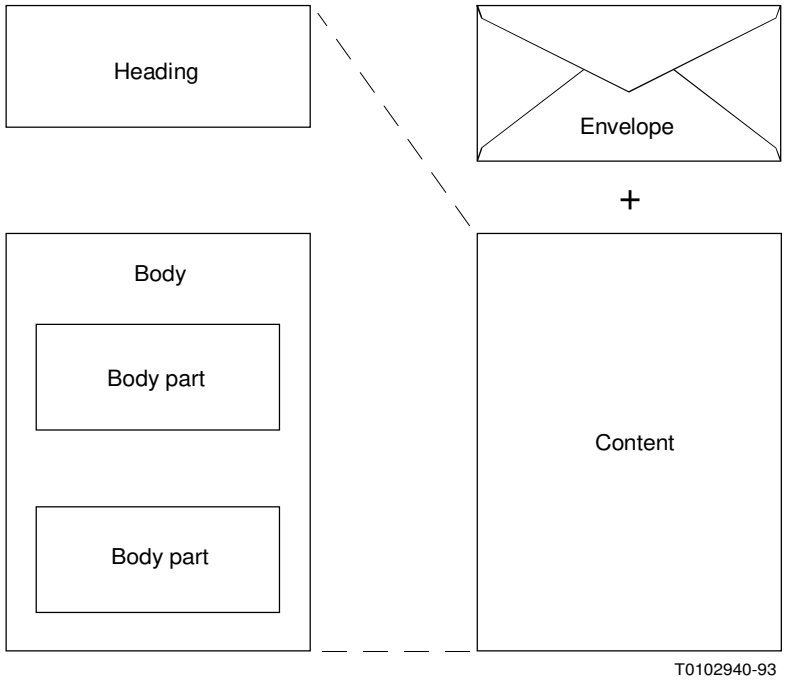


FIGURE 1/F.440
Voice message structure

Figure 2/F.440 shows a mapping between a typical voice-encoded object and the corresponding voice message structure. The voice-encoded object is mapped entirely within one body part, called the primary body part, and may be a G.721 or privately encoded voice object or a forwarded V-message. Unless specified otherwise, this voice object will be assumed to be encoded per G.721 32 kbit/s ADPCM. Other body parts are available to convey information associated with the voice-encoded object such as drawings, additional text information, etc. The heading of the VM contains various fields of information that convey service requests from the originator. This is illustrated in Figure 2/F.440 as V-E-Field *n* for voice encoded information and Field *n* for non-voice encoded information.

The heading and body part(s) form the VM. A VM may contain only one voice-encoded object, which is totally contained in one body part.

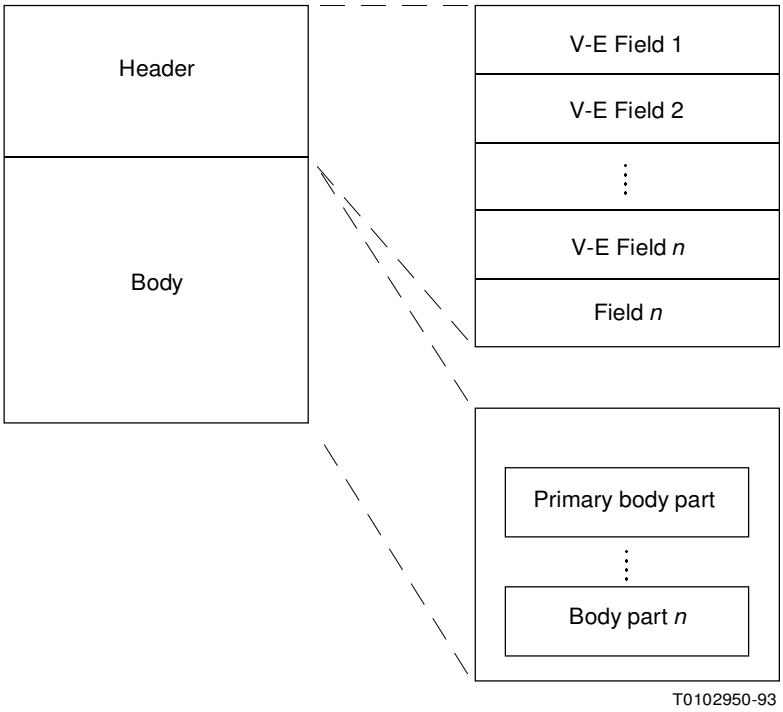


FIGURE 2/F.440
Voice message structure for a typical voice messaging transaction

3.3 *VM forwarding*

A user on the VM-service may cause received messages to be forwarded with or without acceptance. Requests for notifications may also be automatically forwarded along with the forwarded message. Three cases can be distinguished:

a) forwarding of the accepted V-message with requested notifications;

b) forwarding of the V-message and notifications without acceptance; and

c) forwarding of the V-message when notifications were not requested.

The third case is effectively identical to the second case. A user may also request automatic forwarding to be set.

If a V-message is forwarded after acceptance, the primary body part of the forwarded message is the content of the received message with or without changes. Additional VM body parts may be included or removed, but there may not be more than one additional voice encoded body part per instance of forwarding. The forwarded body part may not be removed. Receipt notifications will be issued as requested. In forwarding, a non-receipt notification (NRN) will not be sent back to the originator of the message. VM forwarding may be to one or more recipients, and notification requests may be set for any of these recipients.

Body parts may not be added or deleted if a V-message is forwarded without acceptance. Forwarding may be to more than one recipient. The notification request should be the same as for the original message, but may only be sent to one of the recipients of the forwarded message. This will insure that the original originator only receives the notification that was requested.

4 Conversion between different encoded information types

The MTS provides conversion functions to allow VM-users to input messages in one encoded format, called encoded information type (EIT), and have them delivered in another EIT to cater to users with different terminal types. This capability is inherent in the VM-service, and increases the possibility of delivery by tailoring the message to the recipient's terminal capabilities. The EITs supported for the VM-service are defined in Recommendation X.440.

The MTS may provide automatic conversion between the various standardized encoding schemes when required for the delivery of the message.

The general aspects of conversion and the specific conversion rules for conversion between different EITs in the VM-service are for further study.

5 Naming and addressing in general

In MHS, the principal entity that requires naming is the user (the originator and recipient of messages). In addition distribution lists (DLs) have names for use in MHS. Users of MHS and DLs are identified by O/R names. O/R names are comprised of directory names and/or O/R addresses, all of which are described in this section. Recommendation F.401 provides more detail on naming and addressing for public message handling services, including naming restrictions and responsibilities of Administrations.

5.1 *Directory names*

Users of MHS service, and DLs, may be identified by a name, called a directory name. A directory name was to be looked up in a directory to find out the corresponding O/R address for a particular service. The structure and components of directory names are described in the X.500-Series Recommendations.

A user may access a system directly to find out the O/R address of a user, or O/R addresses of the members of a DL (both of which are outside the scope of these Recommendations).

As an alternative, a user may use the directory name and have the MHS access the directory to resolve the corresponding O/R address or addresses automatically. Every MHS-user or DL will not necessarily have a directory name, unless they are registered in a directory. As directories become more prevalent, it is expected that directory names will be the preferred method of identifying MHS-users to each other.

5.2 *O/R names*

Every MHS-user or DL will have an O/R name. An O/R name comprises a directory name, an O/R address, or both. The directory name unambiguously identifies an MHS-user but not necessarily uniquely. The O/R address uniquely identifies an MHS-user.

Either or both components of an O/R name may be used on submission of a message. If only the directory name is present, the MHS will access a directory to attempt to determine the O/R address, which it will then use to route and deliver the message. If the directory name is absent, it will use the O/R address as given. When both are given on submission, the MHS will use the O/R address, but will carry the directory name and present both to the recipient. If the O/R address is incorrect, it will then attempt to use the directory name as above.

5.3 *O/R addresses*

An O/R address contains information that enables the MHS to uniquely identify a user to deliver a message or return a notification. (The prefix "O/R" recognizes the fact that the user can be acting as either the originator or recipient of the message or notification in question).

Various forms of O/R addresses are currently defined, each serving its own purpose. These forms and their purpose are as follows:

– *Numeric O/R address:* Provides a means of identifying users addressable by numeric keypads.

– *Terminal O/R address:* Provides a means of identifying users with terminals belonging to various networks.

– *Mnemonic O/R address:* Provides a user friendly means of identifying users in the absence of a directory. It is also used for identifying a distribution list.

An O/R address is made up of a collection of information called attributes. These attributes as used in each of the O/R address forms above are detailed in Recommendation F.401.

Management domains shall allow their users to originate messages using any of the above forms. The form in which names are input by or presented to the subscriber is a national matter (as for example the use of distribution lists or of friendly ways of identifying user agents). It is anticipated that the use of the numeric O/R address will be the most prevalent in the VM-service.

Each Administration is responsible for the unique identification of each user agent in its management domain.

6 Operation of the service

6.1 *General*

6.1.1 The VM-service provides that messages can be sent, transferred, delivered and received using fully automatic procedures.

6.1.2 Messages are prepared in, sent from, and delivered to a memory. These memories are part of the UA/MS functionality and are under control of the subscriber.

6.1.3 The transfer of messages between management domains will be in accordance to the Message Transfer service as described in Recommendation F.410.

6.1.4 Each Administration providing the VM-service should validate the subscribers identities, at the time of access.

6.1.5 It is a national matter whether to allow private messaging systems to connect to the public VM-service, in order to allow users of these systems to exchange messages. If these interconnections are provided, they should take place between administration management domains in accordance with CCITT Recommendations.

6.1.6 When implicit conversion is provided by the Administration via the Message Transfer service, the message will be converted if necessary, unless prohibited by the originator. The conversion will be in accordance to the rules specified in Recommendation X.408. See also § 4 of this Recommendation.

6.1.7 Deferred delivery shall be provided by the management domain of the originator, which is responsible for the storage of the message until the date and time specified for intended delivery. Therefore the element of service, deferred delivery, should not be used across international links.

6.2 *Message handling phases*

6.2.1 *General*

The VM-service has different message handling phases visible to the user.

6.2.2 *Preparation phase*

In this phase messages are prepared by making use of the user agent functionality (e.g. capture, editing and filing). The way in which these functions are performed is outside the scope of the Recommendation.

6.2.3 *Sending phase*

In this phase the originator may request the user agent or message store to send a prepared message to one or more recipients and to request certain optional user facilities.

6.2.4 *Receipt phase*

In this phase the subscriber can receive delivered messages and notifications from the user agent or message store. The receipt phase can be initiated by the service (auto-receipt) or by the subscriber for message reception. The operation of the user agent receiving messages is specified in Recommendation X.440.

Subscribers using terminals without user agent functionality may register for a contractual period of time during which they will receive delivered messages automatically from their user agent to a terminal, if the Administration provides for this alternative. Normally the user agent is called to receive incoming messages.

In the case of auto-receipt, the MHS will initiate a call to the subscriber's terminal. In the other case, the subscriber shall initiate a call to the MHS at a time convenient to the subscriber.

The body parts of the message will be received by the subscriber in the form in which the originator has sent it, unless conversion has been performed.

The indication of the optional user facilities requested by the originator are presented by the user agent to the recipient in a form convenient to the user.

Notifications: Four notifications can be received:

- non-delivery notification;
- delivery notification;
- receipt notification;
- non-receipt notification.

Non-delivery notification is automatically originated by the MTS, while delivery notification, receipt and non-receipt notifications depend on the action of the recipient.

6.2.5 *Service notifications*

Service notifications are sent only upon the originator's request. They are sent shortly after the subject message leaves the MTS for the recipient's UA or MS. Service notifications may be generated by a UA or MS or TSAU when requested in the per recipient voice notification (VN) request indicator. Service notification reasons are specified in Annex B for the element of service "VM notification request."

7 Quality of service

7.1 *Message status*

The unique identification of each V-message enables the system to provide information about, e.g. the status of an V-message.

In the event of system failure all accepted and non-delivered messages should be traceable. If messages cannot be delivered, the originator must be informed by a non-delivery notification.

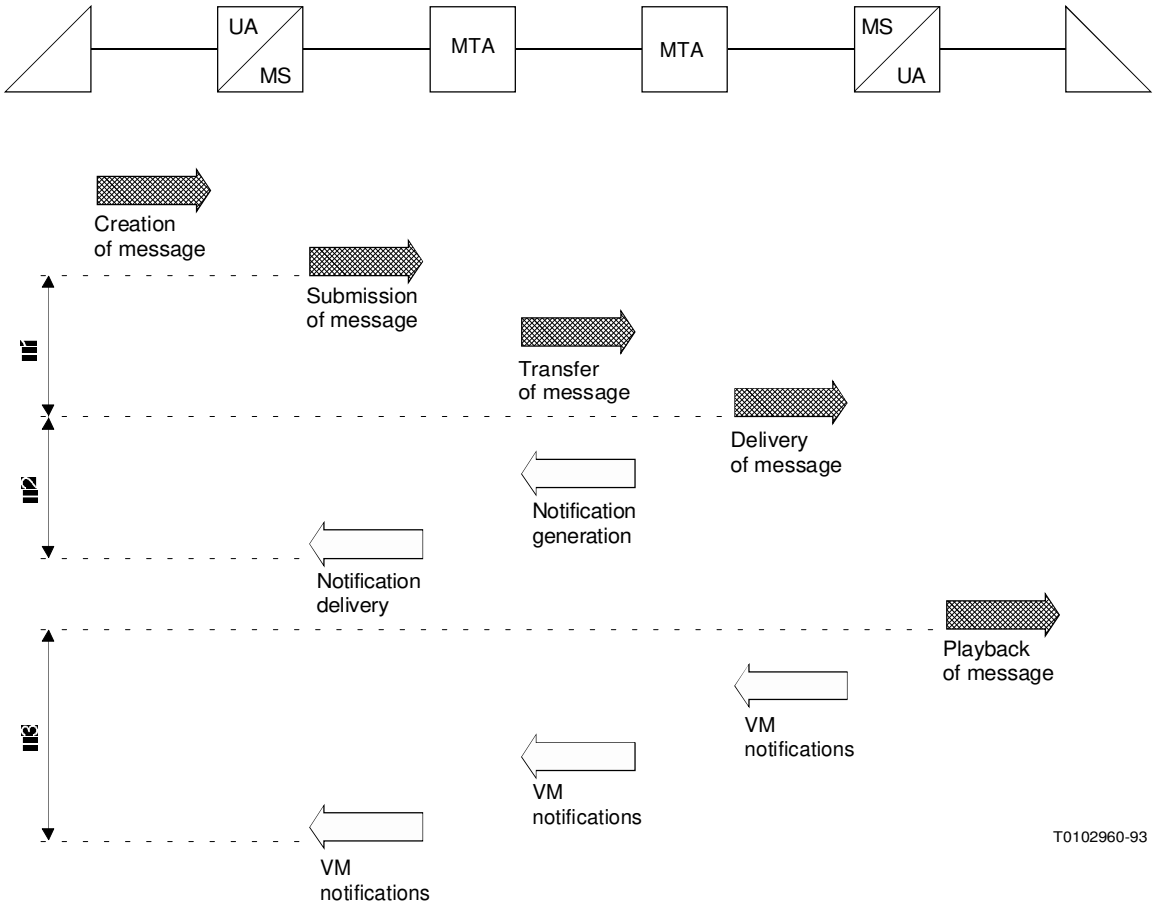
7.2 *Support by Administrations*

Administrations should provide assistance to their subscribers, with regard to non-delivery notifications not being received in due time, as far as public system components are concerned. Additional provision on support of status and tracing of messages may be provided under national responsibility.

When the user agent is provided by an Administration, additional functionality should be provided in order to minimize cases of not reading messages within a certain period of time (the definition of this period is for further study). This functionality could be for example, alert messages sent to an automatic reception terminal.

7.3 *Model of delivery and notification times*

See Figure 3/F.440.



T1 Delivery time
T2 Delivery notification time
T3 VM notifications time

} For more details see Recommendation F.410

Note 1 – Starting time of T3 corresponds to the time the message is played to the user and VM notification is actioned by the user.

Note 2 – Ending time of T3 is the time that the VM notification is made available to the user through the UA or MS.

Note 3 – Similar considerations apply to non-receipt notifications.

FIGURE 3/F.440

Notification time model

7.4 *Message delivery time targets*

The management domain of the recipient UA should force non-delivery notification if the message has not been delivered before *x* hours after submission (or after date and time indicated for deferred delivery), the value of *x* being dependent on the grade of delivery requested by the originator (see Recommendation F.410, § 4.4).

7.5 *Delivery notification time targets*

Non-delivery notifications or requested delivery notifications should be returned on a per-recipient basis, in order not to delay notifications for those messages in a multi-address message which have already been delivered, to enable the originating management domain either to return per-recipient notifications or to batch notifications to its subscribers (see Recommendation F.410, § 4.5).

7.6 *Receipt notifications and non-receipt notifications*

Delivery times for receipt, non-receipt, and service element availability notifications in the first place depend on local arrangements. When they are initiated by the receiving UA/user they have the same time targets as the messages that cause them to occur.

TABLE 1/F.440

Delivery times for notifications

Grade of delivery of the referred message	95% delivered before	Non-delivery forced after
Urgent	0.25 hours	2 hours
Normal	1.0 hours	6 hours
Non-urgent	4.0 hours	12 hours

Note – Intercommunication with PRMDs is not included in the calculation of the time targets.

7.7 *Error protection*

Error protection on transmission is provided by the MHS and underling protocols used in the provision of the VM-service.

7.8 *Availability of service*

In principle the VM-service should be available continuously. The user agent should be available for submission or delivery continuously (unless hold for delivery is invoked). In cases where the UA is not available for delivery continuously, a message store should be used.

7.9 *Minimum storage capacity*

The storage capacity of a user agent and message store shall be sufficient to provide a high grade of service.

Note – This is for further study.

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.