



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

F.440

(08/92)

**SERVICES DE TRAITEMENT
DES MESSAGES
EXPLOITATION ET DÉFINITION DU SERVICE**

**SERVICES DE MESSAGERIE:
LE SERVICE DE MESSAGERIE VOCALE**



Recommandation F.440

AVANT-PROPOS

Le CCITT (Comité consultatif international télégraphique et téléphonique) est un organe permanent de l'Union internationale des télécommunications (UIT). Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée plénière du CCITT, qui se réunit tous les quatre ans, détermine les thèmes d'études et approuve les Recommandations rédigées par ses Commissions d'études. Entre les Assemblées plénières, l'approbation des Recommandations par les membres du CCITT s'effectue selon la procédure définie dans la Résolution n° 2 du CCITT (Melbourne, 1988).

La Recommandation F.440, que l'on doit à la Commission d'études I, a été approuvée le 4 août 1992 selon la procédure définie dans la Résolution n° 2.

NOTE DU CCITT

Dans cette Recommandation, l'expression «Administration» est utilisée pour désigner de façon abrégée aussi bien une Administration de télécommunications qu'une exploitation privée reconnue de télécommunications.

© UIT 1993

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'éditeur.

SERVICES DE MESSAGERIE: LE SERVICE DE MESSAGERIE VOCALE

(1992)

SOMMAIRE

- 1 *Objet et domaine d'application*
 - 1.1 Considérations générales
 - 1.2 Systèmes de messagerie utilisés pour la fourniture du service de messagerie vocale
- 2 *Service de messagerie vocale*
 - 2.1 Spécifications générales du service
 - 2.2 Fonctions du service de messagerie vocale
 - 2.3 Limites des responsabilités
 - 2.4 Mémoire de messages
 - 2.5 Unité d'accès au service téléphonique
 - 2.6 Utilisation de l'annuaire
 - 2.7 Sécurité
 - 2.8 Listes de distribution
- 3 *Types de parties de corps*
 - 3.1 Types de parties de corps possibles
 - 3.2 Structure des messages vocaux
 - 3.3 Retransmission des messages vocaux
- 4 *Conversion entre différents types de codage*
- 5 *Dénomination et adressage en général*
 - 5.1 Noms d'annuaire
 - 5.2 Noms O/R
 - 5.3 Adresses O/R
- 6 *Fonctionnement du service*
 - 6.1 Considérations générales
 - 6.2 Phases de traitement des messages
- 7 *Qualité de service*
 - 7.1 Etat des messages
 - 7.2 Aide des Administrations
 - 7.3 Modèle d'heures de remise et de notification
 - 7.4 Objectifs en matière de délais de remise des messages

- 7.5 Objectifs en matière de délais de notification de remise
- 7.6 Notifications de réception et de non-réception
- 7.7 Protection contre les erreurs
- 7.8 Disponibilité du service
- 7.9 Capacité minimale de mémorisation
- 8 *Principes de tarification et de comptabilité*
- 9 *Caractéristiques du réseau*
- 10 *Informations et aide fournies aux usagers*
- 11 *Utilisation du service de messagerie vocale dans le cadre des services télématiques définis par le CCITT*

Annexe A – Abréviations

Annexe B – Caractéristiques des terminaux et accès d'abonné

Annexe C – Eléments de service de messagerie vocale pour les systèmes modèle 1984

Annexe D – Classification des éléments de service pour la messagerie vocale

Annexe E – Définitions pour les éléments de service propres à la messagerie vocale

Annexe F – Eléments de service propres à l'unité d'accès au service téléphonique

Annexe G – Eléments de service de sécurité en messagerie vocale

Annexe H – Aperçu de la sécurité en messagerie vocale

1 **Objet et domaine d'application**

1.1 *Considérations générales*

La présente Recommandation décrit les caractéristiques générales d'exploitation et de qualité de service du service public international de messagerie vocale. Les services de messagerie vocale offerts par les Administrations appartiennent au groupe des services télématiques définis dans les Recommandations de la série F.

Ce type de service de messagerie (MH) (*message handling*), est un service de télécommunication international offert par les Administrations qui permet aux abonnés d'envoyer un message à un ou plusieurs destinataires et de recevoir des messages au moyen de réseaux de télécommunication utilisant conjointement des techniques d'enregistrement et de retransmission et des techniques d'enregistrement et d'interrogation.

Les fonctions assurées localement, pour lesquelles il n'est pas nécessaire de communiquer avec d'autres abonnés, ne sont pas couvertes par les Recommandations du CCITT.

Le service de messagerie vocale (VM) (*voice messaging*) permet aux abonnés de demander l'exécution de diverses fonctions pendant le traitement et l'échange de messages vocaux codés.

Certaines fonctions sont propres au service de messagerie vocale de base. D'autres fonctions, qui ne sont pas des fonctions de base, peuvent, si elles sont fournies par les Administrations, être sélectionnées par l'utilisateur pour chaque message ou pour une période convenue aux termes d'un contrat.

L'intercommunication avec le service de messagerie de personne à personne (IPM) (*interpersonal messaging*) peut être assurée en option dans le service de messagerie vocale.

Il appartient aux Administrations de fournir les fonctions de base au niveau international. Les fonctions, autres que les fonctions de base, visibles pour l'abonné, sont classées en fonctions essentielles et fonctions supplémentaires.

Les Administrations sont tenues de fournir les fonctions facultatives essentielles au niveau international. Certaines Administrations peuvent fournir des fonctions facultatives supplémentaires pour un usage national et sur le plan international sur la base d'accords bilatéraux. Les fonctions autres que les fonctions de base sont appelées fonctions facultatives d'utilisateur.

Il est possible d'assurer le service de messagerie vocale en empruntant un réseau de communication quelconque. Ce service peut être offert séparément ou en association avec divers services télématiques ou de transmission de données. Il est possible d'y accéder en prenant les dispositions qui s'imposent.

Les spécifications techniques et les protocoles à utiliser dans le service de messagerie vocale sont définis dans les Recommandations de la série X.400.

La définition du service est donnée au § 2. Les conditions à remplir pour que les abonnés puissent communiquer entre eux sont décrites aux § 3 et 4. Le § 5 traite de la dénomination et de l'adressage alors que les § 6, 7 et 8 sont consacrés au fonctionnement du service, à la qualité de service ainsi qu'aux principes de tarification et de comptabilité. Les spécifications de réseau sont données au § 9. La fourniture des informations d'abonné fait l'objet du § 10 et le § 11 donne des informations sur l'utilisation du service de messagerie vocale dans le cadre des services télématiques définis par le CCITT.

1.2 *Systèmes de messagerie utilisés pour la fourniture du service de messagerie vocale*

1.2.1 *Mise en œuvre de 1984*

Dans la présente Recommandation on suppose que les systèmes de messagerie mis en œuvre pour assurer le service qu'elle décrit sont fondés sur la version 1988 des Recommandations de la série X.400. Il est toutefois admis que pendant un certain temps après la publication de la présente Recommandation, la majorité des réalisations du service de messagerie vocale restera fondée sur la version 1984 des Recommandations de la série X.400. Les Administrations sont invitées à adopter les Recommandations du CCITT les plus récentes; toutefois, dans l'intervalle, elles peuvent utiliser la présente Recommandation conjointement avec les réalisations «modèle 1984», comme indiqué plus bas.

1.2.2 *Eléments de service*

Les éléments de service disponibles pour les services de messagerie sont énumérés et classés dans la Recommandation F.400. L'annexe C de la présente Recommandation dresse une liste de tous les éléments de service (intitulée éléments de service en 1984) pour le service de messagerie vocale. Ces éléments, repris de la Recommandation X.400 (version 1984), sont basés sur les éléments de service du service IPM. L'annexe C de la Recommandation F.400 (version 1988) énumère les éléments de service définis en 1988 et indique toute modification par rapport à la classification de 1984. L'annexe D de la présente Recommandation énumère les éléments de service propres au service de messagerie vocale. L'annexe E de la présente Recommandation définit les éléments de service propres à la messagerie vocale autres que ceux qui sont donnés dans la Recommandation F.400. En tout état de cause, on peut utiliser les éléments de service (version 1984) pour la fourniture du service de messagerie vocale tel qu'il est défini dans la présente Recommandation, cela pendant un délai de grâce qui prendra fin en 1996.

Les Administrations sont instamment priées de mettre à niveau leurs réalisations et se conformer ainsi aux Recommandations de 1988.

1.2.3 *Formes des noms*

Les formes de nom à utiliser pour le service de messagerie vocale sont conformes à celles qui sont spécifiées dans les Recommandations F.400 (1988) et X.400 (1988).

1.2.4 *Interfonctionnement*

Afin de protéger les investissements des Administrations qui ont mis en place des systèmes «modèle 1984» pour assurer le service de messagerie vocale, il faudra assurer l'interfonctionnement des réalisations du domaine de gestion d'Administration (ADMD) (*Administration management domain*) modèle 1988 avec celles du modèle 1984, comme spécifié dans l'annexe B de la Recommandation X.419.

L'interfonctionnement des ADMD modèle 1988 et des domaines de gestion privés (PRMD) (*private management domains*) modèle 1984 relève de la compétence nationale.

2 Service de messagerie vocale

2.1 *Spécifications générales du service*

2.1.1 Ce service de messagerie vocale a pour fonction essentielle de fournir une interface publique entre les expéditeurs et les destinataires de communications vocales afin d'améliorer leurs moyens de communication, notamment lorsqu'on ne dispose pas d'un service de télécommunication direct instantané ou commode entre les équipements d'abonné ou lorsque les services de télécommunication disponibles sont incompatibles. Ce service peut aussi offrir les fonctions disponibles pour l'élaboration et la présentation des messages.

2.1.2 Les Administrations assureront le service de messagerie vocale en s'inspirant du service de transfert de messages défini dans la Recommandation F.410 et en utilisant des systèmes conformes aux dispositions des Recommandations de la série X.400.

Les domaines de gestion (MD) (*management domain*) servent à délimiter les responsabilités. Le domaine de gestion géré par une Administration est appelé domaine de gestion d'Administration. Le domaine de gestion géré par une organisation est appelé domaine de gestion privé.

2.1.3 L'échange international de messages se fait entre domaines de gestion d'Administration par l'intermédiaire des services publics de transmission de données normalisés par le CCITT.

2.1.4 Différents types de partie de corps de messages peuvent être échangés par le biais de ce service. La liste des divers types de partie de corps figure au § 3.

2.1.5 Une Administration peut offrir aux abonnés différentes méthodes d'accès au service de messagerie vocale. Les méthodes possibles sont les suivantes:

- 1) directement à partir du terminal de l'utilisateur (par exemple un combiné téléphonique);
- 2) par l'intermédiaire d'un système de messagerie privé.

Remarque – Un domaine de gestion de messagerie vocale peut être résident dans un autocommutateur privé.

2.1.6 Chaque Administration est responsable de l'accès national à son domaine de gestion.

2.1.7 La définition des caractéristiques des interfaces et des méthodes d'accès utilisées entre les terminaux et le service de messagerie vocale relève de la compétence nationale, bien que ces caractéristiques puissent être calquées sur les dispositions du service téléphonique vocal défini par le CCITT. Toutefois, les services complémentaires facultatifs du service de messagerie vocale sont définis et sont indépendants de la méthode d'accès et du terminal de l'utilisateur.

2.1.8 Au niveau de la mise en œuvre nationale, le service de messagerie vocale peut assurer l'intercommunication avec les services existants tels que service IPM, service télétexte, service de télécopie et service vidéotex. Lorsqu'elles sont mises en œuvre, les interfaces entre le service de messagerie vocale et les autres services doivent être conformes aux dispositions des Recommandations pertinentes du CCITT.

2.1.9 Étant donné que le service assure une communication indirecte, il peut y avoir des cas où le message n'est pas remis au destinataire prévu. Le service de messagerie vocale prévoit l'envoi d'une notification de non-remise et, à titre de services complémentaires facultatifs, de la notification de remise, de réception et de non-réception.

2.1.10 Compte tenu du fait que le message est placé dans une mémoire intermédiaire, le service peut offrir des services complémentaires facultatifs de conversion: vitesse, procédures d'accès, réseaux et codage du contenu des messages.

2.1.11 Le message appartient à l'expéditeur jusqu'au moment de la remise. Après la remise, le message appartient au destinataire.

2.1.12 Lorsque l'expéditeur et le destinataire ont des exigences différentes et contradictoires, ce sont les exigences de l'expéditeur qui prévalent (conversion de type de corps ou commande de réacheminement).

2.2 *Fonctions du service de messagerie vocale*

2.2.1 *Introduction*

Le § 19 de la Recommandation F.400 définit les éléments de service disponibles dans le service de messagerie vocale; ils sont classés en deux catégories selon qu'ils appartiennent au service de base ou qu'ils sont des services complémentaires facultatifs de messagerie vocale. Les éléments de service du service de messagerie vocale de base font partie intégrante du service et sont toujours fournis et disponibles. Les services complémentaires facultatifs classés comme essentiels sont toujours fournis et ceux qui sont classés comme supplémentaires peuvent être disponibles au niveau national ou international sur la base d'un accord bilatéral.

2.2.2 *Service de messagerie vocale de base*

Un ensemble d'éléments de service caractérise le service de messagerie vocale de base. Cet ensemble est défini dans la Recommandation F.400 et la liste des éléments est reproduite dans le tableau 10/F.400. Le service de messagerie vocale de base qui s'inspire du service de transfert de messages (MT) (*message transfer*) permet à un usager d'envoyer et de recevoir des messages vocaux.

Un usager prépare des messages vocaux avec l'aide de son agent d'utilisateur (UA) (*user agent*). Les UA, qui sont un ensemble de processus d'application informatiques, coopèrent entre eux pour faciliter la communication entre leurs usagers respectifs. Pour envoyer un message vocal, les usagers-expéditeurs font une demande auprès de leur UA en spécifiant le nom ou l'adresse du destinataire prévu du message vocal. Ce message, avec lequel un identificateur est transporté, est ensuite envoyé par l'UA de l'expéditeur à l'UA du destinataire via le service de transfert de messages.

Une fois remis à l'UA du destinataire, le message vocal peut être reçu par le destinataire. Pour que la communication puisse se dérouler dans les meilleures conditions, l'utilisateur-destinataire peut spécifier le/les type(s) de codage susceptible(s) d'être contenu(s) dans les messages vocaux remis à l'utilisateur, ainsi que la longueur maximale d'un message remis. Le/les type(s) de codage initial, l'indication de toute conversion qui aurait pu être effectuée et le/les type(s) de codage résultant sont fournis avec chaque message vocal remis. De plus, l'heure et la date de dépôt et de remise et d'autres informations sont fournies avec chaque message vocal. La notification de non-remise est assurée par le service de base.

2.2.3 *Services complémentaires facultatifs de la messagerie vocale*

Les services complémentaires facultatifs sont un ensemble d'éléments de service du service de messagerie vocale. La liste de ces services, qui peuvent être sélectionnés pour chaque message ou pour une période convenue aux termes d'un contrat, figure dans les tableaux 11/F.400 et 12/F.400. Les services complémentaires offerts au niveau local peuvent être utilement fournis conjointement avec certains de ces services complémentaires.

Les services complémentaires facultatifs du service de messagerie vocale, qui sont sélectionnés pour chaque message, sont classés tant pour l'expédition que pour la réception par les UA. Si une Administration assure le service de messagerie vocale et offre ces services complémentaires facultatifs pour l'expédition par les UA, un usager est en mesure de créer et d'envoyer des messages vocaux tout en se conformant aux procédures définies pour l'élément de service associé. Si une Administration assure le service de messagerie vocale et offre ces services complémentaires facultatifs pour la réception par les UA, l'UA destinataire sera en mesure de recevoir et de reconnaître l'indication associée à l'élément de service correspondant puis d'informer l'utilisateur du service complémentaire facultatif demandé. Du point de vue de l'expédition comme de la réception, chaque service complémentaire facultatif est classé comme supplémentaire ou essentiel.

2.2.4 *Fonctions locales*

Le système de messagerie (MHS) (*message handling system*) peut exécuter, en plus des fonctions de messagerie vocale, bon nombre de fonctions locales pour le compte de ses abonnés. Par exemple, pour aider les abonnés à préparer et éditer des messages vocaux, le système de messagerie peut assurer une fonction d'édition. Le système de messagerie pourrait alerter les abonnés de l'arrivée de nouveaux messages (par exemple en allumant un témoin sur leur poste téléphonique, en affichant sur leur terminal de bureau le nom de l'expéditeur et l'objet de tous les messages non lus, ou bien encore en déclenchant une indication vocale informatisée).

Si cette fonction d'alerte n'est pas disponible, un abonné devra interroger fréquemment le système de messagerie pour savoir si de nouveaux messages sont arrivés.

Le système de messagerie peut assurer des commandes de base de données locale pour aider l'abonné à retrouver des messages vocaux déjà reçus et classés (par exemple pour retrouver le message de Mme Smith remis au cours du mois d'août). Un abonné en vacances peut demander au système de messagerie de retransmettre automatiquement tous les messages vocaux à un représentant; il peut aussi définir les cas où les messages vocaux ne devront pas être retransmis automatiquement (par exemple des messages personnels).

Les services locaux comme ceux cités ci-dessus, tout en utilisant peut-être certaines des caractéristiques de la messagerie vocale, ne nécessitent pas une coordination ou une coopération avec d'autres abonnés. Ils n'affectent donc pas les protocoles de communication associés au système de messagerie. Par conséquent, les fonctions locales que peuvent offrir les Administrations ne relèvent pas du CCITT.

2.3 *Limites des responsabilités*

Le système de messagerie a pour objet de permettre le dépôt d'un message à expédier et la remise de ce message à un UA ou à une mémoire de messages (MS) (*message store*) dont l'adresse est spécifiée par l'expéditeur.

Côté expédition et côté réception l'utilisateur dialogue, au moyen d'un terminal d'accès, avec un UA. Sur demande, un message est déposé au système de transfert des messages (MTS) (*message transfer system*). Ce système est aussi en mesure de récupérer un message reçu d'un UA ou d'une MS.

La responsabilité du message est transférée au système de messagerie lorsque l'utilisateur-expéditeur donne l'ordre d'envoyer le message. La responsabilité du message passe ensuite à l'UA ou à la MS-destinataire une fois le message remis. Lorsque l'UA ou la MS est fourni par une Administration, la responsabilité du message passe à l'utilisateur-destinataire une fois le message remis. Lorsqu'il est impossible de remettre le message à l'UA ou à la MS-destinataire, le système de messagerie crée une notification de non-remise, ceci étant une fonction de base.

Les conditions applicables à ce critère peuvent aussi dépendre des services complémentaires facultatifs, l'interdiction de conversion par exemple. Un usager-expéditeur peut, pour un message particulier, demander spécifiquement une notification de remise et/ou une notification de réception et/ou une notification de non-réception. Dans le cas d'adresses télématiques, la remise intervient automatiquement lorsque le message est transmis au service télématique. Après la remise du message à une mémoire de documents ou une MS, la responsabilité du message passe à l'utilisateur une fois qu'il a lu le message pour la première fois. Lorsque le message est laissé dans la mémoire, c'est le prestataire de service qui déterminera la responsabilité.

Une perte d'information peut intervenir pendant le processus de conversion dans la mesure où la conversion n'est pas explicitement interdite par l'utilisateur-expéditeur.

La responsabilité d'un domaine de gestion pour des messages qui transitent à travers ce domaine commence au moment où le message pénètre dans le domaine et finit au moment où il en sort; cependant, il doit être possible d'effectuer un audit ultérieur.

Lorsqu'un ADMD interagit avec un PRMD, l'ADMD assume la responsabilité des actes du PRMD se rapportant à cette interaction. L'ADMD non seulement veille à ce que le PRMD fournisse correctement le service de transfert de messages mais est aussi chargé de s'assurer que les opérations de comptabilité, d'enregistrement, de qualité de service et autres relevant du PRMD sont exécutées correctement. Un ADMD joue le rôle d'autorité de dénomination pour les PRMD associés, conformément aux directives nationales.

2.4 *Mémoire de messages*

Les Administrations peuvent, à titre facultatif, fournir une mémoire de messages (ou mémoire MS) pour permettre la remise des messages de sorte que l'UA destinataire n'ait pas à être connecté en permanence. Ceci est décrit au § 7.4 de la Recommandation F.400. Un message remis à une MS est considéré comme remis par le MHS. Le destinataire peut à sa convenance extraire les messages remis à une MS et divers services complémentaires facultatifs offerts à l'utilisateur permettent cette extraction pour un listage, une recherche ou une suppression de message. Au moment de l'inscription à une MS, tous les messages destinés à l'UA sont remis à la MS, et si l'UA est connecté, un signal lui sera envoyé (à partir de la MS) pour indiquer à l'utilisateur qu'un message vient d'arriver.

2.5 *Unité d'accès au service téléphonique*

L'unité d'accès au service téléphonique (TSAU) (*telephone service access unit*) est une unité d'accès qui assure l'interfonctionnement entre les usagers du service de messagerie vocale ou du service IPM et les usagers du service téléphonique. Les usagers du service de messagerie vocale peuvent demander la remise d'un message vocal à tout usager du service téléphonique identifiable au moyen d'une adresse de réseau téléphonique (numéro de téléphone). Les usagers du service téléphonique peuvent utiliser la TSAU pour faire enregistrer et remettre un message vocal aux usagers du service de messagerie vocale et du service IPM.

2.5.1 *Description des fonctions de la TSAU*

Dans un environnement MHS, l'UA du service IPM ou du service de messagerie vocale peut accéder au réseau téléphonique par l'intermédiaire de la TSAU. L'utilisateur du MHS constitue le message vocal en interaction avec l'UA et demande sa remise à un usager de réseau téléphonique. L'utilisateur du MHS spécifie par ailleurs le numéro de téléphone du destinataire en utilisant une adresse expéditeur/destinataire (O/R) (*originator/recipient*) numérique. La partie de corps vocale MHS est envoyée dans une enveloppe F.400 à la TSAU, qui extrait la partie de corps vocale de l'enveloppe MHS et appelle le destinataire sur le réseau téléphonique pour remettre le message vocal à ce destinataire. Lorsque le message vocal est transmis à la TSAU, une notification de remise est envoyée à l'expéditeur. Le problème des algorithmes qui contrôlent la structure d'appel de la TSAU doit être réglé à l'échelon local.

Un usager du réseau téléphonique peut appeler la TSAU, enregistrer un message, fournir une adresse de remise (limitée aux caractères numériques du clavier de l'appareil téléphonique) et demander la remise du message à un usager du service de messagerie vocale ou du service IPM.

2.5.2 *Remise avec assistance des téléphonistes*

Normalement, la TSAU remet le message à toute personne répondant au téléphone à l'adresse du destinataire. La remise avec assistance des téléphonistes permet à un intermédiaire humain (opératrice) de contribuer à la remise du message. Une fois le choix effectué, l'utilisateur du service de messagerie vocale peut spécifier que le message ne peut

être remis qu'à un destinataire désigné. Les téléphonistes vérifient que le destinataire est disponible avant de passer le message vocal et ne remettent ce message que si le destinataire désigné est disponible pour le recevoir. A cet effet, l'indicateur du destinataire peut être utilisé pour vérifier que le destinataire est présent.

2.5.3 *Notification de TSAU*

La TSAU desservant les usagers du service téléphonique utilise une notification de remise MTS pour indiquer le transfert du message depuis le MTS à la TSAU, et des notifications vocales (réception et non-réception) pour indiquer la réception au terminal téléphonique.

2.6 *Utilisation de l'annuaire*

En utilisant des systèmes d'annuaire, les usagers du service IPM peuvent adresser les destinataires en utilisant les noms d'annuaire ou des noms de listes de distribution, plus commodes que les adresses expéditeur/destinataire (O/R). Le MHS pourra accéder à un système d'annuaire et trouver l'adresse ou les adresses O/R correspondant à un nom d'annuaire donné ou un nom de liste de distribution, pour la remise d'un message. Cette capacité est décrite au § 14 de la Recommandation F.400.

2.7 *Sécurité*

Les Administrations peuvent, à titre facultatif, fournir des mécanismes de sécurité comme indiqué au § 15 de la Recommandation F.400 pour parer aux divers dangers de sécurité mentionnés. Cette capacité repose sur un système d'annuaires qui garde en mémoire des copies certifiées de clés publiques pour les usagers du MHS.

2.8 *Listes de distribution*

Un groupe dont les membres figurent dans l'annuaire peut être utilisé comme liste de distribution (DL) (*distribution list*). L'expéditeur fournit simplement le nom de la liste au moment de la présentation du message et le MHS peut obtenir les noms (et ensuite les adresses O/R) des destinataires en consultant l'annuaire. Au moment de la réception d'un message adressé à une liste de distribution, le destinataire peut déterminer par quelle DL le message est parvenu. Un expéditeur peut interdire l'extension de la distribution si un des destinataires spécifiés est une liste de distribution. Le § 14 de la Recommandation F.400 décrit toutes les possibilités offertes aux usagers des DL.

Si un usager envoie sans le savoir un message à une DL, il peut avoir à payer des taxes pour plusieurs remises qu'il n'avait pas prévues. C'est pourquoi les noms des listes de distribution doivent faire état du fait que la désignation porte bien sur une DL. Les détenteurs de DL doivent s'assurer qu'ils respectent le souhait de devenir membre exprimé par un membre éventuel ainsi que les règles du pays dont le membre est ressortissant, qui pourraient interdire l'inscription d'un membre sans accord préalable.

3 **Types de partie de corps**

Les messages qu'envoie ou que reçoit le service de messagerie vocale peuvent se composer d'une ou de plusieurs parties de corps.

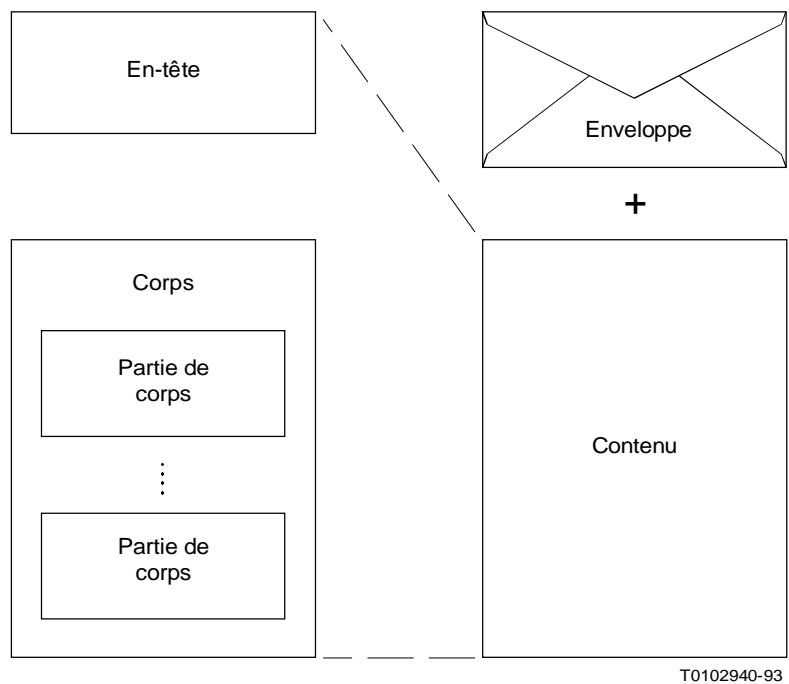
3.1 *Types de partie de corps possibles*

Les types de partie de corps applicables sont définis dans la Recommandation X.440. Ce sont notamment:

- partie vocale;
- partie message (par exemple, pour un message retransmis);
- notifications;
- partie définie extérieurement.

Dans un premier temps, le codage vocal assuré sera le codage de modulation par impulsions et codage différentiel adaptatif (MICDA) à 32 kbit/s décrit dans la Recommandation G.721 (1988). On pourra ajouter par la suite des schémas de codage pour des débits binaires plus faibles.

La catégorie d'agent d'utilisateur de messagerie vocale (VM-UA) (*voice messaging user agent*) crée des messages dont le contenu est spécifique au service de messagerie vocale. Le contenu spécifique envoyé d'un VM-UA à un autre émane d'un expéditeur qui, généralement, est une personne utilisant un téléphone pour composer et envoyer un message appelé «message vocal». Ce message vocal achemine l'objet vocal codé et éventuellement d'autres informations associées à cet objet vocal codé. Un seul objet vocal codé est présent dans un message vocal et chaque message vocal contient une partie de corps vocale codée lors de l'expédition du message vocal. La figure 1/F.440 montre la relation qui existe entre la structure d'un message vocal et celle d'un message de base du système de messagerie. Le message vocal est acheminé dans une enveloppe électronique lorsqu'il est transféré à travers le système de transfert de messages.



T0102940-93

FIGURE 1/F.440
Structure des messages vocaux

La figure 2/F.440 montre la correspondance entre un objet vocal codé typique et la structure du message vocal correspondant. L'objet vocal codé, qui est projeté dans son intégralité à l'intérieur d'une seule partie de corps – partie de corps primaire – peut être un objet vocal codé selon la Recommandation G.721 ou une méthode privée ou bien encore un message vocal retransmis. Sauf spécification contraire, on supposera que l'objet vocal est codé selon le MICDA à 32 kbit/s de la Recommandation G.721. On dispose d'autres parties de corps pour acheminer des informations associées à l'objet vocal codé telles qu'illustrations, notes d'information supplémentaire, etc. L'en-tête d'un message vocal contient divers champs d'information qui acheminent des demandes de service émanant de l'expéditeur. Ceci est illustré par la figure 2/F.440: le champ V-C n correspond à l'information vocale codée et le champ n à l'information codée non vocale.

L'en-tête et la/les parties de corps forment le message vocal. Un message vocal ne peut contenir qu'un seul objet vocal codé, intégralement inclus dans une seule et même partie de corps.

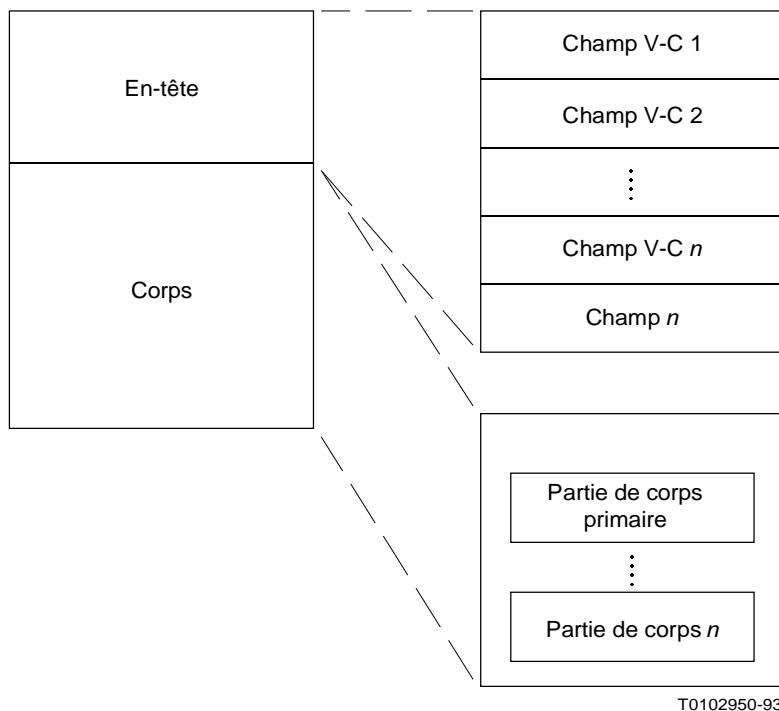


FIGURE 2/F.440

Structure des messages vocaux dans le cas d'une transaction typique de messagerie vocale

3.3 *Retransmission des messages vocaux*

Un usager du service de messagerie vocale peut demander que les messages reçus soient retransmis avec ou sans acceptation. Les demandes de notifications peuvent également être retransmises automatiquement avec les messages. On distingue les trois cas suivants:

- a) retransmission du message vocal accepté avec les notifications demandées;
- b) retransmission du message vocal et des notifications sans acceptation; et
- c) retransmission du message vocal lorsque les notifications n'ont pas été demandées.

De fait, le troisième cas est identique au deuxième. Un usager peut également demander la retransmission automatique.

Si un message vocal est retransmis après acceptation, la partie de corps primaire du message retransmis est le contenu du message reçu avec ou sans modification. Des parties de corps de message vocal supplémentaires peuvent être incluses ou supprimées, mais il ne peut pas y avoir plus d'une partie de corps supplémentaire à codage vocal par cas de retransmission. La partie de corps du message vocal retransmis ne peut pas être supprimée. Les notifications de réception sont établies selon la demande. S'il y a retransmission, une notification de non-réception (NRN) (*non-receipt notification*) n'est pas renvoyée à l'expéditeur du message. En messagerie vocale, la retransmission peut être destinée à un ou à plusieurs destinataires, et les demandes de notification peuvent être prévues pour l'un quelconque des destinataires.

Il est impossible d'ajouter ou de supprimer des parties de corps si un message vocal est retransmis sans acceptation. La retransmission peut être destinée à plus d'un destinataire. La demande de notification doit être la même que pour le message original, mais elle ne peut être envoyée qu'à l'un des destinataires prévus du message retransmis. Cela garantit que l'expéditeur original reçoit seulement la notification demandée.

4 Conversion entre différents types de codage

Le système de transfert de messages assure des fonctions de conversion qui permettent aux usagers de la messagerie vocale d'introduire des messages dans un format de codage donné appelé type de codage (EIT) (*encoded information type*) puis de le remettre dans un autre type de codage pour tenir compte des différents types de terminaux à la disposition des usagers. Cette fonction propre au service de messagerie vocale augmente les possibilités de remise en adaptant le message aux possibilités du terminal du destinataire. Les types de codage acceptés par le service de messagerie vocale sont définis dans la Recommandation X.440.

Le système de transfert de messages peut assurer une conversion automatique entre les divers schémas de codage normalisés, lorsque cela est nécessaire pour la remise d'un message.

Les aspects généraux et les règles spécifiques relatifs à la conversion entre différents types de codage du service de messagerie vocale nécessitent un complément d'étude.

5 Dénomination et adressage en général

Dans un système de messagerie, la principale entité qui exige une dénomination est l'utilisateur (l'expéditeur et le destinataire des messages). De plus, les DL comportent des noms à utiliser dans le système de messagerie. Les usagers du système de messagerie et les DL sont identifiés par des noms O/R. Ces noms sont composés de noms d'annuaire et/ou d'adresses O/R qui sont tous décrits dans le présent paragraphe. La Recommandation F.401 donne de plus amples détails sur la dénomination et l'adressage dans les services de messagerie publics, y compris sur les restrictions de dénomination et les responsabilités des Administrations.

5.1 Noms d'annuaire

Les usagers du service de messagerie et les DL peuvent être identifiés par un nom dit nom d'annuaire. Il faut chercher ce nom dans un annuaire pour trouver l'adresse O/R correspondant à un service particulier. La structure et les composantes des noms d'annuaire sont décrites dans les Recommandations de la série X.500.

Un usager peut accéder directement à un système d'annuaire pour trouver l'adresse O/R d'un usager ou les adresses O/R des membres d'une DL (ces deux types d'adresses n'entrent pas dans le cadre de ces Recommandations).

L'utilisateur peut aussi utiliser le nom d'annuaire et laisser le système de messagerie accéder à l'annuaire pour trouver automatiquement la/les adresse(s) O/R correspondante(s). Un usager du système de messagerie ou une DL ne possède pas forcément de nom d'annuaire à moins qu'il ne soit enregistré dans un annuaire. A mesure que les annuaires se développeront, les noms d'annuaire deviendront le meilleur moyen d'identifier les usagers du système de messagerie.

5.2 Noms O/R

Chaque usager du système de messagerie ou DL aura un nom O/R. Un nom O/R comprend un nom d'annuaire, une adresse O/R ou les deux. Le nom d'annuaire identifie l'utilisateur du système de messagerie de façon non ambiguë mais pas nécessairement unique. L'adresse O/R identifie l'utilisateur du système de messagerie de manière unique.

Chacun des éléments d'un nom O/R ou les deux peuvent être utilisés pour déposer un message. Si le seul nom présent est un nom d'annuaire, le système de messagerie accède à un annuaire pour tenter de déterminer l'adresse O/R qu'il utilisera ensuite pour acheminer et remettre le message. En l'absence de nom d'annuaire, il utilisera l'adresse O/R telle qu'elle est donnée. Si les deux informations sont fournies lors du dépôt du message, le système de messagerie utilisera l'adresse O/R mais acheminera le nom d'annuaire et communiquera les deux informations au destinataire. Si l'adresse O/R est incorrecte, le système de messagerie tentera alors d'utiliser le nom d'annuaire comme ci-dessus.

5.3 Adresses O/R

Une adresse O/R contient des informations qui permettent au MHS d'identifier de manière unique un usager afin de lui remettre un message ou de lui renvoyer une notification. (Le préfixe O/R correspond au fait que l'utilisateur peut être soit l'expéditeur (*originator*) soit le destinataire (*recipient*) du message ou de la notification en question.)

Diverses formes d'adresses O/R sont définies à l'heure actuelle à des fins différentes. Ces diverses formes d'adresse ainsi que leur objet sont décrits ci-après:

- *Adresse O/R numérique:* Fournit un moyen d'identifier l'utilisateur à l'aide de claviers numériques.
- *Adresse de terminal O/R:* Offre un moyen d'identifier les utilisateurs dont les terminaux appartiennent à des réseaux différents.
- *Adresse O/R mnémorique:* Fournit à l'utilisateur un moyen d'identifier facilement les utilisateurs en l'absence d'annuaire. Cette adresse sert aussi à identifier une liste de distribution.

Une adresse O/R se compose de plusieurs informations appelées attributs. Ces attributs utilisés dans les diverses formes d'adresse O/R susmentionnées sont décrits dans la Recommandation F.401.

Les domaines de gestion permettent à leurs utilisateurs d'expédier des messages en utilisant l'une quelconque des formes ci-dessus. La forme sous laquelle les noms sont introduits par l'abonné ou présentés à celui-ci relève des autorités nationales (par exemple, l'emploi de listes de distribution ou de moyens commandés pour identifier les UA). L'utilisation de l'adresse numérique O/R devrait devenir le mode prévalent d'adressage dans le service de messagerie vocale.

Chaque Administration est responsable de l'identification propre à chaque UA dans son domaine de gestion.

6 Fonctionnement du service

6.1 Considérations générales

6.1.1 Le service de messagerie vocale permet l'envoi, le transfert, la remise et la réception des messages par des procédures entièrement automatiques.

6.1.2 Les messages envoyés sont élaborés dans une mémoire, proviennent d'une mémoire et sont remis à une mémoire. Ces mémoires font partie de la fonctionnalité de l'agent d'utilisateur MS et sont commandées par l'abonné.

6.1.3 Le transfert de messages entre domaines de gestion est conforme au service de transfert de messages décrit dans la Recommandation F.410.

6.1.4 Chaque Administration offrant le service de messagerie vocale doit valider l'identité des abonnés au moment de l'accès.

6.1.5 Il appartient à chaque pays d'autoriser le raccordement de systèmes de messagerie privés au service public de messagerie vocale pour permettre aux utilisateurs de ces systèmes d'échanger des messages. Si ces interconnexions sont prévues, elles seront établies entre des domaines de gestion d'Administration conformément aux Recommandations du CCITT.

6.1.6 Lorsqu'une conversion implicite est assurée par l'Administration via le service de transfert de messages, le message sera converti si nécessaire à moins que l'expéditeur n'interdise la conversion. La conversion sera conforme aux règles spécifiées dans la Recommandation X.408. Voir aussi le § 4 de la présente Recommandation.

6.1.7 La remise différée sera assurée par le domaine de gestion de l'expéditeur, ce domaine étant responsable du stockage du message jusqu'à la date et l'heure de remise spécifiées. L'élément de service «remise différée» ne sera donc pas utilisé sur des liaisons internationales.

6.2 Phases de traitement des messages

6.2.1 Considérations générales

Le service de messagerie vocale comporte différentes phases de traitement des messages visibles pour l'utilisateur.

6.2.2 Phase de préparation

Pendant cette phase, les messages sont préparés en utilisant les fonctions d'UA (par exemple saisie, édition, classement). Les modalités d'exécution de ces fonctions n'entrent pas dans le cadre de la présente Recommandation.

6.2.3 *Phase d'expédition*

Pendant cette phase, l'expéditeur peut demander à l'UA ou à la MS d'envoyer un message préparé à un ou plusieurs destinataires et de faire éventuellement appel à certains services complémentaires facultatifs.

6.2.4 *Phase de réception*

Pendant cette phase, l'abonné peut recevoir des messages et des notifications émanant de l'UA ou de la MS. La phase de réception peut être déclenchée par le service (réception automatique) ou par l'abonné. Le fonctionnement de l'UA recevant les messages est spécifié dans la Recommandation X.440 de messagerie vocale.

Les abonnés utilisant des terminaux dépourvus des fonctionnalités d'UA peuvent s'inscrire pour une période contractuelle pendant laquelle les messages envoyés seront automatiquement remis par leur UA au terminal si l'Administration prévoit ce cas de figure. Normalement on appelle l'UA pour recevoir les messages entrants.

En cas de réception automatique, le système de messagerie appellera le terminal de l'abonné. Dans le cas contraire, c'est l'abonné qui appellera le système de messagerie à un moment qui lui convient.

L'abonné recevra les parties de corps du message sous la forme dans laquelle l'expéditeur les a envoyées, sauf s'il y a eu conversion.

Lorsque l'expéditeur a fait appel aux services complémentaires facultatifs, l'UA en communique l'indication au destinataire sous une forme pratique pour ce dernier.

Notifications – Quatre notifications peuvent être reçues:

- notification de non-remise;
- notification de remise;
- notification de réception;
- notification de non-réception.

La notification de non-remise est automatiquement générée par le système de transfert de messages alors que les notifications de remise, de réception et de non-réception dépendent d'une action du destinataire.

6.2.5 *Notifications de service*

Les notifications de service ne sont envoyées qu'à la demande de l'expéditeur. Elles sont transmises peu après que le message ait quitté le MTS pour l'UA ou la MS du destinataire. Les notifications de service peuvent être produites par un UA, une MS ou une TSAU si elles sont demandées dans un indicateur de demande de notification de message vocal (VN) (*voice notification*) pour chaque destinataire. Les raisons de la notification de service sont spécifiées dans l'annexe B pour l'élément de service «demande de notification de message vocal».

7 Qualité de service

7.1 *Etat des messages*

L'identification unique de chaque message vocal permet au système de fournir des informations, par exemple sur l'état d'un message vocal.

En cas de panne du système, il doit être possible de garder la trace de tous les messages acceptés et non remis. Si des messages ne peuvent être remis, l'expéditeur doit en être informé par une notification de non-remise.

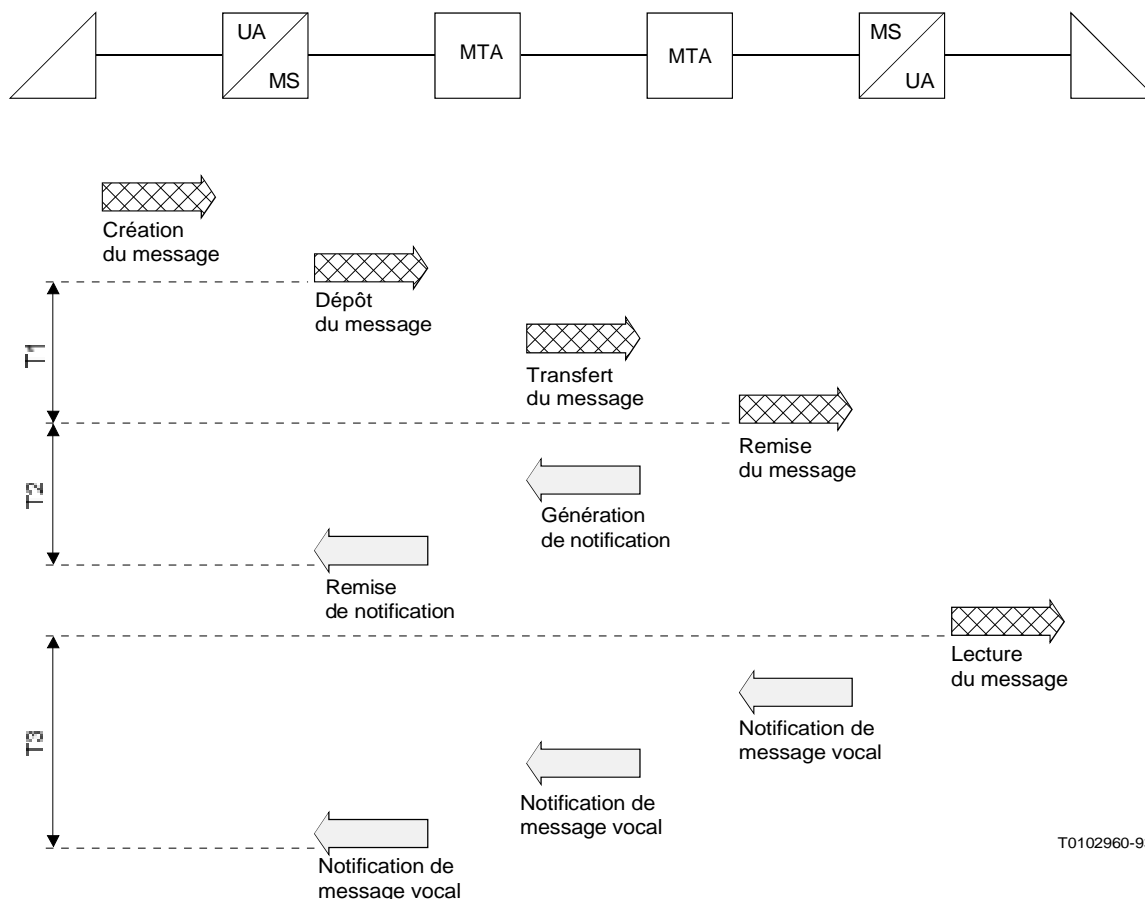
7.2 *Aide des Administrations*

Les Administrations doivent prêter assistance à leurs abonnés pour ce qui est des notifications de non-remise ou de messages qui ne sont pas reçus en temps voulu et cela dans la mesure où interviennent les composantes d'un système public. Il peut être décidé sur le plan national de fournir également une information concernant l'état et le suivi des messages.

Lorsque l'UA est fourni par une Administration, une fonction supplémentaire sera assurée pour minimiser le nombre des messages qui ne seraient pas lus dans un délai donné (la détermination de ce délai nécessite un complément d'étude). Cette fonction pourrait être par exemple l'envoi de messages d'avertissement à un terminal de réception automatique.

7.3 *Modèle d'heures de remise et de notification*

Voir la figure 3/F.440.



T1 Délai de remise
 T2 Délai de notification de remise
 T3 Délai de notification de message vocal

} Pour de plus amples détails, on se reportera à la Recommandation F.410

Remarque 1 – L'instant de début de T3 correspond à l'instant où le message est lu à l'intention de l'utilisateur et où la notification de réception est déclenchée par l'utilisateur.

Remarque 2 – L'instant de fin de T3 est l'instant auquel la notification de message vocal est mise à la disposition de l'utilisateur par l'intermédiaire de l'UA ou de la MS.

Remarque 3 – Des considérations semblables s'appliquent aux notifications de non-réception.

FIGURE 3/F.440
Modèle de délais de notification

7.4 Objectifs en matière de délais de remise des messages

Le domaine de gestion de l'UA destinataire enverra une notification de non-remise si le message n'a pas été remis x heures après le dépôt (ou après la date et l'heure indiquées pour la remise différée), la valeur de x dépendant de l'urgence de remise demandée par l'expéditeur. (Voir le § 4.4 de la Recommandation F.410.)

7.5 Objectifs en matière de délais de notification de remise

Pour chacun des destinataires, une notification de non-remise ou une notification de remise (si elle est demandée) sera envoyée à l'expéditeur pour ne pas retarder la remise des notifications correspondant aux messages déjà remis dans le cas d'un message multidestinataires; cela permet au domaine de gestion de l'expéditeur d'envoyer une notification par destinataire ou de regrouper les notifications pour ses abonnés. (Voir le § 4.5 de la Recommandation F.410.)

7.6 Notifications de réception et de non-réception

La date et l'heure de remise des notifications de réception et de non-réception ainsi que des notifications de disponibilité des éléments de service dépendent avant tout d'accords locaux. Lorsque ces notifications sont envoyées par l'UA/usager destinataire, les délais de remise sont les mêmes que pour les messages auxquels ils se rapportent.

TABLEAU 1/F.440

Objectifs en matière de délais impartis pour les notifications de réception et de non-réception

Urgence de remise (du message en question)	95% des messages remis avant	Non-remise imposée au bout de
Urgent	0,25 h	2 h
Normal	1,0 h	6 h
Non urgent	4,0 h	12 h

Remarque – L'intercommunication avec les PRMD n'est pas prise en compte dans le calcul des délais.

7.7 Protection contre les erreurs

La protection contre les erreurs pendant la transmission est assurée par le système de messagerie et les protocoles sous-jacents utilisés pour la fourniture du service de messagerie vocale.

7.8 Disponibilité du service

En principe, le service de messagerie vocale sera disponible en permanence. L'UA sera disponible en permanence pour le dépôt ou la remise (à moins que ne soit demandée une «attente pour remise ultérieure»). Au cas où l'UA n'est pas disponible en permanence pour la remise, on utilisera une MS.

7.9 Capacité minimale de mémorisation

La capacité de mémorisation d'un UA et d'une MS doit être suffisante pour assurer une qualité de service élevée.

Remarque – Cette question appelle un complément d'étude.

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 using 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.