



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

X.402

(09/92)

**RÉSEAUX DE COMMUNICATIONS
DE DONNÉES**

**SYSTÈMES DE MESSAGERIE:
ARCHITECTURE GLOBALE**



Recommandation X.402

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 révisée X.402, élaborée par la Commission d'études VII, a été approuvée le 10 septembre 1992 selon la procédure définie dans la Résolution n° 2.

NOTES DU CCITT

- 1) Dans cette Recommandation, le terme «Administration» désigne indifféremment une Administration de télécommunication ou une exploitation privée reconnue.
- 2) La liste des abréviations utilisées dans cette Recommandation se trouve dans l'annexe J.

© 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'UIT.

**SYSTÈMES DE MESSAGERIE:
ARCHITECTURE GLOBALE**

(révisée en 1992)

SECTION 1 – INTRODUCTION

0 Introduction

La présente Recommandation s'inscrit dans une série de Recommandations consacrées à la messagerie. La série complète donne un schéma d'ensemble d'un système de messagerie (MHS) réalisé à l'aide d'un nombre quelconque de systèmes ouverts associés.

Un système MHS a pour but de permettre aux utilisateurs d'échanger des messages en mode enregistrement et retransmission. Un message déposé par l'utilisateur (l'expéditeur) est acheminé par le système de transfert de messages (MTS), puis remis aux agents d'un ou plusieurs utilisateurs supplémentaires (les destinataires). Des unités d'accès (AU) relient le système MTS à des systèmes de communication de types différents (systèmes postaux, par exemple). Un utilisateur est assisté dans la préparation, l'enregistrement et l'affichage de ses messages par un agent d'utilisateur (UA). A titre facultatif, il est aidé pour l'enregistrement des messages par une mémoire de messages (MS). Le système MTS comprend plusieurs agents de transfert de messages (MTA) qui assurent collectivement la fonction de transfert de messages en mode enregistrement et retransmission.

La présente Recommandation spécifie l'architecture globale du système MHS et lui sert d'introduction technique.

Le texte de la présente Recommandation fait l'objet d'un accord commun CCITT-ISO. La spécification ISO correspondante est la Norme ISO 10021-2:1990 telle qu'elle est modifiée par les Corrigendums techniques 1, 2, 3 et 4 et le projet de modification 1.

1 Champ d'application

La présente Recommandation définit l'architecture globale du système MHS et lui sert d'introduction technique.

D'autres aspects de la messagerie sont spécifiés dans d'autres Recommandations du CCITT | ISO/CEI 10021. Un aperçu non technique de la messagerie est donné dans la Rec. X.400 du CCITT | ISO/CEI 10021-1. Les essais de conformité des composantes du système MHS sont décrits dans la Recommandation X.403. Les conventions utilisées dans la définition des services abstraits assurés par les composantes du système MHS sont définies dans la Rec. X.407 du CCITT | ISO/CEI 10021-3. Les règles détaillées suivant lesquelles le système MTS convertit le contenu de messages d'un type d'information codée (EIT) en un autre sont définies dans la Recommandation X.408. Le service abstrait assuré par le système MTS et les procédures qui en régissent le fonctionnement décentralisé sont définis dans la Rec. X.411 du CCITT | ISO/CEI 10021-4. Le service abstrait assuré par la mémoire MS est défini dans la Rec. X.413 du CCITT | ISO/CEI 10021-5. Les protocoles d'application qui régissent les interactions des composantes du système MHS sont spécifiés dans la Rec. X.419 du CCITT | ISO/CEI 10021-6. Le système de messagerie de personne à personne qui est une application de la messagerie, est défini dans la Rec. X.420 du CCITT | ISO/CEI 10021-7. L'accès télématique au système de messagerie de personne à personne est spécifié dans la Recommandation T.330.

Le tableau 1/X.402 récapitule les Recommandations du CCITT et les Normes internationales ISO/CEI relatives à la messagerie.

TABLEAU 1/X.402

Spécifications concernant les systèmes de messagerie

CCITT	ISO/CEI	Sujets
Introduction		
X.400	10021-1	Présentation générale des services et des systèmes
X.402	10021-2	Architecture globale
Aspects divers		
X.403	–	Essais de conformité
X.407	10021-3	Conventions utilisées pour la définition du service abstrait
X.408	–	Règles de conversion du type d'information codée
Services abstraits		
X.411	10021-4	Définition du service abstrait MTS et procédures régissant le fonctionnement décentralisé
X.413	10021-5	Définition du service abstrait MS
Protocoles		
X.419	10021-6	Spécifications des protocoles
Système de messagerie de personne à personne		
X.420	10021-7	Système de messagerie de personne à personne
T.330	–	Accès télématique à l'IPMS

L'annuaire, principal moyen de diffusion des informations concernant les communications parmi les composantes du système MHS, est défini dans les Rec. de la série X.500 du CCITT | ISO/CEI 9594 ainsi que le résume le tableau 2/X.402.

TABLEAU 2/X.402

Spécifications concernant les annuaires

CCITT	ISO/CEI	Sujet
X.500	9594-1	Présentation générale
X.501	9594-2	Modèles
X.509	9594-8	Cadre d'authentification
X.511	9594-3	Définition du service abstrait
X.518	9594-4	Procédures régissant le fonctionnement réparti
X.519	9594-5	Spécifications des protocoles
X.520	9594-6	Types d'attributs choisis
X.521	9594-7	Classes d'objets choisis

Les bases architecturales de la messagerie font l'objet d'autres Recommandations | Normes internationales. Le modèle de référence OSI est défini dans la Rec. X.200 du CCITT | ISO/CEI 7498. La notation permettant de spécifier les structures de données des services abstraits et des protocoles d'application, ASN.1, ainsi que les règles de codage correspondantes, sont définies dans les Rec. X.208 et X.209 du CCITT | ISO/CEI 8824 et 8825. Le moyen qui permet d'établir et de libérer des associations, l'élément de service de commande d'association ACSE, est défini dans les Rec. X.217 et X.227 du CCITT | ISO/CEI 8649 et 8650. Le moyen qui permet d'acheminer de manière fiable les unités APDU pendant les associations, l'élément de service de transfert fiable RTSE, est défini dans les Recommandations X.218 et X.228 | ISO/CEI 9066. Le moyen qui permet d'adresser des demandes d'autres systèmes ouverts, l'élément de service d'opérations distantes ROSE, est défini dans les Rec. X.219 et X.229 du CCITT | ISO/CEI 9072.

Le tableau 3/X.402 présente un état récapitulatif des Recommandations du CCITT et des Normes internationales ISO/CEI sur lesquelles repose la messagerie.

TABLEAU 3/X.402

Spécifications concernant les bases du MHS

CCITT	ISO/CEI	Sujet
Modèle		
X.200	7498	Modèle de référence OSI
ASN.1		
X.208	8824	Notation de syntaxe abstraite nyméro un
X.209	8825	Règles de codage de base
Commande d'association		
X.217	8649	Définition des services
X.227	8650	Spécification des protocoles
Transfert fiable		
X.218	9066-1	Définition des services
X.228	9066-2	Spécification des protocoles
Opérations distantes		
X.219	9072-1	Définition des services
X.229	9072-2	Spécification des protocoles

La présente Recommandation est structurée comme suit. La section 1 est l'introduction. La section 2 présente des modèles abstraits de messagerie. La section 3 spécifie comment on peut configurer les systèmes MHS pour répondre à l'une quelconque des spécifications d'ordre fonctionnelle, physique et organisationnelle. La section 4 décrit la dénomination et l'adressage des utilisateurs et des listes de distribution et l'acheminement des objets d'information jusqu'à eux. La section 5 décrit les utilisations possibles de l'annuaire par le système MHS. La section 6 décrit comment le système MHS est réalisé à l'aide de l'OSI. Les annexes donnent d'importants renseignements complémentaires.

Aucune exigence de conformité à la présente Recommandation n'est imposée.

2 Références normatives

Les Recommandations du CCITT et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation et Norme sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Secrétariat du CCITT tient à jour une liste des Recommandations du CCITT actuellement en vigueur.

2.1 *Interconnexion des systèmes ouverts*

La présente Recommandation et d'autres de cette série citent les spécifications OSI suivantes:

- Recommandation X.200 (1988), *Modèle de référence pour l'interconnexion des systèmes ouverts pour les applications du CCITT.*
ISO 7498:1984, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base.*
ISO 7498: 1984/Corr.1:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Corrigendum technique 1.*
ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*
ISO 8822:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Définition du service de présentation en mode connexion.*
- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*
ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de la notation de syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage pour la notation de syntaxe abstraite numéro un (ASN.1).*
ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.217 du CCITT: (1988), *Définition du service de contrôle d'association pour l'interconnexion des systèmes ouverts pour les applications du CCITT.*
ISO 8649:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Définition du service de l'élément du service de contrôle d'association.*
- Recommandation X.218 du CCITT (1988), *Transfert fiable: modèle et définition du service.*
ISO/CEI 9066-1:1989, *Systèmes de traitement de l'information – Communication de texte – Transfert fiable – Partie I: Modèle et définition du service.*
- Recommandation X.219 du CCITT (1988), *Opérations distantes: modèle, notation et définition du service.*
ISO/CEI 9072-1:1989, *Systèmes de traitement de l'information – Communication de texte – Opérations à distance – Partie I: Modèle, notation et définition du service.*
- Recommandation X.227 du CCITT (1988), *Spécification du service de contrôle d'association de l'OSI (interconnexion de systèmes ouverts) pour les applications du CCITT.*
ISO 8650:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Spécification du protocole pour l'élément de service de contrôle d'association.*
- Recommandation X.228 du CCITT (1988), *Transfert fiable: Spécification du protocole.*
ISO/CEI 9066-2:1989, *Systèmes de traitement de l'information – Communication de texte – Transfert fiable – Partie 2: Spécification du protocole.*
- Recommandation X.229 du CCITT (1988), *Opérations distantes: Spécification du protocole.*
ISO/CEI 9072-2:1989, *Systèmes de traitement de l'information – Communication de texte – Opérations à distance – Partie 2: Spécification du protocole.*

2.2 *Systèmes d'annuaire*

La présente Recommandation et d'autres de cette série citent les spécifications de système d'annuaire suivantes:

- Recommandation X.500 du CCITT (1988), *L'annuaire – Aperçu général des concepts, modèles et services*.
ISO/CEI 9594-1:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 1: Présentation générale des concepts, modèles et service*.
- Recommandation X.501 du CCITT (1988), *L'annuaire – Modèles*.
ISO/CEI 9594-2:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 2: Modèles*.
- Recommandation X.509 du CCITT (1988), *L'annuaire – Cadre d'authentification*.
ISO/CEI 9594-8:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 8: Cadre général d'authentification*.
- Recommandation X.511 du CCITT (1988), *L'annuaire – Définition du service abstrait*.
ISO/CEI 9594-3:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 3: Définition du service abstrait*.
- Recommandation X.518 du CCITT (1988), *L'annuaire – Procédures de fonctionnement réparti*.
ISO/CEI 9594-4:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 4: Procédures pour le fonctionnement réparti*.
- Recommandation X.519 du CCITT (1988), *L'annuaire – Spécifications du protocole*.
ISO/CEI 9594-5:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 5: Spécification du protocole*.
- Recommandation X.520 du CCITT (1988), *L'annuaire – Types d'attributs sélectionnés*.
ISO/CEI 9594-6:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 6: Types d'attributs sélectionnés*.
- Recommandation X.521 du CCITT (1988), *L'annuaire – Classes d'objets sélectionnés*.
ISO/CEI 9594-7:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 7: Classes d'objets sélectionnés*.

2.3 *Systèmes de messagerie*

La présente Recommandation et d'autres de cette série citent les spécifications de système de messagerie suivantes:

- Recommandation T.330 du CCITT (1988), *Accès télématique aux systèmes de messagerie de personne à personne*.
- Recommandation X.400 du CCITT (1992), *Système de messagerie – Principes du système et du service de messagerie*.
ISO/CEI 10021-1:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 1: Présentation générale du système et des services*.
ISO/CEI 10021-1:1990/Corr.1: 1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 1: Présentation générale du système et des services – Corrigendum technique 1*.
ISO/CEI 10021-1:1990/Corr.2: 1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 1: Présentation du système et des services – Corrigendum technique 2*.
ISO/CEI 10021-1: 1990/Corr.3:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 1: Présentation générale du système et des services – Corrigendum technique 3*.
ISO/CEI 10021-1:1990/Corr.4: 1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 1: Présentation générale du système et des services – Corrigendum technique 4*.

- Recommandation X.403 du CCITT (1988), *Systèmes de messagerie – Essais de conformité.*
- Recommandation X.407 du CCITT (1988), *Systèmes de messagerie – Conventions pour la définition des services abstraits.*
- ISO/CEI 10021-3:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 3: Conventions relatives à la définition de service abstrait.*
- ISO/CEI 10021-3:1990/Corr.1:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 3: Conventions relatives à la définition de service abstrait – Corrigendum technique 1.*
- Recommandation X.408 du CCITT (1988), *Systèmes de messagerie: règles de conversion entre différents types d'informations codées.*
- Recommandation X.411 du CCITT (1992), *Systèmes de messagerie: Système de transfert de messages: définition des services abstraits et procédures.*
- ISO/CEI 10021-4:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Système de transfert de message: Procédures et définition de service abstrait.*
- ISO/CEI 10021-4:1990/Corr.1:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Système de transfert de message: Procédures et définition de service abstrait – Corrigendum technique 1.*
- ISO/CEI 10021-4:1990/Corr.2:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Système de transfert de message: Procédures et définition de service abstrait – Corrigendum technique 2.*
- ISO/CEI 10021-4:1990/Corr.3:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Système de transfert de message: Procédures et définition de service abstrait – Corrigendum technique 3.*
- ISO/CEI 10021-4:1990/Corr.4:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Systèmes de transfert de message: Procédures et définition de service abstrait – Corrigendum technique 4.*
- ISO/CEI 10021-4:1990/Add.1:1993, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 4: Systèmes de transfert de message: Procédures et définition de service abstrait – Modification 1: Améliorations mineures.*
- Recommandation X.413 du CCITT (1992), *Systèmes de messagerie: Définition du service abstrait d'enregistrement de messages.*
- ISO/CEI 10021-5:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 5: Dépôt de message: Définition de service abstrait.*
- ISO/CEI 10021-5:1990/Corr.1:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 5: Dépôt de message: Définition de service abstrait – Corrigendum technique 1.*
- ISO/CEI 10021-5:1990/Corr.2:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 5: Dépôt de message: Définition de service abstrait – Corrigendum technique 2.*
- ISO/CEI 10021-5:1990/Corr.3:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 5: Dépôt de message: Définition de service abstrait – Corrigendum technique 3.*
- ISO/CEI 10021-5:1990/Corr.4:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 5: Dépôt de message: Définition de service abstrait – Corrigendum technique 4.*
- Recommandation X.419 du CCITT (1992), *Systèmes de messagerie: Spécifications de protocoles.*

ISO/CEI 10021-6:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 6: Spécification de protocole.*

ISO/CEI 10021-6:1990/Corr.1:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 6: Spécification de protocole – Corrigendum technique 1.*

ISO/CEI 10021-6:1990/Corr.2:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 6: Spécification de protocole – Corrigendum technique 2.*

ISO/CEI 10021-6:1990/Corr.3:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 6: Spécification de protocole – Corrigendum technique 3.*

ISO/CEI 10021-6:1990/Corr.4:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 6: Spécification de protocole – Corrigendum technique 4.*

- Recommandation X.420 du CCITT (1992), *Systèmes de messagerie – Système de messagerie de personne à personne.*

ISO/CEI 10021-7:1990, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne.*

ISO/CEI 10021-7:1990/Corr.1:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne – Corrigendum technique 1.*

ISO/CEI 10021-7:1990/Corr.2:1991, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne – Corrigendum technique 2.*

ISO/CEI 10021-7:1990/Corr.3:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne – Corrigendum technique 3.*

ISO/CEI 10021-7:1990/Corr.4:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne – Corrigendum technique 4.*

ISO/CEI 10021-7:1990/Mod.1:1992, *Technologies de l'information – Communication de texte – Systèmes d'échange de texte en mode message – Partie 7: Système de messagerie de personne à personne – Modification 1: Améliorations mineures.*

2.4 Codes de pays et plans de numérotage

La présente Recommandation cite la spécification suivante:

- Recommandation X.121 du CCITT (1988), *Plan de numérotage international pour les réseaux publics pour données.*
- Recommandation E.163 du CCITT (1988), *Plan de numérotage du service téléphonique international.*
- Recommandation E.164 du CCITT (1988), *Plan de numérotage pour le RNIS.*

ISO 3166:1988, Codes pour la représentation des noms de pays.

3 Définitions

Pour les besoins de la présente Recommandation et d'autres Recommandations de cette série, les définitions ci-après sont appliquées.

3.1 Interconnexion des systèmes ouverts

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Rec. X.200 du CCITT | ISO 7498, ainsi que les noms des sept couches du modèle de référence:

- a) syntaxe abstraite;

- b) entité d'application (AE) (*application entity*);
- c) processus d'application;
- d) unité de données de protocole d'application (APDU) (*application protocol data unit*);
- e) élément de service d'application (ASE) (*application service element*);
- f) tâche de traitement réparti de l'information;
- g) couche;
- h) système ouvert;
- i) interconnexion de systèmes ouverts (OSI) (*open systems interconnection*);
- j) homologue;
- k) contexte de présentation;
- l) protocole;
- m) modèle de référence;
- n) syntaxe de transfert;
- o) élément utilisateur (UE) (*user element*).

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans les Rec. X.208 et X.209 du CCITT | ISO/CEI 8824 et 8825, ainsi que les noms des types de données et des valeurs de l'ASN.1:

- a) notation de syntaxe abstraite numéro un (ASN.1) (*abstract syntax notation one*);
- b) règles de codage de base;
- c) explicite;
- d) export;
- e) implicite;
- f) import;
- g) macro;
- h) module;
- i) étiquette;
- j) type;
- k) valeur.

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Rec. X.217 du CCITT | ISO 8649:

- a) association d'application; association;
- b) contexte d'application (AC) (*application context*);
- c) élément de service de contrôle d'association (ACSE) (*association control service element*);
- d) demandeur; et
- e) demandé.

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Rec. X.218 du CCITT | ISO/CEI 9066-1:

- a) transfert fiable (RT) (*reliable transfer*); et
- b) élément de service de transfert fiable (RTSE) (*reliable transfer service element*).

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Rec. X.219 du CCITT | ISO/CEI 9072-1:

- a) argument;
- b) asynchrone;
- c) rattachement;
- d) paramètre;

- e) erreur distante;
- f) opération distante;
- g) opérations distantes (RO) (*remote operations*);
- h) élément de service d'opérations distantes (ROSE) (*remote operations service element*);
- i) résultat;
- j) synchrone; et
- k) détachement.

3.2 *Systèmes d'annuaire*

La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans les Rec. de la série X.500 du CCITT | ISO/CEI 9594:

- a) attribut;
- b) certificat;
- c) autorité de certification;
- d) trajet de certification;
- e) adresse figurant dans l'annuaire; adresse;
- f) agent de système d'annuaire (DSA) (*directory system agent*);
- g) annuaire;
- h) adressage calculé;
- i) nom;
- j) classe d'objet;
- k) objet;
- l) authentification simple; et
- m) authentification ferme.

3.3 *Systèmes de messagerie*

Pour les besoins de la présente Recommandation et d'autres Recommandations de cette série, les définitions répertoriées dans l'annexe I sont applicables.

4 **Abréviations**

Pour les besoins de la présente Recommandation et d'autres Recommandations de cette série, les abréviations répertoriées dans l'annexe I sont applicables.

5 **Conventions**

La présente Recommandation utilise les conventions descriptives identifiées ci-après.

5.1 *ASN.1*

La présente Recommandation utilise plusieurs conventions descriptives fondées sur l'ASN.1 dans ses annexes A et C, pour définir les informations spécifiques à la messagerie que l'annuaire peut contenir. Elle utilise notamment les macros OBJECT-CLASS, ATTRIBUTE ET ATTRIBUTE-SYNTAX de la Rec. X.501 du CCITT | ISO/CEI 9594-2 pour définir les classes d'objets, les attributs et les syntaxes d'attributs propres à la messagerie.

L'ASN.1 figure une première fois dans l'annexe A, pour la clarté de l'exposé, et une nouvelle fois dans l'annexe C, où elle fait en grande partie double emploi, pour référence. Si des différences sont constatées entre les deux, une erreur de spécification est indiquée.

A noter que les étiquettes de l'ASN.1 sont implicites dans le module de l'ASN.1 qui est défini dans l'annexe C; ce module est définitif à cet égard.

5.2 Catégorie

Chaque fois que la présente Recommandation décrit une classe de structure de données (adresses d'O/R, par exemple) ayant des composantes (attributs, par exemple), chaque composante est classée dans l'une des catégories suivantes:

- a) **obligatoire (M)** (*mandatory*): une composante obligatoire doit être présente dans chaque exemple de la classe;
- b) **optionnelle (O)** une composante optionnelle doit être présente dans une instance de la classe à la discrétion de l'objet (utilisateur, par exemple) qui fournit cette instance. Il n'y a pas de valeur par défaut;
- c) **valeur pouvant être prise par défaut (D)** (*defaultable*): une composante qui peut prendre une valeur par défaut doit être présente dans une instance de la classe à la discrétion de l'objet (utilisateur, par exemple) qui fournit cette instance. En l'absence d'une telle composante, une valeur par défaut, spécifiée par la présente Recommandation | partie de ISO/CEI 10021, est appliquée;
- d) **conditionnelle (C)**: une composante conditionnelle doit être présente dans une instance de la classe, comme le stipule la présente Recommandation.

5.3 Termes

Dans le reste de la présente Recommandation, les termes sont présentés en **caractères gras** lorsqu'ils sont définis, en *italique*, lorsqu'ils sont mentionnés avant leur définition et en caractères normaux dans les autres cas.

Les termes qui sont des noms propres sont présentés en majuscules mais non les termes génériques.

SECTION 2 – MODÈLES ABSTRAITS

6 Présentation générale

La présente section présente des modèles abstraits de *Messagerie* qui fournissent la base architecturale pour les spécifications plus détaillées qui figurent dans d'autres Recommandations du CCITT | ISO/CEI 10021.

La **messagerie** est une tâche de traitement de l'information par répartition qui intègre les sous-tâches suivantes qui sont intrinsèquement liées:

- a) **Transfert de messages** – Acheminement (différé) d'objets d'information entre des parties qui utilisent des ordinateurs comme intermédiaires.
- b) **Enregistrement de messages** – Enregistrement automatique d'objets d'information acheminés par le transfert de message, en vue de leur extraction ultérieure.

La présente section porte sur les sujets suivants:

- a) modèle fonctionnel;
- b) modèle d'information;
- c) modèle opérationnel;
- d) modèle de sécurité.

Remarque – La messagerie a diverses applications; l'une d'entre elles, la messagerie de personne à personne, est décrite dans la Rec. X.420 du CCITT | ISO/CEI 10021-7.

7 Modèle fonctionnel

Un modèle fonctionnel de messagerie est présenté ici. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations du CCITT | ISO/CEI 10021.

L'**environnement du système de messagerie (MHE)** (*message handling environment*) comprend des objets fonctionnels «primaires» de plusieurs types, le *système de messagerie (MHS)*, les *utilisateurs* et les *listes de distribution*. Le *système MHS* à son tour peut être décomposé en objets fonctionnels «secondaires» d'importance moindre de plusieurs types: le *système de transfert de messages (MTS)*, les *agents d'utilisateur*, les *mémoires de messages* et les *unités d'accès*. Le *système MTS* peut à son tour être décomposé en objets fonctionnels «tertiaires» d'importance encore moindre d'un seul type: les *agents de transfert de messages*.

Les types d'objets fonctionnels primaires, secondaires et tertiaires ainsi que les types *d'unités d'accès* choisis sont définis et décrits un à un ci-après.

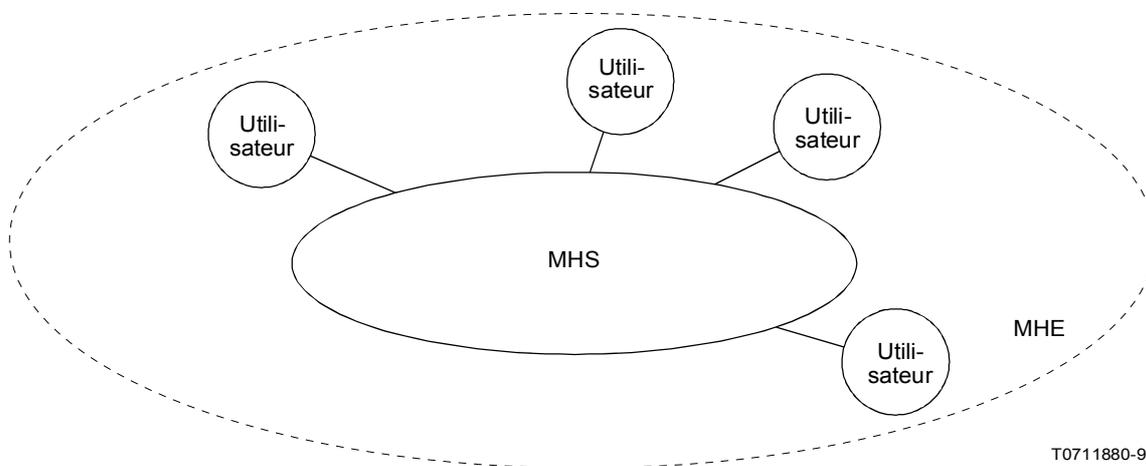
Comme précisé ci-après, les objets fonctionnels sont parfois spécialement adaptés à une ou plusieurs applications de messagerie, par exemple la messagerie de personne à personne (voir les Recommandations X.420 et T.330). Un objet fonctionnel qui a été spécialement adapté à une application comprend la syntaxe et la sémantique du contenu des messages échangés dans celle-ci.

A l'échelon local, les objets fonctionnels peuvent assurer des fonctions autres que celles qui sont spécifiées dans la présente Recommandation ou dans d'autres Recommandations du CCITT | ISO/CEI 10021. En particulier, un *agent d'utilisateur* type assure des fonctions non normalisées de préparation, de présentation et d'enregistrement des messages.

7.1 Objets fonctionnels primaires

L'environnement MHE comprend le *système de messagerie*, les *utilisateurs* et les *listes de distribution*. Ces objets fonctionnels primaires dialoguent entre eux. Leurs types sont définis et décrits ci-après.

La situation est représentée à la figure 1/X.402.



T0711880-91

FIGURE 1/X.402
L'environnement du système de messagerie

7.1.1 Système de messagerie

Le principal but de la messagerie est d'acheminer des objets d'information d'un correspondant à un autre. L'objet fonctionnel au moyen duquel l'acheminement est accompli est appelé **Système de messagerie (MHS)** (*message handling system*).

L'environnement MHE comprend un seul système MHS.

7.1.2 Utilisateurs

Le principal but du système MHS est d'acheminer des objets d'information entre *utilisateurs*. Un objet fonctionnel (une personne, par exemple) qui se sert (sans l'assurer) de la messagerie est appelé un **utilisateur**.

On distingue les sortes d'utilisateurs suivantes:

- a) **utilisateur direct**: utilisateur qui se sert de la messagerie en utilisant directement le système MHS;
- b) **utilisateur indirect**: utilisateur qui se sert de la messagerie en utilisant indirectement le système MHS, c'est-à-dire par l'intermédiaire d'un autre système de communication (un système postal ou le réseau télex, par exemple) auquel le système MHS est relié.

L'environnement MHE comprend un nombre quelconque d'utilisateurs.

7.1.3 Listes de distribution

Au moyen du système MHS, un utilisateur peut faire parvenir des objets d'information à des groupes d'utilisateurs prédéterminés, ainsi qu'à des utilisateurs individuels. L'objet fonctionnel qui représente un groupe d'utilisateurs prédéterminés et d'autres listes *DL* est appelé une **liste de distribution (DL)** (*distribution list*).

Une liste DL identifie zéro, un utilisateur et liste DL ou plusieurs appelés identifiant ses **membres**. On dit que ces listes DL, s'il y en a, sont **imbriquées**. Demander au système MHS de transmettre un objet d'information (un *message*, par exemple) à une liste DL équivaut à lui demander de transmettre l'objet à ses membres. A noter qu'il s'agit d'un phénomène récurrent.

Le droit, ou l'autorisation, de transmettre des *messages* à une liste DL particulière peut être limité. Ce droit est appelé **autorisation de dépôt**. A l'échelon local, l'utilisation d'une liste DL peut faire l'objet d'autres restrictions.

L'environnement MHE comprend un nombre quelconque de listes DL.

Remarque – Une liste DL peut être encore limitée, par exemple à l'acheminement de *messages* d'un *type de contenu* prescrit.

7.2 Objets fonctionnels secondaires

Le système MHS comprend le *système de transfert de messages*, les *agents d'utilisateurs*, les *mémoires de messages* et les *unités d'accès*. Ces objets fonctionnels secondaires dialoguent entre eux. Leurs types sont définis et décrits ci-après.

La situation est représentée à la figure 2/X.402.

7.2.1 Système de transfert de messages

Le système MHS transmet des objets d'information à des utilisateurs individuels et aux membres des listes DL. L'objet fonctionnel qui assure effectivement cette fonction est appelé **Système de transfert de messages (MTS)** (*message transfer system*). Le système MTS est un système de communication avec enregistrement et retransmission; il peut être considéré comme le pivot du système MHS.

Le système MHS est polyvalent, assurant toutes les applications de la messagerie. En outre, il peut être spécialement adapté à une ou plusieurs applications particulières de manière à pouvoir assurer la *conversion*.

Le système MHS comprend un seul système MTS.

7.2.2 Agents d'utilisateurs

L'objet fonctionnel au moyen duquel un utilisateur direct utilise la messagerie est appelé **agent d'utilisateur (UA)** (*user agent*).

Un agent UA type est spécialement adapté à une ou plusieurs applications de messagerie.

Le système MHS comporte un nombre quelconque d'agents UA.

Remarque – Un agent UA qui dessert un usager dialogue habituellement avec celui-ci au moyen de dispositifs d'entrée/sortie (clavier, écran, lecteur, imprimante, par exemple, ou combinaison de plusieurs de ces éléments).

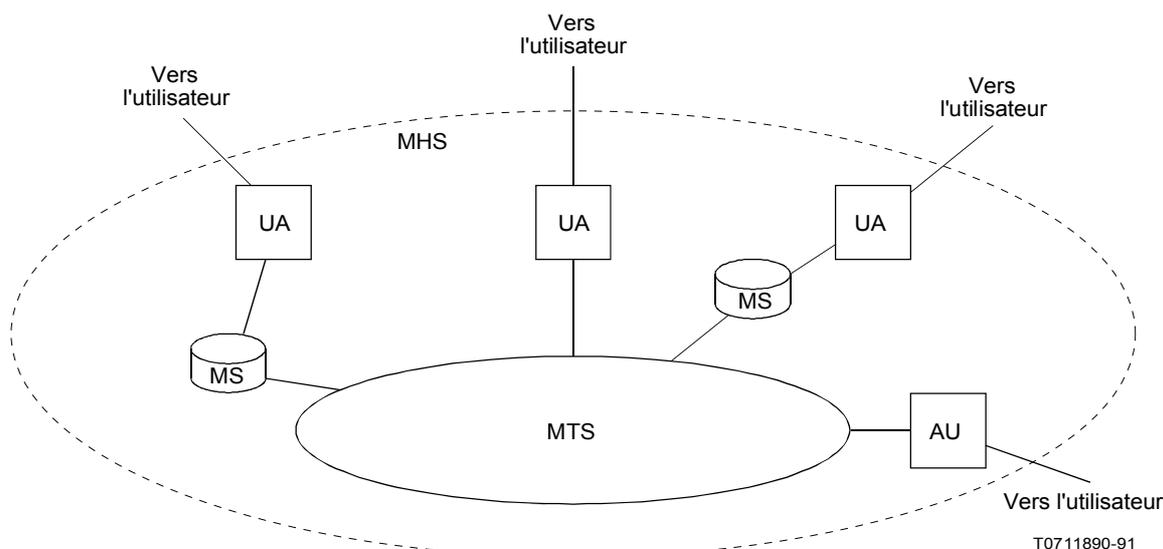


FIGURE 2/X.402
Système de messagerie

7.2.3 Mémoire de messages

Un utilisateur type doit enregistrer les objets d'information qu'il reçoit. L'objet fonctionnel qui donne à un utilisateur direct (unique) des possibilités d'enregistrement de messages est appelé **mémoire de messages (MS)** (*message store*). Chaque mémoire MS est associée à un agent UA, mais chaque agent UA n'a pas une mémoire MS associée.

Chaque mémoire MS est polyvalente, assurant toutes les applications de messagerie. En outre, une mémoire MS peut être spécialement adaptée à une ou plusieurs applications particulières pour être mieux à même d'assurer le *dépôt* et l'*extraction des messages* associés à cette application.

Le système MHS comporte un nombre quelconque de mémoires MS.

Remarque – A l'échelon local, un agent UA peut assurer l'enregistrement d'objets d'information en complément ou en remplacement d'une mémoire MS.

7.2.4 Unités d'accès

L'objet fonctionnel qui relie un système de communication (un système postal ou le réseau télex, par exemple) au système MTS, et par l'intermédiaire duquel les clients de ce système utilisent la messagerie en tant qu'utilisateurs indirects, est appelé une **unité d'accès (AU)** (*access unit*).

Une unité AU type est spécialement adaptée à un système de communication particulier et à une ou plusieurs applications particulières de messagerie.

Le système MHS comporte un nombre quelconque d'unités AU.

7.3 Objets fonctionnels tertiaires

Le MTS comporte des *agents de transfert de messages*. Ces objets fonctionnels tertiaires dialoguent entre eux. Leur type est défini et décrit ci-après.

La situation est représentée à la figure 3/X.402.

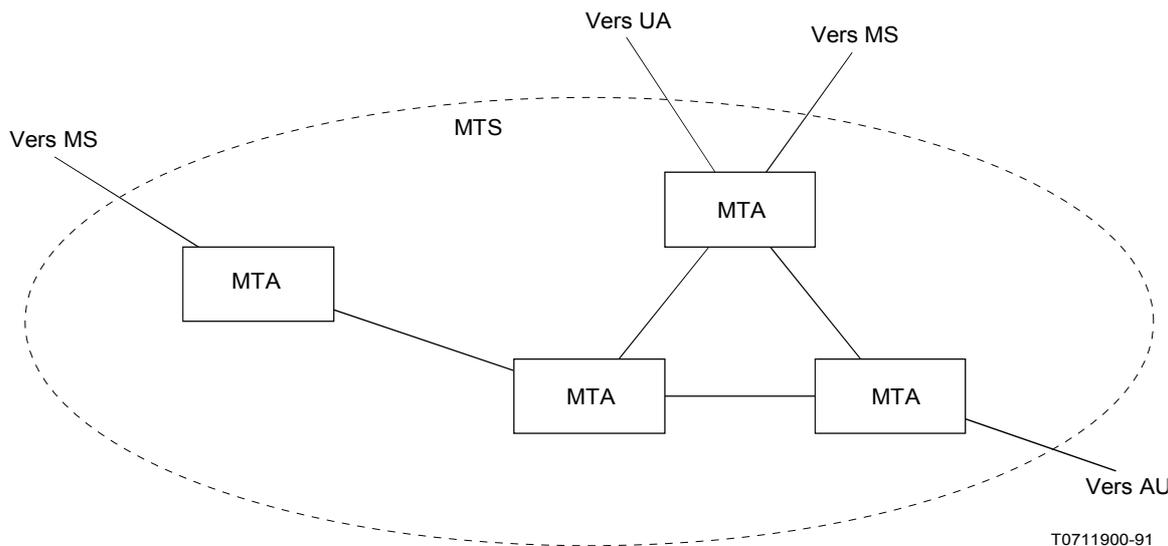


FIGURE 3/X.402
Système de transfert de messages

7.3.1 Agents de transfert de messages

Le système MTS transmet des objets d'information aux utilisateurs et aux listes DL en mode enregistrement et retransmission. Un objet fonctionnel qui assure une liaison dans la chaîne enregistrement et retransmission du système MTS est appelé **agent de transfert de messages (MTA)** (*message transfer agent*).

Chaque agent MTA est polyvalent, assurant toutes les applications de la messagerie. En outre, un agent MTA peut être spécialement adapté à une ou plusieurs applications particulières de manière à pouvoir effectuer la *conversion*.

Le système MTS comporte un nombre quelconque d'agents MTA.

7.4 Types d'unités AU choisis

Comme indiqué plus haut, le système MHS entre en interfonctionnement avec des systèmes de communication de types différents par l'intermédiaire d'unités AU. Plusieurs types d'unités AU choisis – remise physique, télématique et télex – sont présentés dans les paragraphes qui suivent.

7.4.1 Remise physique

Une **unité d'accès de remise physique (PDAU)** (*physical delivery access unit*) est une unité AU qui soumet des *messages* (mais ni des *envois-tests* ni des *rappports*) à la *restitution physique* et qui transmet les *messages physiques* qui en résultent à un *système de remise physique*.

La transformation d'un *message* en un *message physique* est appelée **restitution physique**. Un **message physique** est un objet physique (une lettre et son enveloppe en papier, par exemple) qui renferme un *message*.

Un **système de remise physique (PDS)** (*physical delivery system*) est un système qui effectue la *remise physique*. Les systèmes postaux constituent un genre important de système PDS. La **remise physique** est la transmission d'un message physique à un client d'un système PDS, l'un des utilisateurs indirects auxquels l'unité PDAU offre des possibilités de messagerie.

Parmi les applications de messagerie qu'assure chaque unité PDAU, signalons la messagerie de personne à personne (voir la Rec. X.420 du CCITT | ISO/CEI 10021-7).

7.4.2 Télématique

Les unités d'accès télématique, qui assurent exclusivement la messagerie de personne à personne, sont présentées dans la Rec. X.420 du CCITT | ISO/CEI 10021-7.

7.4.3 Téléx

Les unités d'accès téléx, qui assurent exclusivement la messagerie de personne à personne, sont présentées dans la Rec. X.420 du CCITT | ISO/CEI 10021-7.

8 Modèle d'information

Le présent paragraphe décrit un modèle d'information de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations du CCITT | ISO/CEI 10021.

Le système MHS et le système MTS peuvent transmettre des objets d'information de trois catégories: *message*, *envoi-test*, et *rappports*. Ces catégories sont indiquées dans la première colonne du tableau 4. Pour chaque catégorie, la seconde colonne indique les types d'objets fonctionnels – utilisateurs, agents UA, mémoires MS, agents MTA et unités AU – qui sont les origines premières et les destinations finales de ces objets.

Les objets d'information résumés dans le tableau 4/X.402 sont définis et décrits un à un dans les paragraphes qui suivent.

TABLEAU 4/X.402

Objets d'information acheminables

Objet d'information	Objet fonctionnel				
	Utilisateur	UA	MS	MTA	AU
Message	SD	–	–	–	–
Envoi-test	S	–	–	D	–
Rapport	D	–	–	S	–

S Origine première

D Destination finale

8.1 Messages

L'objectif principal du transfert de message est de transmettre des objets d'information appelés **messages** d'un utilisateur à d'autres utilisateurs. Comme indiqué à la figure 4/X.402, un message comporte les parties suivantes:

- enveloppe:** objet d'information dont la composition varie d'une *étape de transmission* à une autre et qui identifie de manière différente *l'expéditeur* et les *destinataires potentiels* du message, justifie sa précédente transmission, oriente sa transmission ultérieure par le système MTS et décrit son *contenu*;
- contenu:** objet d'information que le système MTS n'examine ni ne modifie, sauf pour la *conversion*, pendant qu'il transmet le message.

Une information portée par l'enveloppe identifie le type du contenu. Le **type de contenu** est un identificateur (un identificateur d'objet ASN.1 ou un nombre entier) qui désigne la syntaxe et la sémantique de la totalité du contenu. Cet identificateur permet au système MTS de déterminer si le message *peut être remis* à des utilisateurs particuliers, et permet aux agents UA et aux mémoires MS d'interpréter et de traiter le contenu.

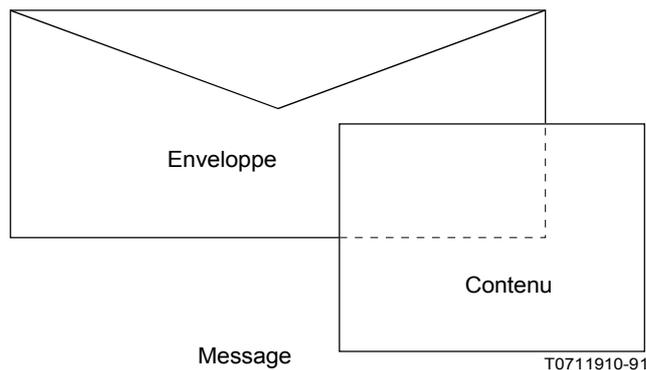


FIGURE 4/X.402
Enveloppe et contenu d'un message

Une autre information portée par l'enveloppe identifie les types d'information codée représentés dans le contenu. Un **type d'information codée (EIT)** (*encoded information type*) est un identificateur (identificateur d'objet ASN.1 ou nombre entier) qui désigne le support et le format (texte IA5 ou télécopie du groupe 3, par exemple) de certaines parties du contenu. Un type EIT permet en outre au système MTS de déterminer si le message peut être remis à des utilisateurs particuliers et d'identifier les occasions qu'il aura de *faire en sorte* que le message puisse être remis en convertissant une portion du contenu d'un type EIT en un autre.

8.2 *Envois-tests*

Le transfert de messages a pour deuxième objectif d'acheminer des objets d'information appelés **envois-tests** d'un utilisateur à la portée immédiate d'autres utilisateurs (c'est-à-dire de les transmettre aux agents MTA qui desservent ces utilisateurs). Un envoi-test décrit une catégorie de message et sert à déterminer si ces messages *peuvent être remis*.

Un message décrit par un envoi-test est appelé un **message décrit**.

Un envoi-test comporte une seule enveloppe. Cette enveloppe contient pratiquement la même information que celle d'un message. Outre le type de contenu et les types d'information codée d'un message décrit, l'enveloppe d'un envoi-test indique la longueur de son contenu.

Le *dépôt* d'un envoi-test entraîne essentiellement le même comportement du système MTS que le *dépôt* d'un message décrit, sauf que, dans ce cas, on renonce *au développement de la liste DL* et à la *remise*. En particulier, et si on excepte les conséquences de la suppression du *développement de la liste DL*, l'envoi-test donne lieu aux mêmes *rappports* que n'importe quel message décrit. C'est ce qui confère aux envois-tests leur utilité.

8.3 *Rappports*

Le transfert des messages a pour troisième objectif de transmettre aux utilisateurs des objets d'information appelés **rappports**. Engendré par le système MTS, un rapport rend compte des résultats ou du déroulement de la *transmission* d'un message ou d'un envoi-test à un ou plusieurs *destinataires potentiels*.

Le message ou l'envoi-test faisant l'objet d'un rapport est respectivement appelé son **message sujet** ou son **envoi-test sujet**.

Un rapport concernant un *destinataire potentiel* particulier est communiqué à l'*expéditeur* du message sujet ou de l'envoi-test sujet à moins que le *destinataire potentiel* ne soit un *destinataire membre*. Dans ce dernier cas, le rapport est transmis à la liste DL dont est membre le *destinataire membre*. A l'échelon local (c'est-à-dire en vertu d'une

politique arrêtée pour cette liste DL), le rapport peut en outre être communiqué au propriétaire de la liste DL, soit à un autre, contenant la liste DL (en cas d'imbrication), soit (dans le cas contraire) à l'expéditeur du message sujet, ou aux deux à la fois.

Les résultats dont un seul rapport peut rendre compte sont des types suivants:

- a) **rapport de remise:** *remise*, *export* ou *affirmation* du message ou envoi-test sujet, ou *développement de liste DL*;
- b) **rapport de non-remise:** *non-remise* ou *non-affirmation* du message ou envoi-test sujet.

Un rapport peut contenir un ou plusieurs rapports de remise et/ou de non-remise. Un message ou un envoi-test peut donner lieu à plusieurs rapports de remise et/ou de non-remise concernant un *destinataire potentiel* particulier. Chacun de ces rapports marque le passage d'une *étape* ou d'un *événement* de transmission différent.

9 Modèle opérationnel

Le présent décrit un modèle opérationnel de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations du CCITT | ISO/CEI 10021.

Le système MHS peut transmettre un objet d'information à des utilisateurs individuels, à des listes DL ou à une combinaison des uns et des autres. Un tel acheminement s'effectue selon un processus appelé *transmission* qui comprend des *étapes* et des *événements*. Ce processus, ses parties, et les rôles que les utilisateurs et les systèmes DL y jouent, sont définis et décrits ci-dessous.

9.1 *Transmission*

L'acheminement ou la tentative d'acheminement d'un message ou d'un envoi-test est appelé **transmission**. La transmission englobe l'acheminement d'un message de son *expéditeur* à ses *destinataires potentiels*, et l'acheminement d'un envoi-test de son *expéditeur* à des agents MTA capables d'*affirmer* que les messages décrits *peuvent être remis* aux *destinataires potentiels* de l'essai. La transmission englobe également l'acheminement ou la tentative d'acheminement à l'*expéditeur* des rapports auxquels le message ou l'envoi-test donne lieu.

Une transmission comporte une séquence d'*étapes et d'événements de transmission*. Une **étape de transmission** (ou **étape**) est l'acheminement d'un message, d'un envoi-test ou d'un rapport d'un objet fonctionnel à un autre objet fonctionnel qui lui est «adjacent». Un **événement de transmission** (ou **événement**) est le traitement d'un message, d'un envoi-test ou d'un rapport à l'intérieur d'un objet fonctionnel qui peut influencer le choix de l'objet fonctionnel de l'étape ou événement de transmission suivant.

Le cheminement de l'information pendant la transmission est représenté à la figure 5/X.402. Cette figure montre les types d'objets fonctionnels – utilisateurs directs, utilisateurs indirects, agents UA, mémoires MS, agents MTA et unités AU – qui peuvent intervenir pendant une transmission, les objets d'information – messages, envois-tests et rapports – qui peuvent être transmis entre eux, et les noms des différentes étapes de transmission.

La figure 5/X.402 montre bien qu'un message ou un rapport peuvent être extraits à plusieurs reprises et que seule la première transmission d'un objet extrait de l'agent UA vers l'utilisateur constitue la *réception*.

Un événement joue un rôle distinctif pendant la transmission. Le *fractionnement* reproduit un message ou un envoi-test et répartit la responsabilité de ses *destinataires immédiats* entre les objets d'information qui en résultent. Les destinataires potentiels associés à une instance particulière d'un message ou d'un envoi-test sont appelés ses **destinataires immédiats**. Un agent MTA déclenche un fractionnement si l'étape ou l'événement suivant nécessaire pour acheminer un message ou un envoi-test à certains destinataires immédiats diffère de l'étape ou de l'événement nécessaire pour acheminer ce message ou cet envoi-test à d'autres. Chacune des descriptions d'étape et d'événement qui suivent suppose que l'étape ou l'événement convient à tous les destinataires immédiats, situation qui peut être créée, si nécessaire, par le fractionnement.

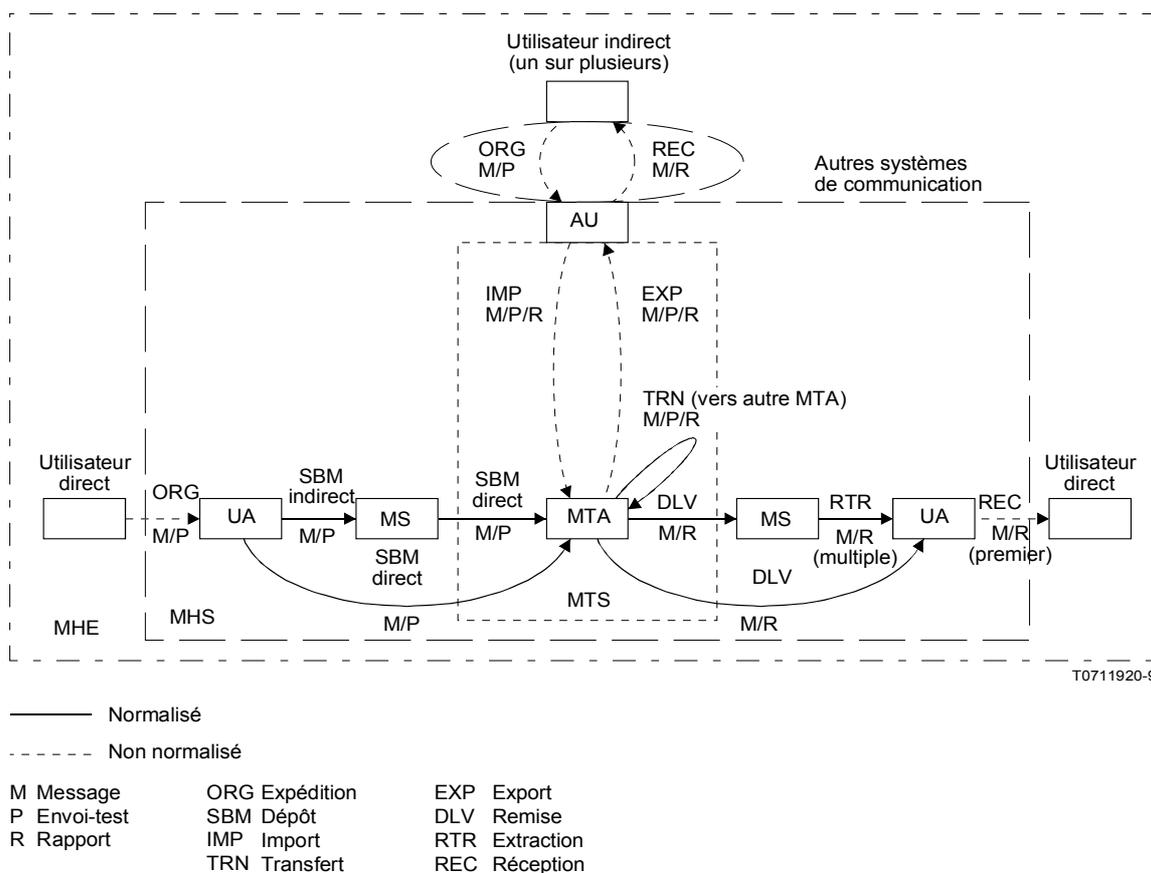


FIGURE 5/X.402

Cheminement de l'information pendant la transmission

9.2 *Rôles de transmission*

Les utilisateurs et les listes DL jouent différents rôles dans la transmission d'un message ou d'un envoi-test. Ces rôles sont informellement classés en rôles «origine» ou «destination» ou en états auxquels les utilisateurs ou les listes DL peuvent être élevés.

Un utilisateur peut jouer, dans la transmission d'un message ou d'un envoi-test, le rôle «source» suivant:

- **expéditeur:** L'utilisateur (mais pas une liste DL) qui est l'origine première d'un message ou d'un envoi-test.

Un utilisateur ou une liste DL peut jouer, dans la transmission d'un message ou d'un envoi-test, l'un quelconque des rôles «destination» suivants:

- destinataire prévu:** l'un des utilisateurs et des listes DL que l'expéditeur spécifie comme étant les destinations prévues d'un message ou d'un envoi-test.
- destinataire suppléant spécifié par l'expéditeur:** l'utilisateur ou la liste DL (le cas échéant) vers lequel (laquelle) l'expéditeur demande d'acheminer un message ou un envoi-test s'il ne peut être transmis à un destinataire prévu particulier.

- c) **destinataire membre:** un utilisateur ou une liste DL auquel (à laquelle) un message (mais pas un envoi-test) est acheminé par suite d'un *développement de la liste DL*.
- d) **destinataire suppléant désigné par le destinataire:** l'utilisateur ou la liste DL (le cas échéant) vers lequel (laquelle) un destinataire prévu, suppléant spécifié par l'expéditeur ou membre peut avoir choisi de *réacheminer* des messages.

Un utilisateur ou une liste DL peut atteindre, au cours de la transmission d'un message ou d'un envoi-test, l'un quelconque des états suivants:

- a) **destinataire potentiel:** un utilisateur ou une liste DL vers lequel (laquelle) un message ou un envoi-test est acheminé à un moment quelconque de la transmission. Il s'agit nécessairement d'un destinataire prévu, suppléant spécifié par l'expéditeur, membre ou suppléant désigné par le destinataire.
- b) **destinataire effectif (ou destinataire):** Un destinataire potentiel pour lequel la *remise* ou l'*affirmation* a lieu.

9.3 Etapes de la transmission

Les types d'étapes qui peuvent se produire au cours d'une transmission sont énumérés dans la première colonne du tableau 5/X.402. Pour chaque type spécifié, la deuxième colonne indique si ces étapes sont normalisées dans la présente Recommandation et d'autres Recommandations du CCITT | ISO/CEI 10021, la troisième colonne précise les types d'objets d'information – messages, envois-tests et rapports – qui peuvent être acheminés pendant cette étape et la quatrième colonne indique les types d'objets fonctionnels – utilisateurs, agents UA, mémoires MS, agents MTA et unités AU – qui peuvent intervenir pendant cette étape en tant que source ou destination de l'objet.

Le tableau 5/X.402 est divisé en trois sections. Les étapes indiquées dans la première section correspondent à la «création» de messages et d'envois-tests, celles indiquées dans la dernière section à la «mise à disposition» des messages et des rapports et celles indiquées dans la section intermédiaire à la «retransmission» des messages, envois-tests et rapports.

Les différentes étapes de transmission, résumées dans le tableau 5/X.402, sont définies et décrites une à une dans les paragraphes qui suivent.

TABLEAU 5/X.402

Etapes de transmission

Etape de transmission	Normalisée?	Objets d'information			Objets fonctionnels				
		M	P	R	Utilisateur	UA	MS	MTA	AU
Expédition	Non	X	X	–	S	D	–	–	–
Dépôt	Oui	X	X	–	–	S	SD	D	–
Import	Non	X	X	X	–	–	–	D	S
Transfert	Oui	X	X	X	–	–	–	SD	–
Export	Non	X	X	X	–	–	–	S	D
Remise	Oui	X	–	X	–	D	D	S	–
Extraction	Oui	X	–	X	–	D	S	–	–
Réception	Non	X	–	X	D	S	–	–	–

M Message

S Source

P Envoi-test

D Destination

R Rapport

X Permis

9.3.1 Expédition

Dans une étape **expédition**, un utilisateur direct transmet un message ou un envoi-test à son agent UA, ou un utilisateur indirect un message ou un envoi-test au système de communication qui le dessert. Cette étape engendre le message ou l'envoi-test et constitue la première étape de sa transmission.

L'utilisateur ci-dessus constitue l'expéditeur du message ou de l'envoi-test. Dans cette étape, l'expéditeur identifie les destinataires prévus. En outre, pour chaque destinataire prévu, l'expéditeur peut (sans toutefois y être obligé) désigner un destinataire suppléant spécifié par l'expéditeur.

9.3.2 Dépôt

Dans une étape **dépôt**, un message ou un envoi-test est transmis à un agent MTA et par conséquent confié au système MTS. On distingue deux types de dépôt:

- a) **dépôt indirect:** Etape de transmission au cours de laquelle l'agent UA de l'expéditeur transmet un message ou un envoi-test à sa mémoire MS et au cours de laquelle la mémoire MS effectue le *dépôt direct*. Cette étape suit l'expédition.

Cette étape ne peut être mise en œuvre que si l'utilisateur est équipé d'une mémoire MS.

- b) **dépôt direct:** Etape de transmission au cours de laquelle l'agent UA de l'expéditeur ou la mémoire MS transmet un message ou un envoi-test à un agent MTA. Cette étape suit l'expédition ou intervient pendant le dépôt indirect.

Cette étape peut être mise en œuvre, que l'utilisateur soit équipé ou non d'une mémoire MS.

Le dépôt indirect et le dépôt direct sont fonctionnellement équivalents, à ceci près que le premier offre parfois des possibilités supplémentaires. Le dépôt indirect peut différer du dépôt direct à d'autres égards (nombre de systèmes ouverts avec lesquels celui qui renferme un agent UA doit dialoguer, par exemple) et, pour cette raison, être préférable au dépôt direct.

L'agent UA ou la mémoire MS qui prennent part à un dépôt direct sont appelés **agents de dépôt**. L'existence d'un agent de dépôt est signalée au système MTS par un processus d'enregistrement, à la suite duquel l'agent de dépôt et le système MTS se tiennent mutuellement informés de leurs noms, de leurs emplacements et de toute autre caractéristique dont ils ont besoin pour dialoguer.

9.3.3 Import

Dans une étape **import**, une unité AU transmet un message, un envoi-test ou un rapport à un agent MTA. Cette étape injecte dans le système MTS un objet d'information créé dans un autre système de communication et suit l'acheminement de cet objet par ce système MTS.

Remarque – Le concept d'importation est un concept générique. Le déroulement de cette étape varie, naturellement, d'un type d'unité AU à un autre.

9.3.4 Transfert

Dans une étape **transfert**, un agent MTA transmet un message, un envoi-test ou un rapport à un autre. Cette étape transporte un objet d'information sur des distances physiques et parfois organisationnelles et fait suite au dépôt direct, à l'import ou à un transfert (préalable).

Cette étape ne peut être mise en œuvre, naturellement, que si le système MTS comporte plusieurs agents MTA.

En fonction du nombre de *domaines de gestion MD* qui entrent en jeu, on distingue les types de transferts suivants:

- a) **transfert interne:** Transfert faisant intervenir plusieurs agents MTA dans un seul *domaine de gestion (MD)*;
- b) **transfert externe:** Transfert faisant intervenir plusieurs agents MTA dans divers *domaines de gestion (MD)*.

9.3.5 *Export*

Dans une étape **export**, un agent MTA transmet un message, un envoi-test ou un rapport à une unité AU. Cette étape éjecte du système MTS un objet d'information lié à un autre système de communication. Elle fait suite au dépôt direct, à l'import ou au transfert.

Au cours de cette étape, l'agent MTA peut produire un rapport de remise. Dans le cas d'unités d'accès, un rapport de remise positif indique que l'unité d'accès a accepté un message (ou un envoi-test). Selon les conditions requises précisées dans les spécifications de messagerie correspondantes, le rapport de remise peut, sinon, indiquer que le message a été reçu par l'utilisateur indirect desservi par cette unité d'accès (voir, par exemple, les Recommandations F.421, F.422, F.423, F.435, F.440, T.300, T.330 et U.204).

Remarque – Le concept d'exportation est un concept générique. Le déroulement de cette étape varie, naturellement, d'un type d'unité AU à un autre.

9.3.6 *Remise*

Dans une étape **remise**, un agent MTA transmet un message ou un rapport à la mémoire MS ou l'agent UA d'un destinataire potentiel du message, ou l'expéditeur du message ou de l'envoi-test sujet du rapport. Cette étape confie l'objet d'information à un représentant de l'utilisateur et fait suite au dépôt direct, à l'import ou au transfert. De plus, elle élève l'utilisateur en question au statut de destinataire effectif.

Au cours de cette étape, dans le cas d'un message, l'agent MTA peut produire un rapport de remise.

La mémoire MS ou l'agent UA en cause est appelé **agents de remise**. L'existence d'un agent de remise est signalée au système MTS par un processus d'enregistrement, à la suite duquel l'agent de remise et le système MTS se tiennent mutuellement informés de leurs noms, de leur emplacement et de toute autre caractéristique dont ils ont besoin pour dialoguer.

9.3.7 *Extraction*

Dans une étape **extraction**, la mémoire MS d'un utilisateur transmet un message ou un rapport à son agent UA. L'utilisateur en question est un destinataire effectif du message ou l'expéditeur du message ou de l'envoi-test sujet. Cette étape extrait de la mémoire l'objet d'information sans le détruire. Elle fait suite à la remise ou à l'extraction (préalable).

Cette étape ne peut être mise en œuvre que si l'utilisateur est équipé d'une mémoire MS.

9.3.8 *Réception*

Dans une étape **réception**, un agent UA transmet un message ou un rapport à son utilisateur direct, ou le système de communication qui dessert un utilisateur indirect transmet un tel objet d'information à cet utilisateur. Dans l'un et l'autre cas, cette étape transmet l'objet à sa destination finale.

Dans le cas d'un utilisateur direct, cette étape suit la remise de l'objet ou la première extraction (uniquement) de celui-ci. Dans le cas d'un utilisateur indirect, elle suit la transmission de l'objet d'information par le système de communication qui dessert l'utilisateur. Dans l'un et l'autre cas, l'utilisateur est un destinataire potentiel (et, dans le cas d'un utilisateur direct, un destinataire effectif) du message en question, ou l'expéditeur du message ou de l'envoi-test sujet.

9.4 *Événements de transmission*

Les types d'événements qui peuvent se produire pendant une transmission sont indiqués dans la première colonne du tableau 6/X.402. Pour chacun de ces types, la deuxième colonne indique les types d'objets d'information – messages, envois-tests et rapports – pour lesquels ces événements peuvent être mis en œuvre, la troisième colonne indiquant les types d'objets fonctionnels – utilisateurs, agents UA, mémoires MS, agents MTA et unités AU – qui peuvent mettre en œuvre ces événements.

Tous ces événements se produisent à l'intérieur du système MTS.

Les différents événements de transmission résumés dans le tableau 6/X.402 sont définis et décrits un à un dans les paragraphes qui suivent.

TABLEAU 6/X.402

Événements de transmission

Événement de transmission	Objets d'information			Objets fonctionnels				
	M	P	R	Utilisateur	UA	MS	MTA	AU
fractionnement	X	X	–	–	–	–	X	–
groupage	X	X	X	–	–	–	X	–
résolution de nom	X	X	–	–	–	–	X	–
développement de liste DL	X	–	–	–	–	–	X	–
réacheminement	X	X	–	–	–	–	X	–
conversion	X	X	–	–	–	–	X	–
non-remise	X	–	X	–	–	–	X	–
non-affirmation	–	X	–	–	–	–	X	–
affirmation	–	X	–	–	–	–	X	–
acheminement	X	X	X	–	–	–	X	–

M Message

P Envoi-test

R Rapport

X Permis

9.4.1 Fractionnement

Dans un événement **fractionnement**, un agent MTA reproduit un message ou un envoi-test, en partageant la responsabilité de ses destinataires immédiats entre les objets d'information qui en résultent. Cet événement permet effectivement à un agent MTA de transmettre de manière indépendante un objet à divers destinataires potentiels.

Un agent MTA prévoit un fractionnement quand l'étape ou l'événement suivant nécessaire à la transmission d'un message ou d'un envoi-test à certains destinataires immédiats diffère de l'étape ou de l'événement nécessaire à la transmission de ce message ou de cet envoi à d'autres destinataires.

9.4.2 Groupage

Dans un événement **groupage**, un agent MTA combine plusieurs instances du même message ou envoi-test, ou deux rapports ou plus de remise et/ou de non-remise pour le même message ou envoi-test sujet.

Un agent MTA peut prévoir un groupe, mais n'y est pas obligé, quand il détermine que les mêmes événements et l'étape suivante sont nécessaires pour acheminer à leurs destinations plusieurs objets d'information étroitement liés.

9.4.3 Résolution du nom

Dans un événement **résolution du nom**, un agent MTA ajoute l'adresse d'O/R correspondant au nom d'O/R qui identifie un des destinataires immédiats d'un message ou d'un envoi-test.

9.4.4 Développement de liste DL

Dans un événement **développement de liste DL**, un agent MTA remplace un destinataire immédiat qui dénote une DL par les membres de cette liste DL qui deviennent de ce fait des destinataires membres. Les événements développement de liste DL se produisent uniquement pour les messages, pas pour les envois-tests.

Une liste DL particulière fait toujours l'objet d'un développement à un emplacement préétabli à l'intérieur du système MTS. Cet emplacement est appelé **point de développement** de la liste DL et est identifié par une *adresse d'O/R*.

Au cours de cet événement, l'agent MTA peut produire un rapport de remise.

Le développement de liste DL est soumis à une autorisation de dépôt. Dans le cas d'une liste DL imbriquée, cette autorisation doit avoir été accordée à la liste DL dont la liste DL imbriquée est membre. Sinon, elle doit avoir été accordée à l'expéditeur.

9.4.5 Réacheminement

Dans un événement **réacheminement**, un agent MTA remplace un utilisateur ou une liste DL figurant parmi les destinataires immédiats d'un message ou d'un envoi-test par un destinataire suppléant spécifié par l'expéditeur ou désigné par le destinataire.

9.4.6 Conversion

Dans un événement **conversion**, un agent MTA convertit des parties du contenu d'un message d'un type d'information codée (EIT) en un autre, ou modifie un envoi-test de façon à faire apparaître la modification des messages décrits. Cet événement, en adaptant un objet d'information à ses destinataires immédiats, accroît la probabilité de remise ou d'affirmation de celui-ci.

Selon comment le type EIT de l'information à convertir et celui qui résultera de la conversion sont choisis, on distingue les types de conversion suivants:

- a) **conversion explicite**: conversion dans laquelle l'expéditeur choisit les types EIT de départ et d'arrivée.
- b) **conversion implicite**: conversion dans laquelle l'agent MTA choisit les types EIT d'arrivée en fonction des types EIT de départ et des possibilités de l'agent UA.

9.4.7 *Non-remise*

Dans un événement **non-remise**, un agent MTA établit que le système MTS ne peut pas remettre un message à ses destinataires immédiats, ou ne peut pas remettre un rapport à l'expéditeur de son message ou envoi-test sujet. Cet événement interrompt l'acheminement d'un objet que le système MTS juge non acheminable.

Au cours de cet événement, dans le cas d'un message, l'agent MTA produit un rapport de non-remise.

Un agent MTA déclenche une non-remise, par exemple, quand il établit que les destinataires immédiats ne sont pas convenablement spécifiés, qu'ils n'acceptent pas la remise de messages tels que celui qui est disponible ou que le message ne leur a pas été remis dans les délais préalablement spécifiés.

9.4.8 *Non-affirmation*

Dans un événement **non-affirmation**, un agent MTA établit que le système MTS n'a pas pu remettre un message décrit aux destinataires immédiats d'un envoi-test. Cet événement détermine en partie ou en totalité la réponse à la question posée par un envoi-test.

Au cours de cet événement, l'agent MTA produit un rapport de non-remise.

Un agent MTA déclenche une non-affirmation, par exemple quand il établit que les destinataires immédiats ne sont pas convenablement spécifiés ou qu'ils n'accepteront pas la remise d'un message décrit.

9.4.9 *Affirmation*

Dans un événement **affirmation**, un agent MTA établit que le système MTS a pu remettre n'importe quel message décrit aux destinataires immédiats d'un envoi-test. Cet événement détermine en partie ou en totalité la réponse à la question posée par un envoi-test et élève les destinataires immédiats au statut de destinataires effectifs.

Au cours de cet événement, l'agent MTA peut produire un rapport de remise.

Un agent MTA déclenche une affirmation après avoir établi que les destinataires immédiats sont convenablement spécifiés et, s'il s'agit d'utilisateurs (mais pas de listes DL), qu'ils accepteront la remise de n'importe quel message décrit. Si les destinataires immédiats sont des listes DL, un agent MTA déclenche une affirmation si la liste DL existe et si l'expéditeur a l'autorisation de dépôt de message correspondante.

9.4.10 *Acheminement*

Dans un événement **acheminement**, un agent MTA choisit l'agent MTA «adjacent» auquel il transférera un message, un envoi-test ou un rapport. Cet événement détermine pas à pas l'itinéraire d'un objet d'information dans le système MTS et (naturellement) ne peut intervenir que si le système MTS comporte plusieurs agents MTA.

On distingue les types d'acheminement ci-après, en fonction du type de transfert auquel ils préparent:

- a) **acheminement interne:** Acheminement préparatoire pour un transfert interne (c'est-à-dire un transfert à l'intérieur d'un *domaine MD*);
- b) **acheminement externe:** Acheminement préparatoire pour un transfert externe (c'est-à-dire un transfert entre *domaines MD*).

Un agent MTA déclenche un acheminement quand il établit qu'il ne peut déclencher aucun autre événement, ni prendre aucune initiative, en ce qui concerne un objet.

10 Modèle de sécurité

Le présent paragraphe décrit un modèle de sécurité abstrait pour le transfert de message. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations du CCITT | ISO/CEI 10021. Le modèle de sécurité offre un cadre pour décrire les services de sécurité destinés à écarter les messages potentiels (voir l'annexe D) qui pèsent sur le système MTS et les éléments de sécurité qui sont à la base de ces services.

Les fonctions de sécurité, extension optionnelle au système MHS peuvent être utilisées pour ramener au minimum le risque de transgression d'une politique de sécurité applicable aux biens et aux ressources (menaces), indépendamment des services de communication assurés par d'autres entités inférieures ou supérieures. Il est possible d'écarter des menaces en utilisant les services de sécurité physique, de sécurité informatique (COMPUSEC) (*computer security*) ou de sécurité du système MHS. Selon les menaces perçues, certains services de sécurité du système MHS seront choisis et associés à des mesures appropriées de sécurité physique et de COMPUSEC. Les services de sécurité assurés par le système MHS sont décrits ci-dessous. Ces services sont dénommés et structurés selon ISO 7498-2.

Remarque – Malgré ces fonctions de sécurité, certaines perturbations peuvent atteindre une communication entre un utilisateur et le système MHS ou entre utilisateurs (par exemple dans le cas d'utilisateurs accédant au système MHS par une unité d'accès ou d'utilisateurs accédant à distance à leurs agents UA). Les solutions de ces problèmes impliquent une extension des présents modèle et services de sécurité, ce qui nécessite un complément d'étude.

Dans un grand nombre de cas, les ripostes contre les principaux types de menaces sont prévues par plusieurs des services énumérés.

Les services de sécurité sont assurés grâce à l'utilisation d'éléments de service de l'enveloppe de message du Service de transfert de messages. Cette enveloppe contient des arguments relatifs à la sécurité, comme indiqué dans la Rec. X.411 du CCITT | ISO/CEI 10021-4. La description des services de sécurité a la forme générale suivante. Les services énumérés au § 10.2 sont accompagnés, dans chaque cas, d'une définition du service et d'une indication de la manière dont il peut être assuré à l'aide des éléments de sécurité indiqués dans la Rec. X.411 du CCITT | ISO/CEI 10021-4. Les éléments de sécurité décrits un à un au § 10.3 sont accompagnés, dans chaque cas, d'une définition de l'élément de service et des références à ses arguments constitutifs figurant dans la Rec. X.411 du CCITT | ISO/CEI 10021-4.

Nombre des techniques employées reposent sur des mécanismes de chiffrement. Les services de sécurité du système MHS laissent une certaine souplesse dans le choix des algorithmes. Toutefois, dans certains cas, seule l'utilisation du chiffrement asymétrique a été entièrement définie dans la présente Recommandation. Une version future de la présente Recommandation utilisera peut-être d'autres mécanismes basés sur un chiffrement symétrique.

Remarque – Les termes «service de sécurité» et «élément de sécurité» utilisés dans le présent paragraphe ne doivent pas être confondus avec les termes «service» et «élément de service» au sens qui leur est donné dans la Rec. X.400 du CCITT | ISO/CEI 10021-1. Les premiers de ces termes sont utilisés dans le présent paragraphe dans un souci de conformité avec ISO 7498-2.

10.1 Politiques de sécurité

Les services de sécurité du système MHS doivent pouvoir admettre une grande diversité de politiques de sécurité applicables au-delà des limites du seul système MHS. Les services choisis et les menaces contre lesquelles une protection est prévue dépendent de chaque application et du niveau de confiance accordé aux différentes parties du système.

Une politique de sécurité définit comment on peut réduire à un niveau acceptable les risques relatifs aux biens.

En outre, des domaines différents, ayant chacun leur propre politique de sécurité, doivent pouvoir interfonctionner. Chaque domaine étant soumis à sa propre politique générale de sécurité, applicable au-delà des limites du seul système MHS, un accord bilatéral d'interfonctionnement entre deux domaines sera donc nécessaire. Cet accord doit être défini de manière à respecter la politique de sécurité des deux domaines et à devenir de fait partie intégrante de la politique générale de sécurité de chacun d'entre eux.

10.2 Services de sécurité

Le présent paragraphe définit les services de sécurité du transfert de message du MHS. Ces services sont dénommés et structurés selon ISO 7498-2.

Les services de sécurité du transfert de message du MHS se répartissent en plusieurs grandes catégories. Ces catégories et les services qu'elles renferment sont énumérés au tableau 7/X.402. Un astérisque (*) porté dans une colonne dont l'en-tête a une forme du type *X/Y* indique que ce service peut être assuré d'un objet fonctionnel du type *X* vers un objet fonctionnel du type *Y*.

Les définitions des services de sécurité données ci-après renvoient à la figure 6/X.402 qui reproduit le modèle fonctionnel du système MHS sous forme simplifiée. Les étiquettes numériques sont mentionnées dans le texte.

10.2.1 *Services de sécurité Authentification de l'origine*

Ces services de sécurité permettent d'authentifier l'identité des entités homologues en communication et des sources de données.

10.2.1.1 *Services de sécurité Authentification de l'origine des données*

Ces services de sécurité confirment à toutes les entités concernées (c'est-à-dire aux agents MTA ou aux utilisateurs MTS destinataires) l'origine d'un message, d'un envoi-test ou d'un rapport, mais ne protègent pas contre la reproduction de messages, d'envois-tests ou de rapports.

10.2.1.1.1 *Service de sécurité Authentification de l'origine du message*

Le service Authentification de l'origine du message confirme la provenance d'un message.

Ce service de sécurité peut être assuré à l'aide des éléments de sécurité Authentification de l'origine du message ou Intégrité des arguments du message. Le premier de ces éléments peut être utilisé pour fournir le service de sécurité à l'une quelconque des parties concernées (numérotées de 1 à 5 sur la figure 6/X.402), alors que le second ne peut être utilisé que pour fournir le service de sécurité aux utilisateurs du système MTS (1 ou 5 sur la figure 6/X.402). L'élément de sécurité choisi dépend de la politique de sécurité appliquée.

10.2.1.1.2 *Service de sécurité Authentification de l'origine de l'envoi-test*

Le service de sécurité Authentification de l'origine de l'envoi-test confirme la provenance d'un envoi-test.

Ce service de sécurité peut être assuré à l'aide de l'élément de sécurité Authentification de l'origine de l'envoi-test. Cet élément de sécurité peut être utilisé pour fournir le service de sécurité à l'un quelconque des agents MTA par l'intermédiaire desquels l'envoi-test est transféré (numérotés de 2 à 4 sur la figure 6/X.402).

10.2.1.1.3 *Service de sécurité Authentification de l'origine du rapport*

Le service de sécurité Authentification de l'origine du rapport confirme la provenance d'un rapport.

Ce service de sécurité peut être assuré à l'aide de l'élément de sécurité Authentification de l'origine du rapport. Cet élément de sécurité peut être utilisé pour fournir le service de sécurité à l'expéditeur du message ou envoi-test sujet, ainsi qu'à l'un quelconque des agents MTA par l'intermédiaire desquels le rapport est transféré (1 à 5 sur la figure 6/X.402).

10.2.1.2 *Service de sécurité Preuve du dépôt*

Ce service de sécurité permet à l'expéditeur d'un message d'obtenir confirmation que son message a été reçu par le système MTS pour être remis au(x) destinataire(s) spécifié(s) au départ.

Ce service de sécurité peut être assuré à l'aide de l'élément de sécurité Preuve du dépôt.

TABLEAU 7/X.402

Services de sécurité du transfert de message du MHS

Service	UA/ UA	MS/ MTA	MTA/ MS	MTA/ UA	UA/ MS	UA/ MTA	MTA/ MTA	MS/ UA
<i>Authentification de l'origine</i>								
Authentification de l'origine du message	*	*	—	*	—	—	—	—
Authentification de l'origine de l'envoi-test	—	—	*	*	—	—	—	—
Authentification de l'origine du rapport	—	—	—	—	*	*	*	—
Preuve du dépôt	—	—	—	—	—	—	*	—
Preuve de remise	*	—	—	—	—	—	—	a)
<i>Gestion de la sécurité de l'accès</i>								
Authentification de l'entité homologue	—	*	*	*	*	*	*	*
Contexte de sécurité	—	*	*	*	*	*	*	*
<i>Confidentialité des données</i>								
Confidentialité de la liaison	—	*	*	*	*	*	*	*
Confidentialité du contenu	*	—	—	—	—	—	—	—
Confidentialité du cheminement du message	*	—	—	—	—	—	—	—
<i>Service d'intégrité des données</i>								
Intégrité de la liaison	—	*	*	*	*	*	*	*
Intégrité du contenu	*	—	—	—	—	—	—	—
Intégrité de la séquence de message	*	—	—	—	—	—	—	—
<i>Non-répudiation</i>								
Non-répudiation d'origine	*	—	—	*	—	—	—	—
Non-répudiation de dépôt	—	—	—	—	—	—	*	—
Non-répudiation de remise	*	—	—	—	—	—	—	a)
<i>Etiquetage de sécurité du message</i>								
Etiquetage de sécurité du message	*	*	*	*	*	*	*	*
<i>Services de gestion de la sécurité</i>								
Modifications des pouvoirs	—	*	—	*	*	*	*	—
Enregistrement	—	*	—	*	—	—	—	—
Enregistrement de la mémoire MS	—	*	—	—	—	—	—	—

a) Ce service est assuré par la mémoire MS du destinataire à l'agent UA de l'expéditeur.

10.2.1.3 Service de sécurité Preuve de remise

Ce service de sécurité permet à l'expéditeur d'un message d'obtenir confirmation que son message a été remis par le système MTS au(x) destinataire(s) prévu(s).

Ce service de sécurité peut être assuré à l'aide de l'élément de sécurité Preuve de remise.

10.2.2 Service de sécurité Gestion de la sécurité de l'accès

Le service de sécurité Gestion de la sécurité de l'accès a pour but de protéger les ressources contre toute utilisation non autorisée. Il se décompose en deux parties, à savoir le service de sécurité Authentification de l'entité homologue et le service de sécurité Contexte de sécurité.

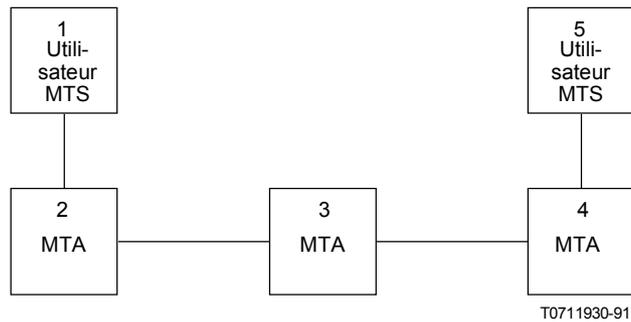


FIGURE 6/X.402

Modèle fonctionnel du système MHS simplifié

10.2.2.1 *Service de sécurité Authentification de l'entité homologue*

Ce service de sécurité est destiné à être utilisé lors de l'établissement d'une liaison pour confirmer l'identité de l'entité qui établit la liaison. Il peut être utilisé sur les liaisons 1-2, 2-3, 3-4 ou 4-5 de la figure 6/X.402 et garantit, au moment de l'utilisation uniquement, qu'une entité ne tente pas un piratage par usurpation d'identité ou par relecture non autorisée des codes d'échange d'une liaison antérieure.

Ce service de sécurité est assuré par l'élément de sécurité Echange d'authentification. A noter que l'utilisation de cet élément de sécurité peut produire d'autres données qui, dans certaines circonstances, peuvent être utilisées pour assurer un service de sécurité Confidentialité de la liaison et/ou Intégrité de la liaison.

10.2.2.2 *Service de sécurité Contexte de sécurité*

Ce service de sécurité est utilisé pour limiter la gamme des possibilités d'échange de messages entre entités en utilisant des Etiquettes de sécurité associées aux messages. Ce service de sécurité est donc étroitement lié au service de sécurité Etiquetage de sécurité du message, qui permet l'association de messages et d'Etiquettes de sécurité.

Le service de sécurité Contexte de sécurité est assuré par les éléments de sécurité Contexte de sécurité et Enregistrement.

10.2.3 *Services de sécurité Confidentialité des données*

Ces services de sécurité protègent les données contre toute divulgation non autorisée.

10.2.3.1 *Service de sécurité Confidentialité de la liaison*

Le système MHS n'assure aucun service de sécurité Confidentialité de la liaison. Toutefois, l'utilisation de l'élément de sécurité Echange d'authentification pour assurer le service de sécurité Authentification de l'entité homologue peut fournir des données concernant l'appel du service de sécurité Confidentialité de la liaison dans les couches sous-jacentes. Ce service de sécurité peut être nécessaire sur n'importe laquelle des liaisons 1-2, 2-3, 3-4 ou 4-5 de la figure 6/X.402.

10.2.3.2 *Service de sécurité Confidentialité du contenu*

Le service de sécurité Confidentialité du contenu garantit que le contenu d'un message n'est connu que de son expéditeur et de son destinataire.

Il peut être assuré en combinant les éléments de sécurité Confidentialité du contenu et Confidentialité de l'argument du message. L'élément de sécurité Confidentialité de l'argument du message peut être utilisé pour transférer un code secret utilisé avec l'élément de sécurité confidentialité du contenu pour chiffrer le contenu du message. L'utilisation de ces éléments de sécurité permet d'assurer le service depuis l'utilisateur MTS 1 jusqu'à l'utilisateur MTS 5 de la figure 6/X.402, le contenu du message étant inintelligible pour les agents MTA.

10.2.3.3 *Service de sécurité Confidentialité du cheminement du message*

Ce service de sécurité assure la protection des informations qui pourraient être tirées de l'observation du cheminement des messages. Seule une forme limitée de ce service de sécurité est assurée par le système MHS.

La technique de double enveloppe permet à un message complet de devenir le contenu d'un autre message. Cette technique peut servir à cacher l'information d'adressage à certaines parties du système MTS. Combinée au remplissage du trafic (qui n'entre pas dans le cadre actuel de la présente Recommandation), cette technique pourrait servir à assurer la confidentialité du cheminement des messages. D'autres éléments de ce service, tel que le contrôle d'acheminement ou les pseudonymes, n'entrent pas non plus dans le cadre de la présente Recommandation.

10.2.4 *Services de sécurité Intégrité des données*

Ces services de sécurité sont destinés à assurer une protection contre les risques d'intrusion active qui menacent le système MHS.

10.2.4.1 *Service de sécurité Intégrité de la liaison*

Le système MHS n'assure aucun service de sécurité Intégrité de la liaison. Toutefois, l'utilisation de l'élément de sécurité Echange d'authentification pour assurer le service de sécurité Authentification de l'entité homologue peut fournir des données concernant l'appel du service Intégrité de la liaison dans les couches sous-jacentes. Ce service de sécurité peut être nécessaire sur l'une quelconque des liaisons 1-2, 2-3, 3-4 ou 4-5 de la figure 6/X.402.

10.2.4.2 *Service de sécurité Intégrité du contenu*

Ce service de sécurité assure l'intégrité du contenu d'un seul message en permettant de déterminer si le contenu du message a été modifié. Ce service de sécurité ne permet pas de détecter la répétition d'un message, possibilité qui est offerte par le service de sécurité Intégrité de la séquence du message.

Ce service de sécurité peut être assuré de deux manières différentes, à l'aide de deux combinaisons différentes d'éléments de sécurité.

L'élément de sécurité Intégrité du contenu, combiné à l'élément de sécurité Intégrité de l'argument du message et, dans certains cas, à l'élément de sécurité Confidentialité de l'argument du message, peut être utilisé pour fournir le service de sécurité à un destinataire d'un message, c'est-à-dire dans le cas d'une communication entre les utilisateurs MTS 1 et MTS 5 représentés sur la figure 6/X.402. L'élément de sécurité Intégrité du contenu sert à calculer un Contrôle d'intégrité du contenu en fonction de l'intégralité du contenu du message. Selon la méthode utilisée pour calculer le Contrôle d'intégrité du contenu, un code secret peut être nécessaire, qui peut être confidentiellement envoyé au destinataire du message à l'aide de l'élément de sécurité Confidentialité de l'argument du message. L'utilisation de l'élément de sécurité Intégrité de l'argument du message protège le Contrôle d'intégrité du contenu de toute modification. L'intégrité des arguments de message confidentiel est assurée par l'élément de sécurité Confidentialité de l'argument du message.

L'élément de sécurité Authentification de l'origine du message peut aussi être utilisé pour assurer ce service de sécurité.

10.2.4.3 *Service de sécurité Intégrité de la séquence du message*

Ce service de sécurité protège l'expéditeur et le destinataire d'une séquence de messages contre toute remise en ordre de cette séquence, et, ainsi, contre toute répétition des messages.

Ce service de sécurité peut être assuré par une combinaison des éléments de sécurité Intégrité de la séquence du message et Intégrité de l'argument du message. Le premier de ces éléments attribue un numéro d'ordre à chaque message, que l'utilisation du second élément protège de toute modification. La confidentialité et l'intégrité du numéro d'ordre des messages peuvent être assurées simultanément à l'aide de l'élément de sécurité Confidentialité de l'argument du message.

Ces éléments de sécurité fournissent ce service aux communications entre les utilisateurs MTS 1 et MTS 5 de la figure 6/X.402, mais non avec les agents MTA intermédiaires.

10.2.5 *Services de sécurité Non-répudiation*

Ces services de sécurité apportent à un tiers, après le dépôt, l'envoi ou la remise du message, la preuve irréfutable que cette opération s'est déroulée comme demandée. A noter que pour assurer un fonctionnement correct de ces services, la politique de sécurité doit expressément englober la gestion de codes asymétriques pour les besoins des services de non-répudiation si des algorithmes asymétriques sont utilisés.

10.2.5.1 *Service de sécurité Non-répudiation de l'origine*

Ce service de sécurité apporte au(x) destinataire(s) d'un message la preuve irréfutable de l'origine du message, du contenu de celui-ci et de l'Étiquette de sécurité associée.

Ce service de sécurité peut être assuré de deux manières différentes à l'aide de deux combinaisons différentes d'éléments de sécurité. A noter que la prestation de ce service est très semblable à la prestation du service de sécurité (plus faible) Intégrité du contenu.

L'élément de sécurité Intégrité du contenu, combiné à l'élément de sécurité Intégrité de l'argument du message et, dans certains cas, à l'élément de sécurité Confidentialité de l'argument du message, peut être utilisé pour fournir le service à un destinataire d'un message, c'est-à-dire pour les communications entre les utilisateurs MTS 1 et MTS 5 de la figure 6/X.402. L'élément de sécurité Intégrité du contenu sert à calculer un Contrôle d'Intégrité du contenu en fonction de l'intégralité du contenu du message. Selon la méthode utilisée pour calculer le Contrôle d'intégrité du contenu, un code secret peut être nécessaire, qui peut être confidentiellement envoyé au destinataire du message à l'aide de l'élément de sécurité Confidentialité de l'argument du message. L'utilisation de l'élément de sécurité Intégrité de l'argument du message protège le Contrôle d'intégrité du contenu et, si besoin est, l'Étiquette de sécurité du message, contre toute modification et/ou répudiation. Les arguments de message confidentiel sont protégés contre une modification et/ou une répudiation à l'aide de l'élément de sécurité Confidentialité de l'argument du message.

Si le service de sécurité Confidentialité du contenu n'est pas nécessaire, l'élément de sécurité Authentification de l'origine du message peut aussi servir de base à ce service de sécurité. En ce cas, le service de sécurité peut être assuré à tous les éléments du système MHS, c'est-à-dire à chacun des éléments 1 à 5 de la figure 6/X.402.

10.2.5.2 *Service de sécurité Non-répudiation de dépôt*

Ce service de sécurité apporte à l'expéditeur du message la preuve irréfutable que ce message a été déposé dans le système MTS pour être remis au(x) destinataire(s) spécifié(s) au départ.

L'élément de sécurité Preuve de dépôt assure ce service de sécurité exactement comme le service de sécurité (plus faible) Preuve de dépôt.

10.2.5.3 *Service de sécurité Non-répudiation de remise*

Ce service de sécurité apporte à l'expéditeur du message la preuve irréfutable que ce message a été remis au(x) destinataire(s) spécifié(s) au départ.

L'élément de sécurité Preuve de remise assure ce service de sécurité exactement comme le service de sécurité (plus faible) Preuve de remise.

10.2.6 *Service de sécurité Etiquetage de sécurité du message*

Ce service de sécurité permet d'associer des Étiquettes de sécurité à toutes les entités du système MHS, c'est-à-dire aux agents MTA et aux utilisateurs du MTS. Combiné au service de sécurité Contexte de sécurité, il permet la mise en œuvre de politiques de sécurité définissant les parties du système MHS qui peuvent traiter des messages comportant des étiquettes de sécurité spécifiées.

Ce service de sécurité est assuré par l'élément de sécurité Étiquette de sécurité du message. L'intégrité et la confidentialité de l'étiquette sont assurées par les éléments de sécurité Intégrité de l'argument du message et Confidentialité de l'argument du message.

10.2.7 *Services de gestion de la sécurité*

Le système MHS nécessite un certain nombre de services de gestion de la sécurité. Les seuls services de gestion prévus dans la Rec. X.411 du CCITT | ISO/CEI 10021-4 concernent la modification des pouvoirs et l'enregistrement des étiquettes de sécurité des utilisateurs du MTS.

10.2.7.1 *Service de sécurité Modification des pouvoirs*

Ce service de sécurité permet à une entité du système MHS de modifier les pouvoirs détenus à son égard par une autre entité du système MHS. Il peut être assuré à l'aide de l'élément de sécurité Modification des pouvoirs.

10.2.7.2 *Service de sécurité Enregistrement*

Ce service de sécurité permet l'établissement, au niveau d'un agent MTA, d'Étiquettes de sécurité que peut admettre un utilisateur donné du MTS. Il peut être assuré à l'aide de l'élément de sécurité Enregistrement.

10.2.7.3 *Service de sécurité Enregistrement de la mémoire MS*

Ce service permet l'établissement de l'étiquette de sécurité, qui est autorisée pour l'utilisateur de la mémoire MS.

10.3 *Éléments de sécurité*

Les paragraphes qui suivent décrivent les éléments de sécurité disponibles dans les protocoles décrits dans la Rec. X.411 du CCITT | ISO/CEI 10021-4 pour prendre en charge les services de sécurité du système MHS. Ces éléments de sécurité se rapportent directement aux arguments de divers services décrits dans la Rec. X.411 du CCITT | ISO/CEI 10021-4. L'objectif du présent paragraphe est de séparer chaque élément des définitions de service de la Rec. X.411 du CCITT | ISO/CEI 10021-4 concernant la sécurité et de définir la fonction de chacun des éléments de sécurité ainsi identifiés.

10.3.1 *Éléments de sécurité Authentification*

Ces éléments de sécurité sont définis afin d'assurer la prise en charge des services de sécurité authentification et intégrité.

10.3.1.1 *Éléments de sécurité Echange d'authentification*

L'élément de sécurité Echange d'authentification est destiné à authentifier, réciproquement si possible, l'identité d'un utilisateur du système MTS pour un agent MTA, d'un agent MTA pour un autre agent MTA, d'un agent MTA pour un utilisateur du système MTS, d'une mémoire MS pour un agent UA ou d'un agent UA pour une mémoire MS. Il est fondé sur l'échange ou l'utilisation de données secrètes: mots de passe, jetons chiffrés en mode asymétrique ou symétrique. L'échange a pour résultat de confirmer l'identité du correspondant et, facultativement, de transférer des données confidentielles qui peuvent servir à assurer les services de sécurité Confidentialité de la liaison et/ou Intégrité de la liaison dans les couches sous-jacentes. Cette authentification n'est valable qu'à l'instant où elle est effectuée. Sa validité persiste selon que l'échange de données confidentielles, ou un autre mécanisme, sert ou non à établir un trajet de communication sûr. L'établissement et l'utilisation d'un tel trajet n'entrent pas dans le cadre de la présente Recommandation.

Cet élément de sécurité utilise l'argument Pouvoirs du demandeur et le résultat Pouvoirs du demandé des services rattachement-MTS, rattachement-MS et rattachement-MTA. Les pouvoirs transférés sont soit des mots de passe, soit des jetons.

10.3.1.2 *Éléments de sécurité Authentification de l'origine des données*

Ces éléments de sécurité sont expressément destinés à assurer la prise en charge des services d'authentification de l'origine des données et de certains services d'intégrité des données.

10.3.1.2.1 *Éléments de sécurité Authentification de l'origine du message*

L'élément de sécurité Authentification de l'origine du message permet à quiconque recevant ou transférant un message d'authentifier l'identité de l'utilisateur du système MTS ayant expédié ce message. Il peut être nécessaire à cette fin d'assurer le service de sécurité Authentification de l'origine du message ou Non-répudiation de l'origine.

Cet élément de sécurité suppose la transmission, dans le message, d'un Contrôle d'authentification de l'origine du message, calculé en fonction du contenu du message, de l'Identificateur du contenu du message et de l'Étiquette de sécurité du message. Si le service de sécurité Confidentialité du contenu est également nécessaire, le Contrôle d'authentification de l'origine du message est calculé en fonction du contenu du message chiffré plutôt qu'en fonction du contenu du message non chiffré. En se fondant sur le contenu du message acheminé dans le message global (c'est-à-dire après l'élément de sécurité optionnel Confidentialité du contenu), toute entité du système MHS peut vérifier l'intégrité du message global, sans être obligée de voir en clair le texte du contenu du message. Toutefois, en cas d'utilisation du service de sécurité Confidentialité du contenu, l'élément de sécurité Authentification de l'origine du message ne peut pas être utilisé pour assurer le service de sécurité Non-répudiation de l'origine.

Cet élément de sécurité utilise le Contrôle d'authentification de l'origine du message, qui est l'un des arguments des services Dépôt de message, Transfert de message et Remise de message.

10.3.1.2.2 *Élément de sécurité Authentification de l'origine de l'envoi-test*

Semblable à l'élément de sécurité Authentification de l'origine du message, l'élément de sécurité Authentification de l'origine de l'envoi-test permet à un agent MTA d'authentifier l'identité de l'utilisateur du système MTS qui a envoyé un envoi-test.

Cet élément de sécurité utilise le contrôle d'authentification de l'origine de l'envoi-test, qui est l'un des arguments du service Dépôt de l'envoi-test.

10.3.1.2.3 *Élément de sécurité Authentification de l'origine du rapport*

Semblable à l'élément de sécurité Authentification de l'origine du message, l'élément de sécurité Authentification de l'origine du rapport permet à un agent MTA ou à un utilisateur du système MTS qui reçoit un rapport d'authentifier l'identité de l'agent MTA qui a envoyé ce rapport.

Cet élément de sécurité utilise le Contrôle d'authentification de l'origine du rapport, qui est l'un des arguments du service Remise de rapport.

10.3.1.3 *Élément de sécurité Preuve de dépôt*

Cet élément de sécurité permet à l'expéditeur d'un message d'établir qu'un message a été accepté par le système MHS pour transmission.

Cet élément de sécurité est constitué de deux arguments: une demande de Preuve de dépôt, envoyée avec un message au moment du dépôt, et la Preuve de dépôt, retournée à l'utilisateur du système MTS avec les résultats du Dépôt de message. La Preuve de dépôt est produite par le système MTS et est calculée en fonction de tous les arguments du message déposé, de l'identificateur de dépôt du message et de l'heure de dépôt du message.

L'argument Preuve de dépôt peut servir à assurer le service de sécurité Preuve de dépôt. Selon la politique de sécurité en vigueur, il peut aussi être en mesure d'assurer le service de sécurité (plus fort) Non-répudiation du dépôt.

La demande de Preuve de dépôt est un argument du service Dépôt de message. La Preuve de dépôt est l'un des résultats du service Dépôt de message.

10.3.1.4 *Élément de sécurité Preuve de remise*

Cet élément de sécurité permet à l'expéditeur d'un message d'établir qu'un message a été remis à son destinataire par le système MHS.

Cet élément de sécurité est constitué de plusieurs arguments. L'expéditeur du message inclut dans le message déposé une demande de Preuve de remise, remise à chaque destinataire avec le message. Un destinataire peut alors calculer la Preuve de remise en fonction de certains arguments associés au message. La Preuve de remise est retournée par le système MTS à l'expéditeur du message, dans un rapport sur les résultats du Dépôt de message initial.

La Preuve de remise peut servir à assurer le service de sécurité Preuve de remise. Selon la politique de sécurité en vigueur, elle peut aussi être en mesure d'assurer le service de sécurité (plus fort) Non-répudiation de remise.

La Demande de preuve de remise est un argument des services Dépôt de message, Transfert de message et Remise de message. La Preuve de remise est à la fois l'un des résultats du service Remise de message et l'un des arguments des services Transfert de rapport et Remise de rapport.

Remarque – La non-réception d'une preuve de remise ne signifie pas nécessairement une non-remise.

10.3.2 *Éléments de sécurité Gestion de la sécurité de l'accès*

Ces éléments de sécurité sont définis afin d'assurer la prise en charge du service de sécurité Gestion de la sécurité de l'accès et des services de gestion de la sécurité.

10.3.2.1 *Élément de sécurité Contexte de sécurité*

Quand un utilisateur du système MTS ou un agent MTA se rattache à un agent MTA ou à un utilisateur du système MTS, l'opération de rattachement spécifie le contexte de sécurité de la liaison. Cela limite la gamme des possibilités d'échange de messages par référence aux étiquettes associées aux messages. De plus, le Contexte de sécurité de la liaison peut être temporairement modifié pour les messages déposés ou remis.

Le Contexte de sécurité lui-même se compose d'une ou plusieurs Etiquettes de sécurité définissant la sensibilité des interactions qui peuvent se produire compte tenu de la politique de sécurité en vigueur.

Le contexte de sécurité est un argument des services de rattachement au MTS et de rattachement au MTA.

10.3.2.2 *Elément de sécurité Enregistrement*

L'élément de sécurité Enregistrement permet d'établir dans un agent MTA les étiquettes de sécurité autorisées d'un utilisateur du système MTS.

Cet élément de sécurité est assuré par le service Enregistrement. Ce service permet à un utilisateur du système MTS de modifier des arguments détenus par le système MTS et relatifs à la remise de messages à cet utilisateur du système MTS.

10.3.2.3 *Elément de sécurité Enregistrement de la mémoire MS*

L'élément de sécurité Enregistrement de la mémoire MS permet d'établir les étiquettes de sécurité autorisées d'un utilisateur de la mémoire MS.

Cet élément de sécurité est assuré par le service Enregistrement de la mémoire MS. Ce service permet à un utilisateur de la mémoire MS de modifier des arguments détenus par la mémoire MS et relatifs à la remise de messages à cet utilisateur de la mémoire MS.

10.3.3 *Eléments de sécurité Confidentialité des données*

Ces éléments de sécurité, basés sur l'utilisation du chiffrement, visent tous à assurer la confidentialité des données transmises d'une entité du système MHS à une autre.

10.3.3.1 *Elément de sécurité Confidentialité du contenu*

L'élément de sécurité Confidentialité du contenu assure au contenu du message, en utilisant un élément de sécurité de chiffrement, une protection contre toute écoute clandestine pendant la transmission. Cet élément de sécurité fonctionne de telle sorte que seuls le destinataire et l'expéditeur du message connaissent le contenu du message en texte clair.

La spécification de l'algorithme de chiffrement, le code utilisé et toutes les autres données d'initialisation sont acheminés à l'aide des éléments de sécurité Confidentialité de l'argument du message et Intégrité de l'argument du message. L'algorithme et le code servent alors à chiffrer ou à déchiffrer le contenu du message.

L'élément de sécurité Confidentialité du contenu utilise l'identificateur d'algorithme de confidentialité de contenu, qui est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.3.2 *Elément de sécurité Confidentialité de l'argument du message*

L'élément de sécurité Confidentialité de l'argument du message assure la confidentialité, l'intégrité et, si besoin est, l'irrévocabilité des données de destinataires associées à un message. Ces données doivent comprendre expressément tous les codes cryptographiques et les données correspondantes nécessaires au bon fonctionnement des éléments de sécurité Confidentialité et Intégrité, si ces éléments de sécurité optionnels sont appelés.

Cet élément de sécurité fonctionne à l'aide du Jeton de message. Les données que l'élément de sécurité Confidentialité de l'argument du message doit protéger constituent les Données chiffrées du Jeton de message. Les Données chiffrées du Jeton de message sont incompréhensibles à tous les agents MTA.

Le Jeton de message est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.4 *Eléments de sécurité Intégrité des données*

Ces éléments de sécurité sont prévus pour assurer les services Intégrité des données, Authentification des données et Non-répudiation.

10.3.4.1 *Elément de sécurité Intégrité de contenu*

L'élément de sécurité Intégrité du contenu empêche le contenu d'un message d'être modifié en cours de transmission.

Cet élément de sécurité fonctionne à l'aide d'un ou plusieurs algorithmes cryptographiques. La spécification de ce ou de ces algorithme(s), le ou le(s) code(s) utilisé(s) et les toutes autres données d'initialisation sont acheminés à l'aide des éléments de sécurité Confidentialité de l'argument du message et Intégrité de l'argument du message. Le

résultat de l'application des algorithmes et du code est le Contrôle de l'intégrité du contenu, qui est envoyé dans l'enveloppe du message. Cet élément de sécurité n'est accessible qu'au(x) destinataire(s) du message du fait qu'il agit sur le texte en clair du contenu de message.

Si le Contrôle de l'intégrité du contenu est protégé à l'aide de l'élément de sécurité Intégrité de l'argument du message, selon la politique de sécurité en vigueur, il peut être utilisé pour aider à assurer le service de sécurité Non-répudiation de l'origine.

Le Contrôle de l'intégrité du contenu est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.4.2 *Elément de sécurité Intégrité de l'argument du message*

L'élément de sécurité Intégrité de l'argument du message assure l'intégrité et, si besoin est, l'irrévocabilité de certains arguments associés à un message. Ces arguments peuvent expressément comprendre un ensemble quelconque d'Identificateur de l'algorithme de confidentialité du contenu, de Contrôle de l'intégrité du contenu, d'Etiquette de sécurité du message, de Demande de preuve de remise et de Numéro d'ordre du message.

Cet élément de sécurité fonctionne à l'aide du Jeton de message. Les données que l'élément de sécurité Intégrité de l'argument du message doit protéger constituent les données signées dans le Jeton de message.

Le Jeton de message est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.4.3 *Elément de sécurité Intégrité de la séquence du message*

L'élément de sécurité Intégrité de la séquence du message empêche l'expéditeur et le destinataire d'un message de recevoir des messages en désordre ou en double.

Un numéro d'ordre de message est associé à chaque message. Ce numéro identifie la position d'un message dans une séquence d'un expéditeur vers un destinataire. Chaque couple expéditeur-destinataire ayant besoin d'utiliser cet élément de service doit donc maintenir une séquence distincte de numéros de message. Cet élément de sécurité n'assure ni l'initialisation, ni la synchronisation des numéros d'ordre de message.

10.3.5 *Eléments de sécurité Non-répudiation*

Aucun élément de sécurité Non-répudiation spécifique n'est défini dans la Rec. X.411 du CCITT | ISO/CEI 10021-4. Les services de Non-répudiation peuvent être assurés à l'aide d'une combinaison d'autres éléments de sécurité.

10.3.6 *Eléments de sécurité Etiquette de sécurité*

Ces éléments de sécurité sont destinés à assurer l'étiquetage de sécurité dans le système MHS.

10.3.6.1 *Elément de sécurité Etiquette de sécurité du message*

Les messages peuvent être étiquetés avec des données comme le spécifie la politique de sécurité en vigueur. L'étiquette de sécurité du message peut être utilisée par des agents MTA intermédiaires dans le cadre de la politique de sécurité globale du système.

Une Etiquette de sécurité du message peut être envoyée sous la forme d'un argument du message; elle peut être protégée par l'élément de sécurité Intégrité de l'argument du message ou Authentification de l'origine du message, tout comme d'autres arguments du message.

Si la confidentialité et l'intégrité sont toutes deux nécessaires, l'Etiquette de sécurité du message peut aussi être protégée à l'aide de l'élément de sécurité Confidentialité de l'argument du message. Dans ce cas, l'Etiquette de sécurité du message ainsi protégée est un argument expéditeur-destinataire et peut différer de l'Etiquette de sécurité de message contenue dans l'enveloppe du message.

10.3.7 *Eléments de sécurité Gestion de la sécurité*

10.3.7.1 *Elément de sécurité Modification des pouvoirs*

L'élément de sécurité Modification des pouvoirs permet la mise à jour des pouvoirs d'un utilisateur du système MTS ou d'un agent MTA.

Cet élément de sécurité est assuré par le service du système MTS Modification des pouvoirs.

10.3.8 *Technique de double enveloppe*

Une protection supplémentaire peut être assurée à un message complet, y compris à ses paramètres d'enveloppe, grâce à la possibilité de spécifier que le contenu d'un message constitue lui-même un message complet, c'est-à-dire en utilisant une technique de double enveloppe.

Cette technique utilise l'argument Type de contenu qui permet de spécifier que le contenu d'un message est une Enveloppe intérieure. Ce Type de contenu signifie que le contenu constitue lui-même un message (enveloppe et contenu). Lors de la remise au destinataire désigné sur l'enveloppe extérieure, celle-ci est ôtée et on décrypte le contenu, si besoin est, de sorte que l'on obtient une Enveloppe intérieure et son contenu. Les informations contenues dans l'Enveloppe intérieure servent à transférer le contenu de l'Enveloppe intérieure vers les destinataires désignés sur l'Enveloppe intérieure.

Le Type de contenu est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.9 *Chiffrement et adressage calculé*

Chaque paramètre du système MTS transféré vers des algorithmes de chiffrement ou d'adressage calculé doit être codé selon les règles de codage de l'ASN.1 spécifiées aux fins de chiffrement ou d'adressage calculé.

Remarque 1 – On ne peut en déduire que le codage de l'enveloppe-remise ou du contenu-remis doit s'effectuer selon les règles de codage spécifiées dans l'identificateur d'algorithme.

Remarque 2 – Dans le cas du contenu, les règles de codage spécifiées dans l'identificateur d'algorithme ne doivent s'appliquer qu'au codage des octets de contenu dans la Chaîne d'octets, non au codage du protocole de contenu (qui reste inchangé).

SECTION 3 – CONFIGURATIONS

11 **Présentation générale**

La présente section indique comment on peut configurer le système MHS en vue de répondre à l'une des diverses spécifications d'ordre fonctionnel, physique et organisationnel.

Elle traite des sujets suivants:

- a) configurations fonctionnelles;
- b) configurations physiques;
- c) configurations organisationnelles;
- d) le système MHS mondial.

12 **Configurations fonctionnelles**

On trouvera ci-dessous la spécification des configurations fonctionnelles possibles du système MHS. Leur variété résulte de la présence ou de l'absence de l'annuaire et de l'utilisation ou de la non-utilisation par un utilisateur direct d'une mémoire MS.

12.1 *Annuaire*

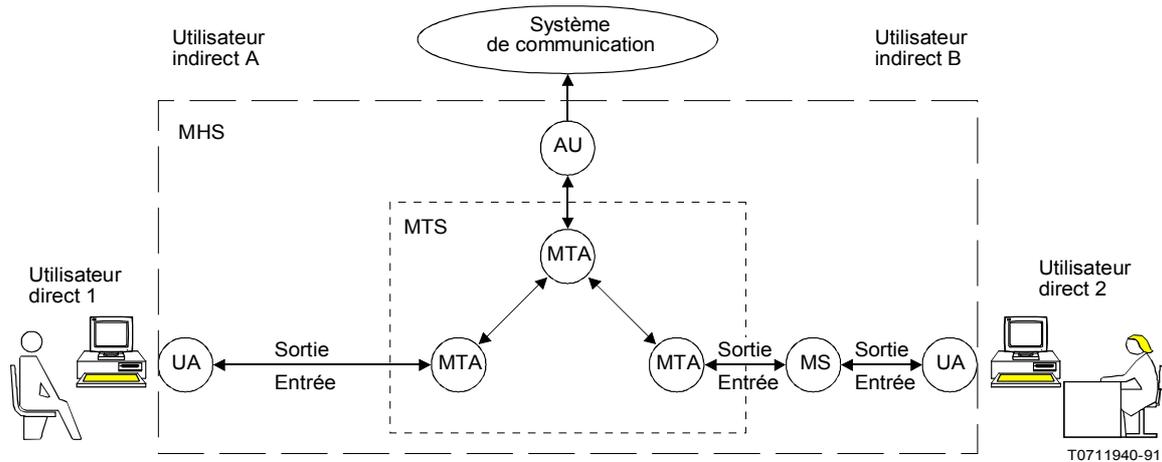
En ce qui concerne l'annuaire, le système MHS peut être configuré pour un utilisateur particulier, ou un groupe d'utilisateurs (voir, par exemple, le § 14.1), avec ou sans l'annuaire. Un utilisateur qui n'a pas accès à l'annuaire peut ne pas disposer des fonctions décrites dans la section 5.

Remarque – Un annuaire partiellement (plutôt que totalement) interconnecté, peut être mis en place pendant une période intérimaire d'élaboration de l'annuaire (mondial), selon les Recommandations du CCITT | Norme internationales relatives aux annuaires.

12.2 Mémoire de messages

En ce qui concerne la mémoire MS, le système MHS peut, pour un utilisateur direct donné, être configuré avec ou sans mémoire MS. Un utilisateur n'ayant pas accès à une mémoire MS ne dispose pas des fonctions de mise en mémoire des messages. Dans ces conditions, un utilisateur dépend de son agent UA pour la mise en mémoire des objets d'information, et cette capacité dépend des autorités locales.

Les deux configurations fonctionnelles précitées sont décrites à la figure 7/X.402 qui illustre en outre une configuration possible du système MTS et sa connexion avec un autre système de communication par l'intermédiaire d'une AU. Sur la figure 7/X.402, l'utilisateur 2 est équipé d'une mémoire MS, alors que l'utilisateur 1 ne l'est pas.



Remarque – Bien que les utilisateurs décrits sur cette figure soient des personnes, celle-ci s'applique au même titre à tout autre type d'utilisateur.

FIGURE 7/X.402

Configurations fonctionnelles concernant la mémoire MS

13 Configurations physiques

On trouvera ci-dessous la spécification des configurations physiques possibles du système MHS, à savoir la façon dont ce système peut être réalisé sous forme d'ensemble de systèmes informatiques interconnectés. Le nombre de configurations n'étant pas limité, ce paragraphe décrit les types de *systèmes de messagerie* à partir desquels le système MHS est constitué et définit quelques configurations particulièrement importantes.

13.1 Systèmes de messagerie

Les modules utilisés dans l'élaboration physique du système MHS sont appelés *systèmes de messagerie*. Un **système de messagerie** est un système informatique (éventuellement, mais pas obligatoirement, un système ouvert) qui contient ou réalise un ou plusieurs objets fonctionnels.

Les différents types de systèmes de messagerie sont décrits à la figure 8/X.402.

Les différents types de systèmes de messagerie décrits sur la figure 8/X.402 sont énumérés à la première colonne du tableau 8/X.402. Pour chaque type cité, la deuxième colonne indique les sortes d'objets fonctionnels – agents UA, mémoire MS, agents MTA et unités AU – pouvant exister dans un tel système, si leur présence est obligatoire ou facultative et si le système en comprend un seul ou, éventuellement plusieurs.

Le tableau 8/X.402 est divisé en deux sections. Les systèmes de messagerie de la première section concernent des utilisateurs uniques, ceux de la seconde section peuvent (sans obligation) desservir plusieurs utilisateurs.

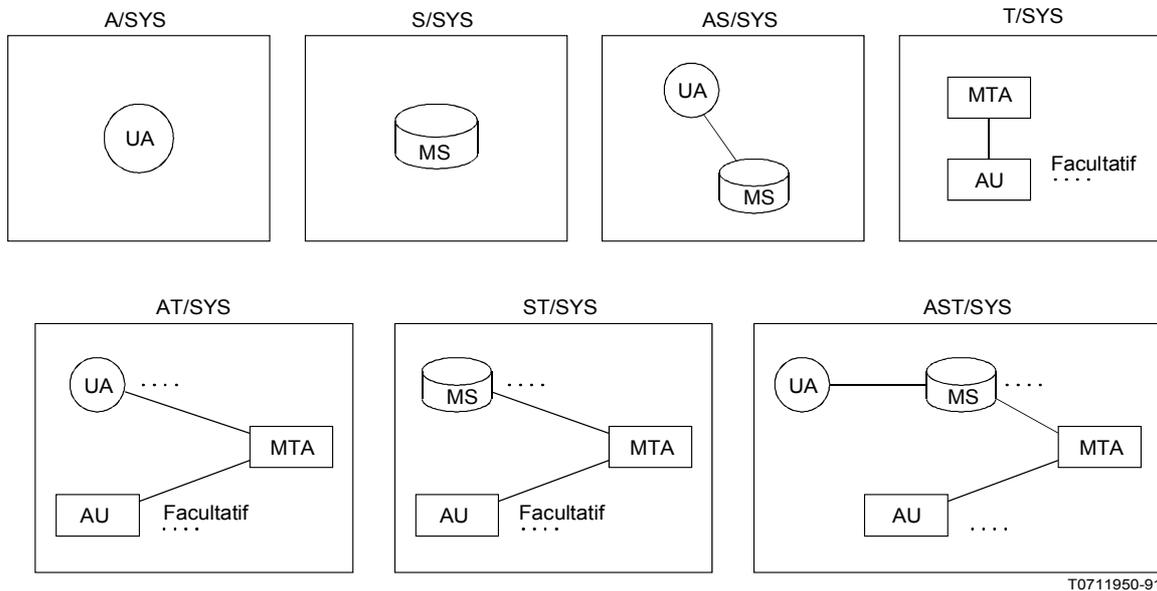


FIGURE 8/X.402
Types de systèmes de messagerie

Les types de systèmes de messagerie résumés dans le tableau 8/X.402 sont définis et décrits individuellement ci-dessous.

Remarque – L'admission des types de systèmes de messagerie a été décidée d'après les principes fondamentaux suivants:

- une unité AU et l'agent MTA avec lequel elle est en interaction sont, en général, installés au même endroit, aucun protocole régissant leur interaction n'étant normalisé;
- un agent MTA est, en règle générale installé au même endroit que des agents UA ou mémoires MS multiples car, parmi les protocoles normalisés, seul le protocole de transfert transmet simultanément un message à plusieurs destinataires. La remise *en série* d'un message à plusieurs destinataires desservis par un système de messagerie, que nécessiterait le protocole de remise, serait inefficace;
- il n'est pas utile d'installer plusieurs agents MTA dans un système de messagerie car un seul agent MTA dessert plusieurs utilisateurs et a pour objet de transmettre des objets entre ces systèmes et non à l'intérieur de ceux-ci (il ne s'agit pas d'exclure la possibilité de faire coexister plusieurs processus concernant l'agent MTA dans un seul système informatique);
- l'installation au même endroit d'une unité AU et d'un agent MTA n'a pas d'influence sur le comportement du système en ce qui concerne les autres aspects du système MHS. En conséquence, un seul type de système de messagerie englobe la présence et l'absence d'une unité AU.

13.1.1 Systèmes d'accès

Un **système d'accès (A/SYS)** (*access system*) contient un agent UA mais ne contient ni une mémoire MS, ni un agent MTA, ni une unité AU.

Un système A/SYS est réservé à un seul utilisateur.

TABLEAU 8/X.402

Systèmes de messagerie

Système d'élaboration de messages	Objets fonctionnels			
	AU	MS	MTA	AU
A/SYS	1	–	–	–
S/SYS	–	1	–	–
AS/SYS	1	1	–	–
T/SYS	–	–	1	[M]
AT/SYS	M	–	1	[M]
ST/SYS	–	M	1	[M]
AST/SYS	M	M	1	[M]

M Multiple

[. . .] Facultatif

13.1.2 *Systèmes de mémorisation*

Un **système de mémorisation (S/SYS)** (*storage system*) contient une mémoire MS mais ne contient ni un agent UA, ni un agent MTA, ni une unité AU.

Un système S/SYS est réservé à un seul utilisateur.

13.1.3 *Systèmes d'accès et de mémorisation*

Un **système d'accès et de mémorisation (AS/SYS)** (*access and storage system*) contient un agent UA et une mémoire MS, mais ne contient ni un agent MTA, ni une unité AU.

Un système AS/SYS est réservé à un seul utilisateur.

13.1.4 *Systèmes de transfert*

Un **système de transfert (T/SYS)** (*transfer system*) contient un agent MTA et, à titre facultatif, une ou plusieurs unités AU, mais il ne contient ni un agent UA, ni une mémoire MS.

Un système T/SYS peut desservir plusieurs utilisateurs.

13.1.5 *Systèmes d'accès et de transfert*

Un **système d'accès et de transfert (AT/SYS)** (*access and transfer system*) contient un ou plusieurs agents UA, un agent MTA et, à titre facultatif, une ou plusieurs unités AU, mais il ne contient pas de mémoire MS.

Un système AT/SYS peut desservir plusieurs utilisateurs.

13.1.6 *Systèmes de mémorisation et de transfert*

Un **système de mémorisation et de transfert (ST/SYS)** (*storage and transfer system*) contient une ou plusieurs mémoires MS, un agent MTA et, à titre facultatif, une ou plusieurs unités AU, mais il ne contient pas d'agent UA.

Un système ST/SYS peut desservir plusieurs utilisateurs.

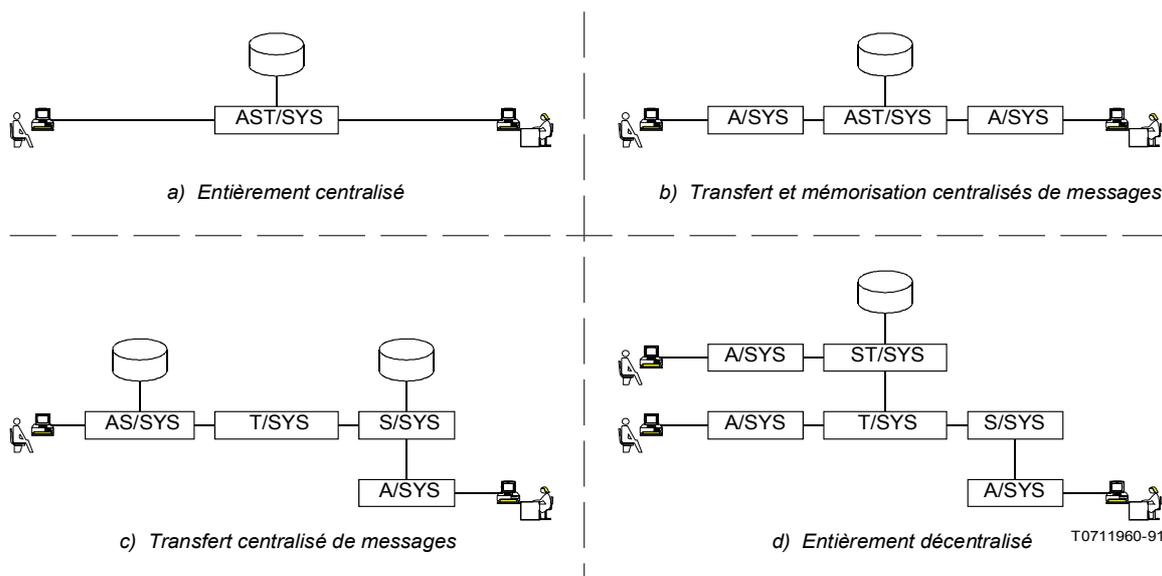
13.1.7 *Systèmes d'accès, de mémorisation et de transfert*

Un **système d'accès, de mémorisation et de transfert (AST/SYS)** (*access, storage and transfer system*) contient un ou plusieurs agents UA, une ou plusieurs mémoires MS, un agent MTA et, à titre facultatif, une ou plusieurs unités AU.

Un système AST/SYS peut desservir plusieurs utilisateurs.

13.2 Configurations représentatives

Les systèmes de messagerie peuvent être combinés de plusieurs façons pour constituer le système MHS. Le nombre des configurations physiques possibles étant illimité, celles-ci ne peuvent être énumérées. Quelques configurations représentatives importantes sont toutefois décrites ci-après et illustrées à la figure 9/X.402.



Remarque 1 – Bien que les utilisateurs décrits sur cette figure soient des personnes, celle-ci s'applique au même titre à tout autre type d'utilisateur.

Remarque 2 – Outre les configurations physiques résultant des approches «pures» ci-après, de nombreuses configurations «hybrides» peuvent être élaborées.

FIGURE 9/X.402
Configurations physiques représentatives

13.2.1 Système MHS entièrement centralisé

Le système MHS peut être entièrement centralisé [partie a) de la figure 9/X.402]. Cette conception s'obtient avec un seul système AST/SYS contenant des objets fonctionnels de toutes sortes et pouvant desservir plusieurs utilisateurs.

13.2.2 Transfert et mémorisation centralisés de messages

Le système MHS peut centraliser le transfert et la mémorisation de messages, mais décentraliser l'accès d'utilisateur [partie b) de la figure 9/X.402]. Cette conception s'effectue avec un seul ST/SYS et, pour chaque utilisateur, un A/SYS.

13.2.3 Transfert centralisé de messages

Le système MHS peut centraliser le transfert de messages tout en décentralisant la mémorisation de messages et l'accès d'utilisateur [partie c) de la figure 9/X.402]. Cette conception s'effectue avec un seul T/SYS et, pour chaque utilisateur, soit un AS/SYS utilisé seul, soit un S/SYS associé à un A/SYS.

13.2.4 *Système MHS entièrement décentralisé*

Le MHS peut décentraliser le transfert de messages [partie *d*] de la figure 9/X.402]. Cette conception fait intervenir plusieurs ST/SYS ou T/SYS.

14 Configurations organisationnelles

On trouvera ci-dessous la spécification des configurations organisationnelles possibles du système MHS, c'est-à-dire la façon dont ce système peut être réalisé sous forme d'ensembles de systèmes de messagerie, interconnectés mais gérés indépendamment (ces systèmes de messagerie étant eux-mêmes interconnectés). Le nombre de configurations étant illimité, la clause décrit les types de *domaines de gestion* à partir desquels le système MHS est constitué et identifie quelques configurations représentatives importantes.

14.1 *Domaines de gestion*

Les modules de base utilisés dans l'élaboration organisationnelle du système MHS sont appelés *domaines de gestion*. Un **domaine de gestion (MD)** (*management domain*) (ou **domaine**) est un ensemble de systèmes de messagerie – dont l'un au moins contient ou réalise un agent MTA – géré par une seule organisation.

Ceci n'empêche pas une organisation de gérer un ensemble de systèmes de messagerie (par exemple, un seul système A/SYS) qui, faute d'un agent MTA, ne peut être considéré comme un domaine MD. Un tel ensemble de systèmes de messagerie, module secondaire utilisé dans l'élaboration du système MHS, «s'interconnecte» avec un domaine MD.

Les domaines MD sont de plusieurs types, définis et décrits individuellement ci-dessous.

14.1.1 *Domaines de gestion d'Administration*

Un **domaine de gestion d'Administration (ADMD)** (*administration management domain*) comprend des systèmes de messagerie gérés par une Administration. La principale distinction technique existant entre un domaine ADMD et un *domaine PRMD* est que le domaine ADMD se situe au-dessus du domaine PRMD dans les systèmes d'adressage hiérarchique (voir le § 18) et d'acheminement du système MHS (voir le § 19).

Remarque – Un domaine ADMD assure au public le service de messagerie.

14.1.2 *Domaines de gestion privés*

Un **domaine de gestion privé (PRMD)** (*private management domain*) comprend des systèmes de messagerie gérés par une organisation autre qu'une Administration. La principale distinction technique existant entre un domaine PRMD et un domaine ADMD est que le domaine PRMD se situe au-dessous du domaine ADMD dans les systèmes d'adressage hiérarchique (voir le § 18) et d'acheminement du système MHS (voir le § 19).

Remarque – Un domaine PRMD assure le service de messagerie, par exemple, aux employés d'une entreprise ou aux employés installés dans un lieu particulier de l'entreprise.

14.2 *Configurations représentatives*

Les domaines MD peuvent être combinés de diverses façons pour constituer le système MHS. Les configurations organisationnelles possibles sont illimitées en nombre et ne peuvent donc pas être énumérées. On trouvera toutefois ci-après, ainsi qu'à la figure 10/X.402, la description de quelques configurations représentatives importantes.

14.2.1 *Système MHS entièrement centralisé*

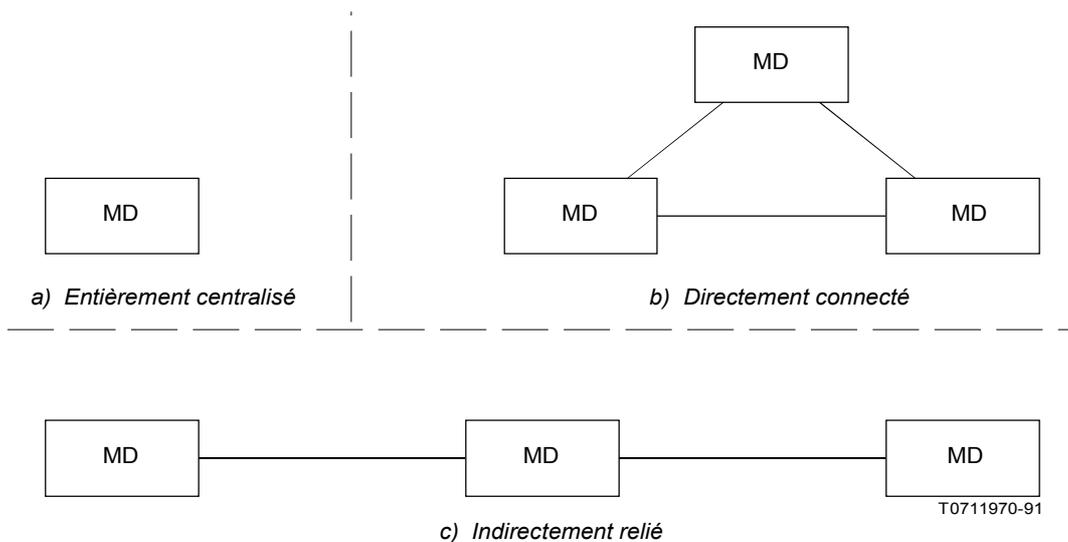
L'ensemble du système MHS peut être géré par une organisation [partie *a*] de la figure 10/X.402]. Cette conception s'effectue avec un seul domaine MD.

14.2.2 Système MHS connecté directement

Le système MHS peut être géré par plusieurs organisations, les systèmes de messagerie de chacune d'elles étant connectés aux systèmes de messagerie de toutes les autres [partie *b*) de la figure 10/X.402]. Cette conception s'effectue à l'aide de multiples domaines MD interconnectés par paire.

14.2.3 Système MHS connecté indirectement

Le système MHS peut être géré par plusieurs organisations, les systèmes de messagerie de chacune d'elles servant d'intermédiaire entre les systèmes de messagerie des autres [partie *c*) de la figure 10/X.402]. Cette conception est réalisée par plusieurs domaines MD, chacun étant interconnecté avec tous les autres.



Remarque – Outre les configurations organisationnelles résultant des approches «pures» ci-après, de nombreuses configurations «hybrides» peuvent être élaborées.

FIGURE 10/X.402

Configurations représentatives organisationnelles

15 Le système MHS mondial

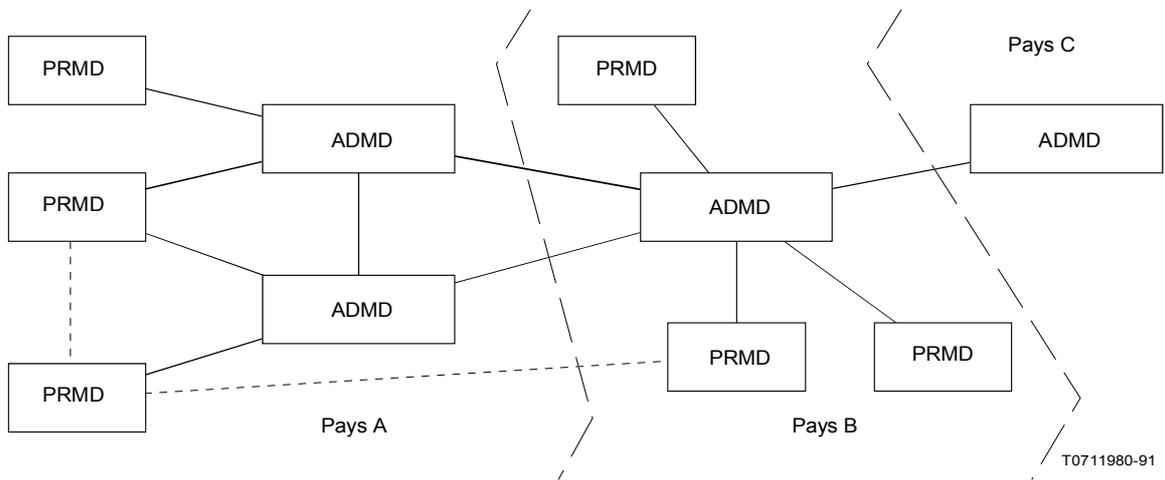
Un des principaux buts de la présente Recommandation et d'autres Recommandations de la même série est de permettre l'élaboration du **système MHS mondial**, un système MHS fournissant à l'échelle mondiale un service de messagerie à la fois à l'intérieur d'une organisation et entre organisations, et au niveau national et international.

Il est presque certain que le système MHS mondial comprendra toutes les configurations fonctionnelles spécifiées au § 12.

La configuration physique du système MHS mondial est un hybride, extrêmement complexe et physiquement très décentralisé, des configurations pures spécifiées au § 13.

La configuration organisationnelle du système MHS mondial est un hybride, extrêmement complexe et fortement décentralisé au niveau de l'organisation, des configurations pures spécifiées dans le § 14.

La figure 11/X.402 représente un exemple d'interconnexions possibles. Elle ne vise pas à identifier toutes les configurations possibles. Selon cette figure, les domaines ADMD jouent un rôle central dans le système MHS mondial. En s'interconnectant à l'échelle internationale, ils constituent la base d'un transfert international de messages. En fonction des réglementations nationales, ils peuvent représenter également, en s'interconnectant à l'échelle nationale, la base des transferts nationaux de messages associés à l'international.



Remarque – La disponibilité des interconnexions représentées en pointillés entre les agents PRMD peut dépendre de la réglementation.

FIGURE 11/X.402
Le système MHS mondial

16 Présentation générale

La présente section décrit la dénomination et l'adressage des utilisateurs et des DL ainsi que l'acheminement des objets d'information vers ceux-ci.

Elle traite des sujets suivants:

- a) dénomination;
- b) adressage;
- c) acheminement.

17 Dénomination

Le présent paragraphe spécifie comment les utilisateurs et les DL sont nommés aux fins de messagerie en général et de transfert de messages en particulier. Il définit les *noms d'O/R* et décrit le rôle que les noms d'annuaire jouent dans ces noms.

En présentant directement un message ou un envoi-test, un agent UA ou une mémoire MS indique au système MTS ses destinataires potentiels. Lorsque le système MTS livre un message, il identifie l'expéditeur pour l'agent UA ou la mémoire MS de chaque destinataire. Les *noms d'O/R* sont les structures de données par lesquelles cette identification s'effectue.

17.1 Noms d'annuaire

Un nom d'annuaire est une composante d'un *nom d'O/R*. Il identifie un objet pour l'annuaire. En présentant ce nom à l'annuaire, le système MHS peut accéder à une entrée de l'annuaire de l'utilisateur ou de la liste DL. A partir de cette entrée, le MTS peut obtenir, par exemple, l'*adresse d'O/R* de l'utilisateur ou de la liste DL.

Les utilisateurs ou les listes DL n'étant pas tous inscrits dans l'annuaire, ils ne possèdent pas tous un nom d'annuaire.

Remarque 1 – De nombreux utilisateurs et listes DL n'auront pas de nom d'annuaire tant que l'annuaire ne sera pas largement diffusé en tant que complément du système MHS. De nombreux utilisateurs indirects (par exemple, les clients des services postaux) n'auront pas de nom d'annuaire tant que l'annuaire ne sera pas largement diffusé en tant que complément des autres systèmes de communication.

Remarque 2 – Les utilisateurs et les listes DL peuvent recevoir des noms d'annuaire même avant la mise en place et la diffusion d'un annuaire entièrement interconnecté, si l'on définit à l'avance les autorités éventuellement chargées de la dénomination pour celui-ci.

Remarque 3 – Le nom d'annuaire type est plus facile à utiliser et plus stable que l'*adresse d'O/R* type car celle-ci s'exprime nécessairement sous forme de structure organisationnelle ou physique du système MHS, ce qui n'est pas obligatoirement le cas du nom d'annuaire. C'est pourquoi on prévoit qu'à long terme, les noms d'annuaire deviendront le principal moyen d'identification des utilisateurs et des listes DL à l'extérieur du système MTS (c'est-à-dire par d'autres utilisateurs) et que l'utilisation des *adresses d'O/R* sera en grande partie limitée au système MTS (pour utilisation, par exemple, par les agents MTA).

17.2 Noms d'O/R

Chaque utilisateur ou liste DL possède au moins un *nom d'O/R*. Un **nom d'O/R** est un identificateur permettant de désigner un utilisateur comme étant l'expéditeur, ou un utilisateur ou une liste DL comme étant un destinataire potentiel d'un message ou d'un envoi-test. Un nom d'O/R distingue un utilisateur ou une liste DL d'un ou d'une autre et peut également identifier son point d'accès au système MHS.

Un nom d'O/R comprend un nom d'annuaire, une *adresse d'O/R*, ou les deux à la fois. S'il est présent (et valable), le nom d'annuaire identifie sans ambiguïté l'utilisateur ou la liste DL (mais il n'est pas nécessairement le seul nom à le faire). Si elle est présente, l'*adresse d'O/R* remplit les mêmes fonctions, auxquelles s'en ajoutent d'autres (voir le § 18.5).

En dépôt direct, l'agent UA ou la mémoire MS de l'expéditeur d'un message ou d'un envoi-test peut comprendre l'un de ces deux éléments ou les deux dans chaque nom d'O/R qu'il (elle) fournit. Si l'adresse d'O/R a été omise, le système MTS l'obtient par l'annuaire grâce au nom d'annuaire. Si le nom d'annuaire est omis, le système MTS agit sans lui. Si les deux indications sont disponibles, le système MTS se base en premier lieu sur l'*adresse d'O/R*. S'il détermine que l'*adresse d'O/R* n'est pas valable (par exemple, périmée), il procède alors comme si elle avait été omise et se base sur le nom d'annuaire.

Lors de la remise d'un message, le système MTS inclut une *adresse d'O/R* et, si possible, un nom d'annuaire dans chaque nom d'O/R qu'il fournit au destinataire d'un message ou à l'expéditeur d'un message ou d'un envoi-test sujet d'un rapport. Le nom d'annuaire est communiqué s'il a été fourni par l'expéditeur ou s'il a été spécifié en tant que membre d'une liste DL développée.

Remarque – Un réacheminement ou un développement de la liste DL peut obliger le système MTS à transmettre à un agent UA ou une mémoire MS, au moment de la remise, des noms d'O/R que l'agent UA ou la mémoire MS n'a pas fourni en dépôt direct.

Pour obtenir des informations sur les organisations opérant dans deux pays ou plus, se reporter à l'annexe G, ainsi qu'au § 7.3.2 de la Rec. X.400 du CCITT | ISO/CEI 10021-1.

18 Adressage

Le présent paragraphe spécifie l'adressage des utilisateurs et des listes DL. Elle définit les *adresses d'O/R*, décrit la structure des *listes d'attributs* à partir desquelles ces adresses sont constituées, traite des jeux de caractères à partir desquels des *attributs* individuels sont composés, fixe les règles servant à déterminer que deux *listes d'attributs* sont équivalentes et à inclure des *attributs* conditionnels dans ces listes, et définit les *attributs normalisés* susceptibles d'apparaître dans ces listes.

Pour transmettre un message, un envoi-test ou un rapport à un utilisateur, ou pour développer une liste DL spécifiée comme étant un destinataire potentiel d'un message ou d'un envoi-test, le système MTS doit localiser l'utilisateur ou la liste DL en fonction de ses propres structures physiques et organisationnelles. Les *adresses d'O/R* sont les structures de données permettant d'effectuer toutes ces localisations.

18.1 Listes d'attributs

Les *adresses d'O/R* des utilisateurs et des listes DL sont des listes d'attributs. Une **liste d'attributs** est un ensemble ordonné d'*attributs*.

Un **attribut** est un élément d'information décrivant un utilisateur ou une liste DL capable également de localiser cet utilisateur ou cette liste DL par rapport à la structure physique ou organisationnelle du système MHS (ou du réseau sous-jacent).

Un attribut est composé des parties suivantes:

- a) **type d'attribut** (ou **type**): identificateur indiquant une classe d'information (par exemple, noms personnels).
- b) **valeur d'attribut** (ou **valeur**): instance de la classe d'information indiquée par le type d'attribut (par exemple, un nom personnel spécifique).

Les attributs sont de deux sortes, à savoir:

- a) **attribut normalisé**: un attribut dont le type est lié par la présente Recommandation à une classe d'information.

La valeur de chaque attribut normalisé, à l'exception du *type de terminal*, est soit une chaîne, soit un ensemble de chaînes.

- b) **attribut défini-par-domaine**: un attribut dont le type est lié à une classe d'information par un domaine MD. Par conséquent, le type et la valeur d'un attribut défini par-domaine sont définis par un domaine MD. Le domaine MD est identifié par un *nom de domaine privé*, un *nom de domaine d'administration*, ou les deux.

Le type et la valeur de chaque attribut défini-par-domaine sont des chaînes ou des ensembles de chaînes.

Remarque – L'utilisation très répandue d'attributs normalisés permet d'obtenir des adresses d'O/R plus uniformes et, en conséquence, plus faciles à utiliser. On prévoit cependant que les domaines MD ne pourront pas tous utiliser immédiatement ces attributs. Les attributs définis par domaine ont pour but de permettre à un domaine MD de maintenir pour un moment ses conventions d'adressage nationales existantes. On prévoit toutefois que tous les domaines MD finiront par utiliser des attributs normalisés et que les attributs définis-par-domaine ne seront utilisés que pour une période intérimaire.

18.2 *Jeux de caractères*

Les valeurs d'attributs normalisés et les types et valeurs d'attributs définis par domaine sont constitués à partir de chaînes numériques, imprimables et télétext de la façon suivante:

- a) le type ou la valeur d'un attribut défini-par-domaine particulier peut être une chaîne imprimable, une chaîne télétext, ou les deux. Le même choix doit être effectué pour le type et la valeur;
- b) les types des chaînes à partir desquelles les valeurs d'attributs normalisés peuvent être constituées et leur constitution (par exemple, en une chaîne ou en plusieurs) varient d'un attribut à l'autre (voir le § 18.3).

La valeur d'un attribut comprend des chaînes composées, selon son type, de l'un des ensembles suivants: uniquement numérique, uniquement imprimable, numérique et imprimable, numérique et télétext. Dans ce domaine, les règles ci-après régissent chaque type de communication:

- a) pour le nom de domaine d'administration, le nom de domaine privé et le code postal, la même valeur numérique peut être représentée par une chaîne numérique ou imprimable;
- b) lorsque les chaînes imprimable et télétext sont toutes deux autorisées, des chaînes de l'une de ces catégories ou des deux à la fois peuvent être fournies. Si à la fois des chaînes imprimables et des chaînes télétext sont fournies, elles doivent toutes identifier sans ambiguïté le même utilisateur.

La longueur de chaque chaîne et de chaque séquence de chaînes d'un attribut doit être limitée selon les indications fournies dans la spécification plus détaillée des attributs (à savoir, l'ASN.1) contenue dans la Recommandation X.411.

Remarque 1 – Des chaînes télétext sont autorisées dans les valeurs d'attributs pour permettre l'inclusion, par exemple, des caractères accentués communément utilisés dans de nombreux pays.

Remarque 2 – Les règles d'adaptation vers le bas énoncées dans l'annexe B de la Rec. X.419 du CCITT | ISO/CEI 10021-6 stipulent qu'il est impossible d'adapter vers le bas une adresse d'O/R si seule la chaîne télétext a été fournie et contient des caractères n'appartenant pas au répertoire de la chaîne imprimable.

18.3 *Attributs normalisés*

Les différents types d'attributs normalisés sont énumérés dans la première colonne du tableau 9/X.402. Pour chaque type cité, la deuxième colonne indique les jeux de caractères – numérique, imprimable et télétext – d'où les valeurs d'attributs peuvent être tirées.

Le tableau 9/X.402 se divise en trois sections. Les types d'attributs de la première sont de portée assez générale, ceux de la deuxième portent sur l'*acheminement vers* un système de remise physique PDS, et ceux de la troisième section portent sur l'*adressage dans* un système PDS.

Les types d'attributs normalisés, résumés dans le tableau 9/X.402, sont définis et décrits dans les paragraphes qui suivent.

18.3.1 *Nom de domaine d'administration*

Un attribut **nom de domaine d'administration (administration-domain-name)** est un attribut normalisé qui identifie un domaine ADMD relatif au pays représenté par un nom-de-pays.

La valeur d'un nom de domaine d'administration est une chaîne numérique ou imprimable sélectionnée dans un ensemble de chaînes de ce type administré à cette fin par le pays précité.

TABLEAU 9/X.402

Attributs normalisés

Type d'attribut normalisé	Jeux de caractères		
	NUM	PRT	TTX
<i>Généraux</i>			
Nom de domaine d'administration (<i>administration-domain-name</i>)	×	×	–
Nom courant (<i>common-name</i>)	–	×	×
Nom de pays (<i>country-name</i>)	×	×	–
Adresse réseau (<i>network-address</i>)	× ^{a)}	–	–
Identificateur numérique d'utilisateur (<i>numeric-user-identifier</i>)	×	–	–
Nom d'organisation (<i>organization-name</i>)	–	×	×
Noms d'unités organisationnelles (<i>organizational-unit-names</i>)	–	×	×
Nom personnel (<i>personal-name</i>)	–	×	×
Nom de domaine privé (<i>private-domain-name</i>)	×	×	–
Identificateur de terminal (<i>terminal-identifier</i>)	–	×	–
Type de terminal (<i>terminal-type</i>)	–	–	–
<i>Acheminement postal</i>			
Nom de système de remise physique (<i>pds-name</i>)	–	×	–
Nom de pays de remise physique (<i>physical-delivery-country-name</i>)	×	×	–
Code postal (<i>postal-code</i>)	×	×	–
<i>Adresse postale</i>			
Extension des composantes d'adresse O/R postale (<i>extension-postal-O/R-address-components</i>)	–	×	×
Extension des composantes d'adresse de remise physique (<i>extension-physical-delivery-address-components</i>)	–	×	×
Attributs postaux locaux (<i>local-postal-attributes</i>)	–	×	×
Nom de bureau de remise physique (<i>physical-delivery-office-name</i>)	–	×	×
Numéro de bureau de remise physique (<i>physical-delivery-office-number</i>)	–	×	×
Nom d'organisation de remise physique (<i>physical-delivery-organization-name</i>)	–	×	×
Nom personnel de remise physique (<i>physical-delivery-personal-name</i>)	–	×	×
Adresse de boîte postale (<i>post-office-box-address</i>)	–	×	×
Adresse de poste restante (<i>poste-restante-address</i>)	–	×	×
Adresse de rue (<i>street-address</i>)	–	×	×
Adresse postale non formatée (<i>unformatted-postal-address</i>)	–	×	×
Nom postal unique (<i>unique-postal-name</i>)	–	×	×

NUM Numérique

PRT Imprimable

TTX Télétex

× Permis

a) Séquence de chaînes d'octets dans certaines circonstances.

Remarque – La valeur d'attribut comprenant un seul espace (« ») doit être réservée aux fins suivantes. S'il est autorisé par le pays représenté par l'attribut nom de pays, un seul espace doit désigner n'importe quel domaine ADMD (c'est-à-dire tous les domaines ADMD) existant dans ce pays. Cela concerne à la fois l'identification des utilisateurs dans le pays et l'acheminement des messages, envois-tests et rapports vers les domaines ADMD de ce pays et entre eux. Pour ce qui est de l'identification des utilisateurs, cela implique que les adresses d'O/R des utilisateurs du pays soient choisies de façon à ne comporter aucune ambiguïté, même en l'absence des noms effectifs des domaines ADMD des utilisateurs. Du point de vue de la deuxième fonction, cette valeur d'attribut permet à la fois aux domaines PRMD situés à l'intérieur du pays et aux domaines ADMD installés à l'extérieur de ce pays, d'acheminer des messages, des envois-tests et des rapports vers l'un des domaines ADMD situés à l'intérieur du pays et implique que ceux-ci s'interconnectent de sorte que les messages, les envois-tests et les rapports soient transmis à leurs destinataires.

18.3.2 *Nom courant (common-name)*

Un **nom courant (common-name)** est un attribut normalisé identifiant un utilisateur ou une liste DL par rapport à l'entité représentée par un autre attribut (par exemple, le nom d'une organisation).

La valeur d'un nom courant est une chaîne imprimable, une chaîne télétexte ou les deux à la fois. Qu'elle soit imprimable ou télétexte, la chaîne est sélectionnée dans un ensemble de chaînes de ce type administré à cette fin (et éventuellement à d'autres fins) par l'entité précitée.

Remarque – Parmi beaucoup d'autres possibilités, un nom courant pourrait identifier un rôle organisationnel (par exemple, «Directeur du service de marketing»).

18.3.3 *Nom de pays (country-name)*

Un **nom de pays (country-name)** est un attribut normalisé identifiant un pays.

La valeur d'un nom de pays est une chaîne numérique indiquant l'un des numéros attribués au pays par la Recommandation X.121 ou une chaîne imprimable donnant la paire de caractères attribuée au pays par ISO 3166.

18.3.4 *Extension des composantes d'adresse O/R postale (extension-postal-O/R-address-components)*

L'attribut **extension des composantes d'adresse O/R postale (extension-postal-O/R-address-components)** est un attribut normalisé qui fournit, dans une adresse postale, des informations additionnelles nécessaires à l'identification du destinataire (par exemple, une unité organisationnelle).

La valeur d'un attribut extension des composantes d'adresse O/R postale est une chaîne imprimable, une chaîne télétexte, ou les deux à la fois.

18.3.5 *Extension des composantes d'adresse de remise physique (extension-physical-delivery-address-components)*

Un attribut **extension des composantes d'adresse de remise physique (extension-physical-delivery-address-components)** est un attribut normalisé qui spécifie, dans une adresse postale, des informations additionnelles nécessaires à l'identification du point exact de remise (par exemple, numéros de l'étage et du bureau, dans un grand bâtiment).

La valeur d'un attribut extension des composantes d'adresse de remise physique est une chaîne imprimable, une chaîne télétexte, ou les deux à la fois.

18.3.6 *Attributs postaux locaux (local-postal-attributes)*

Les **attributs postaux locaux (local-postal attributes)** sont des attributs normalisés identifiant le lieu de distribution, autre que celui indiqué par un attribut nom de bureau de remise physique (par exemple, une zone géographique), de messages physiques d'un utilisateur.

La valeur d'un attribut de type attributs postaux locaux est une chaîne imprimable, une chaîne télétexte, ou les deux à la fois.

18.3.7 *Adresse réseau (network-address)*

Un attribut **adresse réseau (network-address)** est un attribut normalisé qui fournit l'adresse réseau d'un terminal.

La valeur d'un attribut adresse-réseau est l'une des valeurs suivantes:

- a) une chaîne numérique régie par la Recommandation X.121;
- b) deux chaînes numériques régies par les Recommandations E.163 ou E.164;
- c) une adresse du point d'accès au service de présentation PSAP.

Remarque – Parmi les chaînes admises par la Recommandation X.121, on note des numéros de télex et de téléphone précédés d'un chiffre d'échappement.

18.3.8 *Identificateur numérique d'utilisateur (numeric-user-identifier)*

Un attribut **identificateur numérique d'utilisateur (numeric-user-identifier)** est un attribut normalisé qui identifie numériquement un utilisateur par rapport au domaine MD indiqué par un nom de domaine d'administration, un nom de domaine privé ou les deux.

La valeur d'un attribut Identificateur numérique d'utilisateur est une chaîne numérique sélectionnée dans un ensemble de chaînes de ce type régi à cette fin par le domaine MD précité.

18.3.9 *Nom d'organisation (organization-name)*

Un attribut **nom d'organisation (organization-name)** est un attribut normalisé qui identifie une organisation. La valeur d'un nom d'organisation est une chaîne imprimable, une chaîne télétexte, ou les deux à la fois.

Lorsqu'elles apparaissent dans une *adresse d'O/R mnémotechnique* (voir le § 18.5.1), sur le plan national, les organisations peuvent être identifiées soit par rapport au pays désigné par un nom de pays (de sorte que les noms d'organisation soient uniques dans ce pays), soit par rapport au domaine MD désigné par un nom de domaine privé, un nom de domaine d'administration, ou les deux. Qu'elle soit imprimable ou télétexte, la chaîne est sélectionnée dans un ensemble de chaînes de ce type régi à cette fin (et éventuellement à d'autres fins) par le pays ou le domaine MD précité.

Remarque – Dans les pays qui choisissent des noms d'organisation uniques pour tout le pays, une autorité nationale d'enregistrement des noms d'organisation est nécessaire.

Lorsqu'il apparaît dans une *adresse d'O/R de terminal* (voir le § 18.5.4), le nom d'organisation est une valeur à structure non imposée, sans spécification d'enregistrement.

18.3.10 *Noms d'unités organisationnelles (organizational-units-names)*

Un attribut **noms d'unités organisationnelles (organizational-units-names)** est un attribut normalisé qui identifie une ou plusieurs unités (par exemple, divisions ou départements) de l'organisation représentée par un nom d'organisation, chacune étant, à l'exception de la première, une sous-unité des unités nommées avant elle dans l'attribut.

La valeur d'un attribut noms d'unités organisationnelles est une séquence ordonnée de chaînes imprimables, de chaînes télétexte, ou les deux à la fois. Qu'elle soit imprimable ou télétexte, chaque chaîne est sélectionnée dans un ensemble de chaînes de ce type régi à cette fin (et éventuellement à d'autres fins) par l'organisation (ou l'unité englobante) précitée.

18.3.11 *Nom de service de remise physique (nom de pds) (pds-name)*

Un attribut **nom de service de remise physique (nom de pds) (pds-name)** est un attribut normalisé qui identifie un système PDS par rapport au domaine MD représenté par un nom de domaine d'administration, un nom de domaine privé ou les deux.

La valeur d'un nom de pds est une chaîne imprimable sélectionnée dans un ensemble de chaînes de ce type régi à cette fin par le domaine MD précité.

18.3.12 *Nom personnel (personal-name)*

Un attribut **nom personnel (personal-name)** est un attribut normalisé qui identifie une personne par rapport à l'entité désignée par un autre attribut (ou, par exemple, un nom d'organisation).

La valeur d'un nom personnel comprend les quatre éléments d'information suivants, le premier étant obligatoire et les trois autres facultatifs:

- a) le nom de la personne;
- b) le prénom de la personne;

- c) les initiales de tous les noms autres que le nom de famille de la personne;
- d) l'indication de sa génération (par exemple, «fils»).

Les informations ci-dessus sont données sous forme de chaînes imprimables, de chaînes télétext, ou des deux à la fois.

18.3.13 *Nom de pays de remise physique (physical-delivery-country-name)*

Un attribut **nom de pays de remise physique (physical-delivery-country-name)** est un attribut normalisé qui identifie le pays dans lequel un utilisateur reçoit des messages physiques.

La valeur d'un nom de pays de remise physique est soumise aux mêmes contraintes que la valeur d'un nom de pays.

18.3.14 *Nom de bureau de remise physique (physical-delivery-office-name)*

Un attribut **nom de bureau de remise physique (physical-delivery-office-name)** est un attribut normalisé qui identifie la ville, le village, etc. où est situé le bureau de poste par lequel un utilisateur reçoit des messages physiques.

La valeur d'un tel attribut est une chaîne imprimable, une chaîne télétext, ou les deux à la fois.

18.3.15 *Numéro de bureau de remise physique (physical-delivery-office-number)*

Un attribut **numéro de bureau de remise physique (physical-delivery-office-number)** est un attribut normalisé qui permet de distinguer les divers bureaux de poste représentés par un seul nom de bureau de remise physique.

La valeur de cet attribut est une chaîne imprimable, une chaîne télétext, ou les deux à la fois.

18.3.16 *Nom d'organisation de remise physique (physical-delivery-organization-name)*

Un attribut **nom d'organisation de remise physique (physical-delivery-organization-name)** est un attribut normalisé qui identifie une organisation de client des services postaux.

La valeur d'un nom d'organisation de remise physique est une chaîne imprimable, une chaîne télétext, ou les deux à la fois.

18.3.17 *Nom personnel de remise physique (physical-delivery-personal-name)*

Un attribut **nom personnel de remise physique (physical-delivery-personal-name)** est un attribut normalisé qui identifie un client des services postaux.

La valeur d'un nom personnel de remise physique est une chaîne imprimable, une chaîne télétext, ou les deux à la fois.

18.3.18 *Adresse de boîte postale (post-office-box-address)*

Un attribut **adresse de boîte postale (post-office-box-address)** est un attribut normalisé qui spécifie le numéro de la boîte postale par laquelle un utilisateur reçoit des messages physiques.

La valeur d'une adresse de boîte postale est une chaîne imprimable, une chaîne télétext, ou les deux à la fois, sélectionnée(s) dans l'ensemble de chaînes de ce type attribué à cette fin par le bureau postal indiqué par un attribut nom de bureau de remise physique.

18.3.19 *Code postal (postal-code)*

Un attribut **code postal (postal-code)** est un attribut normalisé qui spécifie le code postal de la zone géographique dans laquelle un utilisateur reçoit des messages physiques.

La valeur d'un code postal est une chaîne numérique ou imprimable sélectionnée dans l'ensemble de chaînes de ce type conservé et normalisé à cette fin par l'Administration postale du pays identifié par un attribut nom de pays de remise physique.

18.3.20 *Adresse de poste restante (poste-restante-address)*

Un attribut **adresse de poste restante (poste-restante-address)** est un attribut normalisé qui spécifie le code qu'un utilisateur fournit à un bureau de poste afin de regrouper les messages physiques en attente de remise à cet utilisateur.

La valeur d'une adresse de poste restante est une chaîne imprimable, une chaîne télétex, ou les deux à la fois, sélectionnée(s) dans l'ensemble de chaînes de ce type affecté à cette fin par le bureau de poste indiqué par un attribut nom de bureau de remise physique.

18.3.21 *Nom de domaine privé (private-domain-name)*

Un attribut **nom de domaine privé (private-domain-name)** est un attribut normalisé qui identifie un domaine PRMD. Sur le plan national, l'identification peut s'effectuer soit par rapport au pays indiqué par un nom de pays (de manière que les noms des domaines PRMD soient uniques dans ce pays), soit par rapport au domaine ADMD indiqué par un nom de domaine d'administration.

La valeur d'un nom de domaine privé est une chaîne imprimable sélectionnée dans un ensemble de chaînes de ce type régi à cette fin par le pays ou le domaine ADMD précité.

Remarque – Dans les pays qui choisissent des noms de domaines PRMD uniques pour tout le pays, une autorité nationale d'enregistrement des noms de domaine privé est nécessaire.

18.3.22 *Adresse de rue (street-address)*

Un attribut **adresse de rue (street-address)** est un attribut normalisé qui spécifie l'adresse de rue [par exemple, le numéro de l'habitation, le numéro et le type de la rue (par exemple, «Route»)] à laquelle un utilisateur reçoit des messages physiques.

La valeur d'une adresse de rue est une chaîne imprimable, une chaîne télétex ou les deux.

18.3.23 *Identificateur de terminal (terminal-identifier)*

Un attribut **identificateur de terminal (terminal-identifier)** est un attribut normalisé qui fournit l'identificateur d'un terminal (par exemple, un indicatif télex ou un identificateur de terminal télétex).

La valeur d'un identificateur de terminal est une chaîne imprimable.

18.3.24 *Type de terminal (terminal-type)*

Un attribut **type de terminal (terminal-type)** est un attribut normalisé qui fournit le type d'un terminal.

La valeur d'un type de terminal est l'une des valeurs suivantes: *télex*, *télétex*, *télécopie G3*, *télécopie G4*, *terminal IA5* et *vidéotex*.

18.3.25 *Adresse postale non formatée (unformatted-postal-address)*

Un attribut **adresse postale non formatée (unformatted-postal-address)** est un attribut normalisé qui spécifie l'adresse postale d'un utilisateur dans un format non imposé.

La valeur d'une adresse postale non formatée est soit une séquence de chaînes imprimables, chacune représentant une ligne de texte, soit une seule chaîne télétex, les lignes étant séparées selon les spécifications concernant ce type de chaînes, soit les deux à la fois.

18.3.26 *Nom postal unique (unique-postal-name)*

Un attribut **nom postal unique (unique-postal-name)** est un attribut normalisé qui identifie le point de remise, autre que celui qui est indiqué par une adresse de rue, une adresse de boîte postale, ou une adresse de poste restante (par exemple, un bâtiment ou un hameau), des messages physiques d'un utilisateur.

La valeur d'un nom postal unique est une chaîne imprimable, une chaîne télétex, ou les deux.

18.4 *Equivalence entre les listes d'attributs*

Plusieurs adresses d'O/R, et, par conséquent, plusieurs listes d'attributs, peuvent indiquer le même utilisateur ou la même liste DL. Cette multiplicité d'adresses d'O/R est en partie (mais pas totalement) due aux règles d'équivalence entre les listes d'attributs spécifiées ci-après:

- a) l'ordre relatif des attributs normalisés est non significatif;
- b) lorsque la valeur d'un attribut normalisé peut être une chaîne numérique ou une chaîne imprimable équivalente, le choix entre ces deux types de chaînes doit être considéré comme non significatif.

Remarque – Cette règle s'applique même à l'attribut normalisé nom de pays lorsque le choix entre les formes de la Recommandation X.121 ou de la norme ISO 3166 doit être considéré comme non significatif. Lorsque la Recommandation X.121 attribue plusieurs numéros à un pays, la signification du numéro utilisé n'a pas été normalisée par la présente Recommandation.

- c) lorsque la valeur d'un attribut normalisé peut être une chaîne imprimable, une chaîne télételex équivalente, ou les deux à la fois, le choix entre ces trois possibilités doit être considéré comme non significatif;
- d) lorsque le type ou la valeur d'un attribut défini par domaine, ou la valeur d'un attribut normalisé, comporte des caractères du répertoire Chaîne imprimable, le choix, lorsqu'il est autorisé, entre un codage en chaîne télételex et un codage en chaîne imprimable, doit être considéré comme non significatif;
- e) lorsque la valeur d'un attribut normalisé peut contenir des lettres, les types de caractères de ces lettres doivent être considérés comme non significatifs;
- f) dans un type ou une valeur d'attribut défini par domaine, ou dans une valeur d'attribut normalisé, tous caractères d'espacement placés au début et à la fin du texte, ainsi que, au-delà du premier, tous les caractères d'espacement consécutifs placés entre deux mots doivent être considérés comme non significatifs;
- g) dans une chaîne télételex, le caractère graphique de soulignement à chasse nulle doit être considéré comme non significatif, de même que toutes les fonctions de commande, à l'exception de la fonction d'espacement et des fonctions utilisées pour les procédures d'extension de code;
- h) dans une chaîne télételex, le choix du codage pour le même caractère doit être considéré comme non significatif.

Remarque – Un domaine MD peut imposer des règles d'équivalence supplémentaires aux attributs qu'il affecte à ses propres utilisateurs et listes DL. Il peut définir, par exemple, des règles concernant les caractères de ponctuation dans les valeurs d'attributs, le type de caractères des lettres dans ces valeurs, ou l'ordre relatif des attributs définis par domaine.

18.5 *Formes d'adresses d'O/R*

A chaque utilisateur ou liste DL sont attribuées une ou plusieurs adresses d'O/R. Une **adresse d'O/R** est une liste d'attributs qui distingue un utilisateur d'un autre et identifie le point d'accès de l'utilisateur au MHS ou le point de développement de la liste DL.

Une adresse d'O/R peut prendre l'une quelconque des formes résumées dans le tableau 10/X.402. La première colonne de ce tableau définit les attributs disponibles pour l'élaboration des adresses d'O/R. Pour chaque forme d'adresse d'O/R, la deuxième colonne indique les attributs pouvant apparaître dans ces adresses d'O/R et leurs degrés (voir également le § 18.6).

Le tableau 10/X.402 comporte quatre sections. Les types d'attributs de la première sont d'ordre général. Les types d'attributs de la deuxième et de la troisième sont propres à la remise physique, mais l'adresse postale non formatée peut être utilisée comme une extension de l'adresse de terminal. La quatrième section couvre les attributs définis par domaine.

Les formes d'adresse d'O/R, résumées dans le tableau 10/X.402, sont définies et décrites individuellement ci-dessous.

TABLEAU 10/X.402

Formes d'adresse d'O/R

Type d'attribut	Formes d'adresse d'O/R				
	MNEM	NUMR	POST		TERM
			F	U	
<i>Généraux</i>					
Nom de domaine d'administration (<i>administration-domain-name</i>)	M	M	M	M	C
Nom courant (<i>common-name</i>)	C	-	-	-	C*
Nom de pays (<i>country-name</i>)	M	M	M	M	C
Adresse réseau (<i>network-address</i>)	-	-	-	-	M
Identificateur numérique d'utilisateur (<i>numeric-user-identifier</i>)	-	M	-	-	-
Nom d'organisation (<i>organization-name</i>)	C	-	-	-	C*
Noms d'unités organisationnelles (<i>organizational-unit-names</i>)	C	-	-	-	C*
Nom personnel (<i>personal-name</i>)	C	-	-	-	C*
Nom de domaine privé (<i>private-domain-name</i>)	C	C	C	C	C
Identificateur de terminal (<i>terminal-identifier</i>)	-	-	-	-	C
Type de terminal (<i>terminal-type</i>)	-	-	-	-	C
<i>Acheminement postal</i>					
Nom de système de remise physique (<i>pds-name</i>)	-	-	C	C	-
Nom de pays de remise physique (<i>physical-delivery-country-name</i>)	-	-	M	M	-
Code postal (<i>postal-code</i>)	-	-	M	M	-
<i>Adresse postale</i>					
Extension des composantes d'adresse O/R postale (<i>extension-postal-O/R-address-components</i>)	-	-	C	-	-
Extension des composantes d'adresse de remise physique (<i>extension-physical-delivery-address-components</i>)	-	-	C	-	-
Attributs postaux locaux (<i>local-postal-attributes</i>)	-	-	C	-	-
Nom de bureau de remise physique (<i>physical-delivery-office-name</i>)	-	-	C	-	-
Numéro de bureau de remise physique (<i>physical-delivery-office-number</i>)	-	-	C	-	-
Nom d'organisation de remise physique (<i>physical-delivery-organization-name</i>)	-	-	C	-	-
Nom personnel de remise physique (<i>physical-delivery-personal-name</i>)	-	-	C	-	-
Adresse de boîte postale (<i>post-office-box-address</i>)	-	-	C	-	-
Adresse de poste restante (<i>poste-restante-address</i>)	-	-	C	-	-
Adresse de rue (<i>street-address</i>)	-	-	C	-	-
Adresse postale non formatée (<i>unformatted-postal-address</i>)	-	-	-	M	C*
Nom postal unique (<i>unique-postal-name</i>)	-	-	C	-	-
<i>Défini par domaine</i>					
Défini par domaine (un ou plus) (<i>domain-defined</i>)	C	C	-	-	C

MNEM Mnémotechnique

NUMR Numérique

POST Postal

TERM Terminal

C* Conditionnel, à utiliser à des fins de restitution mais pas pour l'adressage ou l'acheminement dans le système MHS

F Formaté

U Non formaté

M Obligatoire

C Conditionnel

18.5.1 Adresse d'O/R mnémotechnique

L'**adresse d'O/R mnémotechnique** fournit une identification facile à mettre en mémoire, tant pour un utilisateur que pour une liste DL. Elle identifie un domaine MD et un utilisateur ou une liste DL s'y rapportant.

Une adresse d'O/R mnémotechnique comprend les attributs suivants:

- a) un nom de pays, un nom de domaine d'administration et, dans certaines conditions, un nom de domaine privé qui, ensemble, identifient un domaine MD;
- b) un nom d'organisation, un nom d'unité organisationnelle, un nom personnel, un nom courant, un ou plusieurs attributs définis par domaine ou une combinaison de ces éléments qui identifie un usager ou une liste DL relatif au domaine MD du point a) ci-dessus. Si des noms d'unités organisationnelles sont présents, le nom d'organisation doit l'être aussi.

18.5.2 Adresse d'O/R numérique

L'**adresse d'O/R numérique** est une adresse qui identifie de façon numérique un utilisateur. Elle identifie un domaine MD et un utilisateur s'y rapportant.

Une adresse d'O/R numérique comprend les attributs suivants:

- a) un nom de pays, un nom de domaine d'administration et, dans certaines conditions, un nom de domaine privé qui, ensemble, identifient un domaine MD;
- b) un identificateur numérique d'utilisateur qui identifie l'utilisateur relatif au domaine MD du point a) ci-dessus;
- c) sous certaines conditions, un ou plusieurs attributs définis par domaine qui fournissent des informations supplémentaires à celles qui identifient l'utilisateur.

18.5.3 Adresse d'O/R postale

L'**adresse d'O/R postale** est celle qui identifie un utilisateur au moyen de son adresse postale. Elle identifie le système PDS par lequel l'utilisateur doit être atteint et fournit l'adresse postale de l'utilisateur.

On distingue deux types d'adresses d'O/R postales:

- a) **formatée**: adresse d'O/R postale spécifiant l'adresse postale d'un utilisateur au moyen de divers attributs. Pour ce type d'adresse d'O/R postale, la présente Recommandation prescrit de façon assez détaillée la structure des adresses postales.
- b) **non formatée**: adresse d'O/R postale spécifiant l'adresse postale d'un utilisateur dans un seul attribut. Pour ce type d'adresse d'O/R postale, la présente Recommandation ne prescrit pas dans son ensemble la structure des adresses postales.

Une adresse d'O/R postale, formatée ou non, comprend les attributs suivants:

- a) un nom de pays, un nom de domaine d'administration et, dans certaines conditions, un nom de domaine privé qui, ensemble, identifient un domaine MD;
- b) sous certaines conditions, un nom de PDS identifie le système PDS par lequel l'utilisateur doit être atteint;
- c) un nom de pays de remise physique et un code postal qui, ensemble, identifient la région géographique dans laquelle l'utilisateur reçoit des messages physiques.

Une adresse d'O/R postale formatée comprend en outre, à l'exception de l'adresse postale non formatée, un exemplaire de chacun des attributs d'adresse postale (voir le tableau 9/X.402) nécessaires au système PDS pour identifier le client des services postaux.

Une adresse d'O/R postale non formatée comprend, en outre, un attribut d'adresse postale non formatée.

Remarque – Les valeurs de tous les attributs, à l'exception du nom de pays, du nom de domaine d'administration et du nom de système de remise physique d'une adresse d'O/R postale ne doivent pas comporter un nombre total de caractères trop élevé pour que ces caractères puissent être présentés sur 6 lignes de 30 caractères chacune, format correspondant à la taille d'une fenêtre d'enveloppe physique type. L'algorithme de présentation est spécifique à l'unité PDAU, mais il est susceptible d'inclure des séparateurs (par exemple, des espaces) entre certaines valeurs d'attributs.

18.5.4 Adresse d'O/R du terminal

L'**adresse d'O/R du terminal** est une adresse qui identifie un utilisateur au moyen de l'adresse réseau et, si nécessaire, du type de terminal de cet utilisateur. Elle peut également identifier le domaine MD par lequel on accède à ce terminal. Dans le cas d'un terminal télématique, elle donne l'adresse réseau du terminal et, si possible, son identificateur de terminal et son type de terminal. Dans le cas d'un terminal télex, elle donne son numéro télex.

Une adresse d'O/R de terminal comprend les attributs suivants:

- a) une adresse réseau;
- b) sous certaines conditions, un identificateur de terminal;
- c) sous certaines conditions, un type de terminal;
- d) sous certaines conditions, un nom de pays et un nom de domaine d'administration et, dans certaines conditions, un nom de domaine privé qui, ensemble, identifient un domaine MD;
- e) sous certaines conditions, un ou plusieurs attributs choisis parmi le nom d'organisation, les noms d'unités organisationnelles, le nom personnel, l'adresse postale non formatée et le nom courant et, dans certaines conditions, un ou plusieurs attributs définis par domaine, qui fournissent tous des informations supplémentaires permettant d'identifier l'utilisateur.

L'attribut de nom de domaine privé et les attributs définis par domaine ne doivent être présents que si les attributs de nom de pays et de nom de domaine d'administration sont présents.

18.6 Attributs conditionnels

La présence ou l'absence dans une adresse d'O/R particulière, des attributs indiqués comme conditionnels au tableau 10/X.402 sont déterminées ci-après.

La présence de tous les attributs conditionnels propres aux adresses d'O/R postales dans une de ces adresses dépend des règles fixées par le domaine MD indiqué par les attributs nom de pays, nom de domaine d'administration et, s'il est présent, nom de domaine privé. Elle doit respecter ces règles.

Tous les attributs conditionnels propres aux adresses d'O/R postales sont, selon le cas, présents ou absents dans ces adresses de façon à respecter les spécifications d'adressage postal des utilisateurs qu'ils identifient.

19 Acheminement

Pour acheminer un message, un envoi-test, ou un rapport vers un utilisateur ou le point de développement d'une liste DL, un agent MTA doit non seulement localiser l'utilisateur ou la liste DL (c'est-à-dire obtenir son adresse d'O/R), mais également sélectionner un acheminement vers cet emplacement.

L'acheminement externe est un processus incrémentiel, qui n'est normalisé que dans ses grandes lignes. Plusieurs principes d'acheminement externe sont proposés ci-après. L'acheminement interne n'entre pas dans le cadre de la présente Recommandation.

Les principes ci-après sont indiqués à titre d'illustration, mais ne sont pas définitifs:

- a) dans un système MHS comprenant un seul domaine MD, la question de l'acheminement ne se pose naturellement pas;
- b) un domaine PRMD peut être relié à un domaine ADMD seul. Dans ce cas, l'acheminement fait nécessairement intervenir le domaine ADMD;
- c) un domaine ADMD peut être relié à plusieurs domaines PRMD. Dans ce cas, l'acheminement peut s'effectuer d'après des attributs d'adresses d'O/R conditionnels, notamment, mais pas exclusivement, d'après le nom de domaine privé;
- d) un domaine MD peut être relié directement à certains autres domaines MD, mais pas à tous. Lorsque l'adresse d'O/R identifie un domaine MD avec lequel il n'existe aucune connexion directe, l'acheminement peut s'effectuer selon des *accords bilatéraux* avec les domaines MD avec lesquels existent des connexions directes et d'autres règles locales;
- e) lorsque le domaine MD est directement relié au domaine MD identifié par l'adresse d'O/R, l'objet est, en règle générale, acheminé directement vers ce domaine MD;

- f) un *accord bilatéral*, peut permettre à un domaine MD d'acheminer un objet vers un autre domaine MD, par exemple, à des fins de conversion;
- g) un domaine MD peut acheminer un objet vers une adresse d'O/R incorrecte à condition (évidemment) qu'elle contienne au moins les attributs nécessaires à cet acheminement.

Remarque – Les accords bilatéraux et les règles locales susmentionnés n'entrent pas dans le cadre de la présente Recommandation et peuvent se fonder sur des considérations techniques, économiques, politiques, etc.

SECTION 5 – UTILISATION DE L'ANNUAIRE

20 Présentation générale

La présente section décrit les utilisations possibles de l'annuaire, lorsqu'il est présent, par le système MHS. Lorsque le système MHS ne peut accéder à l'annuaire, il revient aux autorités locales de décider des autres moyens dont il peut éventuellement disposer pour accomplir ces mêmes tâches.

La présente section couvre les sujets suivants:

- a) authentification;
- b) résolution de nom;
- c) développement d'une liste DL;
- d) évaluation des possibilités.

21 Authentification

Un objet fonctionnel peut accomplir les tâches d'authentification en utilisant les renseignements stockés dans l'annuaire.

22 Résolution de nom

Un nom fonctionnel peut accomplir une résolution de nom au moyen de l'annuaire.

Pour obtenir la ou les adresses d'O/R d'un utilisateur ou d'une liste DL dont il possède le nom d'annuaire, un objet présente ce nom à l'annuaire et demande à l'entrée d'annuaire les attributs suivants:

- a) *adresse d'O/R du système MHS;*
- b) *méthodes préférées de remise dans le système MHS.*

Pour y parvenir, l'objet doit d'abord s'authentifier auprès de l'annuaire et avoir droit d'accès aux renseignements requis.

23 Développement d'une liste DL

Un objet fonctionnel peut développer une liste DL au moyen de l'annuaire, en vérifiant tout d'abord que les autorisations de dépôt nécessaires existent.

Pour obtenir les membres d'une liste DL dont il possède le nom d'annuaire, l'objet présente ce nom à l'annuaire et demande à l'entrée d'annuaire les attributs suivants:

- a) *membres de la liste DL du système MHS;*
- b) *autorisations de dépôt de la liste DL du système MHS;*
- c) *méthodes préférées de remise dans le système MHS.*

Pour y parvenir, l'agent MTA doit tout d'abord s'authentifier auprès de l'annuaire et avoir droit d'accès aux renseignements requis.

24 Evaluation des capacités

Un objet fonctionnel peut évaluer les capacités d'utilisateur ou de mémoire MS au moyen de l'annuaire.

Les attributs d'annuaire suivants représentent les capacités d'utilisateur pouvant être significatives en messagerie:

- a) *longueur de contenu pouvant être remise dans le système MHS;*
- b) *types de contenus pouvant être remis dans le système MHS;*
- c) *types EIT pouvant être remis dans le système MHS;*
- d) *méthodes préférées de remise dans le système MHS.*

Les attributs d'annuaire suivants représentent les capacités de la mémoire MS pouvant être significatives en messagerie:

- a) *actions automatiques prises en charge dans le système MHS;*
- b) *types de contenus pris en charge dans le système MHS;*
- c) *attributs optionnels pris en charge dans le MHS.*

Pour évaluer une capacité particulière d'un utilisateur ou d'une mémoire MS dont il possède le nom d'annuaire, l'objet présente ce nom à l'annuaire et demande à l'entrée d'annuaire, l'attribut associé à cette capacité.

Pour y parvenir, l'agent MTA doit d'abord s'authentifier auprès de l'annuaire et avoir droit d'accès aux renseignements requis.

SECTION 6 – RÉALISATION OSI

25 Présentation générale

La présente section décrit la façon dont le système MHS est mis en œuvre au moyen de l'OSI.

Elle traite des sujets suivants:

- a) éléments de service d'application;
- b) contextes d'application.

26 Éléments de service d'application

Le présent paragraphe spécifie les éléments de service d'application (ASE) figurant dans la réalisation OSI de la messagerie.

Dans l'OSI, les capacités de communication des systèmes ouverts sont organisées en groupes de capacités liées entre elles, appelés éléments ASE. On trouvera ici l'analyse de ce concept sur la base du modèle de référence OSI, la distinction établie entre les éléments ASE *symétriques* et *asymétriques* et la présentation des éléments ASE conçus pour la messagerie ou la prenant en charge.

Remarque – Outre les éléments ASE étudiés dans la présente section, le système MHS compte sur l'élément de service d'accès à l'annuaire défini dans la Rec. X.519 du CCITT | ISO/CEI 9594-6. Cependant, cet élément ASE ne figurant pas dans les contextes d'application *AC* concernant la messagerie (voir la Rec. X.419 du CCITT | ISO/CEI 10021-6), il n'est pas étudié ici.

Ce concept est illustré à la figure 12/X.402, qui décrit deux systèmes ouverts communicants. Seules les parties des systèmes ouverts liées à l'OSI, appelées entités d'application AE, sont indiquées. Chaque entité AE comprend un élément d'utilisateur UE et un ou plusieurs éléments ASE. Un élément UE représente la partie commande ou organisation d'une entité AE qui définit le rôle du système ouvert (par exemple, celui d'un agent MTA). Un élément ASE représente un des ensembles de capacités de communication, ou services (par exemple, au dépôt ou au transfert de messages), dont l'élément UE a besoin pour remplir son rôle.

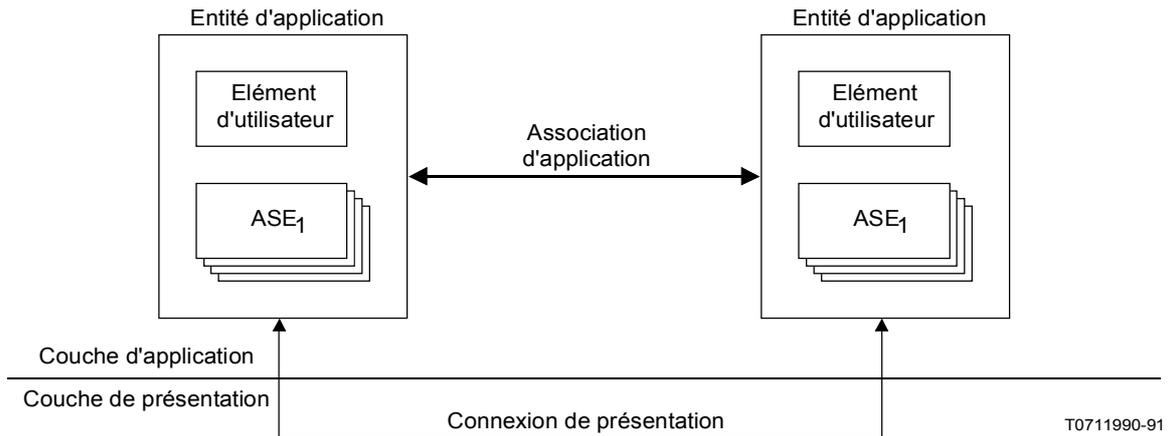


FIGURE 12/X.402
Le concept d'élément ASE

La relation entre deux entités AE dans différents systèmes ouverts est appelée association d'application. Les éléments ASE de chaque système ouvert communiquent avec leurs homologues dans l'autre système ouvert par l'intermédiaire d'une connexion de présentation entre eux. Cette communication constitue ce qui permet de créer et de maintenir la relation existant dans l'association d'application. Pour que la combinaison de plusieurs éléments ASE en une seule entité AE soit réussie, ces éléments ASE doivent être conçus de façon que leur utilisation de l'association d'application soit coordonnée.

Un élément ASE joue le rôle principalement mécanique de traduire les demandes et les réponses formulées par ses éléments UE dans et à partir de la forme prescrite par le protocole d'application régissant l'interaction de l'élément ASE avec son homologue dans le système ouvert auquel l'association le relie. L'élément ASE réalise un service abstrait, ou une partie de ce service, aux fins d'une communication OSI (voir la Rec. X.407 du CCITT | ISO/CEI 10021-3).

Remarque – A proprement parler, le rôle d'un système ouvert est déterminé par le comportement de ses processus d'application. Dans le contexte de la messagerie, un processus d'application réalise un objet fonctionnel de l'un des types définis au § 7. Un élément UE fait, à son tour, partie d'un processus d'application.

26.2 *Éléments ASE symétriques et asymétriques*

On peut distinguer deux types d'éléments ASE, illustrés sur la figure 13/X.402:

- a) **symétrique**: se dit d'un élément ASE grâce auquel un élément UE à la fois assure et utilise un service. Par exemple, l'élément ASE destiné au transfert de messages est symétrique car les deux systèmes ouverts, qui comprennent chacun un agent MTA, offrent et peuvent utiliser, grâce à lui, le service de transfert de messages.

- b) **asymétrique**: se dit d'un élément ASE grâce auquel un élément UE assure ou utilise un service, selon la configuration de l'élément ASE, mais n'effectue pas les deux. Par exemple, l'élément ASE destiné à la remise de messages est asymétrique car seul le système ouvert comprenant un agent MTA offre le service associé et seul l'autre système ouvert, qui comprend un agent UA ou une mémoire MS, l'utilise.

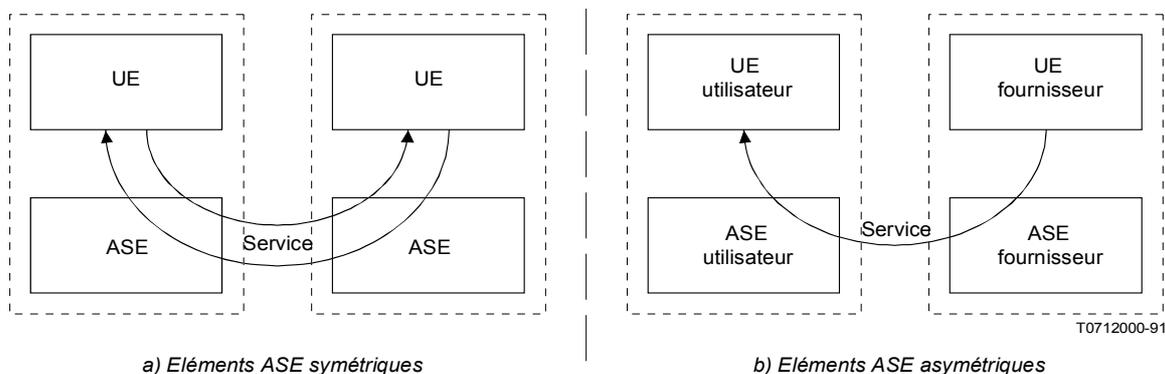


FIGURE 13/X.402
Eléments ASE symétriques et asymétriques

En ce qui concerne un élément ASE asymétrique particulier, un élément UE assure un service que l'autre utilise. Les éléments ASE situés au même emplacement que les éléments UE aident ces derniers à assurer et à utiliser le service. Quatre rôles sont ainsi définis et décrits sur la figure 14/X.402 dans les termes suivants:

- élément UE fournisseur-x**: processus d'application qui assure le service représenté par l'élément ASE asymétrique x.
- élément ASE fournisseur-x**: élément ASE asymétrique x conçu pour être installé au même emplacement qu'un élément UE fournisseur-x.
- élément UE utilisateur-x**: processus d'application qui utilise le service représenté par l'élément ASE asymétrique x.
- élément ASE utilisateur-x**: élément ASE asymétrique conçu pour être installé au même emplacement qu'un élément UE utilisateur-x.

Comme indiqué, les quatre rôles décrits ci-dessus sont définis en fonction d'un élément ASE particulier. Lorsqu'une entité AE comprend plusieurs éléments ASE asymétriques, ces rôles sont confiés indépendamment à chaque élément ASE. En conséquence, comme l'indique la figure 15/X.402, un même élément UE peut servir d'utilisateur pour un élément ASE et de fournisseur pour un autre.

26.3 Eléments ASE de messagerie

Les éléments ASE assurant les divers services de messagerie sont énumérés dans la première colonne du tableau 11/X.402. Pour chaque élément ASE cité, la deuxième colonne spécifie s'il est symétrique ou asymétrique. La troisième colonne indique les objets fonctionnels – agents UA, mémoires MS, agents MTA et unités AU – associés à cet élément ASE, qu'il soit utilisateur ou fournisseur.

Les éléments ASE de messagerie, résumés dans le tableau 11/X.402, sont présentés individuellement ci-dessous. Chacun d'eux est défini dans la Rec. X.419 du CCITT | ISO/CEI 10021-6.

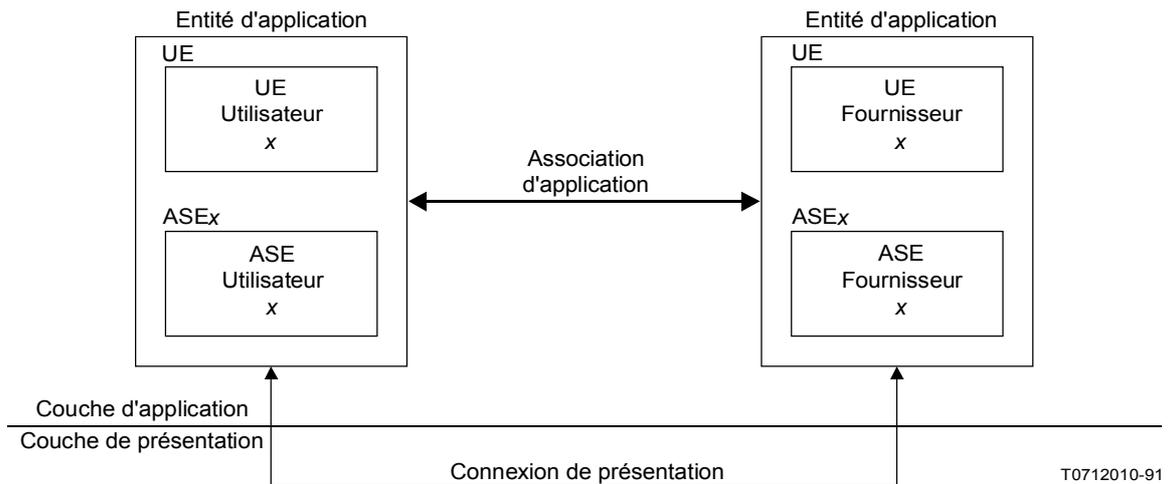


FIGURE 14/X.402
Terminologie relative aux éléments ASE asymétriques

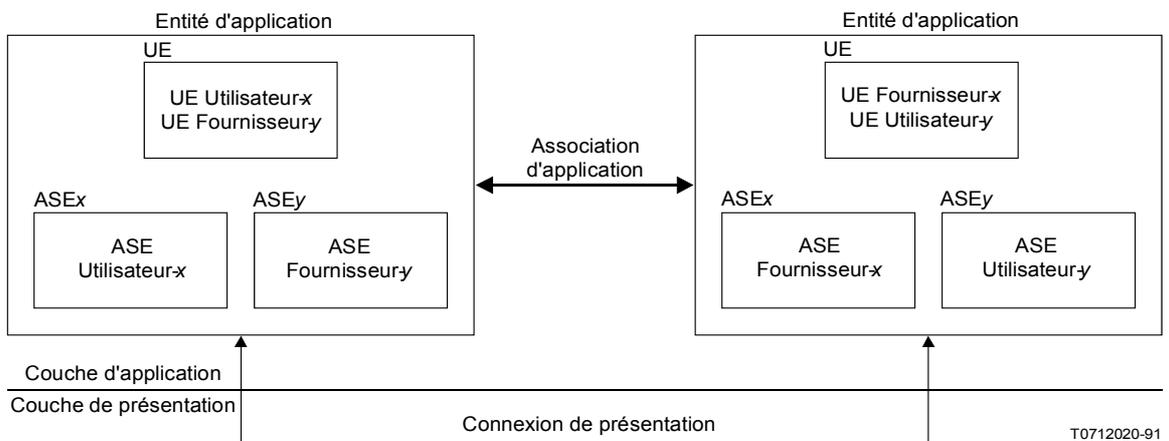


FIGURE 15/X.402
Éléments ASE asymétriques multiples

26.3.1 Transfert de messages

L'élément de service de transfert de messages (MTSE) (*message transfer service element*) est le moyen par lequel l'étape de transmission «transfert» s'effectue.

26.3.2 Dépôt de messages

L'élément de service de dépôt de messages (MSSE) (*message submission service element*) est le moyen par lequel s'effectue l'étape de transmission «dépôt».

TABLEAU 11/X.402

Éléments ASE de messagerie

ASE	Forme	Objets fonctionnels			
		UA	MS	MTA	AU
MTSE	SY	–	–	CS	–
MSSE	ASY	C	CS	S	–
MDSE	ASY	C	C	S	–
MRSE	ASY	C	S	–	–
MASE	ASY	C	CS	S	–

SY Symétrique

ASY Asymétrique

C Utilisateur

S Fournisseur

26.3.3 Remise de messages

L'élément de service de remise de messages (MDSE) (*message delivery service element*) est le moyen par lequel s'effectue l'étape de transmission «remise».

26.3.4 Retrait de messages

L'élément de service de retrait de messages (MRSE) (*message retrieval service element*) est le moyen par lequel s'effectue l'étape de transmission «retrait».

26.3.5 Gestion de messages

L'élément de service de gestion de messages (MASE) (*message administration service element*) est le moyen par lequel un agent UA, une mémoire MS ou un agent MTA regroupe dans des fichiers des informations permettant et commandant leur interaction ultérieure au moyen des éléments MSSE, MDSE, MRSE et MASE.

26.4 Éléments ASE supports

Les éléments ASE à caractère général dont dépendent les éléments ASE de messagerie sont énumérés dans la première colonne du tableau 12/X.402. Pour chaque élément ASE énuméré, la deuxième colonne indique s'il est symétrique ou asymétrique.

Les éléments ASE supports, résumés dans le tableau 12/X.402, sont présentés individuellement ci-dessous.

TABLEAU 12/X.402

Éléments ASE supports

ASE	Forme
ROSE	SY
RTSE	SY
ACSE	SY

SY Symétrique

26.4.1 *Opérations distantes*

L'élément de service opérations distantes (ROSE) est le moyen par lequel les éléments ASE de messagerie asymétriques structurent leurs interactions demande-réponse entre les systèmes ouverts utilisateurs et fournisseurs.

L'élément ROSE est défini dans la Rec. X.219 du CCITT | ISO/CEI 9072-1.

26.4.2 *Transfert fiable*

L'élément de service transfert fiable (RTSE) est le moyen par lequel divers éléments ASE de messagerie symétriques et asymétriques transmettent des objets d'information – en particulier les objets volumineux (par exemple, des messages de télécopie) – entre des systèmes ouverts afin de garantir qu'ils sont correctement mémorisés à destination.

L'élément RTSE est défini dans la Rec. X.218 du CCITT | ISO/CEI 9066-1.

26.4.3 *Commande d'association*

L'élément de service commande d'association (ACSE) est le moyen par lequel toutes les associations d'application entre systèmes ouverts sont établies, libérées et, sous d'autres aspects, gérées.

L'élément ACSE est défini dans la Rec. X.217 du CCITT | ISO/CEI 8649.

27 **Contextes d'application**

Dans le système OSI, les capacités de communication (c'est-à-dire les éléments ASE) de deux systèmes ouverts sont triées dans un but spécifique au moyen de contextes d'application (AC). Un contexte AC est une spécification détaillée de l'utilisation d'une association entre deux systèmes ouverts, c'est-à-dire un protocole.

Un contexte AC spécifie comment l'association doit être établie (par exemple, quels paramètres d'initialisation doivent être échangés), quels éléments ASE doivent être utilisés pour une communication entre homologues sur cette association, quelles contraintes (le cas échéant) doivent être imposées à l'utilisation individuelle par les éléments ASE de cette association, quel est, du demandeur et de son interlocuteur, l'utilisateur de chaque élément ASE asymétrique et comment l'association doit être libérée (par exemple, quels paramètres de fin doivent être échangés).

Un nom est donné à chaque contexte AC (par un identificateur d'objets ASN.1). Le demandeur d'une association indique à son interlocuteur le contexte AC qui régira l'utilisation de l'association en lui transmettant le nom du contexte AC au moyen de l'élément ACSE.

Un contexte AC identifie également par un nom (un identificateur d'objets ASN.1) les syntaxes abstraites des unités APDU qu'une association peut acheminer lorsqu'elle a été utilisée par les éléments ASE du contexte AC. Par convention, on attribue un nom à l'ensemble des unités APDU associées soit à chaque élément ASE, soit à l'ensemble du contexte AC. Le demandeur d'une association indique à son interlocuteur la ou les syntaxes abstraites associées au contexte AC en lui communiquant leurs noms par l'intermédiaire de l'élément ACSE.

La syntaxe abstraite d'une unité APDU constitue sa structure en tant qu'objet d'information (par exemple, un ensemble ASN.1 comprenant un code de commande intégré et un argument de commande de chaîne IA5). Cette syntaxe se distingue de la syntaxe de transfert de l'unité APDU, qui est la représentation de l'objet d'information aux fins de transmission entre deux systèmes ouverts (par exemple, un octet représentant un ensemble ASN.1, suivi par un octet indiquant la longueur de cet ensemble, etc.).

Les contextes AC permettant d'assurer les divers services de messagerie sont spécifiés dans la Rec. X.419 du CCITT | ISO/CEI 10021-6. Ces protocoles sont appelés P1, P3 et P7.

Remarque – La nature du contenu d'un message n'entre pas dans la définition des contextes AC de messagerie car ce contenu fait partie (sous forme de chaîne d'octets) des protocoles au moyen desquels il est transmis.

Classes d'objets et attributs d'annuaire

(Cette annexe fait partie intégrante de la présente Recommandation)

Plusieurs classes d'objets, attributs et syntaxes d'attributs d'annuaire sont spécifiques à la messagerie. Ils sont respectivement définis dans la présente annexe à l'aide des macros OBJECT-CLASS, ATTRIBUTE et ATTRIBUTE-SYNTAX de la Rec. X.501 du CCITT | ISO/CEI 9594-2.

A.1 *Classes d'objets*

Les classes d'objets spécifiques à la messagerie sont spécifiées ci-dessous.

Remarque – Les classes d'objets d'annuaire décrites dans la présente annexe peuvent être combinées avec d'autres classes d'objets, par exemple celles définies dans la Rec. X.521 du CCITT | ISO/CEI 9594-7. Voir également le § 9 de la Rec. X.501 du CCITT | ISO/CEI 9594-2 pour une explication montrant comment des classes d'objets d'annuaire peuvent être combinées en une entrée d'annuaire. L'annexe B de la Rec. X.521 du CCITT | ISO/CEI 9594-7 donne quelques informations complémentaires relatives aux formes de nom d'annuaire et aux structures arborescentes possibles d'information d'annuaire.

A.1.1 *Liste de distribution du système MHS*

Un objet **liste de distribution du système MHS** est une liste DL. Les attributs contenus dans son entrée identifient ses nom courant, autorisation de dépôt et adresses d'O/R et, dans la mesure où les attributs pertinents sont présents, décrivent la liste DL, identifient son organisation, ses unités organisationnelles et son propriétaire, citent les objets apparentés et identifient ses types de contenu et types EIT pouvant être remis, ses membres et les méthodes de remise préférées.

```

mhs-distribution-list OBJECT-CLASS
  SUBCLASS OF top
  MUST CONTAIN {
    commonName,
    mhs-dl-submit-permissions,
    mhs-or-addresses }
  MAY CONTAIN {
    description,
    organizationName,
    organizationalUnitName,
    owner,
    seeAlso,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-dl-members,
    mhs-preferred-delivery-methods }
  ::= id-oc-mhs-distribution-list

```

A.1.2 *Mémoire de message du système MHS*

Un objet **mémoire de message du système MHS** est une entité AE qui réalise une mémoire MS. Les attributs contenus dans son entrée, pour autant qu'ils soient présents, décrivent la mémoire MS, identifient son propriétaire et énumèrent les attributs optionnels, les actions automatiques et les types de contenu qu'elle admet.

```

mhs-message-store OBJECT-CLASS
  SUBCLASS OF applicationEntity
  MAY CONTAIN {
    owner,
    mhs-supported-optional-attributes,
    mhs-supported-automatic-actions,
    mhs-supported-content-types }
  ::= id-oc-mhs-message-store

```

A.1.3 *Agent de transfert de message du système MHS*

Un objet **agent de transfert de message du système MHS** est une entité AE qui met en oeuvre un agent MTA. Les attributs contenus dans son entrée, dans la mesure où ils sont présents, décrivent l'agent MTA et identifient son propriétaire et la longueur de contenu pouvant être remise.

```
mhs-message-transfer-agent OBJECT-CLASS  
SUBCLASS OF applicationEntity  
MAY CONTAIN {  
    owner,  
    mhs-deliverable-content-length }  
::= id-oc-mhs-message-transfer-agent
```

A.1.4 *Utilisateur du système MHS*

Un objet **utilisateur du système MHS** est un utilisateur du système MHS générique. (Le système MHS générique peut avoir, par exemple, une adresse professionnelle, une adresse privée, ou les deux.) Les attributs contenus dans son entrée identifient l'adresse d'O/R de l'utilisateur et, dans la mesure où les attributs pertinents sont présents, la longueur de contenu qui peut être remis à l'utilisateur, les types de contenu, les types EIT, sa mémoire MS et ses méthodes de remise préférées.

```
mhs-user OBJECT-CLASS  
SUBCLASS OF top  
MUST CONTAIN {  
    mhs-or-addresses }  
MAY CONTAIN {  
    mhs-deliverable-content-length,  
    mhs-deliverable-content-types,  
    mhs-deliverable-eits,  
    mhs-message-store-dn,  
::= id-oc-mhs-user
```

Remarque – L'information contenue dans la méthode de remise préférée de l'utilisateur du système MHS est héritée, dans l'ensemble d'attributs télécommunications, de la classe d'objet de dénomination de l'utilisateur de l'annuaire.

A.1.5 *Agent d'utilisateur du système MHS*

Un objet **agent d'utilisateur du système MHS** est une entité AE qui réalise un agent UA. Les attributs contenus dans son entrée, dans la mesure où ils sont présents, identifient le propriétaire de l'agent UA, la longueur de contenu qui peut être remise, les types de contenu, les types EIT et son adresse d'O/R.

```
mhs-user-agent OBJECT-CLASS  
SUBCLASS OF applicationEntity  
MAY CONTAIN {  
    owner,  
    mhs-deliverable-content-length,  
    mhs-deliverable-content-types,  
    mhs-deliverable-eits,  
    mhs-or-addresses }  
::= id-oc-mhs-user-agent
```

A.2 *Attributs*

Les attributs propres à la messagerie sont spécifiés ci-dessous.

A.2.1 *Longueur de contenu pouvant être remise dans le système MHS (MHS Deliverable Content Length)*

L'attribut **longueur de contenu pouvant être remise dans le système MHS** identifie la longueur maximale du contenu des messages qu'un utilisateur accepte de recevoir.

La valeur de cet attribut est un nombre entier.

```
mhs-deliverable-content-length ATTRIBUTE  
WITH ATTRIBUTE-SYNTAX integerSyntax  
SINGLE VALUE  
::= id-at-mhs-deliverable-content-length
```

A.2.2 *Types de contenu pouvant être remis dans le système MHS (MHS Deliverable Content Types)*

L'attribut **types de contenu pouvant être remis dans le système MHS** identifie les types de contenu des messages dont un utilisateur acceptera la remise.

La valeur de cet attribut est un identificateur d'objets.

mhs-deliverable-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-content-types

A.2.3 *Types EIT pouvant être remis dans le système MHS (MHS Deliverable EITs)*

L'attribut **types EIT pouvant être remis dans le système MHS** identifie les types EIT des messages dont un utilisateur acceptera la remise.

La valeur de cet attribut est un identificateur d'objets.

mhs-deliverable-eits ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-eits

A.2.4 *Membres de listes DL dans le système MHS (MHS DL Members)*

L'attribut **membres de liste DL dans le système MHS** identifie les membres d'une liste DL.

La valeur de cet attribut est un nom d'O/R.

mhs-dl-members ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
MULTI VALUE
::= id-at-mhs-dl-members

A.2.5 *Autorisations de dépôt de liste DL dans le système MHS (MHS DL Submit Permissions)*

L'attribut **autorisations de dépôt de liste DL dans le système MHS** identifie les utilisateurs et les listes DL qui peuvent déposer des messages dans une liste DL.

La valeur de cet attribut est une autorisation de dépôt d'une liste DL.

mhs-dl-submit-permissions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
MULTI VALUE
::= id-at-mhs-dl-submit-permissions

A.2.6 *Nom d'annuaire d'une mémoire de message dans le système MHS (MHS Message Store Directory Name)*

L'attribut **nom d'annuaire d'une mémoire de message dans le système MHS** identifie la mémoire MS d'un utilisateur par son nom.

La valeur de cet attribut est un nom particulier d'annuaire.

mhs-message-store-dn ATTRIBUTE
WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
SINGLE VALUE
::= id-at-mhs-message-store-dn

A.2.7 *Adresses d'O/R dans le système MHS (MHS O/R Addresses)*

L'attribut **adresses d'O/R dans le système MHS** spécifie les adresses d'O/R d'un utilisateur ou d'une liste DL.

La valeur de cet attribut est une adresse d'O/R.

mhs-or-addresses ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
MULTI VALUE
::= id-at-mhs-or-addresses

A.2.8 *Actions automatiques prises en charge dans le système MHS (MHS Supported Automatic Actions)*

L'attribut **actions automatiques prises en charge dans le système MHS** identifie les actions automatiques qu'une mémoire MS assure entièrement.

La valeur de cet attribut est un identificateur d'objets.

mhs-supported-automatic-actions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-automatic-actions

A.2.9 *Types de contenus pris en charge dans le système MHS (MHS Supported Content Types)*

L'attribut **types de contenus pris en charge dans le système MHS** identifie les types de contenus des messages dont une mémoire MS assure entièrement la syntaxe et la sémantique.

La valeur de cet attribut est un identificateur d'objets.

mhs-supported-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-content-types

A.2.10 *Attributs optionnels pris en charge dans le système MHS (MHS Supported Optional Attributes)*

L'attribut **attributs optionnels pris en charge dans le système MHS** identifie les attributs optionnels qu'une mémoire MS assure entièrement.

La valeur de cet attribut est un identificateur d'objets.

mhs-supported-optional-attributes ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-optional-attributes

A.3 *Syntaxes d'attributs*

Les syntaxes d'attributs propres à la messagerie sont spécifiées ci-après.

A.3.1 *Autorisation de dépôt de liste DL dans le système MHS (MHS DL Submit Permission)*

La syntaxe d'attribut **autorisation de dépôt de liste DL dans le système MHS** caractérise un attribut dont chacune des valeurs est une autorisation de dépôt.

mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
SYNTAX DLSubmitPermission
MATCHES FOR EQUALITY
::= id-as-mhs-dl-submit-permission

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

La valeur présentée d'une autorisation de dépôt de liste DL doit être du type *individual* (individuel).

Selon son type, une autorisation de dépôt de liste DL, n'accorde l'accès de dépôt à aucun utilisateur et à aucune liste DL ou l'accorde à un ou plusieurs utilisateurs et listes DL suivants:

- Individual* (individuel): l'utilisateur ou la liste DL (non développée) dont l'un quelconque des noms d'O/R est égal au nom d'O/R spécifié.
- Member-of-dl* (membre de liste dl): Chaque membre de la liste DL, dont l'un quelconque des noms d'O/R est égal au nom d'O/R spécifié, ou de chaque liste DL imbriquée, de manière récurrente.
- Pattern-match* (correspondance de structure): Chaque utilisateur ou liste DL (non développée) dont l'un quelconque des noms d'O/R correspond à la structure du nom d'O/R spécifié.

ORNamePattern ::= ORName

- d) *Member-of-group* (membre de groupe): Chaque membre du groupe de noms dont le nom est spécifié, ou de chaque groupe de noms imbriqué, de manière récurrente.

La valeur présentée est égale à une valeur cible de ce type si les deux sont identiques, attribut par attribut. En outre, l'égalité peut être déclarée dans d'autres conditions fixées à l'échelon local.

A.3.2 Adresse d'O/R dans le système MHS (MHS O/R Address)

La syntaxe d'attribut **adresse d'O/R dans le système MHS** caractérise un attribut dont chacune des valeurs est une adresse d'O/R.

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX  
SYNTAX ORAddress  
MATCHES FOR EQUALITY  
::= id-as-mhs-or-address
```

La valeur présentée d'une adresse d'O/R est égale à une valeur cible d'adresse d'O/R aux conditions spécifiées au § 18.4.

A.3.3 Nom d'O/R dans le système MHS (MHS O/R Name)

La syntaxe d'attribut **nom d'O/R dans le système MHS** caractérise un attribut dont chacune des valeurs est un nom d'O/R.

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX  
SYNTAX ORName  
MATCHES FOR EQUALITY  
::= id-as-mhs-or-name
```

La valeur présentée d'un nom d'O/R est égale à une valeur cible de nom d'O/R si les deux sont identiques, attribut par attribut. En outre, l'égalité peut être déclarée dans d'autres conditions fixées à l'échelon local.

ANNEXE B

(à la Recommandation X.402)

Définition de référence des identificateurs d'objets

(Cette annexe fait partie intégrante de la présente Recommandation)

Elle définit, à des fins de référence, divers identificateurs d'objets cités dans le module ASN.1 des annexes A et C. Elle utilise l'ASN.1.

Tous les identificateurs d'objets traités par la présente Recommandation sont fixés dans la présente annexe. Celle-ci est définitive pour tous les identificateurs d'objets à l'exception de ceux destinés aux modules ASN.1 et au système MHS lui-même. Les affectations définitives pour les modules ASN.1 se font dans les modules eux-mêmes; d'autres références à ceux-ci apparaissent dans les paragraphes IMPORT. Le système MHS est fixe.

```
MHSObjectIdentifiers { joint-iso-ccitt mhs-motis(6) arch(5) modules(0) object-identifiers(0) }  
DEFINITIONS IMPLICIT TAGS ::=  
BEGIN
```

```
-- Prologue  
-- Exporte tout.
```

```
IMPORTS -- rien -- ;
```

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

```
-- Aspects dans le système MHS
```

```
id-mhs-protocols ID ::= { joint-iso-ccitt mhs-motis(6) protocols(0) }
```

```
-- Contextes d'application et protocoles du système MHS  
-- Voir Rec. X.419 du CCITT | ISO/CEI 10021-6.
```

```
id-ipms ID ::= { joint-iso-ccitt mhs-motis(6) ipms(1) }
```

```

-- Messagerie de personne à personne
-- Voir Rec. X.420 du CCITT | ISO/CEI 10021-7.
id-asdc          ID ::= { joint-iso-ccitt mhs-motis(6) asdc (2) }

-- Conventions de définition de service abstrait
-- Voir Rec. X.407 du CCITT | ISO/CEI 10021-3.
id-mts          ID ::= { joint-iso-ccitt mhs-motis(6) mts (3) }

-- Système de transfert de message
-- Voir Rec. X.411 du CCITT | ISO/CEI 10021-4.
id-ms           ID ::= { joint-iso-ccitt mhs-motis(6) ms (4) }

-- Mémoire de message
-- Voir Rec. X.413 du CCITT | ISO/CEI 10021-5.
id-arch        ID ::= { joint-iso-ccitt mhs-motis(6) arch (5) }

-- Architecture globale
-- Voir la présente Recommandation
id-group       ID ::= { joint-iso-ccitt mhs-motis(6) group (6) }

-- Réservé

-- Catégories

id-mod ID ::= { id-arch 0 } -- modules; non définitive
id-oc  ID ::= { id-arch 1 } -- classes d'objets
id-at  ID ::= { id-arch 2 } -- types d'attribut
id-as  ID ::= { id-arch 3 } -- syntaxes d'attribut

-- Modules

id-object-identifiers ID ::= { id-mod 0 } -- non définitif
id-directory-objects-and-attributes ID ::= { id-mod 1 } -- non définitif

-- Classes d'objets

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

-- Attributs

id-at-mhs-deliverable-content-length ID ::= { id-at 0 }
id-at-mhs-deliverable-content-types ID ::= { id-at 1 }
id-at-mhs-deliverable-eits ID ::= { id-at 2 }
id-at-mhs-dl-members ID ::= { id-at 3 }
id-at-mhs-dl-submit-permissions ID ::= { id-at 4 }
id-at-mhs-message-store-dn ID ::= { id-at 5 }
id-at-mhs-or-addresses ID ::= { id-at 6 }
-- Value { id-at 7 } is no longer defined
id-at-mhs-supported-automatic-actions ID ::= { id-at 8 }
id-at-mhs-supported-content-types ID ::= { id-at 9 }
id-at-mhs-supported-optional-attributes ID ::= { id-at 10 }

-- Syntaxes d'attribut

id-as-mhs-dl-submit-permission ID ::= { id-as 0 }
id-as-mhs-or-address ID ::= { id-as 1 }
id-as-mhs-or-name ID ::= { id-as 2 }

```

END -- d'annuaire dans le système MHS

Définition de référence des classes d'objets et attributs d'annuaire

(Cette annexe fait partie intégrante de la présente Recommandation)

La présente annexe, qui complète l'annexe A, définit à des fins de référence les classes d'objets, les attributs et les syntaxes d'attributs spécifiques à la messagerie. Elle utilise les macros OBJECT CLASS, ATTRIBUTE et ATTRIBUTE SYNTAX de la Rec. X.501 du CCITT | ISO/CEI 9594-2.

```

MHSDirectoryObjectsAndAttributes { joint-iso-ccitt
  mhs-motis(6) arch(5) modules(0) directory(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

  -- Prologue
  -- Exporte tout

IMPORTS

  -- Identificateurs d'objets dy système MHS

  id-as-mhs-dl-submit-permission, id-as-mhs-or-address, id-as-mhs-or-name,
  id-at-mhs-deliverable-content-length, id-at-mhs-deliverable-content-types,
  id-at-mhs-deliverable-eits, id-at-mhs-dl-members, id-at-mhs-dl-submit-permissions,
  id-at-mhs-message-store-dn, id-at-mhs-or-addresses, id-at-mhs-preferred-delivery-methods,
  id-at-mhs-supported-automatic-actions, id-at-mhs-supported-content-types,
  id-at-mhs-supported-optional-attributes, id-oc-mhs-distribution-list,
  id-oc-mhs-message-store, id-oc-mhs-message-transfer-agent, id-oc-mhs-user,
  id-oc-mhs-user-agent
  ----
  FROM MHSObjectIdentifiers { joint-iso-ccitt
    mhs-motis(6) arch(5) modules(0) object-identifiers(0) }

  -- Service abstrait de système MTS (de la Rec. X.411)
  ORAddress, ORName, RequestedDeliveryMethod
  ----
  FROM MTSAbstractService { joint-iso-ccitt
    mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

  -- Cadre général d'information (de la Rec. X.501)
  ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS
  ----
  FROM InformationFramework { joint-iso-ccitt
    ds(5) modules(1) informationFramework(1) }

  -- Classes d'objets sélectionnées (de la Rec. X.521)

  applicationEntity, top
  ----
  FROM SelectedObjectClasses { joint-iso-ccitt ds(5) modules(1) selectedObjectClasses(6) }

  -- Types d'attributs sélectionnés (de la Rec. X.520)

  commonName, description, distinguishedNameSyntax, integerSyntax, objectIdentifiersSyntax,
  organization, organizationalUnitName, owner, seeAlso
  ----
  FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) modules(1) selectedAttributeTypes(5) };

-- CLASSES D'OBJETS

  -- Liste de distribution du système MHS
  mhs-distribution-list OBJECT-CLASS
  SUBCLASS OF top
  MUST CONTAIN {
    commonName,
    mhs-dl-submit-permissions,
    mhs-or-addresses }

```

```
MAY CONTAIN {
    description,
    organizationName,
    organizationalUnitName,
    owner,
    seeAlso,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-dl-members,
    mhs-preferred-delivery-methods }
::= id-oc-mhs-distribution-list
```

-- Mémoire de message du système MHS

```
mhs-message-store OBJECT-CLASS
SUBCLASS OF applicationEntity
MAY CONTAIN {
    owner,
    mhs-supported-optional-attributes,
    mhs-supported-automatic-actions,
    mhs-supported-content-types }
::= id-oc-mhs-message-store
```

-- Agent de transfert de message du système MHS

```
mhs-message-transfer-agent OBJECT-CLASS
SUBCLASS OF applicationEntity
MAY CONTAIN {
    owner,
    mhs-deliverable-content-length }
::= id-oc-mhs-message-transfer-agent
```

-- Utilisateur du système MHS

```
mhs-user OBJECT-CLASS
SUBCLASS OF top
MUST CONTAIN {
    mhs-or-addresses }
MAY CONTAIN {
    mhs-deliverable-content-length,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-message-store-dn,
::= id-oc-mhs-user
```

-- Agent utilisateur du système MHS

```
mhs-user-agent OBJECT-CLASS
SUBCLASS OF applicationEntity
MAY CONTAIN {
    owner,
    mhs-deliverable-content-length,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-or-addresses }
::= id-oc-mhs-user-agent
```

-- ATTRIBUTES

-- Longueur de contenu pouvant être remis dans le système MHS

```
mhs-deliverable-content-length ATTRIBUTE
WITH ATTRIBUTE-SYNTAX integerSyntax
SINGLE VALUE
::= id-at-mhs-deliverable-content-length
```

-- Types de contenu pouvant être remis dans le système MHS

mhs-deliverable-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-content-types

-- Types EIT pouvant être remis dans le système MHS

mhs-deliverable-eits ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-eits

-- Membres de liste DL dans le système MHS

mhs-dl-members ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
MULTI VALUE
::= id-at-mhs-dl-members

-- Autorisations de dépôt de liste DL dans le système MHS

mhs-dl-submit-permissions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
MULTI VALUE
::= id-at-mhs-dl-submit-permissions

-- Adresses d'O/R dans le système MHS

mhs-or-addresses ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
MULTI VALUE
::= id-at-mhs-or-addresses

-- Nom d'annuaire de Mémoire de message dans le système MHS

mhs-message-store-dn ATTRIBUTE
WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
SINGLE VALUE
::= id-at-mhs-message-store-dn

-- Actions automatiques prises en charge dans le système MHS

mhs-supported-automatic-actions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-automatic-actions

-- Types de contenu prise en charge dans le système MHS

mhs-supported-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-content-types

-- Attributs optionnels pris en charge dans le système MHS

mhs-supported-optional-attributes ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-optional-attributes

-- SYNTAXES D'ATTRIBUTS

-- Autorisation de dépôt de liste DL dans le système MHS

mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
SYNTAX DLSubmitPermission
MATCHES FOR EQUALITY
::= id-as-mhs-dl-submit-permission

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

```
ORNamePattern ::= ORName
```

-- Adresse d'O/R dans le système MHS

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX
SYNTAX ORAddress
MATCHES FOR EQUALITY
::= id-as-mhs-or-address
```

-- Nom d'O/R dans le système MHS

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX
SYNTAX ORName
MATCHES FOR EQUALITY
::= id-as-mhs-or-name
```

END -- d'annuaire dans le système MHS

ANNEXE D

(à la Recommandation X.402)

Menaces concernant la sécurité

(Cette annexe ne fait pas partie intégrante de la présente Recommandation)

Un aperçu général des risques auxquels le système MHS est exposé est donné au § 15.1 de la Rec. X.400 du CCITT | ISO/CEI 10021-1, où sont examinés les risques rencontrés dans un système MHS à différents niveaux: à l'accès, entre les messages, à l'intérieur même des messages et dans la mémoire de message. Ces risques peuvent prendre les différentes formes suivantes:

- a) usurpation d'identité;
- b) mise en séquence de messages;
- c) modification d'informations;
- d) refus de service;
- e) fuite d'informations;
- f) répudiation;
- g) autres risques.

En outre, ces incidents peuvent survenir par accident ou être causés dans une intention malveillante et peuvent être actifs ou passifs. Les tentatives d'agression visant ce système MHS seront dirigées sur ses éventuels points faibles et peuvent être de nature différente. La présente annexe traite des risques individuels et bien qu'elle prenne en considération plusieurs grandes catégories de risques, elle n'est pas exhaustive.

Le tableau D-1/X.402 indique comment ces risques peuvent être évités à l'aide des services de sécurité du système MHS. La liste des risques présentée ici est donnée à titre indicatif, elle n'est pas définitive.

TABLEAU D-1/X.402

Utilisation des services de sécurité du système MHS

Risque	Services
<p><i>Usurpation d'identité</i></p> <p>Usurpation d'identité et usage abusif du système MTS</p> <p>Accusé de réception mensonger Prétendue expédition d'un message Usurpation de l'identité d'un agent MTA vis-à-vis d'un utilisateur du système MTS</p> <p>Usurpation d'identité d'un agent MTA vis-à-vis d'un autre agent MTA</p>	<p>Authentification de l'origine du message Authentification de l'origine de l'envoi-test Gestion de la sécurité de l'accès Preuve de la remise Authentification de l'origine du message Preuve du dépôt Authentification de l'origine du rapport Gestion de la sécurité de l'accès Authentification de l'origine du rapport Gestion de la sécurité de l'accès</p>
<p><i>Mise en séquence des messages</i></p> <p>Relecture des messages Remise en ordre des messages Lecture anticipée de messages Retard des messages</p>	<p>Intégrité de la séquence du message Intégrité de la séquence du message</p>
<p><i>Modification des informations</i></p> <p>Modification de messages</p> <p>Destruction de messages Modification de l'information d'acheminement ou d'une autre information de gestion</p>	<p>Intégrité de la liaison Intégrité du contenu Intégrité de la séquence du message</p>
<p><i>Refus de service</i></p> <p>Refus de communications Adressage sous forme avalanche d'un agent MTA Adressage sous forme avalanche du système MTS</p>	
<p><i>Répudiation</i></p> <p>Refus d'origine Refus de dépôt Refus de remise</p>	<p>Non-répudiation d'origine Non-répudiation de dépôt Non-répudiation de remise</p>
<p><i>Fuite d'informations</i></p> <p>Perte de confidentialité</p> <p>Perte d'anonymat Détournement de messages Analyse du trafic</p>	<p>Confidentialité de la liaison Confidentialité du contenu Confidentialité du cheminement du message Gestion de la sécurité de l'accès Confidentialité du cheminement du message</p>
<p><i>Autres risques</i></p> <p>Expéditeur non autorisé pour l'étiquette de sécurité de message (dépôt inapproprié) Agent MTA/utilisateur MTS non autorisé pour le contexte de sécurité Acheminement erroné</p> <p>Politiques d'étiquetage différentes</p>	<p>Gestion de la sécurité de l'accès Etiquetage de sécurité de message Gestion de la sécurité de l'accès</p> <p>Gestion de la sécurité de l'accès Etiquetage de sécurité de message</p>

D.1 *Usurpation d'identité*

Il y a usurpation d'identité quand une entité prétend avec succès être une entité différente; il en existe plusieurs formes. Un utilisateur du système MTS non autorisé peut usurper l'identité d'un autre pour accéder sans autorisation aux services du système MTS ou agir au détriment de l'utilisateur légitime, par exemple en mettant au rebut ses messages. Un utilisateur du système MTS peut usurper l'identité d'un autre et ainsi accuser indûment réception d'un message à la place du destinataire légitime. Un message peut être introduit dans le système MTS par un utilisateur se faisant passer pour un autre. Un utilisateur du système MTS peut se faire passer pour un autre, une mémoire MS pour une autre et un agent MTA pour un autre.

Les risques d'usurpation d'identité sont les suivants:

- a) usurpation d'identité et usager abusif du système MTS;
- b) accusé de réception mensonger;
- c) prétendue expédition d'un message;
- d) usurpation de l'identité d'un agent MTA vis-à-vis d'un utilisateur du système MTS;
- e) usurpation de l'identité d'un agent MTA vis-à-vis d'un autre agent MTA.

Une usurpation d'identité comprend généralement d'autres formes d'attaque et, dans un système sûr, peut nécessiter des séquences d'authentification de la part des utilisateurs légitimes, par exemple lors de la relecture ou de la modification des messages.

D.2 *Mise en séquence d'un message*

Les risques de mise en séquence d'un message surviennent quand une partie ou la totalité d'un message est répétée, différée ou remise en ordre. La mise en séquence d'un message peut être utilisée pour exploiter l'information d'authentification d'un message correct et remettre en séquence ou différer des messages corrects. Bien que les services de sécurité du système MHS ne permettent absolument pas d'éviter le risque de relecture, on peut déceler ce risque et en éliminer les effets.

Les risques de mise en séquence d'un message sont les suivants:

- a) relecture des messages;
- b) remise en ordre des messages;
- c) lecture anticipée des messages;
- d) retard des messages.

D.3 *Modification des informations*

L'information destinée à un destinataire prévu, l'information d'acheminement et d'autres données de gestion peuvent être perdues ou modifiées sans que cette perte ou cette modification soit décelée. Cet incident peut concerner n'importe quel aspect du message, par exemple son étiquetage, son contenu, ses attributs, son destinataire ou son expéditeur. Une modification de l'information d'acheminement ou d'une autre information de gestion, enregistrée dans les agents MTA ou utilisée par ceux-ci, peut entraîner la perte des messages dans le système MTS à perdre des messages ou un fonctionnement incorrect de celui-ci.

Les risques de modification des informations sont les suivants:

- a) modification de messages;
- b) destruction de messages;
- c) modification de l'information d'acheminement ou d'une autre information de gestion.

D.4 *Refus de service*

Il y a refus de service lorsqu'une entité ne parvient pas à remplir ses fonctions ou empêche d'autres entités de remplir les leurs. Il peut s'agir d'un refus d'accès, d'un refus de communications (ce qui aboutit à d'autres problèmes comme la surcharge), une suppression délibérée des messages vers un destinataire particulier, ou la fabrication de trafic supplémentaire. Le système MTS peut être refusé en cas de panne ou de fonctionnement incorrect d'un agent MTA. En outre, un utilisateur du système MTS peut amener le système MTS à refuser un service à d'autres utilisateurs en «inondant» ce service de messages susceptibles de surcharger la capacité de commutation d'un agent MTA ou de remplir tout l'espace disponible pour l'enregistrement de messages.

Les risques de refus de service sont les suivants:

- a) refus de communications;
- b) adressage sous forme avalanche d'un agent MTA;
- c) adressage sous forme avalanche du système MTS.

D.5 *Répudiation*

La répudiation peut se produire quand un utilisateur du système MTS ou le système MTS ont ultérieurement la possibilité de refuser le dépôt, la réception ou l'expédition d'un message.

Les risques de répudiation sont les suivants:

- a) refus d'origine;
- b) refus de dépôt;
- c) refus de remise.

D.6 *Fuite d'informations*

Un correspondant non autorisé peut acquérir des informations de trois manières: par surveillance des émissions, par accès non autorisé aux informations stockées dans une entité du système MHS ou par usurpation d'identité. Dans certains cas, la présence d'un utilisateur du système MTS sur le système peut être confidentielle, et il peut être nécessaire de préserver son anonymat. Un utilisateur du système MTS autre que le destinataire prévu peut obtenir un message, par suite d'une usurpation d'identité et d'un usage abusif du système MTS, ou en provoquant un fonctionnement incorrect d'un agent MTA. Il est possible de tirer d'autres détails sur les informations acheminées dans un système MTS en observant le trafic.

Les risques de fuite d'informations sont les suivants:

- a) perte de confidentialité;
- b) perte d'anonymat;
- c) détournement de messages;
- d) analyse du trafic.

D.7 *Autres risques*

Dans un système à un ou plusieurs niveaux de sécurité, il peut exister un certain nombre de risques relatifs à l'étiquetage de sécurité, par exemple en cas d'acheminement par l'intermédiaire d'un noeud dont le niveau de fiabilité n'est pas suffisant pour assurer la transmission d'informations d'une valeur particulière ou lorsque des systèmes utilisent des politiques d'étiquetage différentes. D'autres risques peuvent compromettre la mise en application d'une politique de sécurité fondée sur une séparation logique utilisant des étiquettes de sécurité. Un utilisateur du système MTS peut expédier un message et lui affecter une étiquette qu'il n'est pas autorisé à lui affecter. Un utilisateur du système MTS ou un agent MTA peut établir ou accepter une association avec un contexte de sécurité sans avoir l'autorisation correspondante.

Les risques visés dans ce paragraphe sont les suivants:

- a) expéditeur non autorisé pour l'étiquette de sécurité de message (dépôt inapproprié);
- b) agent MTA utilisateur du système MTS non autorisé pour le contexte de sécurité;
- c) acheminement erroné;
- d) politiques d'étiquetage différentes.

ANNEXE E

(à la Recommandation X.402)

Prestation de services de sécurité décrits dans la Rec. X.411 du CCITT | ISO/CEI 10021-4

(Cette annexe fait partie intégrante de la présente Recommandation)

Le tableau E-1/X.402 indique les éléments de service tirés de la Rec. X.411 du CCITT | ISO/CEI 10021-4 qui peuvent être utilisés pour assurer les services de sécurité décrits dans le § 10.2.

TABLEAU E-1/X.402

Prestation des services de sécurité dans le système MHS

Service	Arguments/services du système MTS
<i>Services de sécurité d'authentification de l'origine</i> Authentification de l'origine du message Authentification de l'origine de l'envoi-test Authentification de l'origine du rapport Preuve du dépôt Preuve de remise	Contrôle d'authentification de l'origine du message Jeton de message Contrôle d'authentification de l'origine de l'envoi-test Contrôle d'authentification de l'origine du rapport Demande de preuve du dépôt Preuve du dépôt Demande de preuve de la remise Preuve de la remise
<i>Services de sécurité de gestion de la sécurité de l'accès</i> Authentification de l'entité homologue Contexte de sécurité	Pouvoirs du demandeur Pouvoirs du demandé Contexte de sécurité
<i>Services de sécurité de confidentialité des données</i> Confidentialité de la liaison Confidentialité du contenu Confidentialité du cheminement du message	Non assurée Identificateur de l'algorithme de confidentialité du contenu Jeton de message Type de contenu
<i>Services de sécurité d'intégrité des données</i> Intégrité de la liaison Intégrité du contenu Intégrité de la séquence du message	Non assurée Contrôle d'intégrité du contenu Jeton de message Contrôle d'authentification de l'origine du message Numéro de séquence de message Jeton de message
<i>Services de sécurité de non-répudiation</i> Non-répudiation d'origine Non-répudiation de dépôt Non-répudiation de remise	Contrôle d'intégrité du contenu Jeton de message Contrôle d'authentification de l'origine du message Demande de preuve du dépôt Preuve du dépôt Preuve de la demande de remise Preuve de la remise
Etiquetage de sécurité du message	Etiquette de sécurité du message Jeton de message Contrôle d'authentification de l'origine du message
<i>Services de sécurité de gestion de la sécurité</i> Modification des pouvoirs Enregistrement	Modification des pouvoirs Enregistrement

ANNEXE F

(à la Recommandation X.402)

Représentation des adresses d'O/R pour les usagers

(Cette annexe ne fait pas partie intégrante de la présente Recommandation)

Ce document se compose de l'annexe B de la Recommandation F.401.

ANNEXE G

(à la Recommandation X.402)

Utilisation des adresses d'O/R par des organisations multinationales

(Cette annexe ne fait pas partie intégrante de la présente Recommandation)

Voir également l'annexe E de la Recommandation F.400.

Il est bien connu que, lorsque les réglementations le permettent, de nombreuses organisations souhaitent utiliser des systèmes de messagerie implantés dans plus d'un pays. Ces organisations comprennent à la fois des organisations privées et des fournisseurs publics de services de messagerie. Les politiques d'adressage et d'acheminement de ces systèmes doivent être conformes au modèle général du système de messagerie afin de permettre l'interfonctionnement avec le reste du système de messagerie mondial.

La disponibilité des services d'annuaire peut influencer considérablement sur les politiques d'adressage que les organisations choisissent d'adopter. Si un service universel d'annuaire est disponible, les expéditeurs et les destinataires des messages peuvent être mentionnés à l'aide d'un nom d'annuaire facile à utiliser; les adresses d'O/R peuvent être obtenues dans l'annuaire par le système de messagerie. Dans ce cas, les usagers n'ont jamais besoin de connaître les valeurs d'adresse d'O/R utilisées et la politique d'adressage peut être choisie selon des critères purement techniques. Si un tel service d'annuaire n'est pas disponible, les utilisateurs doivent traiter les adresses d'O/R manuellement. Dans ce cas, des considérations d'ordre esthétique et d'autres facteurs humains influencent également le choix de la politique d'adressage.

G.1 *Principes d'adressage*

L'univocité mondiale des noms dans le système MHS est assurée par une structure d'enregistrement hiérarchique et l'utilisation cohérente des conventions de dénomination, c'est-à-dire que lorsqu'une adresse d'O/R est utilisée, il faut enregistrer les valeurs d'attribut d'adresse selon les procédures applicables dans le pays indiqué par la valeur de l'attribut nom de pays country-name. Dans le cas du nom de domaine privé et du nom de domaine d'administration, cet enregistrement doit s'effectuer par l'intermédiaire des autorités d'enregistrement dont relève ce pays ou domaine. Ces principes constituent la base de la messagerie mondiale.

L'interconnexion de domaines (domaine PRMD vers domaine ADMD, domaine ADMD vers domaine ADMD, domaine PRMD vers domaine PRMD) est soumise à des accords bilatéraux. Ces accords portent sur des critères d'ordre commercial et technique et peuvent notamment spécifier la gamme des valeurs d'adresse d'O/R acceptées.

Lorsqu'une organisation spécifie que des noms de domaine doivent comporter plus d'un code de pays, il est nécessaire d'enregistrer ces noms selon les procédures de chaque pays. Il est souvent possible d'enregistrer la même valeur de nom de domaine privé (ou de nom de domaine d'administration, selon le cas) dans chaque pays; cependant, des facteurs extérieurs au système MHS (comme le propriétaire légal des noms) imposent parfois à une organisation supranationale d'utiliser des valeurs différentes pour leur nom de domaine selon le code de pays utilisé.

Dans l'idéal, les utilisateurs du système MHS aimeraient disposer d'une adresse, qui serait indiquée en tête des lettres et sur des cartes professionnelles (mentionnant le pays dans lequel l'utilisateur est situé), que leurs partenaires éventuels utiliseraient pour communiquer dans les systèmes MHS mondiaux. Les possibilités d'accès à des partenaires éloignés, par l'intermédiaire d'un fournisseur de services, dépend de la connectivité offerte.

G.2 Exemples de configuration

Des organisations multinationales peuvent choisir d'organiser leurs systèmes de messagerie de toutes les manières compatibles avec ces principes de base. On trouvera ci-après des exemples de configurations possibles pour un domaine PRMD multinational:

G.2.1 Domaines PRMD multiples indépendants

Voir la figure G-1/X.402.

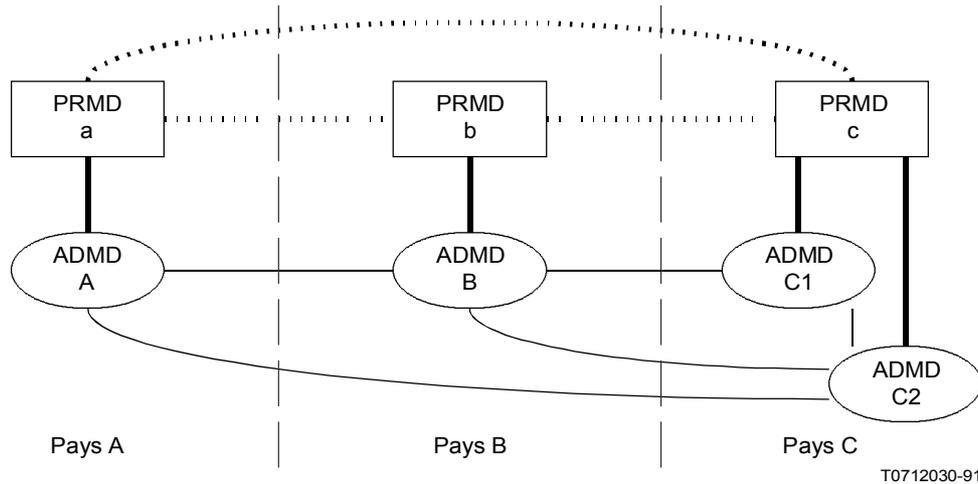


FIGURE G-1/X.402
Domaines PRMD multiples indépendants

L'organisation multinationale peut diviser son système de messagerie de façon logique en parties entièrement contenues dans un pays. Chacune de ces parties fonctionne comme un domaine PRMD distinct et utilise les adresses enregistrées dans le pays en question.

Chaque domaine PRMD peut se connecter avec un ou plusieurs domaines PRMD dans ce pays. Lorsque le domaine PRMD est connecté à plus d'un domaine ADMD et que le nom de domaine ADMD à un seul espace n'est pas utilisé, chaque utilisateur (ou liste DL) doit avoir plusieurs adresses d'O/R (pseudonymes) ayant des valeurs différentes pour l'attribut nom de domaine d'administration. Toutes ces valeurs de pseudonyme peuvent être utilisées comme valeurs de l'adresse d'O/R de l'expéditeur. Lorsque le pays en question autorise l'utilisation du nom de domaine ADMD à un seul espace et que le domaine PRMD choisit de l'utiliser, chaque utilisateur (ou liste DL) peut avoir une seule valeur d'adresse d'O/R, indépendamment du nombre de domaines ADMD auxquels le domaine PRMD est connecté, en supposant que tous les domaines concernés puissent appliquer cette convention.

Remarque 1 – Le choix d'un pseudonyme entraîne un certain nombre de conséquences étudiées ci-après.

Remarque 2 – L'utilisation, au niveau international, du nom de domaine ADMD à un seul espace peut être limitée, ainsi que son acceptation par des domaines ADMD d'autres pays.

Remarque 3 – Il faudra peut-être réviser les procédures MTS pour pouvoir prendre en charge les domaines PRMD multinationaux dans un environnement mondial de messagerie.

Ce cas n'est pas spécifique aux organisations multinationales: il ne peut se distinguer du cas de domaines PRMD multiples utilisés par des organisations distinctes.

Cette configuration tient compte des réglementations différentes dans plusieurs pays et prévoit également l'attribution d'adresses d'O/R uniques. Pour d'autres informations, voir également l'annexe E de la Recommandation F.400 (1992) qui utilise la même sémantique que le § G.2.1.

G.2.2 Un seul domaine PRMD désigné d'après un pays «natal»

Voir la figure G-2/X.402.

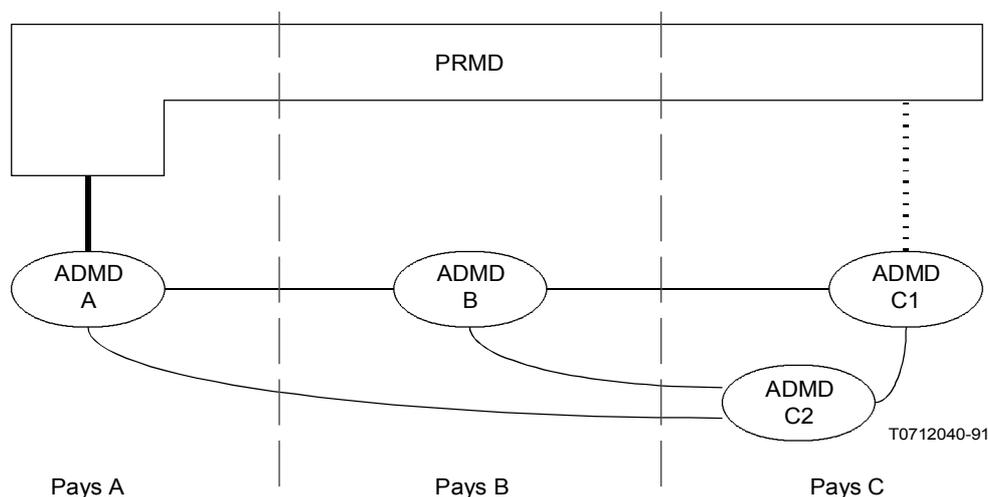


FIGURE G-2/X.402

Un seul domaine PRMD doté d'un seul nom

L'organisation multinationale peut utiliser un seul domaine de gestion physiquement implanté dans plus d'un pays. Un seul pays est choisi comme le pays natal aux fins d'adressage. Dans ce cas, les adresses de tous les agents UA situés dans ce domaine MD ont les mêmes valeurs de nom de pays, de nom de domaine d'administration et de nom de domaine privé. Cet ensemble de valeurs d'attribut est enregistré selon les spécifications du pays choisi.

Le domaine PRMD peut se connecter à un ou plusieurs domaines ADMD dans son pays natal, ainsi (selon la réglementation nationale et des critères commerciaux) qu'à des domaines ADMD situés dans d'autres pays. La connexion avec des domaines ADMD situés hors du pays natal implique que ces domaines ADMD puissent et veuillent acheminer directement des messages vers un domaine PRMD lorsque le nom de pays utilisé dans l'adresse d'O/R est différent de celui utilisé par le domaine ADMD.

Cette configuration ne pose aucun problème technique, ni aux partenaires implantés hors du domaine PRMD, ni aux fournisseurs de services intervenant lors du transfert ou de la remise des messages. Il se peut que l'utilisation conséquente, dans l'adresse d'O/R, du nom d'un pays, ne convienne pas à des utilisateurs de ces domaines PRMD, pour la raison qu'ils n'appartiennent peut-être pas à ce pays.

G.2.3 Un seul domaine PRMD doté de noms de pays et de domaine multiples

Voir la figure G-3/X.402.

L'organisation multinationale peut utiliser un seul système de messagerie et des noms de domaine PRMD enregistrés dans plus d'un pays. Au moment de la formation des adresses d'O/R, le nom de domaine d'administration doit être l'une des valeurs autorisées par le pays indiqué par la valeur du nom du pays. La valeur du nom de domaine privé utilisée dans une adresse d'O/R donnée doit être l'une de celles qui sont enregistrées de manière compatible avec le nom de pays et le nom de domaine d'administration, selon les procédures du pays ou du domaine ADMD concerné.

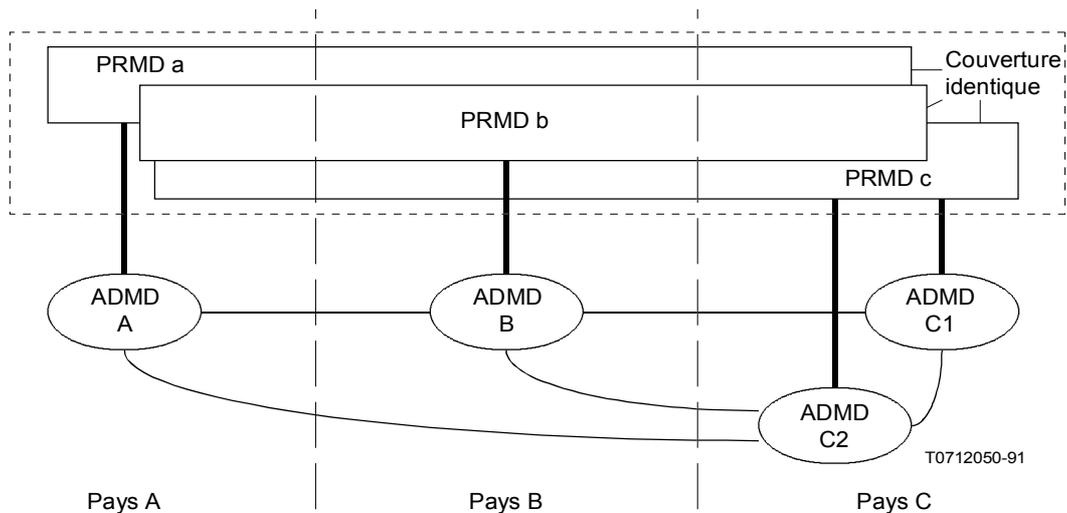


FIGURE G-3/X.402

Un seul domaine PRMD doté de noms de pays et de domaine multiples

Le domaine PRMD multinational peut se connecter à un ou plusieurs domaines ADMD. Chaque utilisateur (ou liste DL) possède à présent plusieurs adresses d'O/R pseudonymes, dans lesquelles le nom de pays, le nom de domaine d'administration et le nom de domaine privé ont des valeurs différentes. L'une quelconque de ces valeurs peut être utilisée comme valeur de l'adresse d'O/R de l'expéditeur; les utilisateurs peuvent choisir d'utiliser une adresse qui identifie le pays dans lequel ils sont physiquement implantés, mais ce choix n'est pas obligatoire, dans la mesure où le domaine ADMD concerné accepte l'adresse d'O/R choisie de l'expéditeur prévue.

Si le même utilisateur a plusieurs adresses d'O/R (pseudonymes), cela peut causer des problèmes à ses partenaires. L'expéditeur et le destinataire doivent déterminer l'adresse d'O/R qu'ils doivent utiliser dans différentes situations. Une mauvaise détermination gêne le fonctionnement des communications ouvertes. De plus, les taxes correspondant à un message donné peuvent varier selon le point d'accès choisi pour le premier domaine ADMD.

Remarque – Le choix d'un nom de pseudonyme entraîne un certain nombre de conséquences étudiées ci-après.

Les accords bilatéraux conclus entre un domaine PRMD et chacun des domaines ADMD auxquels il se connecte doivent déterminer les critères utilisés par ce domaine ADMD pour acheminer des messages vers le domaine PRMD: ces accords peuvent choisir d'acheminer directement les messages adressés à l'un quelconque des pseudonymes du domaine PRMD, ou seulement les messages adressés à l'aide de l'indicatif de pays local, en acheminant les autres par l'intermédiaire d'un domaine ADMD situé dans le pays spécifié dans l'adresse d'O/R du destinataire, tant que les principes de taxation et de comptabilité peuvent être appliqués par les fournisseurs de service concernés.

Remarque – Il peut être nécessaire de réexaminer les procédures dans le système MTS pour prendre en charge les domaines PRMD multinationaux dans un environnement de messagerie mondial.

G.3 Adresses d'O/R pseudonymes

Il ressort des cas étudiés ci-dessus qu'il existe des noms pseudonymes de domaine de gestion. La présence de pseudonymes implique un certain nombre de conséquences, tant pour les utilisateurs que pour les responsables de la mise en application du système.

Remarque – Des adresses pseudonymes peuvent également exister pour des utilisateurs à l'intérieur d'un domaine; leur traitement est généralement indépendant des pseudonymes de domaine de gestion.

Un utilisateur individuel peut choisir un domaine ADMD préféré parmi ceux qui sont disponibles, et indiquer entre guillemets les nom de pays, nom de domaine d'administration et nom de domaine privé correspondants lorsqu'il communique son adresse d'O/R, par exemple, sur une carte professionnelle ou dans l'adresse d'O/R de l'expéditeur des messages.

Un utilisateur peut également rencontrer quelques difficultés pour utiliser les services d'autres domaines ADMD auxquels le domaine PRMD est connecté. Dans certaines conditions, l'utilisateur (ou l'agent d'utilisateur) peut avoir la possibilité de sélectionner un autre des pseudonymes du domaine PRMD lorsqu'il arrive sur le domaine ADMD avec lequel il veut alors correspondre, et modifier en conséquence l'adresse d'O/R de l'expéditeur. Cependant, cela n'est possible que dans le cas où le même domaine ADMD sert à atteindre tous les destinataires d'un message, et le choix de ce domaine ADMD est alors connu au moment du dépôt. Il n'est pas possible de modifier l'adresse d'O/R de l'expéditeur après le dépôt, car ce serait incompatible avec les services de sécurité. Les utilisateurs peuvent également être induits en erreur en recevant des messages provenant du même expéditeur mais comportant des adresses d'O/R différentes.

Toutes ces raisons font qu'il peut être plus intéressant pour l'utilisateur de n'employer qu'une seule adresse d'O/R, et pour certains domaines ADMD d'accepter des messages pour lesquels l'adresse d'O/R de l'expéditeur ne correspond pas à ce nom de pays et à ce nom de domaine d'administration. Il se peut également que les adresses d'O/R de l'expéditeur ne correspondent pas au domaine PRMD local si les services de listes de distribution et de réacheminement (par exemple, le service destinataire suppléant désigné par le destinataire) sont mis en oeuvre. Des accords bilatéraux conclus entre les exploitants des domaines ADMD doivent tenir compte de l'utilisation de ces capacités (entre autres) en cas de transit par plus d'un domaine. Une accessibilité mondiale n'est pas réalisable.

L'adresse d'O/R de l'expéditeur utilisée pour envoyer des messages peut influencer le trajet emprunté par des messages envoyés en réponse. En général, les messages de réponse sont acheminés via le pays et le domaine ADMD spécifiés dans l'adresse d'O/R. Des accords bilatéraux conclus entre les domaines PRMD ou entre le domaine PRMD et des domaines ADMD peuvent permettre l'utilisation d'autres trajets. Ces facteurs peuvent influencer le choix, par l'utilisateur, d'un nom de domaine pouvant être utilisé dans l'adresse d'O/R. Il convient de garder à l'esprit que des adresses d'O/R multiples pour le même utilisateur influencent également les destinataires potentiels. Cette source de confusion peut gêner l'établissement d'une communication ouverte satisfaisante.

ANNEXE H

(à la Recommandation X.402)

Différences entre la Recommandation du CCITT et la Norme ISO

(Cette annexe ne fait pas partie intégrante de la présente Recommandation)

La présente annexe donne la liste des différences existant entre la présente Recommandation du CCITT et la Norme internationale ISO correspondante, à l'exception des différences d'ordre purement stylistique.

Ces différences sont les suivantes:

- a) La Norme internationale ISO n'impose pas de relations hiérarchiques entre les domaines ADMD et les domaines PRMD aux fins d'adressage et d'acheminement, contrairement à la présente Recommandation (voir les § 14.1.1, 14.1.2, 15 et 19).
- b) Dans le § 18.3.1, le paragraphe définissant l'attribution d'un seul espace au nom de domaine d'administration est une partie normative de la Norme ISO/CEI, mais ne constitue qu'une remarque de la Recommandation du CCITT. Le paragraphe définissant l'attribution d'un zéro seul au nom de domaine d'administration est une partie normative de la Norme ISO/CEI, mais il est omis dans la Recommandation du CCITT.
- c) La représentation des adresses d'O/R pour un usage par l'homme forme une annexe informative à la Norme internationale ISO. Dans la présente Recommandation, le texte renvoie, pour ce qui est de l'annexe F, à l'annexe B informative de la Recommandation F.401.

ANNEXE I

(à la Recommandation X.402)

(Cette annexe ne fait pas partie intégrante de la présente Recommandation)

Index

La présente annexe constitue l'index à la présente Recommandation. Elle indique les numéros des pages contenant les définitions de chaque point dans chacune des catégories. Elle recense de manière exhaustive les dits points.

La présente annexe donne l'index des points (le cas échéant) contenus dans les catégories suivantes:

- a) abréviations;
- b) termes;
- c) éléments d'information;
- d) modules ASN.1;
- e) macros ASN.1;
- f) types ASN.1;
- g) valeurs ASN.1;
- h) accords bilatéraux;

I.1 *Abréviations*

	<i>Page</i>		<i>Page</i>
A/SYS	36	MRSE	59
AC	8	MS	13
ACSE	8,60	MSSE	58
ADMD	39	MTA	14
AE	8	MTS	12
APDU	8	MTSE	58
AS/SYS	37	O	10
ASE	8	OSI	8
ASN.1	8	P1	60
AST/SYS	37	P3	60
AT/SYS	37	P7	60
AU	13	PDAU	14
C	10	PDS	14
COMPUSEC	24	PRMD	39
D	10	RO	9
DL	12	ROSE	9
DSA	9	RT	8
EIT	16	RTSE	8
M	10	S/SYS	37
MASE	59	ST/SYS	37
MD	39	T/SYS	37
MDSE	59	UA	12
MHE	11	UE	8
MHS	11		

I.2 *Termes*

access, storage, and transfer system	37	administration-domain-name	44
access and storage system	37	administration management domain	39
access and transfer system	37	affirmation	23
access system	36	application association; association	8
access unit	13	application context (AC)	8
actual recipient	19	argument	8

	<i>Page</i>		<i>Page</i>
Association Control Service Element (ACSE)	8	local-postal-attributes	46
asymmetric	57	macro	8
asynchronous	8	management domain	39
attribute	9,43	mandatory	10
attribute type	43	member recipient	19
attribute value	43	members	12
attribute list	43	message	15
bind	8	Message Handling	10
certificate	9	Message Handling Environment	11
certification authority	9	Message Handling System	11
certification path	9	Message Storage	10
common-name	46	message store	13
conditional	10	Message Transfer	10
consuming ASE	57	message transfer agent	14
consuming UE	57	Message Transfer System	12
content	15	messaging system	35
content type	15	mnemonic O/R address	52
conversion	23	module	8
country-name	46	name	9
defaultable	10	name resolution	22
delivery	21	nested	12
delivery agent	21	network-address	46
delivery report	16	non-affirmation	23
described message	16	non-delivery	23
direct submission	20	non-delivery report	17
direct user	12	numeric-user-identifier	47
Directory	9	numeric O/R address	52
directory entry; entry	9	O/R address	50
directory system agent (DSA)	9	O/R name	42
distribution list	12	object	9
DL expansion	22	object class	9
domain	39	optional	10
domain-defined attribute	43	organization-name	47
encoded information type	16	organizational-unit-names	47
envelope	15	origination	20
event	17	originator	18
expansion point	22	originator-specified alternate recipient	18
explicit	8	parameter	8
explicit conversion	23	pds-name	47
export	8,21	personal-name	47
extension-physical-delivery-address-components	46	physical-delivery-country-name	48
extension-postal-O/R-address-components	46	physical-delivery-office-name	48
external routing	24	physical-delivery-office-number	48
external transfer	20	physical-delivery-organization-name	48
formatted	52	physical-delivery-personal-name	48
Global MHS	40	Physical delivery	14
grade	10	physical delivery access unit	14
hash function	9	physical delivery system	14
immediate recipient	17	physical message	14
implicit	8	physical rendition	14
implicit conversion	23	post-office-box-address	48
import	8,20	postal-code	48
indirect submission	20	postal O/R address	52
indirect user	12	poste-restante-address	49
initiator; and	8	potential recipient	19
intended recipient	18	private-domain-name	49
internal routing	24	private management domain	39
internal transfer	20	probe	16
joining	22	receipt	21

	<i>Page</i>		<i>Page</i>
recipient	19	submission agent	20
recipient-assigned alternate recipient	19	submit permission	12
redirection	23	supplying ASE	57
remote error	9	supplying UE	57
remote operation	9	symmetric	56
Remote Operations (RO)	9	synchronous; and	9
Remote Operations Service Element (ROSE)	9	tag	8
report	16	terminal O/R address	53
responder	8	terminal-identifier	49
result	9	terminal-type	49
retrieval	21	transfer	20
ROSE	60	transfer system	37
routing	23	transmittal	17
RTSE	60	transmittal event	17
simple authentication; and	9	transmittal step	17
splitting	22	type	43
standard attribute	43	type; and	8
step	17	unbind	9
storage and transfer system	37	unformatted	52
storage system	37	unformatted-postal-address	49
street-address	49	unique-postal-name	49
strong authentication	9	user	12
subject message	16	user agent	12
subject probe	16	value	8,43
submission	20		
I.3		<i>Eléments d'information</i>	
MHS Deliverable Content Length	62	MHS O/R Address	65
MHS Deliverable Content Types	63	MHS O/R Addresses	63
MHS Deliverable EITs	63	MHS O/R Name	65
MHS DL Members	63	MHS Supported Automatic Actions	64
MHS DL Submit Permission	64	MHS Supported Content Types	64
MHS DL Submit Permissions	63	MHS Supported Optional Attributes	64
MHS Message Store	61	MHS User	62
MHS Message Store Directory Name	63	MHS Distribution List	61
MHS Message Transfer Agent	62	MHS User Agent	62
I.4		<i>Modules ASN.1</i>	
MHSDirectoryObjectsAndAttributes	67	MHSObjectIdentifiers	65
I.5		<i>Macros ASN.1</i>	
ATTRIBUTE	67	OBJECT-CLASS	67
ATTRIBUTE-SYNTAX	67		
I.6		<i>Types ASN.1</i>	
DLSubmitPermission	64,70	ORName	67
ID	65	ORNamePattern	64,70
ORAddress	65,67	RequestedDeliveryMethod	67
I.7		<i>Valeurs ASN.1</i>	
applicationEntity	67	id-arch	66
commonName	67	id-as	66
description	67	id-as-mhs-dl-submit-permission	66
distinguishedNameSyntax	67	id-as-mhs-or-address	66

	<i>Page</i>		<i>Page</i>
id-as-mhs-or-name	66	id-oc-mhs-user-agent	66
id-asdc	66	IntegerSyntax	67
id-at	66	mhs-deliverable-content-length	62,68
id-at-mhs-deliverable-content-length	66	mhs-deliverable-content-types	63,69
id-at-mhs-deliverable-content-types	66	mhs-deliverable-eits	63,69
id-at-mhs-deliverable-eits	66	mhs-distribution-list	61,67
id-at-mhs-dl-members	66	mhs-dl-members	63,69
id-at-mhs-dl-submit-permissions	66	mhs-dl-submit-permission-syntax	64,69
id-at-mhs-message-store-dn	66	mhs-dl-submit-permissions	63,69
id-at-mhs-or-addresses	66	mhs-message-store	61,68
id-at-mhs-supported-automatic-actions	66	mhs-message-store-dn	63,69
id-at-mhs-supported-content-types	66	mhs-message-transfer-agent	62,68
id-at-mhs-supported-optional-attributes	66	mhs-or-address-syntax	65,70
id-directory-objects-and-attributes	66	mhs-or-addresses	63,69
id-group	66	mhs-or-name-syntax	65,70
id-ipms	65	mhs-supported-automatic-actions	64,69
id-mhs-protocols	65	mhs-supported-content-types	64,69
id-mod	66	mhs-supported-optional-attributes	64,69
id-ms	66	mhs-user	62,68
id-mts	66	mhs-user-agent	62,68
id-object-identifiers	66	objectIdentifiersSyntax	67
id-oc	66	organization	67
id-oc-mhs-distribution-list	66	organizationalUnitName	67
id-oc-mhs-message-store	66	owner	67
id-oc-mhs-message-transfer-agent	66	seeAlso	67
id-oc-mhs-user	66	top	67
I.8	<i>Accords bilatéraux</i>		
routing	54		

ANNEXE J

(à la Recommandation X.402)

Liste alphabétique des abréviations utilisées dans la présente Recommandation

A/SYS	Système d'accès (<i>access system</i>)
AC	Contexte d'application (<i>application context</i>)
ACSE	Élément de service de contrôle d'association (<i>association control service element</i>)
ADMD	Domaine de gestion d'Administration (<i>administration management domain</i>)
AE	Entité d'application (<i>application-entity</i>)
APDU	Unité de données de protocole d'application (<i>application protocol data unit</i>)
AS/SYS	Système d'accès et de mémorisation (<i>access and storage system</i>)
ASE	Élément de service d'application (<i>application service element</i>)
ASN.1	Notation de syntaxe abstraite numéro un (<i>abstract syntax notation one</i>)
AST/SYS	Système d'accès, de mémorisation et de transfert (<i>access, storage and transfer system</i>)
AT/SYS	Système d'accès et de transfert (<i>access and transfer system</i>)
AU	Unité d'accès (<i>access unit</i>)

C	Conditionnelle (<i>conditional</i>)
COMPUSEC	Sécurité informatique (<i>computer security</i>)
D	Valeur pouvant être prise par défaut (<i>defaultable</i>)
DL	Liste de distribution (<i>distribution list</i>)
DSA	Agent de système d'annuaire (<i>directory system agent</i>)
EIT	Type d'information codée (<i>encoded information type</i>)
IA5	Alphabet international n° 5 (<i>International Alphabet No. 5</i>)
M	Obligatoire (<i>mandatory</i>)
MASE	Élément de service de gestion de messages (<i>message administration service element</i>)
MD	Domaine de gestion (<i>management domain</i>)
MDSE	Élément de service de remise de messages (<i>message delivery service element</i>)
MHE	Environnement du système de messagerie (<i>message handling environment</i>)
MHS	Système de messagerie (<i>message handling system</i>)
MRSE	Élément de service de retrait de messages (<i>message retrieval service element</i>)
MS	Mémoire de messages (<i>message store</i>)
MSSE	Élément de service de dépôt de messages (<i>message submission service element</i>)
MTA	Agent de transfert de messages (<i>message transfer agent</i>)
MTS	Système de transfert de messages (<i>message transfer system</i>)
MTSE	Élément de service de transfert de messages (<i>message transfer service element</i>)
O	Optionnelle (<i>optional</i>)
O/R	Expéditeur/destinataire (<i>originator/recipient</i>)
OSI	Interconnexion de systèmes ouverts (<i>open systems interconnection</i>)
P1	Protocole 1 (<i>protocol 1</i>)
P3	Protocole 3 (<i>protocol 3</i>)
P7	Protocole 7 (<i>protocol 7</i>)
PDAU	Unité d'accès de remise physique (<i>physical delivery access unit</i>)
PDS	Système de remise physique (<i>physical delivery system</i>)
PRMD	Domaine de gestion privé (<i>private management domain</i>)
RO	Opérations distantes (<i>remote operation</i>)
ROSE	Élément de service d'opérations distantes (<i>remote operation service element</i>)
RT	Transfert fiable (<i>reliable transfer</i>)
RTSE	Élément de service de transfert fiable (<i>reliable transfer service element</i>)
S/SYS	Système de mémorisation (<i>storage system</i>)
ST/SYS	Système de mémorisation et de transfert (<i>storage and transfer system</i>)
T/SYS	Système de transfert (<i>transfer system</i>)
UA	Agent d'utilisateur (<i>user agent</i>)
UE	Élément utilisateur (<i>user element</i>)

Imprimé en Suisse

Genève, 1993