UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

X.402

(11/1988)

SÉRIE X: RÉSEAUX DE COMMUNICATIONS DE DONNÉES: SYSTÈMES DE MESSAGERIE

SYSTEMES DE MESSAGERIE: ARCHITECTURE GLOBALE

Réédition de la Recommandation du CCITT X.402 publiée dans le Livre Bleu, Fascicule VIII.7 (1988)

NOTES

1 La Recommandation X.402 du CCITT a été publiée dans le fascicule VIII.7 du Livre Bleu. Ce fichier est un extrait du Livre Bleu. La présentation peut en être légèrement différente, mais le contenu est identique à celui du Livre Bleu et les conditions en matière de droits d'auteur restent inchangées (voir plus loin).

2 Dans la présente Recommandation, le terme «Administration» désigne indifféremment une administration de télécommunication ou une exploitation reconnue.

Recommandation X.402

SYSTEMES DE MESSAGERIE: ARCHITECTURE GLOBALE[1)]

(Melbourne, 1988)

La création dans divers pays de services télématiques et de services de messagerie informatisée en mode enregistrement et retansmission, en liaison avec les réseaux publics pour données, montre qu'il faut établir des normes facilitant les échanges internationaux de messages entre abonnés à ces services.

Le CCITT,

considérant

(a) que des systèmes de messagerie sont nécessaires;

(b) qu'il est nécessaire de transférer et de stocker des messages de types différents;

(c) que la Recommandation X.200 définit le modèle de référence pour l'interconnexion de systèmes ouverts pour les applications du CCITT;

(d) que les Recommandations X.208, X.217, X.218 et X.219 fournissent les bases pour les applications du CCITT;

(e) que les Recommandations de la série X.500 définissent les systèmes d'annuaire;

(f) que les systèmes de messagerie sont définis dans les Recommandations X.400, X.402, X.403, X.407, X.408, X.411, X.413 et X.419;

(g que la messagerie de personne à personne est définie dans les Recommandations X.420 et T.330,

déclare à l'unanimité

(1) que les modèles abstraits d'un système de messagerie sont définis dans la section 2;

(2) que les configurations d'un système de messagerie sont définies dans la section 3;

(3) que la dénomination, l'adressage et l'acheminement dans les systèmes de messagerie sont définis dans la section 4;

(4) que l'utilisation de l'annuaire par les systèmes de messagerie est définie dans la section 5;

(5) que la réalisation OSI d'un système de messagerie est spécifiée dans la section 6.

SOMMAIRE

---

[1] La Recommandation X.402 et la norme ISO 10021-2, Systèmes de traitement de l'information - Communication de textes - MOTIS -Architecture globale, ont été élaborées en collaboration étroite et sont alignées sur le plan technique, à l'exception des différences notées dans l'annexe F.

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 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 MTS à des systèmes de communication de types différents (systèmes postaux, par example). Un utilisateur est assité dans la préparation, l'enregistrement et l'affichage des ses messages par un agent d'utilisateur (AU). A titre facultatif, il est aidé pour l'enregistrement des messages par une mémoire de messages (MS). Le 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 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.

1 Domaine d'application

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

D'autres aspects de la messagerie sont spécifiés dans d'autres Recommandations. Un aperçu non technique de la messagerie est donné dans la Recommandation X.400. Les essais de conformité des composantes MHS sont décrits dans la Recommandation X.403. Les conventions utilisées dans la définition des services abstraits assurés par les composantes MHS sont définies dans la Recommandation X.407. Les règles détaillées suivant lesquelles le MTS convertit le contenu de messages d'un type de codage (EIT) en un autre sont définies dans la Recommandation X.408. Le service abstrait assuré par le MTS et les procédures qui en régissent le fonctionnement décentralisé sont définis dans la Recommandation X.411. Le service abstrait assuré par la MS est défini dans la Recommandation X.413. Les protocoles d'application qui régissent les interactions des composantes MHS sont spécifiés dans la Recommandation X.419. Le système de messagerie de personne, qui est une application de la messagerie, est défini dans la Recommandation X.420. 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 relatives à la messagerie.

TABLEAU 1/X.402

Spécifications concernant les systèmes de messagerie

CCITT	ISO	Sujets
Introduction		
X.400	8505-1	Présentation générale des services et des systèmes
X.402	8505-2	Architecture globale
Aspects divers		
X.403	–	Essais de conformité
X.407	8883-2	Conventions utilisées pour la définition du service abstrait
X.408	–	Règles de conversion du type de codage
Services abstraits		
X.411	8883-1	Définition du service abstrait MTS et procédures régissant le fonctionnement décentralisé
X.413	TBS-1	Définition du service abstrait MS
Protocoles		
X.419	8505-2	Spécifications des protocoles
Système de messagerie de personne à personne		
X.420	9065	Système de messagerie de personne à personne
T.330	–	Accès télématique à l'IMPS

L'annuaire, le principal moyen de diffuser des informations en rapport avec les communications parmi les composantes MHS, est défini dans les Recommandations de la série X.500 ainsi que le résume le tableau 2/X.402.

Les bases architecturales de la messagerie font l'objet d'autres Recommandations. Le modèle de référence OSI est défini dans la Recommandation X.200. 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 définis dans les Recommandations X.208 et X.209. Le moyen qui permet d'établir des associations et d'y mettre fin, l'ACSE, est défini dans les Recommandations X.217 et X.227. Le moyen qui permet d'acheminer de manière fiable les APDU pendant les associations, le RTSE, est défini dans les Recommandations X.218 et X.228. Le moyen qui permet d'adresser des demandes d'autres systèmes ouverts, le ROSE, est défini dans les Recommandations X.219 et X.229.

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

TABLEAU 2/X.402

Spécifications concernant les annuaires

CCITT	ISO	Sujet
Modèle		
X.200	7498	Modèle de référence OSI
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

TABLEAU 3/X.402

Spécifications concernant les bases du MHS

CCITT	ISO	Sujet
Modèle		
X.200	7498	Modèle de référence OSI
ASN.1		
X.208	8824	Notation de syntaxe abstraite
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 MHS pour satisfaire l'un quelconque des divers besoins fonctionnels, physiques et organisationnels. 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 que le MHS peut faire de l'annuaire. La section 6 décrit la manière dont les MHS est réalisé à l'aide de l'OSI. Les annexes donnent d'importants renseignements complèmentaires.

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

2 Références

La présente Recommandation et d'autres de cette série citent les documents ci-dessous.

2.1 *Interconnexion de systèmes ouverts*

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

X.200 Modèle de référence pour l'interconnexion des systèmes ouverts pour les applications CCITT (voir aussi la norme ISO 7498)

X.208 Spécification de la syntaxe abstraite numéro un (ASN.1) (voir aussi la norme ISO 8824)

X.209 Spécification des règles de codage pour la notation de syntaxe abstraite numéro un (ASN.1) (voir aussi la norme ISO 8825)

X.217 Définition du service de contrôle d'association pour l'interconnexion des systèmes ouverts pour les applications du CCITT (voir aussi la norme ISO 8649)

X.218 Transfert fiable: modèle et définition du service (voir aussi la norme ISO 9066-1)

X.219 Téléopérations: modèle, notation et définition du service (voir aussi la norme ISO 9072-1)

X.227 Spécification du service de contrôle d'association de l'OSI (interconnexion de services ouverts) pour les applications du CCITT (voir aussi la norme ISO 8650)

X.228 Transfert fiable: spécification du protocole (voir aussi la norme ISO 9066-2)

X.229 Opérations distantes: spécification du protocole (voir aussi la norme ISO 9072-2).

2.2 *Systèmes d'annuaire*

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

X.500 Annuaire – Aperçu général des concepts, modèles et services (voir aussi la norme ISO 9594-1)

X.501 Annuaire – Modèles (voir aussi la norme ISO 9594-2)

X.509 Annuaire – Cadre d'authentification (voir aussi la norme ISO 9594-8)

X.511 Annuaire – Définition du service abstrait (voir aussi la norme ISO 9594-3)

X.518 Annuaire – Procédures de fonctionnement réparti (voir aussi la norme ISO 9594-4)

X.519 Annuaire – Spécifications du protocole (voir aussi la norme ISO 9594-5)

X.520 Annuaire – Types d'attributs séléctionnés (voir aussi la norme ISO 9594-6)

X.521 Annuaire – Catégories d'objets choisies (voir aussi la norme ISO 9594-7).

2.3 *Systèmes de messagerie*

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

T.330 Accès télématique aux systèmes de messagerie de personne à personne

X.400 Systèmes de messagerie – Principes du système et du service de messagerie (voir aussi la norme ISO 10021-1)

X.403 Systèmes de messagerie – Essais de conformité

X.407 Systèmes de messagerie – Conventions pour la définition des services abstraits (voir aussi la norme ISO 10021-3)

X.408 Systèmes de messagerie – Règles de conversion entre differents types d'information codées

X.411 Systèmes de messagerie – Système de transfert de messages: définition des services abstraits et procédures (voir aussi la norme ISO 10021-4)

X.413 Systèmes de messagerie – Définition du service abstrait d'enregistrement de messages (MS) (voir aussi la norme ISO 10021-5)

X.419 Systèmes de messagerie – Spécification de protocoles (voir aussi la norme ISO 10021-6)

X.420 Systèmes de messagerie – Système de messagerie de personne à personne (voir aussi la norme ISO 10021-7).

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 de systèmes ouverts*

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

a) syntaxe abstraite;

b) entité d'application (AE);

c) processus d'application;

d) unité de données de protocole d'application (APDU);

e) élément de service d'application (ASE);

f) tâche de traitement de l'information par répartition;

g) couche;

h) système ouvert;

i) interconnexion de systèmes ouverts (OSI);

j) homologue;

k) contexte de présentation;

l) protocole;

m) modèle de référence;

n) syntaxe de transfert;

o) élément utilisateur (UE).

3.1.2 La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans les Recommandations X.208 et X.209, ainsi que les noms des types de données et des valeurs de l'ASN.1:

a) notation de syntaxe abstraite un (ASN.1);

b) règles de codage de base;

c) explicite;

d) export;

e) implicite;

f) import;

g) macro;

h) module;

i) Etiquette;

j) type;

k) valeur.

3.1.3 La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Recommandation X.217:

a) association d'application; association;

b) contexte d'application (AC);

c) élément de service de commande d'association (ACSE);

d) demandeur;

e) demandé.

3.1.4 La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Recommandation X.218:

a) transfert fiable (RT);

b) élément de service de transfert fiable (RTSE).

3.1.5 La présente Recommandation et d'autres de cette série utilisent les termes ci-après qui sont définis dans la Recommandation X.219:

a) argument;

b) asynchrone;

c) rattachement;

d) paramètre;

e) erreur distante;

f) opération distante;

g) opérations distantes (RO);

h) élément de service d'opérations distantes (ROSE);

i) résultat;

j) synchrone;

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 Recommandations X.500 et suivantes:

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 (DAS);

g) annuaire;

h) fonction hash;

i) nom;

j) classe d'objet;

k) objet;

l) authentification simple;

m) authentification ferme.

3.3 *Systèmes de messagerie*

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

4 Abréviations

Pour les besoins de la présente Recommandation et d'autres Recommandations de cette série, les abréviations répertoriées dans l'annexe G 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'ANS.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 CLASSE-OBJET, ATTRIBUT, et SYNTAXE-ATTRIBUT de la Recommandation X.501 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 définit dans l'annexe C; ce module est défini 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):** une composante obligatoire doit être présente dans chaque exemple de la classe.

b) **facultative (O):** une composante facultative doit être présente dans un exemple de la classe à la discrétion de l'objet (utilisateur, par exemple) qui fournit cet exemple. Il n'y a pas de valeur par défaut.

c) **possibilité de prise d'une valeur par défaut (D):** une composante qui peut prendre une valeur par défaut doit être présente dans un exemple de la classe à la discrétion de l'objet (utilisateur, par exemple) qui fournit cet exemple. En l'absence d'une telle composante, une valeur par défaut, spécifiée par la présente Recommandation, est appliquée.

d) **conditionnelle (C):** une composante conditionnelle doit être présente dans un exemple 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'il sont définis, en italique, lorsqu'ils sont mentionnés avant leur définition et sans restitution graphique dans les autres cas.

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

SECTION 2 – MODELES ABSTRAITS

6 Présentation générale

La présente section présente les modèles abstraits de Messagerie qui fournissent la base architecturale pour les spécifications plus détaillées qui figurent dans d'autres Recommandations de cette série.

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 (pas en temps réel) 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 Recommandation X.420.

7 Modèle fonctionnel

Un modèle fonctionnel de messagerie est présenté ici. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations de cette série.

L'environnement, du MHS (MHE) comprend des objets fonctionnels «primaires» de plusieurs types, le système de messagerie (MHS), les utilisateurs et les listes de distribution. Le 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 MTS à son tour peut 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 cette application.

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 de cette série. En particulier, un agent d'utilisateur type assure des fonctions non normalisées de préparation, de mise en valeur et d'enregistrement des messages.

7.1 *Objets fonctionnels primaires*

Le 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.

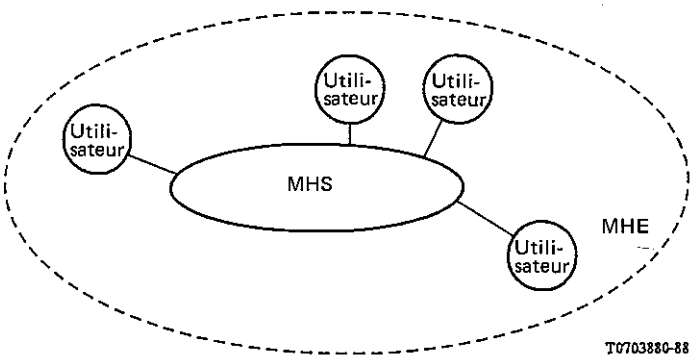


FIGURE 1/X.402

L'environnement du MHS

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)**.

Le MHE comprend un seul MHS.

7.1.2 *Utilisateurs*

Le principal but du MHS est d'acheminer des objets d'information entre utilisateurs. Un objet fonctionnel (une personne, par exemple) qui se lance dans la messagerie (plutôt qu'il ne l'assure) est appelé un utilisateur.

On distingue les sortes d'utilisateurs suivantes:

a) **utilisateur direct** – Utilisateur qui se lance dans la messagerie en utilisant directement le MHS.

b) **utilisateur indirect** – Utilisateur qui se lance dans la messagerie en utilisant indirectement le 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 MHS est relié;

Le MHE comprend un nombre quelconque d'utilisateurs.

7.1.3 *Listes de distribution*

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

Une DL peut n'identifier aucun utilisateur comme elle peut en identifier plusieurs; les DL appelées identifient leurs **membres**. On dit que ces dernières DL (le cas échéant) sont imbriquées. Demander au MHS de transmettre un objet d'information (un message, par exemple) à une DL équivaut à lui demander de transmettre l'objet à ses membres. A noter qu'il s'agit là d'un phénomène récurrent.

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

Le MHE comprend un nombre quelconque de DL.

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

7.2 *Objets fonctionnels secondaires*

Le 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.

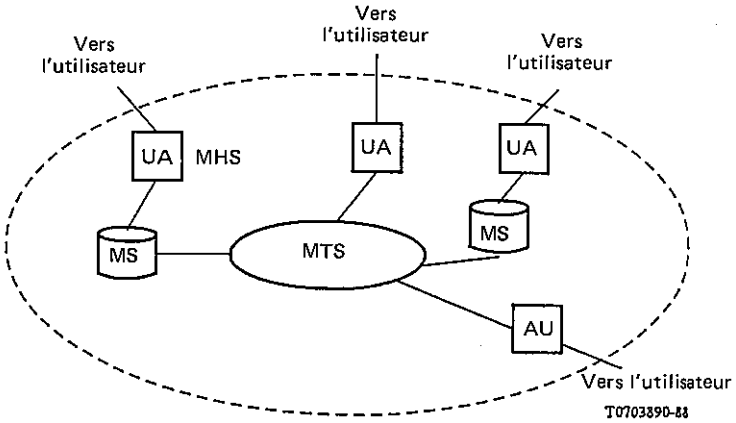


FIGURE 2/X.402

Système de messagerie

7.2.1 *Système de ransfert de messages*

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

Le 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 MHS comprend un seul 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)**.

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

Le MHS comporte un nombre quelconque d'UA.

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

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). Chaque MS est associée à un UA, mais les UA n'ont pas tous une MS qui leur est associée.

Chaque MS est polyvalente, assurant toutes les applications de messagerie. En outre, une 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 MHS comporte un nombre quelconque de MS.

Remarque – A l'échelon local, un UA peut assurer l'enregistrement d'objets d'information en sus ou à la place d'une 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 MTS, et par l'intermédiaire duquel les clients de ce système recourent à la messagerie en tant qu'utilisateurs indirects, est appelé une **unité d'accès (AU)**.

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

Le MHS comporte un nombre quelconque d'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.

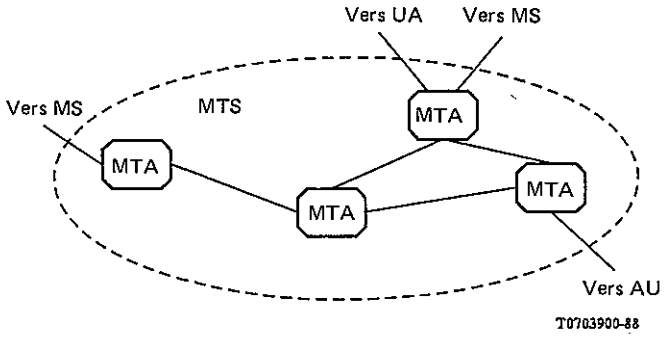


FIGURE 3/X.402

Système de transfert de messages

7.3.1 *Agents de transfert de messages*

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

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

Le MTS comporte un nombre quelconque de MTA.

7.4 *Types d'AU choisis*

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

7.4.1 *Remise physique*

Une **unité d'accès à la remise physique (PDAU)** est une AU qui soumet des messages (mais ni des essais ni des rapports) à la mise en valeur physique et qui transmet les messages physiques qui en résultent à un système de remise physique.

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

Parmi les applications de messagerie qu'assure chaque PDAU, signalons la messagerie de personne à personne (voir la Recommandation X.420).

7.4.2 *Télématique*

Les unités d'accès télématique, qui assurent la messagerie de personne à personne exclusivement, sont présentées dans la Recommandation X.420.

7.4.3 *Télex*

Les unités d'accès télex, qui assurent la messagerie de personne à personne exclusivement, sont présentées dans la Recommandation X.420.

8 Modèle d'information

Le présent paragraphe présente un modèle d'information de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations de cette série.

Le MHS et le MTS peuvent transmettre des objets d'information de trois catégories: message, essais, et rapports. Ces catégories sont indiquées dans la première colonne du tableau 4/X.402. Pour chaque catégorie indiquée, la seconde colonne indique les types d'objets fonctionnels – utilisateurs, UA, MS, MTA et AU – qui sont les sources et les destinations ultimes de ces objets.

TABLEAU 4/X.402

Objets d'information acheminables

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

S Source ultime

D Destination ultime

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

8.1 *Messages*

Le principal but 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:

a) **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, documente sa précédente transmission et dirige sa transmission ultérieure par le MTS et en caractérise le contenu.

b) **contenu** – Objet d'information que le MTS n'examine ni ne modifie, sauf pour la conversion, pendant qu'il transmet le message.

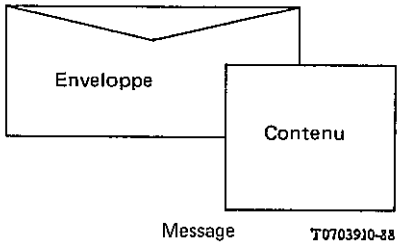


FIGURE 4/X.402

Enveloppe et contenu d'un message

Une information portée par l'enveloppe identifie le type de 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 MTS de déterminer si le message peut être remis à des utilisateurs particuliers, et permet aux UA et aux MS d'interpréter et de traiter le contenu.

Une autre information portée par l'enveloppe identifie les types de codage représentés dans le contenu. Un **type de codage** (EIT) est un identificateur (un identificateur d'objet ASN.1 ou un nombre entier) qui désigne le support et le format (texte et AI5 ou télécopie du groupe 3, par exemple) de portions individuelles de contenu. Un EIT permet en outre au 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 de codage en un autre.

8.2 *Essais*

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

Un message décrit par un essai est appelé un **message décrit**

Un essai comporte une seule enveloppe. Cette enveloppe contient pratiquement la même information que celle d'un message. Outre le type de contenu et les types de codage d'un message décrit, l'enveloppe d'un essai porte la longueur de son contenu.

Le dépot d'un essai engendre dans le MTS essentiellement le même comportement que le dépot de n'importe quel message décrit, sauf que, dans ce cas, l'on renonce à l'allongement de la DL et à la remise. En particulier, les conséquences de la suppression de l'allongement de la DL mises à part, l'essai donne lieu aux mêmes rapports que n'importe quel message décrit. C'est ce qui confère aux essais leur utilité.

8.3 *Rapports*

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

Le message ou l'essai faisant l'objet d'un rapport sont respectivement appelés **message d'objet** ou **essai objet**.

Un rapport concernant un destinataire potentiel particulier est communiqué à l'expéditeur du message ou essai d'objet à moins que le destinataire potentiel ne soit un destinataire membre. Dans ce dernier cas, le rapport est transmis à la DL dont est membre le destinataire membre. A l'échelon local (c'est–à–dire en vertu d'une politique arrêtée pour cette DL), le rapport peut en outre être communiqué au propriétaire de la DL; soit à un autre, contenant la DL (en cas d'imbrication) soit (dans le cas contraire) à l'expéditeur du message d'objet, ou aux deux à la fois.

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

a) **rapport de remise –** *Remise*, export ou *affirmation* du message ou essai d'objet, ou *allongement de DL*;

b) **rapport de non-remise** – *Non-remise* ou *non-affirmation* du message ou essai d'objet.

Un même rapport peut contenir un ou plusieurs rapports de remise et/ou de non–remise.

Un message ou un essai 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

Ce paragraphe présente un modèle opérationnel de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres Recommandations de cette même série.

Le MHS peut transmettre un objet d'information à des utilisateurs individuels, à des DL ou à une combinaison des uns et des autres. Un tel acheminement s'effectue par un processus appelé transmission qui comprend des étapes et des événements. Ce processus, ses parties, et les rôles que les utilisateurs et les 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 essai sont appelés **transmission**. La transmission englobe l'acheminement d'un message par son expéditeur à ses destinataires potentiels, et l'acheminement d'un essai par son expéditeur à des 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 éventuels rapports auxquels le message ou l'essai donnent 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 essai ou d'un rapport par 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 essai 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. La figure montre les types d'objets fonctionnels – utilisateurs directs, utilisateurs indirects, UA, MS, MTA et AU – qui peuvent intervenir pendant une transmission, les objets d'information – messages, essais et rapports – qui peuvent être transmis entre eux, et les noms des étapes de transmission par l'intermédiaire desquelles ces transmissions sont accomplies.

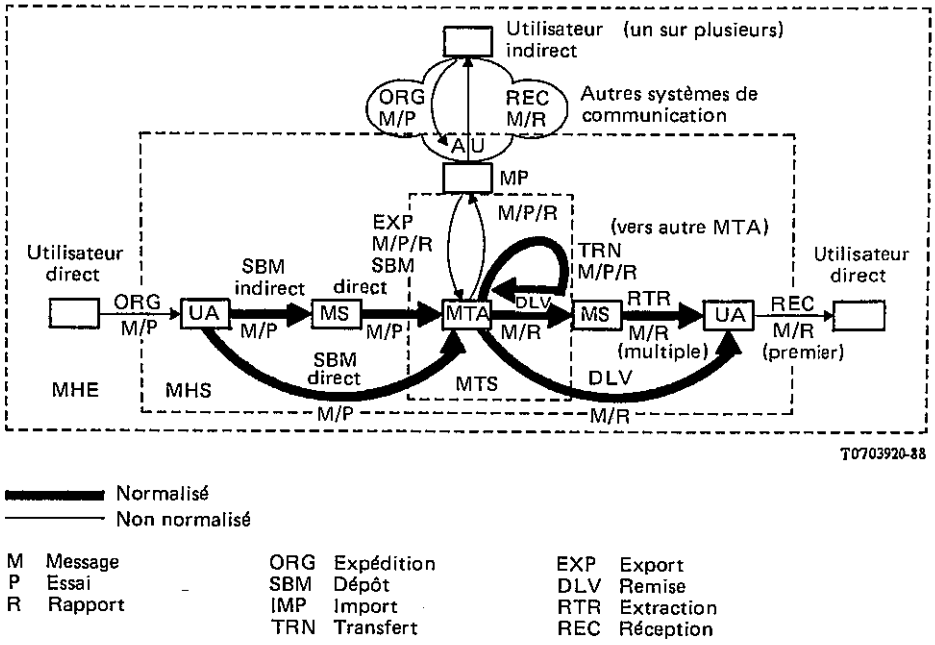


FIGURE 5/X.402

Cheminement de l'information au cours de la transmission

La figure 5/X.402 souligne qu'un message ou un rapport peuvent être trouvés à plusieurs reprises et que seule la première transmission d'un objet retrouvé de l'UA vers l'utilisateur constitue la réception.

Un événement joue un rôle notable pendant la transmission. Le fractionnement reproduit un message ou un essai et répartit la responsabilité de ses destinataires immédiats entre les objets d'information qui en résultent. Les destinataires potentiels associés à un exemple particulier de message ou d'essai sont appelés **destinataires immédiats**. Un MTA déclenche un fractionnement si l'étape ou l'événement suivants nécessaires pour acheminer un message ou un essai à des destinataires immédiats diffèrent de l'étape ou de l'événement nécessaires pour acheminer ce message ou cet essai à d'autres. Chacune des descriptions de l'étape et de l'événement qui suivent suppose que l'étape ou l'événement conviennent à tous les destinataires immédiats, situation qui peut être créée, si nécessaire, par le fractionnement.

9.2 *Rôles de transmission*

Les utilisateurs et les DL jouent différents rôles dans la transmission d'un message ou d'un essai. Ces rôles sont informellement classés en rôle «source», en rôle «destination» ou en états auxquels les utilisateurs ou les DL peuvent être élevés.

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

a) **expéditeur** – Utilisateur (mais pas la DL) qui est la source ultime d'un message ou d'un essai.

9.2.2 Un utilisateur ou une DL peuvent jouer, dans la transmission d'un message ou d'un essai, l'un quelconque des rôles «destination» suivants:

a) **destinataire prévu** – Un des utilisateurs et une des DL que l'expéditeur spécifie comme étant les destinations prévues d'un message ou d'un essai.

b) **destinataire suppléant spécifié par l'expéditeur** – Utilisateur ou la DL (le cas échéant) auquel (à laquelle) l'expéditeur demande qu'un message ou un essai soit acheminé s'il ne peut être acheminé à un destinataire prévu particulier.

c) **destinataire membre** – Utilisateur ou une DL auquel (à laquelle) un message (mais pas un essai) est acheminé par suite d'une expansion DL.

d) **destinataire suppléant désigné par le destinataire** – Utilisateur ou la DL (le cas échéant) auquel (à laquelle) la personne prévue en tant que suppléant spécifié comme expéditeur ou destinataire membre peut avoir choisi de réacheminer des messages.

9.2.3 Un utilisateur ou une DL peuvent atteindre, au cours de la transmission d'un message ou d'un essai, l'un quelconque des états suivants:

a) **destinataire potentiel** – Utilisateur ou une DL quelconque vers lequel (ou vers laquelle) un message ou un essai est acheminé à un moment quelconque au cours de la transmission. Il s'agit nécessairement de l'un des suppléants spécifiés par l'expéditeur, membre ou des destinataires suppléants désignés par le destinataire.

b) **destinataire effectif (ou destinataire)** – Destinataire potentiel pour lequel la remise ou l'affirmation a lieu.

9.3 *Etapes de transmission*

Les types d'étapes qui peuvent se produire au cours d'une transmission sont énumérées 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 ou dans d'autres Recommandations de cette série, la troisième colonne précise les types d'objets d'information – messages, essais et rapports – qui peuvent être acheminés au cours d'une telle étape et la quatrième colonne indique les types d'objets fonctionnels – utilisateurs, UA, MS, MTA et AU – qui peuvent intervenir au cours d'une telle 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 s'appliquent à la «création» de messages et d'essais; celles indiquées dans la dernière section s'appliquent à la «finalité» des messages et des rapports et celles indiquées dans la section intermédiaire s'appliquent à la «retransmission» des messages, essais et rapports.

Les types d'étapes de transmission, résumés dans le tableau 5/X.402, sont définis et décrits un à un 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 Essai D Destination

R Rapport X Permis

9.3.1 *Expédition*

Dans une étape expédition, un utilisateur direct transmet un message ou un essai à son UA, ou un utilisateur indirect transmet un message ou un essai au système de communication qui le dessert. Cette étape engendre le message ou l'essai et constitue la première étape dans la transmissin de ce message ou de cet essai.

L'utilisateur ci–dessus constitue l'expéditeur du message ou de l'essai. Dans cette étape, l'expéditeur identifie les destinataires prévus du message ou de l'essai. 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 essai est transmis à un MTA et par conséquent confié au MTS. On distingue deux types de dépôt:

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

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

b) **dépôt direct** – Etape de transmission au cours de laquelle l'UA de l'expéditeur ou la MS transmettent un message ou un essai à un MTA. Cette étape suit l'expédition ou intervient pendant le dépôt indirect.

   Cette étape peut être mise en oeuvre, que l'utilisateur soit équipé ou non d'une 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 UA doit dialoguer, par exemple) et, pour cette raison, être préférable au dépôt direct.

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

9.3.3 *Import*

Dans une étape **import**, un AU transmet un message, un essai ou un rapport à un MTA. Cette étape injecte dans le MTS un objet d'information qui a pris naissance dans un autre système de communication et suit l'acheminement de cet objet par ce système.

Remarque – Le concept d'importation est un concept générique. La manière dont cette étape est effectuée varie, naturellement, d'un type d'AU à un autre.

9.3.4 *Transfert*

Dans une étape transfert, un MTA transmet un message, un essai 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 oeuvre, naturellement, que si le MTS comporte plusieurs MTA.

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

a) **transfert interne** – Transfert faisant intervenir plusieurs MTA au sein d'une seule MD.

b) **transfert externe** – Transfert faisant intervenir plusieurs MTA au sein de diverses MD.

9.3.5 *Export*

Dans une étape export, un MTA transmet un message, un essai ou un rapport à un AU. Cette étape éjecte du 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, le MTA peut produire un rapport de remise.

Remarque – Le concept d'exportation est un concept générique. La manière dont cette étape est effectuée varie, naturellement, d'un type d'AU à un autre.

9.3.6 *Remise*

Dans une étape **remise**, un MTA transmet un message ou un rapport à une MS ou un UA. La MS et l'UA sont ceux d'un destinataire potentiel du message, ou l'expéditeur du message ou de l'essai d'objet 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, le MTA peut produire un rapport de remise.

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

9.3.7 *Extraction*

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

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

9.3.8 *Réception*

Dans une étape **réception**, un 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'essai d'objet.

9.4 *Evénements de transmission*

Les types d'événements qui peuvent se produire dans une transmission sont indiqués dans la première colonne du tableau 6/X.402. Pour chaque type indiqué, la deuxième colonne indique les types d'objets d'information – messages, essais et rapports – pour lesquels ces événements peuvent être mis en oeuvre, la troisième colonne indiquant les types d'objets fonctionnels – utilisateurs, UA, MS, MTA et AU – qui peuvent mettre en oeuvre ces événements.

Tous les événements se produisent à l'intérieur du MTS.

TABLEAU 6/X.402

Evénements de transmission

Evénement de transmission	Objets d'information			Objets fonctionnels				
	M	P	R	Utilisateur	UA	MS	MTA	AU
Fractionnement	X	X	–	–	–	–	X	–
Association	X	X	X	–	–	–	X	–
Résolution de nom	X	X	–	–	–	–	X	–
Allongement de 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 Essai

R Rapport

X Permis

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

9.4.1 *Fractionnement*

Dans un événement **fractionnement**, un MTA reproduit un message ou un essai, en partageant la responsabilité de ses destinataires directs entre les objets d'information qui en résultent. Cet événement permet effectivement à un MTA de transmettre en toute indépendance un objet à divers destinataires potentiels.

Un MTA prévoit un fractionnement quand l'étape ou l'événement suivants nécessaires pour la transmission d'un message ou d'un essai à des destinataires directs diffèrent de l'étape ou de l'événement nécessaires à la transmission de ce message ou de cet essai à d'autres destinataires.

9.4.2 *Association*

Dans un événement **association**, un MTA combine plusieurs exemples du même message ou essai, ou deux rapports ou plus de remise et/ou de non–remise pour le même message ou essai d'objet.

Un MTA peut prévoir une association, 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 de nom*

Dans un événement **résolution de nom**, un 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 essai.

9.4.4 *Allongement de la DL*

Dans un événement **allongement de la DL**, un MTA établit une DL entre les destinataires immédiats d'un message (mais pas d'un essai) à ses membres qui deviennent de ce fait des destinataires membres. Cet événement supprime toute inexactitude de la spécification des destinataires immédiats.

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

Au cours de cet événement, le MTA peut produire un rapport de remise.

L'allongement de la DL est soumise à une permission de dépôt. Dans le cas d'une DL imbriquée, cette permission doit avoir été accordée à la DL dont la DL imbriquée est membre. Autrement, elle doit avoir été accordée à l'expéditeur.

9.4.5 *Réacheminement*

Dans un événement **réacheminement**, un MTA remplace un utilisateur ou une DL parmi les destinataires directs d'un message ou d'un essai par un destinataire suppléant spécifié par l'expéditeur ou désigné par le destinataire.

9.4.6 *Conversion*

Dans un événement **conversion**, un MTA convertit des parties du contenu d'un message d'un type de codage (EIT) en un autre, ou change un essai de manière qu'il apparaisse que les messages décrits ont été modifiés en conséquence. Cet événement accroît la probabilité qu'un objet d'information a de pouvoir être remis ou affirmé par adaptation à ses destinataires directs.

En fonction de la manière dont l'EIT de l'information à convertir et l'EIT qui résultera de la conversion sont choisis, on distingue les types de conversion suivants:

a) **conversion explicite** – Conversion dans laquelle l'expéditeur choisit les EIT initiaux et finals.

b) **conversion implicite** – Conversion dans laquelle le MTA choisit les EIT finals en fonction des EIT initiaux et les possibilités de l'UA.

9.4.7 *Non-remise*

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

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

Un MTA déclenche une non–remise, par exemple, quand il établit que les destinataires directs 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 MTA établit que le MTS n'a pas pu remettre un mesage décrit aux destinataires directs d'un essai. Cet événement détermine en partie ou en totalité la réponse à la question posée par un essai.

Au cours de cet événement, le MTA produit un rapport de non–remise.

Un MTA déclenche une non-affirmation, par exemple quand il établit que les destinataires directs 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 MTA établit que le MTS pouvait remettre n'importe quel message décrit aux destinataires directs d'un essai. Cet événement détermine en partie ou en totalité la réponse à la question posée par un essai et élève les destinataires immédiats au statut de destinataires effectifs.

Au cours de cet événement, le MTA peut produire un rapport de remise.

Un MTA déclenche une affirmation après avoir établi que les destinataires directs sont convenablement spécifiés et, si les destinataires directs sont des utilisateurs (mais pas des DL), qu'ils accepteront la remise de n'importe quel message décrit. Si les destinataires directs sont des DL, un MTA déclenche une affirmation si la DL existe et si l'expéditeur a la permission de présenter son message.

9.4.10 *Acheminement*

Dans un événement **acheminement**, un MTA choisit le MTA «adjacent» auquel il transférera un message, un essai ou un rapport. Cet événement détermine pas à pas l'itinéraire de l'objet d'information à travers le MTS et (naturellement) ne peut être accepté que si le MTS comporte plusieurs 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 MD).

b) **acheminement externe** – Acheminement préparatoire pour un transfert externe (c'est-à-dire un transfert entre MD).

Un 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 de cette série. Le modèle de sécurité offre un cadre pour décrire les services de sécurité qui évitent les risques potentiels (voir l'annexe D) qui pèsent sur le MTS et les éléments de sécurité apportés en soutien à ces services.

Les fonctions de sécurité sont des extensions optionnelles du MHS qui peuvent être utilisées pour ramener au minimum le risque d'exposition des biens et des ressources à des violations d'une politique de sécurité (risques). Elles ont pout but d'assurer des fonctions indépendamment des services de communication assurés par d'autres entités inférieures ou supérieures. Des menaces peuvent être contrées moyennant l'utilisation de services de sécurité physique, de sécurité informatique (COMPUSEC) ou de sécurité assurés par le MHS. En fonction des menaces perçues, certains services de sécurité MHS seront choisis en combinaison avec des mesures appropriées de sécurité physique et COMPUSEC. Les services de sécurité assurés par le MHS sont décrits ci–dessous. La dénomination et la structuration des services sont fondées sur la norme ISO 7498–2.

Remarque – Malgré ces fonctions de sécurité, des attaques peuvent être perpétrées contre la communication entre un utilisateur et le MHS ou contre la communication entre utilisateurs (par exemple lorsque l'utilisateur a accès au MHS par une entité d'accès ou qu'il communique avec cette unité par téléconsultation. Pour parer à ces attaques, il faudrait étendre le modèle et les services de sécurité, ce qui nécessite un complément d'étude.

Dans un grand nombre de cas, les grandes catégories de menaces sont couvertes par plusieurs des services énumérés.

Les services de sécurité sont assurés grâce à l'utilisation d'éléments de service de l'enveloppe message du Service de transfert de messages. Cette enveloppe contient des arguments relatifs à la sécurité, comme indiqué dans la Recommandation X.411. La description des services de sécurité prend la forme générale suivante. Les services sont énumérés au § 10.2, 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 Recommandation X.411. Les éléments de sécurité sont décrits un à un au § 10.3, accompagnés, dans chaque cas, d'une définition de l'élément de service et des références à ses arguments constitutifs figurant dans la Recommandation X.411.

Nombre des techniques employées sont tributaires de mécanismes de chiffrement. Les services de sécurité du 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 Recommandation X.400. Les premiers de ces termes sont utilisés dans le présent paragraphe dans un souci de conformité avec la norme ISO 7498–2.

10.1 *Politiques de sécurité*

Les services de sécurité du MHS doivent pouvoir admettre une grande diversité de politiques de sécurité applicables au-delà des limites du seul MHS. Les services choisis et les risques encourus dépendront de chaque application et des niveaux de confiance dans les différentes parties du système.

Une politique de sécurité définit comment les risques auxquels les biens sont exposés peuvent être réduits à un niveau acceptable.

En outre, des domaines différents, ayant chacun leur propre politique de sécurité, devront pouvoir entrer en interfonctionnement. Comme chaque domaine sera soumis à sa propre politique générale de sécurité, laquelle s'appliquera au-delà des limites du seul MHS, un accord bilatéral sur l'interfonctionnement entre deux domaines sera nécessaire. Cet accord doit être défini de manière à ne pas être en contradiction avec la politique de sécurité de l'un ou l'autre domaine et à devenir de fait partie intégrante de la politique générale de sécurité de chaque domaine.

10.2 *Services de sécurité*

Le présent paragraphe définit les services de sécurité du transfert de message du MHS. La dénomination et la structuration des services sont fondées sur la norme 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.

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

10.2.1 *Services de sécurité Authentification d'origine*

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

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

Ces services de sécurité donnent aux entités concernées (c'est-à-dire MTA ou utilisateurs-MTS destinataires) confirmation de l'origine d'un message, d'un essai ou d'un rapport. Ces services de sécurité ne protègent pas contre la reproduction de messages, d'essais ou de rapports.

10.2.1.1.1 *Service de sécurité Authentification de l'origine des messages*

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

Ce service de sécurité peut être assuré à l'aide de l'élément de sécurité Authentification de l'origine des messages ou de l'élément de sécurité Intégrité de l'argument des messages. Le premier de ces éléments peut être utilisé pour assurer 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 assurer le service de sécurité aux utilisateurs-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 des essais*

Le service de sécurité Authentification de l'origine des essais confirme la provenance d'un essai.

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

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
Authentification d'origine	*	*	–	*	–	–	–	–
Authentification de l'origine du message								
Authentification de l'origine de l'essai	–	–	*	*	–	–	–	–
Authentification de l'origine du rapport	–	–	–	–	*	*	*	–
Preuve du dépôt	–	–	–	–	–	–	*	–
Preuve de la remise	*	–	–	–	–	–	–	a)
Gestion d'accès sur	–	*	*	*	*	*	*	*
Authentification de l'entité homologue								
Contexte de sécurité	–	*	*	*	*	*	*	*
Confidentialité des données	–	*	*	*	*	*	*	*
Confidentialité de la communication								
Confidentialité du contenu	*	–	–	–	–	–	–	–
Confidentialité du cheminement du message	*	–	–	–	–	–	–	–
Service d'intégrité des données	–	*	*	*	*	*	*	*
Intégrité de la communication								
Intégrité du contenu	*	–	–	–	–	–	–	–
Intégrité de la séquence de message	*	–	–	–	–	–	–	–
Non–répudiation	*	–	–	*	–	–	–	–
Non–répudiation d'origine								
Non–répudiation de dépôt	–	–	–	–	–	–	*	–
Non–répudation de remise	*	–	–	–	–	–	–	–
Etiquetage de sécurité du message	*	*	*	*	*	*	*	*
Etiquetage de sécurité du message								
Services de gestion de sécurité	–	*	–	*	*	*	*	–
Modifications des pouvoirs								
Enregistrement	–	*	–	*	–	–	–	–
MS–Enregistrement	–	*	–	–	–	–	–	–

* Un astérisque sous l'en–tête de la forme X/Y indique que le service peut être assuré à partir d'un objet fonctionnel de type X vers un objet fonctionnel de type Y.

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

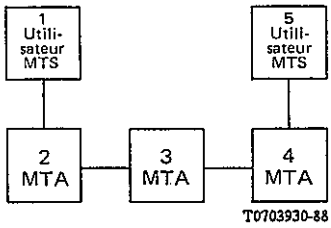


FIGURE 6/X.402

Modèle fonctionnel MHS simplifié

10.2.1.2 *Service de sécurité Preuve de dépôt*

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

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

10.2.1.3 *Service de sécurité Preuve de la remise*

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

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

10.2.2 *Service de sécurité Gestion d'accès sûr*

Le service de sécurité Gestion d'accès sûr 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.

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 communication pour confirmer l'identité de l'entité qui établit la communication. Il peut être utilisé sur les liaisons 1-2, 2-3, 3-4 ou 4-5, représentées sur la figure 6/X.402, et garantit, au moment de l'utilisation uniquement, qu'une entité ne tente pas d'abuser de la confiance d'une autre en se faisant passer pour elle ou de repasser sans autorisation une communication 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 avoir pour effet de produire d'autres données qui, dans certaines circonstances, peuvent être utilisées pour assurer un service de sécurité Confidentialité de la communication et/ou Intégrité de la communication.

10.2.2.2 *Service de sécurité Contexte de sécurité*

Ce service de sécurité est utilisé pour limiter la possibilité de passage de messages entre entités moyennant référence aux étiquettes de sécurité associées aux messages. Ce service de sécurité est donc étroitement lié au service de sécurité Etiquetage de sécurité des messages, qui permet l'association de messages et d'étiquettes 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 des communications*

Le MHS n'assure aucun service de sécurité Confidentialité des communications. Toutefois, des données permettant l'appel d'un tel service de sécurité dans les couches sous–jacentes peuvent être fournies par suite de l'utilisation de l'élément de sécurité Echange d'authentification pour assurer le service de sécurité Authentification de l'entité homologue. Le service de sécurité peut devoir être assuré 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.

On peut, pour l'assurer, recourir à une combinaison des 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 MTA.

10.2.3.3 *Service de sécurité Confidentialité du cheminement des messages*

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

La technique de double enveloppement 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 MTS. Utilisée conjointement avec la technique de 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 périodique 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 assurés pour éviter les risques effectifs auxquels le MHS est exposé.

10.2.4.1 *Services de sécurité Intégrité des communications*

Le MHS n'assure aucun service de sécurité Intégrité des communications. Néanmoins, des données permettant l'appel d'un tel service de sécurité dans les couches adjacentes peuvent être fournies moyennant l'utilisation de l'élément de sécurité Echange d'authentification afin d'assurer le service de sécurité Authentification de l'entité homologue. Le service de sécurité peut devoir être assuré 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. Pour ce faire, il faut établir si le contenu du message a été modifié. Ce service de sécurité n'offre pas de possibilité de détection de la répétition d'un message, possibilité qui est offerte par le service de sécurité Intégrité de la séquence des messages.

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, conjointement à l'élément de sécurité Intrégrité de l'argument du message et, dans certains cas, l'élément de sécurité Confidentialité de l'argument du message, peut être utilisé pour assurer le service de sécurité au destinataire d'un message, c'est-à-dire pour établir une communication depuis l'utilisateur-MTS 1 jusqu'à l'utilisateur-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 met le contrôle d'intégrité du contenu à l'abri de tout changement. L'intégrité des arguments de message confidentiel est assuré à l'aide de 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 des messages*

Ce service de sécurité protège l'expéditeur et le destinataire d'une séquence de messages contre tout réagencement de la séquence. Ce faisant, il évite toute répétition des messages.

Ce service de sécurité peut être assuré à l'aide d'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, lequel peut être mis à l'abri de tout changement moyennant l'utilisation du second élément. La confidentialité et l'intégrité du numéro d'ordre des messages peuvent être simultanément assurées à l'aide de l'élément de sécurité Confidentialité de l'argument du message.

Ces éléments de sécurité mettent en communication l'utilisateur–MTS 1 et l'utilisateur–MTS 5 de la figure 6/X.402, mais non les MTA intermédiaires.

10.2.5 *Services de sécurité Non-répudiation*

Ces services de sécurité apportent à un tiers, après que le message a été déposé, émis ou remis, la preuve irréfutable que le dépôt, l'émission ou la réception se sont déroulés comme demandé. A noter que pour que cela fonctionne correctement, 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 d'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 du message qui lui est 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 (plus faible) de sécurité Intégrité du contenu.

L'élément de sécurité Intégrité du contenu, conjointement avec l'élément de sécurité Intégrité de l'argument du message et, dans certains cas, l'élément de sécurité Confidentialité de l'argument du message, peut être utilisé pour assurer le service au destinataire d'un message, c'est-à-dire pour permettre à l'utilisateur-MTS 1 d'entrer en communication avec l'utilisateur-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 met le contrôle d'intégrité du contenu et, si besoin est, l'étiquette de sécurité du message, à l'abri de tout changement et/ou répudiation. Les arguments de message confidentiel sont mis à l'abri d'un changement et/ou d'une répudiation à l'aide de l'élément de sécurité Confidentialité de l'argument du message.

Si le service de sécurité Confidentialité du contenu ne doit pas être assuré, 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 MHS, c'est-à-dire pour 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 MTS pour être remis au(x) destinataire(s) spécifié(s) au départ.

Ce service de sécurité est assuré à l'aide de l'élément de sécurité Preuve de dépôt d'une manière tout à fait comparable à celle dont l'élément de sécurité est utilisé pour assurer 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 à son (ses) destinataire(s) spécifié(s) au départ.

Ce service de sécurité est assuré à l'aide de l'élément de sécurité Preuve de remise d'une manière tout à fait comparable à celle dont l'élément de sécurité est utilisé pour assurer 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 MHS, c'est–à–dire aux MTA et aux utilisateurs–MTS. Conjointement avec le service de sécurité Contexte de sécurité, il permet la mise en œuvre de politiques de sécurité définissant les parties du MHS qui peuvent traiter des messages assortis d'étiquettes de sécurité spécifiées.

Ce service de sécurité est assuré par l'élément de sécurité Etiquette de sécurité de 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 sécurité*

Le MHS exige un certain nombre de services de gestion de sécurité. Les seuls services de gestion prévus dans la Recommandation X.411 concernent la modification de pouvoirs et l'enregistrement d'étiquettes de sécurité d'utilisateurs-MTS.

10.2.7.1 *Service de sécurité Modification des pouvoirs*

Ce service de sécurité permet à une entité du MHS de modifier les pouvoirs détenus à son égard par une autre entité du 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 MTA, d'étiquettes de sécurité que peut admettre un autre utilisateur-MTS particulier. Il peut être assuré à l'aide de l'élément de sécurité Enregistrement.

10.2.7.3 *Service de sécurité MS-Enregistrement*

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

10.3 *Eléments de sécurité*

Les paragraphes qui suivent décrivent les éléments de sécurité disponibles dans les protocoles décrits dans la Recommandation X.411 pour assurer les services de sécurité du MHS. Ces éléments de sécurité se rapportent directement aux arguments de divers services décrits dans la Recommandation X.411. L'objectif du présent paragraphe est de séparer chaque élément des définitions de service de la Recommandation X.411 touchant à la sécurité et de définir la fonction de chacun de ces éléments de sécurité identifiés.

10.3.1 *Eléments de sécurité Authentification*

Ces éléments de sécurité sont définis afin d'assurer les services de sécurité Authentification et Intégrité.

10.3.1.1 *Eléments de sécurité Echange d'authentification*

L'élément de sécurité Echange d'authentification est destiné à authentifier l'identité d'un utilisateur-MTS pour un MTA, l'identité d'un MTA pour un MTA, l'identité d'un MTA pour un utilisateur-MTS, l'identité d'un MS pour une UA ou l'identité d'une UA pour un MS, et vice versa, si possible. Il est fondé sur l'échange ou l'utilisation de données secrètes: mots de passe, jetons chiffrés en mode asymétrique ou jetons chiffrés en mode symétrique. L'échange a pour résultat de confirmer l'identité du correspondant et, facultativement, de transférer des données confidentielles qui peuvent servir à assurer le service de sécurité confidentialité de la communication et/ou Intégrité de la communication dans les couches sous-jacentes. Cette authentification n'est valable que pour l'instant où elle est donnée et son maintien est subordonné au fait 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 champ 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 *Eléments de sécurité Authentification de l'origine des données*

Ces éléments de sécurité sont expressément destinés à assurer les services d'authentification de l'origine des données, bien qu'ils puissent aussi être utilisés pour assurer certains services d'intégrité des données.

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

L'élément de sécurité Authentification de l'origine du message permet à quiconque reçoit ou transfère un message d'authentifier l'identité de l'utilisateur-MTS qui a expédié ce message. Il se peut qu'il soit 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 corps du message, d'un contrôle d'authentification de l'origine du message, calculé en fonction du contenu du message, de l'identificateur de 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 tel qu'acheminé dans le message global (c'est-à-dire après l'élément de sécurité Confidentialité du contenu optionnel), toute entité MHS peut vérifier l'intégrité du message global, sans qu'elle doive 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 d'origine.

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

10.3.1.2.2 *Elément de sécurité Authentification de l'origine de l'essai*

S'apparentant à l'élément de sécurité Authentification de l'origine du message, l'élément de sécurité Authentification de l'origine de l'essai permet à un MTA d'authentifier l'identité de l'utilisateur-MTS qui est à l'origine d'un essai.

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

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

S'apparentant à l'élément de sécurité Authentification de l'origine du message, l'élément de sécurité Authentification de l'origine du rapport permet à un MTA ou à un utilisateur-MTS qui reçoit un rapport d'authentifier l'identité du MTA qui est à l'origine de ce rapport.

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

10.3.1.3 *Elément de sécurité Preuve de dépôt*

Cet élément de sécurité donne à l'expéditeur d'un message les moyens d'établir qu'un message a été accepté par le 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-MTS avec les résultats Dépôt de message. La Preuve de dépôt est produite par le 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 du message. La Preuve de dépôt est un des résultats du service Dépôt du message.

10.3.1.4 *Elément de sécurité Preuve de remise*

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

L'élément de sécurité est constitué de plusieurs arguments. L'expéditeur du message assortit le message déposé d'une demande de Preuve de remise, demande qui est remise à chaque destinataire avec le message. Un destinataire peut alors calculer la Preuve de remise en fonction de différents arguments associés au message. La Preuve de remise est retournée par le 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 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, Transfert de message et Remise de message. La Preuve de remise est à la fois un des résultats du service Remise de message et 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 *Eléments de sécurité Gestion d'accès sûr*

Ces éléments de sécurité sont définis afin d'assurer le service de sécurité Gestion d'accès sûr et les services de gestion de sécurité.

10.3.2.1 *Elément de sécurité Contexte de sécurité*

Quand un utilisateur-MTS ou un MTA se rattache à un MTA ou à un utilisateur-MTS, l'opération de rattachement spécifie le contexte de sécurité de la communication. Cela limite la possibilité de passage des messages par référence aux étiquettes associées aux messages. En second lieu, le contexte de sécurité de la communication peut être temporairement modifié pour les messages déposés ou remis.

Le contexte de sécurité lui-même consiste en une ou plusieurs étiquettes 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 rattachement-MTS et rattachement-MTA.

10.3.2.2 *Elément de sécurité Enregistrement*

L'élément de sécurité Enregistrement permet l'établissement dans un MTA d'étiquettes de sécurité admissibles d'un utilisateur-MTS.

Cet élément de sécurité est assuré par le service Enregistrement. Le service Enregistrement permet à un utilisateur-MTS de modifier des arguments en possession du MTS et relatifs à la remise de messages à cet utilisateur-MTS.

10.3.2.3 *Elément de sécurité MS-Enregistrement*

L'élément de sécurité MS-Enregistrement permet l'établissement d'étiquettes de sécurité admissibles d'un utilisateur-MS.

Cet élément de sécurité est assuré par le service MS-Enregistrement. Le service MS-Enregistrement permet à un utilisateur-MS de modifier des arguments en possession du MS et relatifs à la remise de messages à cet utilisateur-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 par une entité 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 une protection contre toute écoute indiscrète pendant la transmission moyennant l'utilisation d'un élément de sécurité de chiffrement. 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 autres données d'initialisation sont acheminés à l'aide des éléments de sécurité Confidentialité de l'argument de message et Intégrité de l'argument de 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 d'argument de message*

L'élément de sécurité Confidentialité d'argument de message assure la confidentialité, l'intégrité et, si besoin est, l'irrévocabilité des données de destinataires associées à un message. Spécifiquement, ces données comprendront des codes cryptographiques et les données correspondantes nécessaires au bon fonctionnement des éléments de sécurité Confidentialité et Intégrité, dans l'hypothèse où ces éléments de sécurité optionnels seraient appelés.

Cet élément de sécurité fonctionne à l'aide du jeton de message. Les données que l'élément de sécurité Confidentialité d'argument de message doit protéger constituent les données chiffrées du jeton de message. Les données chiffrées du jeton de message sont inintelligibles pour tous les 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 de 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 algorithmes, le ou les codes utilisés et les autres données d'initialisation sont acheminés à l'aide des éléments de sécurité Confidentialité d'argument de message et Intégrité d'argument de message. Le résultat de l'application des algorithmes et du code est le contrôle d'intégrité de 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 d'intégrité de contenu est protégé à l'aide de l'élément de sécurité Intégrité d'argument de message, selon la politique de sécurité en vigueur, il peut être utilisé pour aider à assurer le service de sécurité Non-répudiation d'origine.

Le contrôle d'intégrité de contenu est un argument des services Dépôt de message, Transfert de message et Remise de message.

10.3.4.2 *Elément de sécurité Intégrité d'argument de message*

L'élément de sécurité Intégrité d'argument de message assure l'intégrité et, si besoin est, l'irrévocabilité de certains arguments associés à un message. Spécifiquement, ces arguments peuvent comprendre, au choix l'identificateur d'algorithme de confidentialité de contenu, le contrôle d'intégrité de contenu, l'étiquette de sécurité de message, la demande de preuve de remise et le 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 d'argument de 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 séquence de message*

L'élément de sécurité Intégrité de séquence de 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 devra 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 Recommandation X.411. 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 MHS.

10.3.6.1 *Elément de sécurité Etiquette de sécurité de message*

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

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

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

10.3.7 *Eléments de sécurité Gestion de 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-MTS ou d'un MTA.

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

10.3.8 *Technique de double enveloppement*

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

Cette technique peut être mise en œuvre grâce à l'utilisation de l'argument Type de contenu qui permet de spécifier que le contenu d'un message est une enveloppe interne. Ce type de contenu signifie que le contenu constitue en lui-même un message (enveloppe et contenu) destiné à être retransmis par le destinataire dont le nom figure sur l'enveloppe extérieure au destinataire dont le nom figure sur l'enveloppe intérieure.

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

SECTION 3 – CONFIGURATIONS

11 Présentation générale

La présente section indique la façon dont on peut assurer la configuration du MHS en vue de répondre à l'un des divers besoins fonctionnels, physiques et d'organisation.

Elle traite des sujets suivants:

a) configurations fonctionnelles;

b) configurations physiques;

c) configurations d'organisation;

d) *MHS mondial.*

12 Configurations fonctionnelles

On trouvera ci–dessous la spécification des configurations fonctionnelles possibles du MHS. Leur variété provient 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 MS.

12.1 *Annuaire*

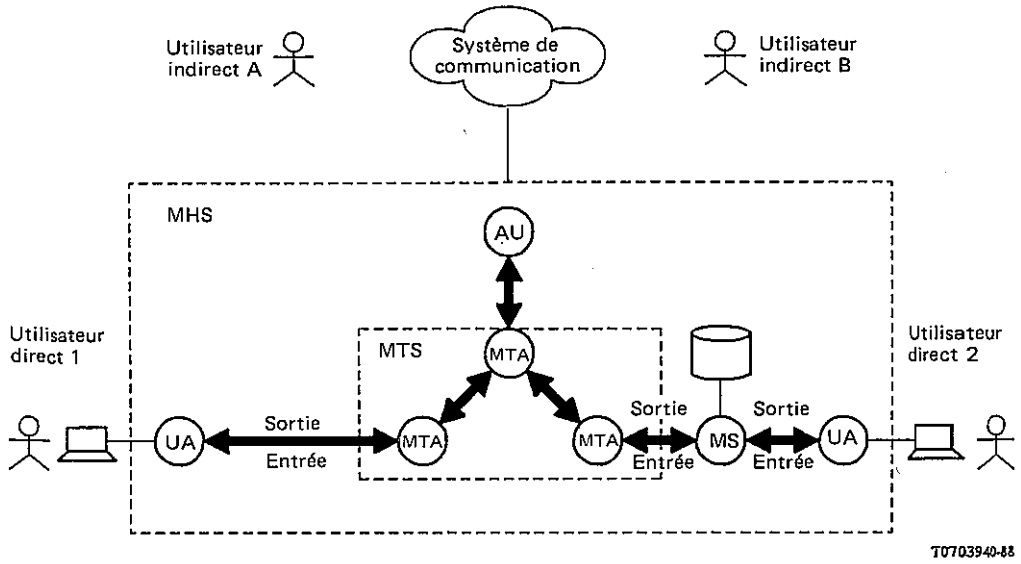
En ce qui concerne l'annuaire, le MHS peut être configuré pour un utilisateur en particulier, ou un groupe d'utilisateurs (voir, par exemple, le § 14.1), avec ou sans l'annuaire. Les possibilités décrites dans la section 5 peuvent ne pas être offertes à l'utilisateur qui n'a pas accès à l'annuaire.

Remarque – Un annuaire en partie (et non totalement) interconnecté, peut être mis en place pour une période intérimaire au cours de laquelle il est procédé à l'élaboration de l'annuaire (mondial), élaboration possible grâce aux Recommandations en matière d'annuaires.

12.2 *Mémoire de messages*

En ce qui concerne la MS, le MHS peut être composé pour un utilisateur direct particulier, avec ou sans MS. Un utilisateur n'ayant pas accès à une MS ne dispose pas de la possibilité de mise en mémoire des messages. Dans ces conditions, un utilisateur dépend de son 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 MTS et son lien avec un autre système de communication par l'intermédiaire d'un UA. Sur cette figure, l'utilisateur 2 est équipé d'une 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 MS

13 Configurations physiques

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

13.1 *Systèmes de messagerie*

Les modules utilisés dans l'élaboration physique du 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 dans 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 – UA, MS, MTA et AU – pouvant exister dans un tel système, que leur présence soit obligatoire ou facultative et que le système en comprenne un ou, éventuellement, plusieurs.

Le tableau 8/X.402 est divisé en deux sections. Les systèmes de messagerie de la première section sont consacrés aux utilisateurs uniques et les systèmes de la seconde section peuvent (bien que cela ne soit pas obligatoire) desservir plusieurs utilisateurs.

Remarque – L'admission des types de systèmes de messagerie est régie par les principes fondamentaux suivants:

a) une AU et le MTA avec lequel elle est en interaction sont, en général, cositués, aucun protocole régissant leur interaction n'étant normalisé;

b) un MTA est, en règle générale, cositué avec des UA ou MS multiples car, parmi les protocoles normalisés, seul le protocole portant sur le transfert permet de transmettre 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;

c) il n'est pas utile de cosituer plusieurs MTA dans un système de messagerie car un seul MTA dessert plusieurs usagers et son but est de transmettre des objets entre ces systèmes et non à l'intérieur de chacun d'eux (il ne s'agit pas d'exclure la possibilité de faire coexister plusieurs processus concernant le MTA dans un seul système informatique);

d) un emplacement commun à une AU et à un MTA n'a pas d'influence sur le comportement du système en ce qui concerne les autres aspects du MHS. En conséquence, un seul type de système de messagerie englobe la présence et l'absence d'une AU.

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

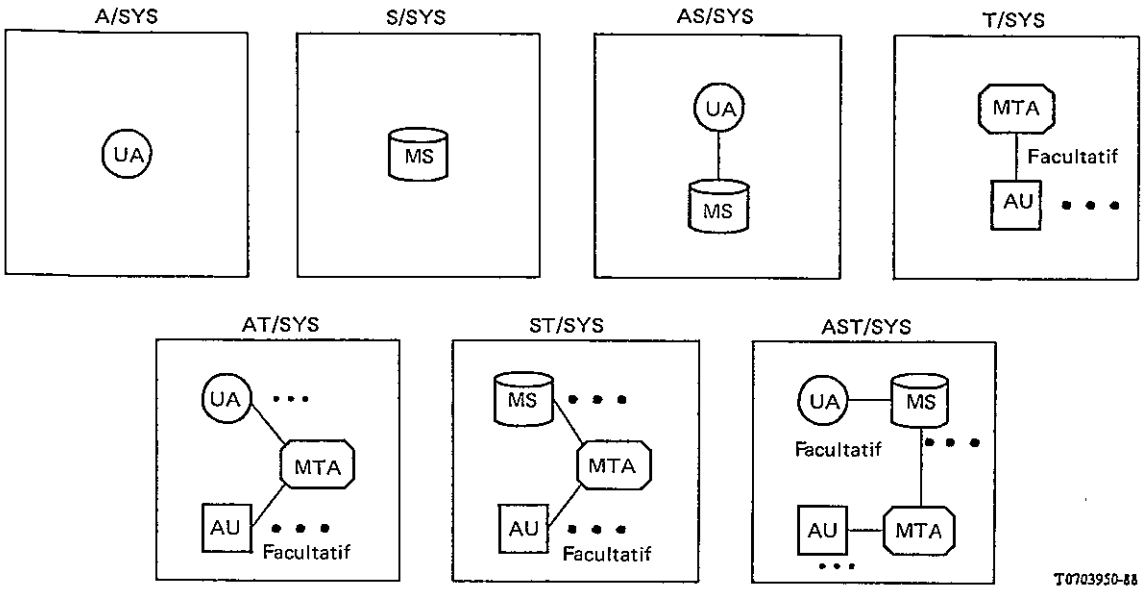


FIGURE 8/X.402

Types de systèmes de messagerie

TABLEAU 8/X.402

Systèmes de messagerie

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

M Multiple

[. . .] Facultatif

13.1.1 *Systèmes d'accès*

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

Un A/SYS est réservé à un seul utilisateur.

13.1.2 *Systèmes de mémorisation*

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

Un 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)** contient un UA, une MS, mais ne contient ni un MTA, ni une AU.

Un AS/SYS est réservé à un seul utilisateur.

13.1.4 *Systèmes de transfert*

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

Un T/SYS peut desservir plusieurs utilisateurs.

13.1.5 *Systèmes d'accès et de transfert*

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

Un AT/SYS peut desservir plusieurs utilisateurs.

13.1.6 *Systèmes de mémorisation et de transfert*

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

Un ST/SYS peut desservir plusieurs usagers.

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

Un **système d'accès, de mémorisation et de transfert (AST/SYS)** contient un ou plusieurs UA, une ou plusieurs MS, un MTA et, à titre facultatif, une ou plusieurs AU.

Un AST/SYS peut desservir plusieurs usagers.

13.2 *Configurations représentatives*

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

13.2.1 *MHS entièrement centralisé*

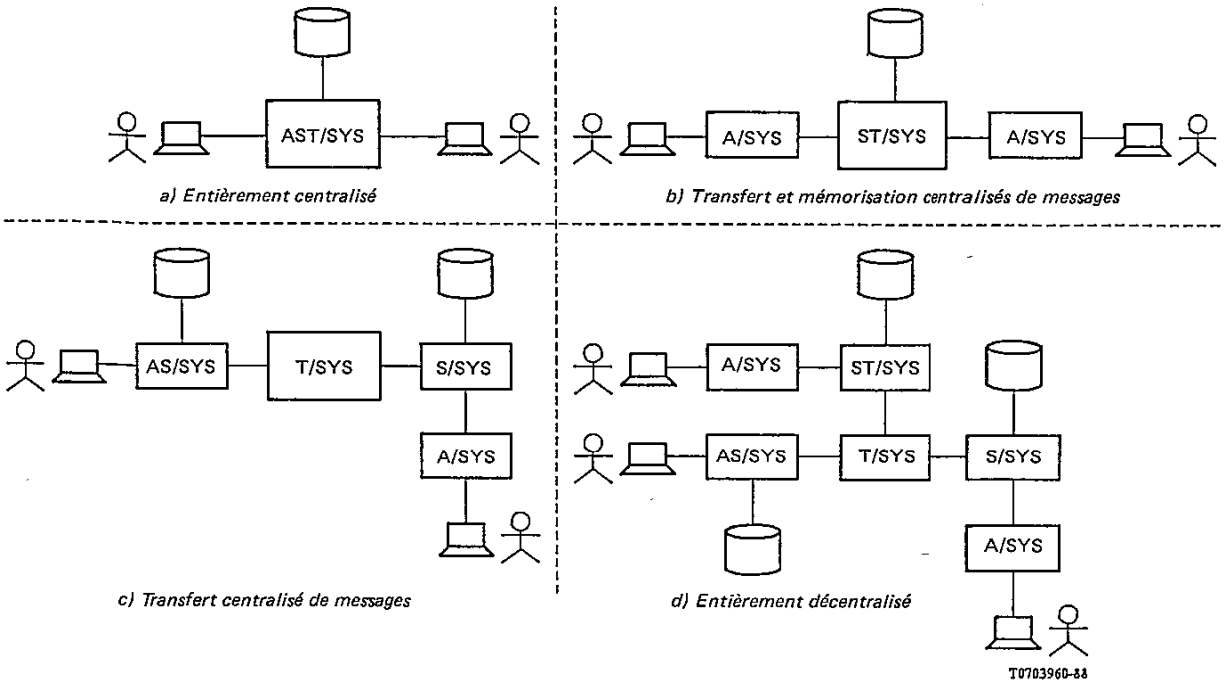
Le MHS peut être entièrement centralisé [partie a) de la figure 9/X.402]. Cette conception s'obtient avec un seul AST/SYS contenant des objets fonctionnels de toutes sortes et pouvant desservir plusieurs utilisateurs.

13.2.2 *Transfert et mémorisation centralisés de messages*

Le MHS peut centraliser le transfert et la mémorisation de messages, l'accès d'utilisateur étant toutefois assuré de façon décentralisée [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 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.



Remarque 1 – Bien que les usagers 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

13.2.4 *MHS entièrement décentralisé*

Le MHS peut même 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 d'organisation

On trouvera ci-dessous la spécification des configurations d'organisation possibles du 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 n'étant pas limité, la clause décrit les types de domaines de gestion à partir desquels le MHS est constitué et identifie quelques configurations représentatives importantes.

14.1 *Domaines de gestion*

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

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

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

14.1.1 *Domaines de gestion administratifs*

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

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

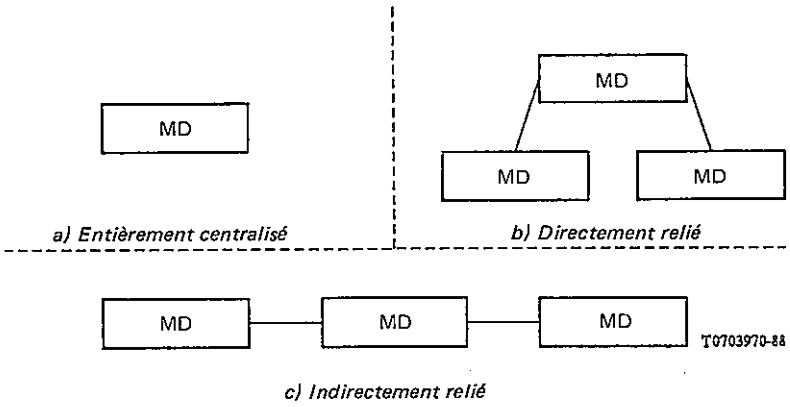
14.1.2 *Domaines de gestion privés*

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

Remarque – Un 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 MD peuvent être combinés de diverses façons en vue de constituer le MHS. Les configurations d'organisation possibles ne sont pas limitées dans leur 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.



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

FIGURE 10/X.402

Configurations représentatives d'organisation

14.2.1 *MHS entièrement centralisé*

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

14.2.2 *MHS directement connecté*

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

14.2.3 *MHS indirectement connectés*

Le 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 MD, chacun étant interconnecté avec tous les autres.

15 MHS mondial

Un des principaux buts de la présente Recommandation et d'autres Recommandations de la même série est de permettre l'élaboration du MHS mondial, un 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 MHS mondial comprendra toutes les configurations fonctionnelles spécifiées au § 12.

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

La configuration d'organisation du MHS mondial est un hybride des configurations pures spécifiées dans le § 14, hybride extrêmement complexe et dont la décentralisation au niveau de l'organisation est élevée.

La figure 11/X.402 représente un exemple d'interconnexions possibles. Elle ne vise pas à montrer toutes les configurations possibles. Selon cette figure, les ADMD jouent un rôle central dans le MHS mondial. En s'interconnectant mutuellement à l'échelle internationale, ils constituent la clef de voûte du transfert international de messages. En fonction des réglementations nationales, ils peuvent représenter également, en s'interconnectant mutuellement à l'échelle nationale, la clef de voûte du transfert de messages au niveau national et non seulement international. Les AMD sont également utilisés comme services de désignation de base dans l'attribution *d'adresses d'O/R* aux utilisateurs et aux DL.

Les PRMD jouent un rôle périphérique dans le MHS mondial, reliés au point central que constitue l'ADMD, qui joue le rôle d'intermédiaire entre eux.

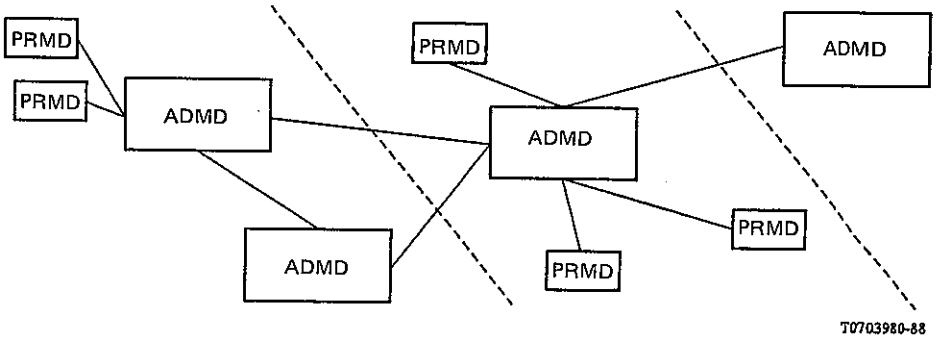


FIGURE 11/X.402

MHS mondial

SECTION 4 – DÉSIGNATION, ADRESSAGE ET ACHEMINEMENT

16 Présentation générale

La présente section décrit la désignation et l'adressage des utilisateurs et des DL ainsi que l'acheminement vers ces derniers des objets d'information.

Elle traite des sujets suivants:

a) désignation;

b) adressage;

c) acheminement.

17 Désignation

Ce paragraphe spécifie la façon dont les utilisateurs et les DL sont désignés 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 essai, un UA ou une MS indique au MTS ses destinataires éventuels. Lorsque le MTS livre un message, il identifie l'expéditeur pour chaque UA ou MS de destination. 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 repère un objet pour l'annuaire. En présentant ce nom à l'annuaire, le MHS peut avoir accès à une inscription d'usager ou de DL dans l'annuaire. A partir de cette inscription, le MTS peut obtenir, par exemple, l'*adresse d'O/R* de l'usager ou de la DL.

Les utilisateurs ou les DL ne sont pas tous inscrits dans l'annuaire, c'est pourquoi ils ne possèdent pas tous un nom d'annuaire.

Remarque 1 – De nombreux utilisateurs et DL n'auront pas de nom d'annuaire avant que celui-ci ne soit très répandu comme complément du MHS. De nombreux utilisateurs indirects (par exemple, les usagers des services postaux) n'auront pas de nom d'annuaire avant que celui–ci ne soit très répandu comme complément des autres systèmes de communication.

Remarque 2 – Les utilisateurs et les 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 chargées de la désignation dont dépendra en fin de compte l'annuaire.

Remarque 3 – Le nom d'annuaire type est d'un accès plus facile tout en étant plus stable que l'adresse d'O/R type car celle-ci s'exprime nécessairement sous forme de structure d'organisation ou de structure physique du 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 par lequel les utilisateurs et les DL seront identifiés à l'extérieur du MTS (c'est-à-dire par d'autres usagers) et que l'utilisation des *adresses d'O/R* sera en grande partie limitée au MTS (pour utilisation, par exemple, par les MTA).

17.2 *Noms d'O/R*

Chaque utilisateur ou DL possède au moins un *nom d'O/R*. Un **nom d'O/R** est un identificateur par lequel un utilisateur peut être désigné comme étant l'expéditeur, ou par lequel un utilisateur ou une DL peut être désigné comme étant un récepteur éventuel d'un message ou d'un essai. Un nom d'O/R distingue un utilisateur ou une DL d'un ou d'une autre et peut également identifier son point d'accès au MHS.

Un nom d'O/R comprend un nom d'annuaire et une *adresse d'O/R*, ou les deux à la fois. S'il est présent, le nom identifie très clairement (s'il est valable) l'utilisateur ou la 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'UA ou la MS de l'expéditeur d'un message ou d'un essai peut comprendre l'un ou les deux éléments dans chaque nom d'O/R qu'il (elle) fournit. Si l'on oublie de fournir l'*adresse d'O/R*, le MTS l'obtient par l'annuaire grâce au nom d'annuaire. Si l'on oublie de fournir ce dernier, le MTS agit sans lui. Si les deux indications sont disponibles, le 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 cette *adresse d'O/R* avait été omise et se base sur le nom d'annuaire.

Lors de la remise d'un message, le MTS inclut une *adresse d'O/R* et, éventuellement, un nom d'annuaire dans chaque nom d'O/R qu'il fournit à un destinataire de message ou à l'expéditeur d'un message ou d'un essai contenant le 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 DL allongée.

Remarque – Un changement de destination ou un allongement de la DL peuvent obliger le MTS à transmettre à un UA ou une MS, au moment de la remise, des noms d'O/R que l'UA ou MS n'ont pas fournis en dépôt direct.

18 Adressage

Cette clause spécifie la façon dont les utilisateurs et les DL seront adressés. Elle définit les *adresses d'O/R*, décrit la structure des *listes d'attributs* à partir desquelles elles 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 essai ou un rapport à un utilisateur, ou pour allonger une DL spécifiée comme étant un destinataire éventuel d'un message ou d'un essai, le MTS doit localiser l'utilisateur ou la DL en fonction de ses propres structures physiques et d'organisation. Les *adresses d'O/R* sont les structures de données permettant toutes les localisations de ce type.

18.1 *Listes d'attributs*

Les *adresses d'O/R* à la fois celles des utilisateurs et celles des DL sont des listes d'attributs. Une **liste d'attributs** est un ensemble organisé d'attributs.

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

Un attribut est composé des parties suivantes:

a) **type d'attribut** (ou **type**) – Identificateur représentant une catégorie d'information (par exemple, noms personnels).

b) **valeur d'attribut** (ou **valeur**) – Exemple de la catégorie d'information que le type d'attribut représente (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 catégorie d'information.

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

b) **attribut défini par domaine** – Un attribut dont le type est lié à une catégorie d'information par un MD.

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

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

18.2 *Jeux de caractères*

Des valeurs d'attributs normalisés et des types et valeurs d'attributs définis par domaine sont constitués à partir de chaînes numériques, imprimables et télétex de la façon suivante:

a) le type ou la valeur d'un attribut particulier défini par domaine peut être une chaîne imprimable, une chaîne télétex, ou les deux. Un choix identique devra être effectué à la fois pour le type et la valeur;

b) les types de chaînes à partir desquelles les valeurs d'attributs normalisées peuvent être constituées et la façon dont cette constitution s'opère (par exemple, une ou plusieurs chaînes) varient d'un attribut à l'autre (voir le § 18.3).

Les valeurs d'un attribut comprend des chaînes constituées, selon leur type, d'un des ensembles suivants: uniquement numérique, uniquement imprimable, numérique et imprimable et numérique et télétex. Dans ce domaine, les règles ci-après régissent chaque type de communication:

a) chaque fois que les chaînes numériques et les chaînes imprimables sont toutes deux autorisées, les chaînes de chaque type (mais non les deux) peuvent être fournies au même titre;

b) chaque fois que les chaînes imprimables et les chaînes télétex sont toutes deux autorisées, chacune d'elles ou les deux à la fois peuvent être fournies, mais les chaînes imprimables doivent être utilisées au minimum chaque fois que des attributs sont transmis à l'échelle internationale. Si à la fois des chaînes imprimables et des chaînes télétex sont fournies, elles doivent toutes transmettre la même information, afin que l'on puisse sans risque ne pas tenir compte de l'une ou l'autre catégorie de chaîne à la réception.

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

Remarque 1 – Des chaînes télétex 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 dispositifs d'entrée et de sortie ne permettent pas tous l'entrée et l'affichage, par exemple, de caractères accentués. Des chaînes imprimables sont nécessaires au niveau international afin que les limites de ces dispositifs n'empêchent pas la communication d'avoir lieu.

18.3 *Attributs normalisés*

Les 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 – numériques, imprimables et télélex – d'où 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 PDS, et ceux de la troisième section portent sur l'*adressage dans* un PDS.

TABLEAU 9/X.402

Attributs normalisés

Type d'attribut normalisé	Jeux de caractères		
	NUM	PRT	TTX
Généraux			
Nom-domaine-administration	×	×	–
Nom-courant	–	×	×
Nom-pays	×	×	–
Adresse-réseau	× [a]	–	–
Identificateur-utilisateur-numérique	×	–	–
Nom-organisation	–	×	×
Noms-unités-organisation	–	×	×
Nom-personnel	–	×	×
Nom-domaine-privé	×	×	–
Identificateur-terminal	–	×	–
Type-terminal	–	–	–
Acheminement postal			
Nom-service-remise-physique	–	×	–
Nom-pays-remise-physique	×	×	–
Code-postal	×	×	–
Adressage postal			
Composantes-adresse-O/R-extension-postale	–	×	×
Composantes-adresse-remise-physique-extension	–	×	×
Attributs-postaux-locaux	–	×	×
Nom-bureau-remise-physique	–	×	×
Numéro-bureau-remise-physique	–	×	×
Nom-organisation-remise-physique	–	×	×
Nom-personnel-remise-physique	–	×	×
Adresse-boîte/case postale	–	×	×
Adresse-poste-restante	–	×	×
Adresse-rue	–	×	×
Adresse-postale-non formatée	–	×	×
Nom-postal-unique	–	×	×

NUM Numérique

PRT Imprimable

TTX Télétex

× Autorisé

[a] Séquence de chaîne d'octets dans certaines circonstances

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-domaine-administration*

Un **nom-domaine-administration** est un attribut normalisé permettant d'identifier un ADMD relatif à un pays représenté par un nom de pays.

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

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 ADMD (c'est-à-dire l'ensemble des ADMD) existant dans le pays. Cela concerne à la fois l'identification des usagers dans le pays et l'acheminement de messages, d'essais et de rapports aux ADMD de ce pays et entre eux. En ce qui concerne l'identification des usagers, cela suppose que les adresses d'O/R des usagers du pays soient choisies de façon à ne comporter aucune ambiguïté, même en l'absence des noms des ADMD d'usagers. En ce qui concerne l'acheminement de messages, d'essais et de rapports aux ADMD et entre ces ADMD, cette valeur d'attribut permet à la fois aux PRMD à l'intérieur du pays et aux ADMD à l'extérieur de ce pays, d'acheminer sans discrimination des messages, des essais ou des rapports à l'un quelconque des ADMD à l'intérieur du pays et suppose que ces derniers s'interconnectent de sorte que les messages, les essais et les rapports soient transmis à leurs destinataires.

18.3.2 *Nom-courant*

Un **nom-courant** est un attribut normalisé identifiant un utilisateur ou une 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 télétex ou les deux à la fois. Qu'elle soit imprimable ou télétex, la chaîne est sélectionnée à partir d'un ensemble de chaînes de ce type administrées à cette fin (et éventuellement à d'autres fins) par l'entité précitée.

Remarque – Parmi d'autres possibilités, un nom-courant pourrait identifier la fonction de l'intéressé dans l'organisation (par exemple, «Directeur des marchés»).

18.3.3 *Nom-pays*

Un **nom-pays** est un attribut normalisé identifiant un pays.

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

18.3.4 *Composantes-adresse-O/R-extension-postale*

L'attribut **composantes-adresse-O/R-extension-postale** est un attribut normalisé qui fournit, dans une adresse postale, l'information supplémentaire nécessaire à l'identification du destinataire (par exemple, une unité d'organisation).

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

18.3.5 *Composantes-adresse-remise-physique-extension*

Un attribut **composantes-adresse-remise-physique-extension** est un attribut normalisé qui spécifie dans une adresse postale l'information supplémentaire nécessaire à l'identification du point exact de remise (par exemple, numéros de l'étage et du bureau, dans le cas d'un grand bâtiment).

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

18.3.6 *Attributs-postaux-locaux*

Les **attributs-postaux-locaux** constituent un attribut normalisé identifiant le lieu de distribution autre que celui représenté par un attribut nom-bureau-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 télétex, ou les deux à la fois.

18.3.7 *Adresse-réseau*

Une **adresse-réseau** est un attribut normalisé qui fournit l'adresse du réseau d'un terminal.

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

a) chaîne numérique régie par la Recommandation X.121;

b) deux chaînes numériques régies par les Recommandations E.163 et E.164;

c) adresse PSAP.

Remarque – Parmi les chaînes admises par la Recommandation X.121, on notera un numéro télex précédé du chiffre de libération télex (8).

18.3.8 *Identificateur-utilisateur-numérique*

Un **identificateur-utilisateur-numérique** est un attribut normalisé qui identifie numériquement un utilisateur par rapport à l'ADMD représenté par un nom-domaine-administration.

La valeur d'un Identificateur-utilisateur-numérique est une chaîne numérique sélectionnée à partir d'un ensemble de chaînes de ce type régies à cette fin par l'ADMD précité.

18.3.9 *Nom-organisation*

Un **nom-organisation** est un attribut normalisé qui identifie une organisation. Sur le plan national, cette identification peut être soit relative au pays désigné par un nom-de-pays (de sorte que les noms-organisation soient uniques dans le pays), soit relative au MD désigné par un nom-de-domaine-privé, ou un nom-de-domaine-d'administration, ou les deux.

La valeur d'un nom-organisation est une chaîne imprimable, une chaîne télétex, ou les deux à la fois. Qu'elle soit imprimable ou télétex, la chaîne est sélectionnée à partir d'un ensemble de chaînes de ce type régies à cette fin (et peut-être à d'autres fins) par le pays ou le MD précité.

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

18.3.10 *Noms-unités-organisations*

Un attribut **noms-unités-organisations** est un attribut normalisé qui identifie une ou plusieurs unités (par exemple, divisions ou départements) de l'organisation représentée par un nom-organisation, chaque unité, à l'exception de la première, constituant une sous-unité des unités dont les noms la précèdent dans l'attribut.

La valeur d'un attribut noms-unités-organisations est une séquence ordonnée de chaînes imprimables, une séquence ordonnée de chaînes télétex, ou les deux à la fois. Qu'elle soit imprimable ou télétex, chaque chaîne est sélectionnée à partir d'un ensemble de chaînes de ce type régies à cette fin (et peut-être à d'autres) par l'organisation (ou l'unité englobant l'ensemble des sous-unités) précitée.

18.3.11 *Nom-service-remise-physique (pds)*

Un **nom-service-remise-physique (pds)** est un attribut normalisé qui identifie un PDS par rapport à l'ADMD représenté par un nom-domaine-administration.

La valeur d'un nom-pds est une chaîne imprimable sélectionnée à partir d'un ensemble de chaînes de ce type régies à cette fin par l'ADMD précité.

18.3.12 *Nom-personnel*

Un **nom-personnel** est un attribut normalisé qui identifie une personne par rapport à l'entité représentée par un autre attribut (ou, par exemple, un nom-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»).

L'information ci-dessus est fournie sous forme de chaînes imprimables, de chaînes télétex, ou des deux à la fois.

18.3.13 *Nom-pays-remise-physique*

Un **nom-pays-remise-physique** est un attribut normalisé qui identifie le pays dans lequel un utilisateur prend livraison de messages physiques.

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

18.3.14 *Nom-bureau-remise-physique*

Un **nom-bureau-remise-physique** est un attribut normalisé qui identifie la ville, le village, etc. où se situe le bureau de poste par lequel un utilisateur prend livraison de messages physiques.

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

18.3.15 *Numéro-bureau-remise-physique*

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

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

18.3.16 *Nom-organisation-remise-physique*

Un **nom-organisation-remise-physique** est un attribut normalisé qui identifie une organisation d'usagers des services postaux.

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

18.3.17 *Nom-personnel-remise-physique*

Un **nom-personnel-remise-physique** est un attribut normalisé qui identifie un groupe d'usagers des services postaux.

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

18.3.18 *Adresse-boîte/case postale*

Une **adresse-boîte/case postale** est un attribut normalisé qui spécifie le numéro de la boîte/case postale par laquelle un utilisateur prend livraison de messages physiques.

La valeur d'une adresse boîte/case postale est une chaîne imprimable, une chaîne télétex, ou les deux à la fois, sélectionnées à partir de l'ensemble de chaînes de ce type attribuées à la fin par le bureau postal représenté par un attribut nom-bureau-remise-physique.

18.3.19 *Code-postal*

Un **code-postal** est un attribut normalisé qui spécifie le code postal pour la zone géographique dans laquelle un utilisateur prend livraison de messages physiques.

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

18.3.20 *Adresse-poste-restante*

Une **adresse-poste-restante** 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-poste-restante est une chaîne imprimable, une chaîne télétex, ou les deux à la fois, sélectionnées à partir de l'ensemble de chaînes attribuées à cette fin par le bureau de poste représenté par un attribut nom-bureau-remise-physique.

18.3.21 *Nom-domaine-privé*

Une **nom-domaine-privé** est un attribut normalisé qui identifie un PRMD. Sur le plan national, l'identificateur peut être soit par rapport au pays désigné par un nom-de-pays (de manière que les noms de PRMD soient uniques dans le pays), soit par rapport à l'ADMD désigné par un nom-domaine-administration.

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

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

18.3.22 *Adresse-rue*

Une **adresse-rue** est un attribut normalisé qui spécifie l'adresse dans la rue [par exemple, le numéro de l'habitation, le numéro et le type de la rue (par exemple, «Route»)] dans laquelle un utilisateur prend livraison de messages physiques.

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

18.3.23 *Identificateur-terminal*

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

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

18.3.24 *Type-terminal*

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

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

18.3.25 *Adresse-postale-non-formatée*

Une **adresse-postale-non-formatée** 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*

Un **nom-postal-unique** est un attribut normalisé qui identifie le point de remise, autre que celui qui est représenté par une adresse-rue, une adresse-boîte/case postale, ou une adresse-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-listes-attributs*

Plusieurs adresses d'O/R, et, par conséquent, plusieurs listes d'attributs, peuvent représenter le même utilisateur ou la même DL. Cette multiplicité d'adresses d'O/R est en partie (mais pas totalement) due aux règles d'équivalence de listes d'attributs suivantes:

a) L'ordre relatif des attributs normalisés est dépourvu de signification.

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 dépourvu de signification.

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 dépourvu de signification. 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 télétex équivalente, ou les deux à la fois, le choix entre les trois possibilités doit être considéré comme dépourvu de signification.

d) Lorsque la valeur d'un attribut normalisé peut contenir des lettres, les types de caractères de ces lettres doivent être considérés comme dépourvus de signification.

e) Dans un type ou une valeur d'attribut défini par domaine, ou dans une valeur d'attribut normalisé, tous les espaces au début, en fin et consécutifs (à l'exception d'un, en ce qui concerne ces derniers), doivent être considérés comme dépourvus de signification.

Remarque 1 – Un MD peut imposer des règles d'équivalence supplémentaires aux attributs qu'il affecte à ses propres utilisateurs et DL. Il peut définir par exemple des règles concernant les caractères de ponctuation dans les valeurs d'attributs, le cas des lettres dans ces valeurs, ou l'ordre relatif des attributs définis par domaine.

Remarque 2 – Il peut être décidé à l'échelon national que les MD imposent des règles d'équivalence supplémentaires concernant les attributs normalisés dont les valeurs sont données comme chaînes télétex et, en particulier, les règles destinées à obtenir les chaînes imprimables équivalentes.

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

A chaque utilisateur ou 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 utilisateur et identifie le point d'accès de l'utilisateur au MHS ou le point d'allongement de la DL.

Une adresse d'O/R peut prendre l'une quelconque des formes résumées au tableau 10/X.402. La première colonne de ce tableau définit les attributs disponibles pour l'élaboration d'adresse 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).

Ce tableau 10/X.402 a 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. La quatrième section couvre les attributs définis par domaine.

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

18.5.1 *Adresse d'O/R mnémotechnique*

Une **adresse d'O/R mnémotechnique** est une adresse qui identifie de façon mnémotechnique un utilisateur ou une DL. Elle identifie un ADMD et un utilisateur ou une DL s'y rapportant.

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

a) un nom-pays et un nom-domaine-administration qui, ensemble, identifient un ADMD;

b) un nom-domaine-privé, un nom-organisation, un nom-unités-organisation, un nom-personnel ou nom-courant ou une combinaison de ces noms et, à titre facultatif, un ou plusieurs attributs définis par domaine qui, ensemble, identifient un usager ou une DL relatifs à l'ADMD du point a) ci-dessus.

18.5.2 *Adresse d'O/R numérique*

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

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

a) un nom-pays et un nom-domaine-administration qui, ensemble, identifient un ADMD;

b) un identificateur-utilisateur-numérique et, sous certaines conditions, un nom-domaine-privé qui, ensemble, identifient l'utilisateur relatif à l'ADMD 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*

Une **adresse d'O/R postale** est celle qui identifie un utilisateur au moyen de son adresse postale. Elle identifie le 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.

TABLEAU 10/X.402

Formes d'adresse d'O/R

Type d'attributs	Formes d'adresse d'O/R				
	MNEM	NUMR	POST		TERM
			F	U	
Généraux					
Nom-domaine-administration	M	M	M	M	C
Nom-courant	C	–	–	–	–
Nom-pays	M	M	M	M	C
Adresse-réseau	–	–	–	–	M
Identificateur-utilisateur-numérique	–	M	–	–	–
Nom-organisation	C	–	–	–	–
Nom-unités-organisation	C	–	–	–	–
Nom-personnel	C	–	–	–	–
Nom-domaine-privé	C	C	C	C	C
Identificateur-terminal	–	–	–	–	C
Type-terminal	–	–	–	–	C
Acheminement postal					
Nom-service-remise-physique	–	–	C	C	–
Nom-pays-remise-physique	–	–	M	M	–
Code-postal	–	–	M	M	–
Adressage postal					
Composantes-adresse-O/R-extension-postale	–	–	C	–	–
Composantes-adresse-remise-physique-extension	–	–	C	–	–
Attributs-postaux-locaux	–	–	C	–	–
Nom-bureau-remise-physique	–	–	C	–	–
Numéro-bureau-remise-physique	–	–	C	–	–
Nom-organisation-remise-physique	–	–	C	–	–
Nom-personnel-remise-physique	–	–	C	–	–
Adresse-boîte/case postale	–	–	C	–	–
Adresse-poste-restante	–	–	C	–	–
Adresse-rue	–	–	C	–	–
Adresse-postale-non-formatée	–	–	–	M	–
Nom-postal-unique	–	–	C	–	–
Défini-domaine					
Défini-domaine (un ou plus)	C	C	–	–	C

MNEM Mnémotechnique
NUMR Numérique
POST Postal
TERM Terminal
F Formaté
U Non formaté
M Oblitagoire
C Conditionnel

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

a) un nom-pays et un nom-domaine-administration qui, ensemble, identifient un ADMD;

b) sous certaines conditions, un nom-domaine-privé, un nom-PDS, ou les deux à la fois qui, ensemble, identifient le PDS par lequel l'utilisateur doit être atteint;

c) un nom-pays-remise-physique et un code-postal qui, ensemble, identifient la région géographique dans laquelle l'utilisateur prend livraison de messages physiques.

Une adresse d'O/R postale formatée comprend en outre un exemplaire de chaque attribut d'adressage postal (voir le tableau 9/X.402), à l'exception de l'adresse-postale-non-formatée, dont a besoin le PDS pour identifier les usagers des services postaux.

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

Remarque – Le nombre total de caractères contenus dans les valeurs de tous les attributs, à l'exception du nom-pays, du nom-domaine-administration et du nom-service-remise-physique dans une adresse d'O/R postale doit être assez faible pour que ces caractères puissent être présentés sur 6 lignes de 30 caractères chacune, correspondant au format d'une fenêtre d'enveloppe physique type. L'algorithme de rendu est spécifique à la PDAU mais il est susceptible de comprendre des séparateurs (par exemple, des espaces) entre certaines valeurs d'attributs.

18.5.4 *Adresse d'O/R terminale*

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

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

a) une adresse-réseau;

b) sous certaines conditions, un identificateur-terminal;

c) sous certaines conditions, un terminal-type;

d) sous certaines conditions, à la fois un nom-pays et un nom-domaine-administration qui, ensemble, identifient un ADMD;

e) sous certaines conditions, un nom-domaine-privé et un ou plusieurs attributs définis par domaine, qui fournissent des informations supplémentaires à celles qui identifient l'utilisateur.

Le nom-domaine-privé et les attributs définis par domaine ne doivent être présents que si le nom-pays et les attributs nom-domaine-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.

Si l'accès à un utilisateur ou à une DL se fait par un PRDM, les attributs utilisés pour acheminer les messages jusqu'à ce dernier sont présents dans l'adresse d'O/R en fonction des règles fixées par l'ADMD désigné par les attributs nom-pays et nom-domaine-administration de l'adresse et conformément à ces règles. L'ADMD n'impose aucune autre contrainte aux attributs de l'adresse d'O/R. Si l'accès à un utilisateur ne se fait pas par un PRMD, la présence de tous les attributs conditionnels, à l'exception de ceux qui sont propres aux adresses d'O/R postales, dépend des règles établies par l'ADMD représenté par les attributs nom-pays et nom-domaine-administration.

Tous les attributs conditionnels propres aux adresses d'O/R postales sont, selon le cas, présents ou absents dans ces adresses de façon à répondre aux besoins de l'adressage postal des usagers qu'ils définissent.

19 Acheminement

Pour transmettre un message, un essai, ou un rapport vers un utilisateur ou le point d'allongement d'une DL, un MTA doit non seulement localiser l'utilisateur ou la 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 d'accroissement, 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 MHS comprenant un seul MD, la question de l'acheminement ne se pose naturellement pas.

b) Un PRMD peut être relié à un seul ADMD. Si c'est le cas, l'acheminement comprend toujours obligatoirement l'ADMD.

c) Un ADMD peut être relié à plusieurs PRMD. Si c'est le cas, l'acheminement peut être basé sur des attributs d'adresses d'O/R conditionnels, notamment, mais pas exclusivement, l'attribut nom-domaine-privé.

d) Un MD peut être relié directement à certains autres MD, mais pas à tous. Lorsque l'adresse d'O/R identifie un MD avec lequel il n'existe aucune connexion directe, l'acheminement peut être fondé sur des accords bilatéraux avec les MD avec lesquels des connexions directes et d'autres règles locales existent.

e) Lorsque le MD est directement relié au MD identifié par l'adresse d'O/R, l'objet est, en règle générale, acheminé directement vers ce MD.

f) Par accord bilatéral, un MD peut éventuellement acheminer un objet vers un autre MD pour, par exemple, une conversion.

g) Un MD peut s'acheminer vers une adresse d'O/R dont le format est incorrect à condition (évidemment) qu'elle contienne au moins les attributs nécessaires à cette fonction.

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, de politique générale, etc.

SECTION 5 – UTILISATION DE L'ANNUAIRE

20 Présentation générale

La présente section décrit les utilisations que le MHS peut faire de l'annuaire, s'il y a accès. Dans le cas contraire, il revient aux autorités locales de décider des autres moyens dont peut éventuellement disposer le MHS pour accomplir ces mêmes tâches.

La présente section couvre les sujets suivants:

a) authentification;

b) résolution du nom;

c) allongement d'une DL;

d) évaluation des possibilités.

21 Authentification

Un objet fonctionnel peut accomplir les tâches d'authentification au moyen de 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 DL dont il possède le nom d'annuaire, un objet présente le nom à l'annuaire et demande à l'entrée figurant dans l'annuaire et correspondant à l'objet, les attributs suivants:

a) *adresse d'O/R MHS*;

b) *méthodes préférées de remise dans le MHS*.

Pour que cette opération s'effectue avec succès, l'objet doit d'abord s'authentifier auprès de l'annuaire et avoir droit d'accès aux renseignements requis.

23 Allongement d'une DL

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

Pour obtenir les membres d'une DL dont il possède le nom d'annuaire, l'objet présente ce nom à l'annuaire et demande à l'inscription figurant dans l'annuaire et correspondant à l'objet en question de fournir les attributs suivants:

a) *membres DL du MHS*;

b) *autorisation de dépôt DL du MHS*;

c) *méthodes préférées de remise dans le MHS*.

Pour que cette opération s'opère avec succès, le 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'un usager ou d'un MS au moyen de l'annuaire.

Les attributs d'annuaire suivants représentent les capacités de l'usager pouvant avoir une importance dans le cadre de la messagerie:

a) *longueur du contenu livrable dans le MHS*;

b) *types de contenus livrables dans le MHS*;

c) *EIT livrables dans le MHS*;

d) *méthodes préférées de remise dans le MHS*.

Les attributs d'annuaire suivants représentent les capacités du MS pouvant avoir une importance dans la messagerie:

a) *actions automatiques admises dans le cadre du MHS*;

b) *types de contenus admis dans le MHS*;

c) *attributs facultatifs admis dans le MHS*.

Pour évaluer une possibilité particulière d'un utilisateur ou d'une MS dont il possède la nom d'annuaire, l'objet présente ce nom à l'annuaire et demande à l'inscription figurant dans l'annuaire et correspondant à l'objet, l'attribut lié à cette capacité.

Pour que cette opération s'effectue avec succès, le 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 MHS s'effectue au moyen de l'OSI.

Il traite des sujets suivants:

a) éléments de service d'application;

b) contextes d'application.

26 Eléments de service d'application

Cette clause spécifie les éléments de service d'application (ASE) figurant dans la réalisation OSI de la messagerie.

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

Remarque – Outre les ASE étudiés dans la présente section, le MHS compte sur l'élément de service d'accès à l'annuaire défini dans la Recommandation X.519. Mais cet ASE ne figurant pas dans les AC concernant la messagerie (voir la Recommandation X.419), il n'en sera pas tenu compte dans la présente section.

26.1 *Concept ASE*

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 AE, sont indiquées. Chaque AE comprend un UE et un ou plusieurs ASE. Un UE représente la partie contrôle ou organisation d'un AE qui définit le rôle du système ouvert (par exemple, celui d'un MTA). Un ASE représente un des ensembles de capacités de communication, ou services (destinés, par exemple, au dépôt ou au transfert de messages), dont l'UE a besoin pour remplir son rôle.

La relation entre deux AE dans différents systèmes ouverts est appelée association d'application. Les ASE de chaque système ouvert communiquent avec les ASE équivalents 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 ASE en une seule AE soit réussie, ces ASE doivent être conçus de façon que leur utilisation de l'association d'application soit coordonnée.

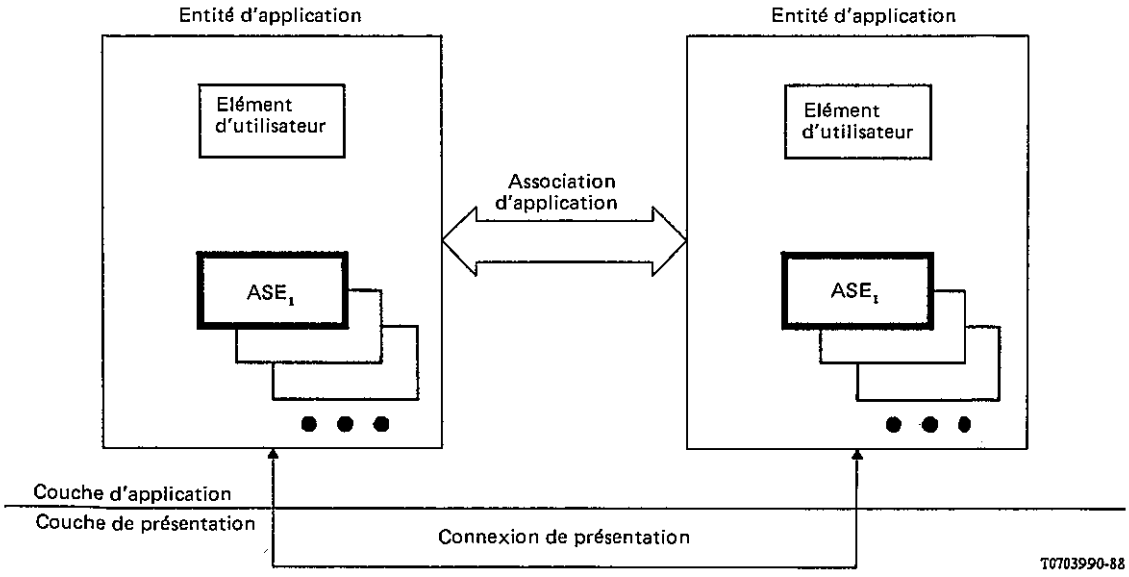


FIGURE 12/X.402

Concept ASE

Un ASE joue le rôle principalement mécanique de traduire des demandes et des réponses formulées par ses UE dans et à partir de la forme prescrite par le protocole d'application régissant l'interaction de l'ASE avec son correspondant dans le système ouvert auquel l'association le relie. L'ASE réalise un service abstrait, ou une partie de ce service, aux fins d'une communication OSI (voir la Recommandation X.407).

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 d'un des types définis au § 7. Un UE fait, à son tour, partie d'un processus d'application.

26.2 *ASE symétrique et asymétrique*

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

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

b) **asymétrique** – Se dit d'un ASE grâce auquel un UE assure ou utilise un service, selon la configuration de l'ASE, mais ne permet pas les deux à la fois. Par exemple, l'ASE destiné à la remise de messages est asymétrique car seul le système ouvert comprenant un MTA offre le service correspondant et seul l'autre système ouvert, qui comprend un UA ou une MS, l'utilise.

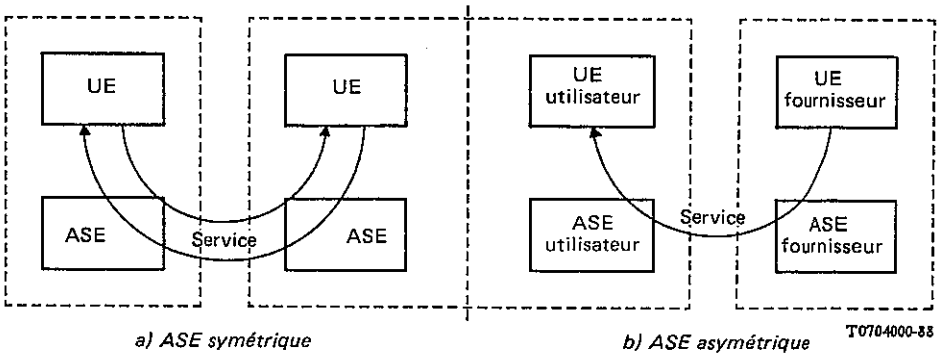


FIGURE 13/X.402

ASE symétrique et asymétrique

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

a) **UE fournisseur-x** – Processus d'application qui assure le service représenté par l'ASE asymétrique x.

b) **ASE fournisseur-x** – ASE asymétrique x conçu pour être installé au même emplacement qu'un UE fournisseur-x.

c) **UE utilisateur-x** – Processus d'application qui utilise le service représenté par l'ASE asymétrique x.

d) **ASE utilisateur-x** – ASE asymétrique conçu pour être installé au même emplacement qu'un UE utilisateur-x.

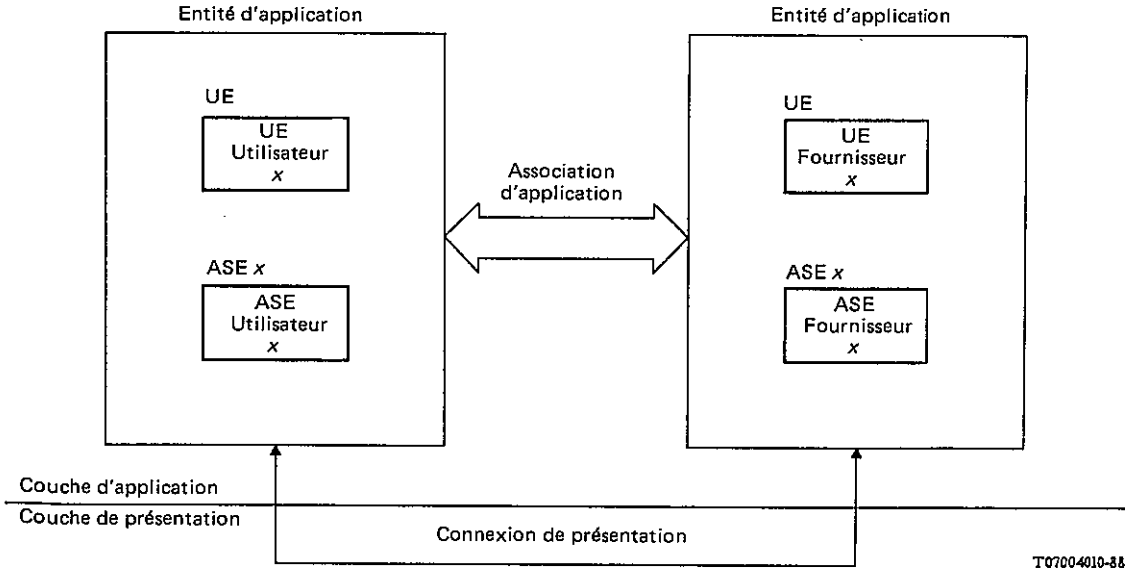


FIGURE 14/X.402

Terminologie relative aux ASE asymétriques

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

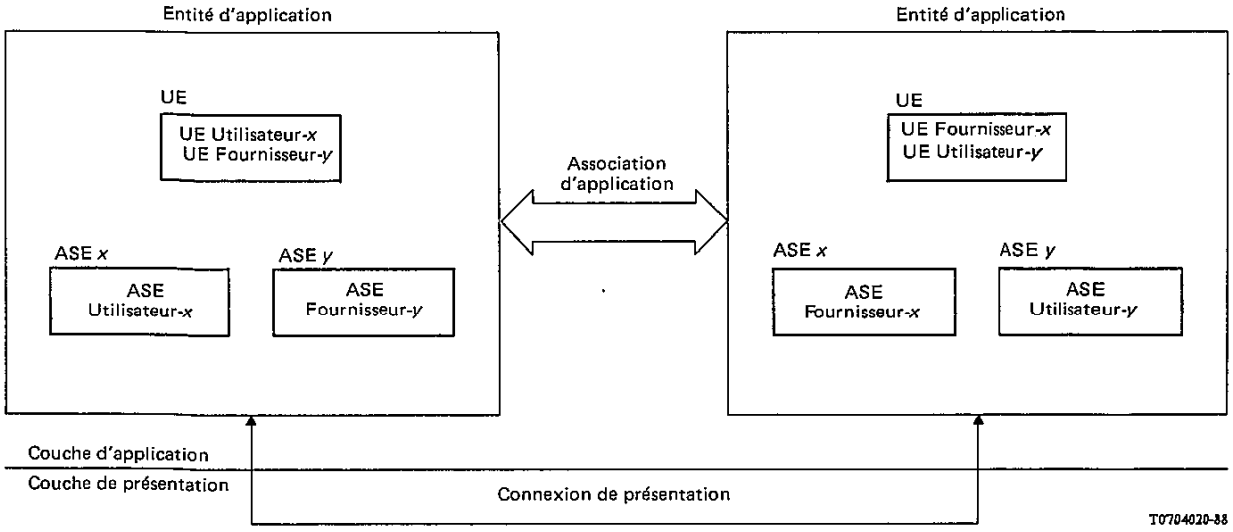


FIGURE 15/X.402

ASE asymétriques multiples

26.3 *ASE de messagerie*

Les ASE assurant les divers services de messagerie sont énumérés dans la première colonne du tableau 11/X.402. Pour chaque ASE cité, la deuxième colonne spécifie s'il est symétrique ou asymétrique. La troisième colonne indique les objets fonctionnels – UA, MS, MTA et AU – associés à l'ASE, qu'ils soient utilisateurs ou fournisseurs.

TABLEAU 11/X.402

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

Des ASE de messagerie, résumés dans le tableau 11/X.402, sont présentés individuellement ci-dessous. Chaque d'eux est défini dans la Recommandation X.419.

26.3.1 *Transfert de messages*

L'élément de service de transfert de messages (MTSE) est le moyen par lequel l'étape de transmission par transfert s'effectue.

26.3.2 *Dépôt de messages*

L'élément de service dépôt de messages (MSSE) est le moyen par lequel s'effectue l'étape de transmission de dépôt.

26.3.3 *Remise de messages*

L'élément de service remise de messages (MDSE) est le moyen par lequel s'effectue l'étape de transmission de remise.

26.3.4 *Extraction de messages*

L'élément de service retrait de messages (MRSE) est le moyen par lequel s'effectue l'étape de transmission d'extraction.

26.3.5 *Administration de messages*

L'élément de service d'administration de messages (MASE) est le moyen par lequel un UA, une MS ou un MTA classe les informations reçues des uns et des autres qui devront en permettre et en contrôler ultérieurement l'interaction au moyen des MSSE, MDSE, MRSE et MASE.

26.4 *ASE de soutien*

Les ASE destinés à des fins non spécifiques dont dépendent les ASE de messagerie sont énumérés dans la première colonne du tableau 12/X.402. Pour chaque ASE énuméré, la deuxième colonne indique s'il est symétrique ou asymétrique.

TABLEAU 12/X.402

ASE de soutien

ASE	Forme
ROSE	SY
RTSE	SY
ACSE	SY

SY Symétrique

Les ASE de soutien, résumés dans le tableau ci-dessus, sont présentés individuellement ci-dessous.

26.4.1 *Opérations distantes*

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

Le ROSE est défini dans la Recommandation X.219.

26.4.2 *Transfert fiable*

L'élément de service transfert fiable (RTSE) est le moyen par lequel diverses ASE de messagerie symétriques et asymétriques transmettent des objets d'information - en particulier les objets volumineux (par exemple, les messages de télécopie) – entre systèmes ouverts afin d'assurer leur mémorisation sûre à leurs destinations.

Le RTSE est défini dans la Recommandation X.218.

26.4.3 *Commande d'association*

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

Le ACSE est défini dans la Recommandation X.217.

27 Contextes d'application

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

Un AC spécifie la façon dont l'association doit être établie (par exemple, quels paramètres d'initialisation doivent être échangés), quels ASE doivent être utilisés pour une communication entre homologues sur l'association, quelles contraintes (le cas échéant) doivent être imposées à l'utilisation individuelle par les ASE de l'association, quel est, entre l'initiateur et le répondeur, l'utilisateur de chaque ASE asymétrique et comment l'association doit être libérée (par exemple, quels paramètres de finalisation doivent être échangés).

Un nom est donné à chaque AC (par un identificateur d'objets ASN.1). L'initiateur d'une association indique au répondeur l'AC qui régira l'utilisation de l'association en lui transmettant le nom de l'AC au moyen de l'ACSE.

Un AC identifie également par un nom (un identificateur d'objets ASN.1) les syntaxes abstraites des APDU qu'une association peut véhiculer pour avoir été utilisée par les ASE de l'AC. La méthode classique consiste à attribuer un nom à l'ensemble des APDU associées soit à chaque ASE, soit à l'ensemble de l'AC. L'initiateur d'une association indique au répondeur la ou les syntaxes abstraites liées à l'AC en lui communiquant leurs noms par l'intermédiaire de l'ACSE.

La syntaxe abstraite d'une APDU représente 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'APDU qui est la façon dont l'objet d'information est représenté pour transmission entre deux systèmes ouverts (par exemple, un octet représentant un ensemble ASN.1, suivi par un octet indiquant la longueur de l'ensemble, etc.).

Les AC par lesquels les divers services de messagerie sont assurés sont spécifiés dans la Recommandation X.419. Ces protocoles sont appelés P1, P3 et P7.

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

ANNEXE A

(à la Recommandation X.402)

Classes d'objets et attributs d'annuaire

La présente annexe fait partie intégrante de la présente Recommandation.

Plusieurs classes d'objets, attributs et syntaxes d'attributs d'annuaire sont spécifiqus à la messagerie. Ils sont respectivement définis dans la présente annexe à l'aide des macros de la Recommandation X.501 CLASSE-OBJET, ATTRIBUT ET SYNTAXE-ATTRIBUT.

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 Recommandation X.521. Voir également le § 9 de la Recommandation X.501 pour une explication montrant comment des classes d'objets d'annuaire peuvent être combinées en une entrée d'annuaire. L'annexe B de la Recommandation X.521 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 MHS*

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

Un objet **mémoire de message MHS** est un AE qui réalise une MS. Les attributs contenus dans son entrée, pour autant qu'ils soient présents, décrivent le MHS, identifient son propriétaire et énumèrent les attributs facultatifs, les actions automatiques et les types de contenu qu'il assure.

```
mhs-message-store OBJECT-CLASSSUBCLASS OF applicationEntity
    MAY CONTAIN {
        description,
        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 MHS*

Un objet **agent de transfert de message MHS** est un AE qui met en oeuvre un MTA. Les attributs contenus dans son entrée, dans la mesure où ils sont présents, décrivent le MTA et identifient son propriétaire et sa longueur de contenu qui peut être remis.

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

A.1.4 *Utilisateur MHS*

Un objet **utilisateur MHS** est un utilisateur générique MHS. Celui-ci peut avoir 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, identifient la longueur de contenu qui peut être remis à l'utilisateur, les types de contenu de celui-ci, ses EIT, sa 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,
        mhs-preferred-delivery-methods }
    ::= id-oc-mhs-user
```

A.1.5 *Agent d'utilisateur MHS*

Un objet **agent d'utilisateur MHS** est un AE qui réalise un UA. Les attributs contenus dans son entrée, dans la mesure où ils sont présents, identifient le propriétaire de l'UA, sa longueur de contenu qui peut être remis, ses types de contenu, ses 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 remis au MHS*

L'attribut **longueur de contenu pouvant être remis au MHS** identifie la longueur de contenu maximale des messages dont un utilisateur acceptera la remise.

Une 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 au MHS*

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

Une 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 *EIT pouvant être remis au MHS*

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

Une 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 DL MHS*

L'attribut **membres DL MHS** identifie les membres d'une DL.

Une 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 *Permissions de dépôt DL MHS*

L'attribut **permissions de dépôt DL MHS** identifie les utilisateurs et les DL qui peuvent déposer des messages dans une DL.

Une valeur de cet attribut est une permission de dépôt d'une 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 *Mémoire de message MHS*

L'attribut **mémoire de message MHS** identifie la MS d'un utilisateur par son nom.

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

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

A.2.7 *Adresses d'O/R MHS*

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

Une 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 *Méthodes préférées de remise MHS*

L'attribut **méthodes préférées de remise MHS** identifie, par ordre de préférence décroissante, les méthodes de remise qu'un utilisateur préfère.

Une valeur de cet attribut est une méthode préférée de remise.

```
mhs-preferred-delivery-methods ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
    MATCHES FOR EQUALITY
    SINGLE VALUE
    ::= id-at-mhs-preferred-delivery-methods
```

A.2.9 *Actions automatiques assurées par le MHS*

L'attribut **actions automatiques assurées par le MHS** identifie les actions automatiques qu'une MS assure entièrement.

Une 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.2.10 *Types de contenus assurés par le MHS*

L'attribut **types de contenus assurés par le MHS** identifie les types de contenus des messages dont une MS assure entièrement la syntaxe et la sémantique.

Une 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.2.11 *Attributs facultatifs assurés par le MHS*

L'attribut **attributs facultatifs assurés par le MHS** identifie les attributs facultatifs qu'une MS assure entièrement.

Une 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 *Permission de dépôt DL MHS*

La syntaxe d'attribut **permission de dépôt DL MHS** caractérise un attribut dont chacune des valeurs est une permission 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 }
```

Une valeur présentée de permission de dépôt DL doit être du type individual (individuel).

Une permission de dépôt DL, selon son type, peut n'autoriser l'accès de dépôt à aucun utilisateur et à aucune DL ou autoriser cet accès aux utilisateurs et aux DL suivants:

a) *Individual* (individuel) – L'utilisateur ou la DL (non élargie) dont l'un quelconque des noms d'O/R est égal au nom d'O/R spécifié.

b) *Member-of-dl* (membre-de-dl) – Chaque membre de la DL, dont l'un quelconque des noms d'O/R est égal au nom d'O/R spécifié ou de chaque DL imbriquée, de manière récurrente.

c) *Pattern-match* (correspondance-structure) – Chaque utilisateur ou DL (non élargie) 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 imbriqués, de manière récurrente.

Une 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 MHS*

La syntaxe d'attribut **adresse d'O/R 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-nhs-or-address
```

Une valeur présentée d'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 MHS*

La syntaxe d'attribut **nom d'O/R 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
```

Une valeur présentée de 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)

Définitions de référence des identificateurs d'objets

La présente annexe fait partie intégrante de la Recommandation.

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

Tous les identificateurs d'objets que la présente Recommandation affecte sont affectés 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 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 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 MHS

id-mhsac ID ::= { joint-iso-ccitt mhs-motis(6) mhsac(0) }
          -- MHS Application Contexts
          -- See Recommendation X.419.



    id-ipms   ID ::= { joint-is-ccitt mhs-motis(6) ipms(1) }
              -- Interpersonal Messaging
              -- See Recommendation X.420.

    id-asdc   ID ::= { joint-iso-ccitt mhs-motis(6) asdc (2) }
              -- Abstract Service Definition Conventions
              -- See Recommendation X.407.

    id-mts    ID ::= { joint-iso-ccitt mhs-motis(6) mts (3) }
              -- Message Transfer System
              -- See Recommendation X.411.

    id-ms     ID ::= { joint-iso-ccitt mhs-motis(6) ms (4) }
              -- Message Store
              -- See Recommendation X.413.

    id-arch   ID ::= { joint-iso-ccitt mhs-motis(6) arch (5) }
              -- Overall Architecture
              -- See this Recommendation.

    id-group  ID ::= { joint-iso-ccitt mhs-motis(6) group (6) }
              -- Reserved.


  -- Catégories

  id-mod    ID ::= { id-arch 0 } -- modules, not definitive
  id-oc     ID ::= { id-arch 1 } -- object classes
  id-at     ID ::= { id-arch 2 } -- attribute types
  id-as     ID ::= { id-arch 3 } -- attribute syntaxes
```

```
-- Modules

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


-- 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                           ID ::= { id-oc 3 }
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                  ID ::= { id-at 5 }
id-at-mhs-or-addresses                   ID ::= { id-at 6 }
id-at-mhs-preferred-delivery-methods     ID ::= { id-at 7 }
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'identificateurs d'objets MHS
```

ANNEXE C

(à la Recommandation X.402)

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

La présente 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 de la Recommandation X.501 CLASSE-OBJET, ATTRIBUT et SYNTAXE-ATTRIBUT.

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

IMPORTS

      -- Identificateurs d'objets 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,
            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) }

      -- MTS Abstract Service
            ORAddress, ORName, RequestedDeliveryMethod
            ----
            FROM MTSAbstractService { joint-iso-ccitt
                  mhs-motis(6) mts(3) modules(0) mTS-abstract-service(3) }

      -- Information Framework
            ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS
            ----
            FROM informationFramework { joint-iso-ccitt
                  ds(5) modules(1) informationFramework(1) }

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

      -- Selected Attribute Types
            commonName, description, distinguishedNameSyntax,
            integerSyntax, objectIdentifierSyntax, organization,
            organizationalUnitName, owner, seeAlso
            ----
            FROM SelectedAttributeTypes { joint-iso-ccitt
                  ds(5) modules(1) selectedAttributeTypes(5) }
```

```
-- CLASSES D'OBJETS

    -- Liste de distribution MHS
        mhs-distribution-list OBJECT-CLASS
            SUBCLASS OF top
            MUST CONTAIN {
                commonName,
                mhs-dl-submit-permissions,
                mhs-or-addresses }
            MAY CONTAIN {
                description,
                organization,
                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 MHS
        mhs-message-store OBJECT-CLASS
            SUBCLASS OF applicationEntity
            MAY CONTAIN {
                description,
                owner,
                mhs-supported-optional-attributes,
                mhs-supported-automatic-actions,
                mhs-supported-content-types }
            ::= id-oc-mhs-message-store

    -- Agent de transfert de message MHS
        mhs-message-transfer-agent OBJECT-CLASS
            SUBCLASS OF applicationEntity
            MAY CONTAIN {
                description,
                owner,
                mhs-deliverable-content-length }
            ::= id-oc-mhs-message-transfer-agent

    -- Utilisateur 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,
                mhs-preferred-delivery-methods }
            ::= id-oc-mhs-user

    -- Agent d'usager MHS
        mhs-user-agent OBJECT-CLASS
            SUBCLASS OF applicationEntity
            MAY CONTAIN {
                owner,
                mhs-deliverab;e-content-length,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-or-addresses }
            ::= id-oc-mhs-user-agent
```

```
-- ATTRIBUTS

    -- Longueur de contenu pouvant être remis MHS
        mhs-deliverable-content-length ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX integerSyntax
            SINGLE VALUE
            ::= id-at-mhs-deliverable-content-length

    -- Types de contenu pouvant être remis MHS
        mhs-deliverable-content-types ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-content-types

    -- EIT pouvant être remis MHS
        mhs-deliverable-eits ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-eits

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

    -- Permission de dépôt DL 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 MHS
        mhs-or-addresses ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
            MULTI VALUE
            ::= id-at-mhs-or-addresses

    -- Mémoire de message MHS
        mhs-message-store ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
            SINGLE VALUE
            ::= id-at-mhs-message-store

    -- Méthode de remise préférée MHS
        mhs-preferred-delivery-methods ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
            MATCHES FOR EQUALITY
            SINGLE VALUE
            ::= id-at-mhs-preferred-delivery-methods

    -- Actions automatiques assurées par le MHS
        mhs-supported-automatic-actions ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-automatic-actions

    -- Types de contenu assurés par le MHS
        mhs-suppported-content-types ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-content-types

    -- Attributs facultatifs assurés par le MHS
        mhs-supported-optional-atributes ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-optional-attributes
```

```
-- SYNTAXES D'ATTRIBUTS

    -- Permission de dépôt DL 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 MHS
        mhs-or-address-syntax ATTRIBUTE-SYNTAX
            SYNTAX ORAddress
            MATCHES FOR EQUALITY
            ::= id-as-mhs-or-address

    -- Nom d'O/R MHS
        mhs-or-name-syntax ATTRIBUTE-SYNTAX
            SYNTAX ORName
            MATCHES FOR EQUALITY
            ::= id-as-mhs-or-name

END -- d'annuaire MHS
```

ANNEXE D

Menaces pour la sécurité

La présente annexe ne fait pas partie de la Recommandation.

Un aperçu général des risques auxquels le MHS est exposé est donné au § 15.1 de la Recommandation X.400, où sont examinés les risques rencontrés dans un MHS à différents niveaux: lors de 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) identité usurpée;

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 inconvénients peuvent survenir par accident ou être causés dans une intention malveillante et peuvent être actifs ou passifs. Des tentatives de porter atteinte au 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 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 MHS

Risque	Services
Identité usurpée	
Usurpation d'identité et usage abusif du MTS	Authentification de l'origine du message Authentification de l'origine de l'essai Gestion d'accès sûr
Accusé de réception mensonger	Preuve de la remise
Prétendue expédition d'un message	Authentification de l'origine du message
Usurpation de l'identité d'un MTA vis-à-vis d'un utilisateur-MTS	Preuve du dépôt Authentification de l'origine du rapport Gestion d'accès sûr
Usurpation d'identité d'un MTA vis-à-vis d'un autre MTA	Authentification de l'origine du rappport Gestion d'accès sûr
Mise en séquence des messages	
Répétition des messages	Intégrité de séquence de message
Réagencement des messages	Intégrité de séquence de message
Lecture anticipée de messages	
Retard des messages	
Modification d'informations	
Modification de messages	Intégrité de la communication Intégrité du contenu
Destruction de messages	Intégrité de séquence de message
Altération de l'information d'acheminement ou d'une autre information de gestion	
Refus de service	
Refus de communications	
Débordement du MTA	
Débordement du MTS	
Répudiation	
Refus d'origine	Non-répudiation d'origine
Refus de dépôt	Non-répudiation de dépôt
Refus de remise	Non-répudiation de remise
Fuite d'informations	
Perte de confidentialité	Confidentialité de la connexion Confidentialité du contenu
Perte d'anonymat	Confidentialité du cheminement du message
Détournement de messages	Gestion d'accès sûr
Analyse du trafic	Confidentialité du cheminement du message
Autres risques	
Expéditeur non autorisé pour l'étiquette de sécurité de message (dépôt inapproprié)	Gestion d'accès sûr Etiquetage de sécurité de message
Utilisateur MTA/MTS non autorisé pour le contexte de sécurité	Gestion d'accès sûr
Acheminement erroné	Gestion d'accès sûr Etiquetage de sécurité de message
Politique d'étiquetage différentes	

D.1 *Identité usurpée*

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

Les risques d'identité usurpée sont les suivants:

a) usurpation d'identité et usager abusif du MTS;

b) accusé de réception mensonger;

c) prétendue expédition d'un message;

d) usurpation de l'identité d'un MTA vis-à-vis d'un utilisateur-MTS;

e) usurpation de l'identité d'un MTA vis-à-vis d'un autre MTA.

Une identité usurpée consiste généralement en 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 répétition ou de la modification de 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, décalée dans le temps ou réagencée. La mise en séquence d'un message peut être utilisée pour exploiter l'information d'authentification dans un message en bonne et due forme et remettre en séquence ou décaler dans le temps les messages en bonne et due forme. Bien qu'avec les services de sécurité MHS, il soit impossible d'éviter le risque de répétition, on peut déceler ce risque et en éliminer les effets.

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

a) répétition de messages;

b) réagencement de messages;

c) lecture anticipée de messages;

d) retard de messages.

D.3 *Modification d'informations*

L'information destinée à un destinataire prévu, l'information d'acheminement et d'autres données de gestion peuvent être perdues ou modifiées sans détection. Cela peut arriver à n'importe quel aspect du message, par exemple son étiquetage, son contenu, ses attributs, son destinataire ou son expéditeur. Une altération de l'information d'acheminement ou d'une autre information de gestion, enregistrée dans les MTA ou utilisée par ceux-ci, peut amener le MTS à perdre des messages ou à fonctionner incorrectement à un autre égard.

Les risques de modification d'informations sont les suivants:

a) modification de messages;

b) destruction de messages;

c) altération 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. Ce refus de service peut être un refus d'accès, un refus de communications (ce qui aboutit à d'autres problèmes comme la surcharge), une suppression délibérée de messages vers un destinataire particulier, ou une fabrication de trafic supplémentaire. Le MTS peut être refusé si une intervention a provoqué une défaillance ou un fonctionnement incorrect du MTA. En outre, un utilisateur-MTS peut amener le MTS à refuser un service à d'autres utilisateurs en «inondant» ce service de messages susceptibles de surcharger la capacité de commutation d'un 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) débordement du MTA;

c) débordement du MTS.

D.5 *Répudiation*

La répudiation peut se produire quand un utilisateur-MTS ou le 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 MHS quelconque ou par abus de confiance. Dans certains cas, la présence d'un utilisateur-MTS sur le système peut poser un problème délicat, d'où la nécessité pour cet utilisateur de préserver, le cas échéant, son anonymat. Un utilisateur-MTS autre que le destinataire prévu peut obtenir un message, cela par suite d'une usurpation de l'identité du MTS et d'un usage abusif de celui-ci, ou encore d'une intervention ayant entraîné un fonctionnement incorrect d'un MTA. De plus amples détails sur les informations écoulées dans un MTS peuvent être obtenus à partir de l'observation du 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 sûr à plusieurs niveaux ou à un seul, il peut exister plusieurs risques relatifs à l'étiquetage de sécurité, par exemple en cas d'acheminement par l'intermédiaire d'un point nodal auquel il n'est pas possible de confier des informations revêtant une importance particulière ou lorsque les systèmes utilisent des politiques d'étiquetage différentes. D'autres facteurs peuvent compromettre la mise en application d'une politique de sécurité fondée sur une séparation logique utilisant des étiquettes de sécurité. Un utilisateur-MTS peut expédier un message et lui affecter une étiquette qu'il n'est pas autorisé à lui affecter. Un utilisateur-MTS ou un MTA peut établir ou accepter une association avec un contexte de sécurité sans avoir d'autorisation pour ce faire.

Les risques visés dans ce paragraphe sont les suivants:

a) expéditeur non autorisé pour l'étiquette de sécurité du message (dépôt inapproprié);

b) utilisateur-MTA/MTS non autorisé pour le contexte de sécurité;

c) acheminement erroné;

d) politiques d'étiquetage différentes.

ANNEXE E

(à la Recommandation X.402)

Prestation des services de sécurité décrits dans la Recommandation X.411

La présente annexe fait partie intégrante de la Recommandation.

Le tableau E-1/X.402 indique les éléments de service de la Recommandation X.411 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 MHS

Service	Arguments/service MTS
Services de sécurité authentification d'origine	
Authentification de l'origine du message	Contrôle d'authentification de l'origine du message Jeton de message
Authentification de l'origine de l'essai	Contrôle d'authentification de l'origine de l'essai
Authentification de l'origine du rapport	Contrôle d'authentification de l'origine du rapport
Preuve de dépôt	Demande de preuve de dépôt Preuve de dépôt
Preuve de remise	Demande de preuve de remise Preuve de remise
Services de sécurité de gestion d'accès sûr	
Authentification de l'entité homologue	Pouvoir du demandeur Pouvoir du demandé
Contexte de sécurité	Contexte de sécurité
Services de sécurité confidentialité des données	
Confidentialité de la communication	Non assurée
Confidentialité du contenu	Identificateur de l'algorithme du contenu Jeton de message
Confidentialité du cheminement du message	Type de contenu
Services de sécurité intégrité des données	
Intégrité de la communication	Non assurée
Intégrité du contenu	Contrôle d'intégrité du contenu Jeton de message Contrôle d'authentification de l'origine du message
Intégrité de séquence de message	Numéro de séquence de message Jeton de message
Services de sécurité non répudiation	
Non-répudiation d'origine	Contrôle d'intégrité du contenu Jeton de message Contrôle d'authentification de l'origine du message
Non-répudiation de dépôt	Demande de preuve de dépôt Preuve de dépôt
Non-répudiation de remise	Demande de preuve de remise Preuve de remise
Etiquetage de sécurité du message	Etiquette de sécurité du message Jeton de message Contrôle d'authentification de l'origine du message
Services de sécurité de gestion de sécurité	
Modification des pouvoirs	Modification des pouvoirs
Enregistrement	Enregistrement

ANNEXE F

Différences entre la Recommandation du CCITT et la norme ISO

La présente annexe ne fait pas partie de la Recommandation.

La présente annexe donne la liste des différences entre la présente Recommandation et la norme internationale ISO correspondante, à l'exception des différences d'ordre purement stylistique.

Les différences qui existent sont les suivantes:

a) La norme ISO internationale correspondant à la présente Recommandation décrit une connexion directe de deux domaines de gestion privés (PRMD) du même pays, une connexion directe de deux PRMD de pays différents et un seul PRMD relié à deux domaines de gestion administratifs (ADMD), tandis que la présente Recommandation ne le décrit pas (voir la figure 11/X.402).

b) La norme ISO internationale correspondant à la présente Recommandation ne nécessite pas que les ADMD et les PRMD soient hiérarchiquement liés pour les besoins d'adressage et d'acheminement, tandis que cela est nécessaire dans la présente Recommandation (voir les § 14.1.1, 14.1.2, 15 et 19).

c) Lorsqu'un attribut adresse-O/R admet des chaînes imprimables et des chaînes télétex, la norme ISO internationale correspondant à la présente Recommandation ne nécessite pas que la chaîne imprimable soit pourvue au minimum à chaque fois que des attributs sont acheminés au niveau international, tandis que cela est nécessaire dans la présente Recommandation (voir le § 18.2).

ANNEXE G

Index

La présente annexe ne fait pas partie de la Recommandation.

La présente annexe constitue l'index à la présente Recommandation. Elle recense de manière exhaustive les points contenus dans chacune des catégories.

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) points **nécessitant un complément d'étude**;

j) points **à fournir**.

G.1 *Abréviations*

G.2 *Termes*

SÉRIES DES RECOMMANDATIONS UIT–T

Série A	Organisation du travail de l'UIT–T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données et communication entre systèmes ouverts**
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication

Imprimé en Suisse

Genève, 2008