



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**X.402**

(06/1999)

SÉRIE X: RÉSEAUX DE DONNÉES ET  
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Systemes de messagerie

---

**Technologies de l'information – Systemes de  
messagerie: architecture globale**

Recommandation UIT-T X.402

---

RECOMMANDATIONS UIT-T DE LA SÉRIE X  
**RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS**

<b>RÉSEAUX PUBLICS DE DONNÉES</b>	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
<b>INTERCONNEXION DES SYSTÈMES OUVERTS</b>	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
<b>INTERFONCTIONNEMENT DES RÉSEAUX</b>	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
<b>SYSTÈMES DE MESSAGERIE</b>	<b>X.400–X.499</b>
<b>ANNUAIRE</b>	<b>X.500–X.599</b>
<b>RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES</b>	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
<b>GESTION OSI</b>	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
<b>SÉCURITÉ</b>	<b>X.800–X.849</b>
<b>APPLICATIONS OSI</b>	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
<b>TRAITEMENT RÉPARTI OUVERT</b>	<b>X.900–X.999</b>
<b>SÉCURITÉ DES TÉLÉCOMMUNICATIONS</b>	<b>X.1000–</b>

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

**Technologies de l'information – Systèmes de messagerie:  
architecture globale**

**Résumé**

La présente Recommandation | Norme internationale contient les définitions des attributs et des classes d'objets d'annuaire, certaines de ces définitions étant nouvelles et d'autres étant révisées pour les besoins des nouvelles Recommandations X.680 et X.880. De nombreuses corrections de défaut ont été introduites. La présente Recommandation | Norme internationale contient également des améliorations relatives aux organismes internationaux d'enregistrement à l'utilisation des caractères ISO/CEI 10646 dans les adresses OR, à la protection des modifications de pouvoirs et à l'utilisation de l'annuaire 1997.

**Source**

La Recommandation X.402 de l'UIT-T a été approuvée le 18 juin 1999. Un texte identique est également publié comme Norme internationale ISO/CEI 10021-2.

Conformément à la décision de l'UIT-T visant à publier de nouvelles éditions de l'ensemble de Recommandations relatives à la messagerie, la présente édition de la Rec. UIT-T X.402 intègre la Rec. X.402 (11/1995), le Corrigendum technique 1 de la Rec. X.402 (08/1997) et l'Amendement 1 de la Rec. X.402 (12/1997).

## AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de la CMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2004

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

## TABLE DES MATIÈRES

	<i>Page</i>
SECTION 1 – INTRODUCTION .....	1
1    Domaine d'application.....	1
2    Références normatives.....	3
2.1   Interconnexion des systèmes ouverts .....	3
2.2   Systèmes d'annuaire .....	4
2.3   Systèmes de messagerie .....	4
2.4   Codes de pays.....	5
2.5   Adresses dans le réseau.....	5
2.6   Code de langue.....	5
2.7   Jeux de caractères.....	5
3    Définitions.....	5
3.1   Interconnexion des systèmes ouverts .....	5
3.2   Systèmes d'annuaire .....	7
3.3   Systèmes de messagerie .....	7
4    Abréviations .....	7
5    Conventions.....	7
5.1   ASN.1.....	7
5.2   Catégorie .....	8
5.3   Termes.....	8
SECTION 2 – MODÈLES ABSTRAITS.....	8
6    Aperçu général .....	8
7    Modèle fonctionnel.....	8
7.1   Objets fonctionnels primaires.....	9
7.1.1   Système de messagerie.....	9
7.1.2   Utilisateurs .....	9
7.1.3   Listes de distribution .....	9
7.2   Objets fonctionnels secondaires .....	10
7.2.1   Système de transfert de messages .....	10
7.2.2   Agents d'utilisateurs .....	10
7.2.3   Mémoires de message .....	10
7.2.4   Unités d'accès.....	11
7.3   Objets fonctionnels tertiaires.....	11
7.3.1   Agents de transfert de messages.....	11
7.4   Types d'unités AU choisis.....	11
7.4.1   Remise physique .....	12
7.4.2   Télématique.....	12
7.4.3   Télex .....	12
8    Modèle informationnel.....	12
8.1   Messages .....	12
8.2   Envois-tests .....	13
8.3   Rapports .....	13
9    Modèle opérationnel.....	14
9.1   Transmission .....	14
9.2   Rôles de transmission.....	15
9.3   Etapas de la transmission .....	16
9.3.1   Expédition .....	16
9.3.2   Dépôt.....	17
9.3.3   Import.....	17
9.3.4   Transfert .....	17
9.3.5   Export.....	17
9.3.6   Remise.....	17
9.3.7   Extraction .....	18
9.3.8   Réception .....	18

9.4	Evénements de transmission .....	18
9.4.1	Fractionnement.....	18
9.4.2	Groupage.....	19
9.4.3	Résolution du nom .....	19
9.4.4	Développement de liste DL.....	19
9.4.5	Réacheminement .....	19
9.4.6	Conversion .....	19
9.4.7	Non-remise.....	19
9.4.8	Non-affirmation .....	19
9.4.9	Affirmation .....	20
9.4.10	Acheminement .....	20
10	Modèle de sécurité.....	20
10.1	Politiques de sécurité.....	21
10.2	Services de sécurité .....	21
10.2.1	Services de sécurité Authentification de l'origine .....	22
10.2.2	Service de sécurité Gestion de la sécurité de l'accès .....	23
10.2.3	Services de sécurité Confidentialité des données.....	23
10.2.4	Services de sécurité Intégrité des données .....	24
10.2.5	Services de sécurité Non-répudiation.....	25
10.2.6	Service de sécurité Etiquetage de sécurité du message .....	25
10.2.7	Services de gestion de la sécurité.....	26
10.3	Eléments de sécurité.....	26
10.3.1	Eléments de sécurité Authentification.....	26
10.3.2	Eléments de sécurité Gestion de la sécurité de l'accès .....	27
10.3.3	Eléments de sécurité Confidentialité des données.....	28
10.3.4	Eléments de sécurité Intégrité des données.....	28
10.3.5	Eléments de sécurité Non-répudiation .....	29
10.3.6	Eléments de sécurité Etiquette de sécurité .....	29
10.3.7	Eléments de sécurité Gestion de la sécurité .....	29
10.3.8	Technique de double enveloppe.....	30
10.3.9	Chiffrement et adressage calculé.....	30
SECTION 3 – CONFIGURATIONS .....		30
11	Aperçu général .....	30
12	Configurations fonctionnelles .....	30
12.1	Annuaire.....	30
12.2	Mémoire de messages .....	30
13	Configurations physiques .....	31
13.1	Systèmes de messagerie .....	31
13.1.1	Systèmes d'accès .....	32
13.1.2	Systèmes de mémorisation.....	32
13.1.3	Systèmes d'accès et de mémorisation.....	32
13.1.4	Systèmes de transfert.....	32
13.1.5	Systèmes d'accès et de transfert .....	33
13.1.6	Systèmes de mémorisation et de transfert.....	33
13.1.7	Systèmes d'accès, de mémorisation et de transfert.....	33
13.2	Configurations représentatives .....	33
13.2.1	Système MHS entièrement centralisé .....	33
13.2.2	Transfert et mémorisation centralisés de messages.....	34
13.2.3	Transfert centralisé de messages.....	34
13.2.4	Système MHS entièrement décentralisé.....	34
14	Configurations organisationnelles .....	34
14.1	Domaines de gestion .....	34
14.1.1	Domaines de gestion d'administration.....	34
14.1.2	Domaines de gestion privés .....	34
14.2	Configurations représentatives .....	34
14.2.1	Système MHS entièrement centralisé .....	35
14.2.2	Système MHS connecté directement.....	35
14.2.3	Système MHS connecté indirectement.....	35

15	Le système MHS mondial .....	35
SECTION 4 – DÉNOMINATION, ADRESSAGE ET ACHEMINEMENT .....		36
16	Aperçu général .....	36
17	Dénomination .....	36
17.1	Noms d'annuaire .....	36
17.2	Entités OR-name .....	37
18	Adressage .....	37
18.1	Listes d'attributs .....	37
18.2	Jeux de caractères .....	38
18.3	Attributs normalisés .....	39
18.3.1	Nom de domaine d'administration .....	40
18.3.2	Nom courant (common-name) .....	40
18.3.3	Nom de pays (Country-name) .....	41
18.3.4	Extension des composantes d'entité OR-address postale (extension-postal-OR-address-components) .....	41
18.3.5	Extension des composantes d'adresse de remise physique (extension-physical-delivery-address-components) .....	41
18.3.6	Attributs postaux locaux (local-postal-attributes) .....	41
18.3.7	Adresse réseau (network-address) .....	41
18.3.8	Identificateur numérique d'utilisateur (numeric-user-identifier) .....	41
18.3.9	Nom d'organisation (organization-name) .....	42
18.3.10	Noms d'unités organisationnelles (organizational-unit-names) .....	42
18.3.11	Nom de service de remise physique (nom de pds) (pds-name) .....	42
18.3.12	Nom personnel (personal-name) .....	42
18.3.13	Nom de pays de remise physique (physical-delivery-country-name) .....	42
18.3.14	Nom de bureau de remise physique (physical-delivery-office-name) .....	42
18.3.15	Numéro de bureau de remise physique (physical-delivery-office-number) .....	43
18.3.16	Nom d'organisation de remise physique (physical-delivery-organization-name) .....	43
18.3.17	Nom personnel de remise physique (physical-delivery-personal-name) .....	43
18.3.18	Adresse de boîte postale (post-office-box-address) .....	43
18.3.19	Code postal (postal-code) .....	43
18.3.20	Adresse de poste restante (poste-restante-address) .....	43
18.3.21	Nom de domaine privé (private-domain-name) .....	43
18.3.22	Adresse de rue (street-address) .....	43
18.3.23	Identificateur de terminal (terminal-identifier) .....	44
18.3.24	Type de terminal (terminal-type) .....	44
18.3.25	Adresse postale non formatée (unformatted-postal-address) .....	44
18.3.26	Nom postal unique (unique-postal-name) .....	44
18.4	Equivalence entre les listes d'attributs .....	44
18.5	Formes d'entités OR-address .....	45
18.5.1	Entité OR-address mnémotechnique .....	46
18.5.2	Entité OR-address numérique .....	47
18.5.3	Entité OR-address postale .....	47
18.5.4	Entité OR-address du terminal .....	47
18.5.5	Détermination des formes d'adresse .....	48
18.6	Attributs conditionnels .....	48
19	Acheminement .....	48
SECTION 5 – UTILISATION DE L'ANNUAIRE .....		50
20	Aperçu général .....	50
21	Authentification .....	50
22	Résolution de nom .....	50
23	Développement d'une liste DL .....	50
24	Evaluation des capacités .....	50

SECTION 6 – RÉALISATION OSI.....	51
25 Aperçu général .....	51
26 Eléments de service d'application.....	51
26.1 Concept d'élément ASE.....	51
26.2 Eléments ASE symétriques et asymétriques .....	52
26.3 Eléments ASE de messagerie.....	53
26.3.1 Transfert de messages .....	54
26.3.2 Dépôt de messages .....	54
26.3.3 Remise de messages.....	54
26.3.4 Retrait de messages.....	54
26.3.5 Gestion de messages .....	54
26.4 Eléments ASE supports.....	54
26.4.1 Opérations distantes .....	55
26.4.2 Transfert fiable.....	55
26.4.3 Contrôle d'association .....	55
27 Contextes d'application.....	55
SECTION 7 – CONVENTIONS POUR LA DÉFINITION DU SERVICE ABSTRAIT.....	56
28 Aperçu général .....	56
29 Composantes du modèle abstrait .....	56
29.1 Objets abstraits.....	56
29.2 Contrats abstraits.....	56
29.3 Paquets de connexion.....	56
29.4 Accès abstraits.....	57
29.5 Opérations abstraites et erreurs abstraites .....	57
30 Réalisation du service ROS.....	57
Annexe A – Classes d'objets et attributs d'annuaire.....	58
A.1 Classes d'objets .....	58
A.1.1 Liste de distribution du système MHS .....	58
A.1.2 Mémoire de message du système MHS .....	58
A.1.3 Agent de transfert de message du système MHS .....	59
A.1.4 Utilisateur du système MHS .....	59
A.1.5 Agent d'utilisateur du système MHS.....	59
A.2 Attributs .....	60
A.2.1 Types d'informations codées acceptables ( <i>mhs-acceptable-eits</i> ) .....	60
A.2.2 Classes livrables ( <i>mhs-deliverable-classes</i> ) .....	60
A.2.3 Types de contenu livrables ( <i>mhs-deliverable-content-types</i> ) .....	60
A.2.4 Service d'archives DL ( <i>mhs-dl-archive-service</i> ) .....	60
A.2.5 Membres de liste DL ( <i>mhs-dl-members</i> ).....	60
A.2.6 Politique de liste DL ( <i>mhs-dl-policy</i> ).....	61
A.2.7 Listes apparentées à la liste DL ( <i>mhs-dl-related-lists</i> ).....	61
A.2.8 Autorisations de dépôt de liste DL ( <i>mhs-dl-submit-permissions</i> ).....	61
A.2.9 Service d'abonnement de liste DL ( <i>mhs-dl-subscription-service</i> ).....	61
A.2.10 Types EIT exclusivement acceptables ( <i>mhs-exclusively-acceptable-eits</i> ) .....	61
A.2.11 Longueur maximale de contenu ( <i>mhs-maximum-content-length</i> ).....	62
A.2.12 Nom d'annuaire d'une mémoire de message ( <i>mhs-message-store-directory-name</i> ).....	62
A.2.13 Adresses OR-address ( <i>mhs-or-addresses</i> ).....	62
A.2.14 Adresses OR-address avec capacités ( <i>mhs-or-addresses-with-capabilities</i> ).....	62
A.2.15 Attributs pris en charge ( <i>mhs-supported-attributes</i> ) .....	62
A.2.16 Actions automatiques prises en charge ( <i>mhs-supported-automatic-actions</i> ) .....	63
A.2.17 Types de contenus pris en charge ( <i>mhs-supported-content-types</i> ).....	63
A.2.18 Règles de correspondance prises en charge ( <i>mhs-supported-matching-rules</i> ).....	63
A.2.19 Types d'informations codées inacceptables ( <i>mhs-unacceptable-eits</i> ) .....	63
A.3 Syntaxes d'attributs .....	63
A.3.1 Autorisation de dépôt de liste DL (DL Submit Permission) .....	63
A.3.2 Politique des listes DL .....	65
A.3.3 Entité OR-address (OR-Address).....	67

	<i>Page</i>
A.3.4 Adresse OR-address avec capacités .....	67
A.3.5 Entité OR-name (OR-Name).....	67
A.4 Contextes.....	68
A.4.1 Annotation d'administrateur de liste DL (DL-Administrator-Annotation).....	68
A.4.2 Liste DL imbriquée dans liste DL (DL Nested DL).....	69
A.4.3 Réinitialisation de l'expéditeur de la liste DL (DL-Reset-Originator).....	69
A.5 Variantes nominatives d'entité de certificat.....	69
A.5.1 Nom d'agent de transfert de messages.....	69
Annexe B – Définition de référence des identificateurs d'objets .....	70
Annexe C – Définition de référence des classes d'objets et attributs d'annuaire.....	72
Annexe D – Menaces concernant la sécurité .....	79
D.1 Usurpation d'identité .....	79
D.2 Mise en séquence d'un message .....	79
D.3 Modification des informations .....	80
D.4 Refus de service .....	81
D.5 Répudiation .....	81
D.6 Fuite d'informations .....	81
D.7 Autres risques.....	81
Annexe E – Prestation de services de sécurité décrits dans la Rec. UIT-T X.411   ISO/CEI 10021-4 .....	82
Annexe F – Représentation des entités OR-address pour l'utilisateur .....	83
F.1 Objet.....	83
F.2 Domaine d'application.....	83
F.3 Format.....	83
F.3.1 Généralités .....	83
F.3.2 Format étiqueté .....	84
F.3.3 Format explicite .....	86
F.4 Interface d'utilisateur.....	86
Annexe G – Utilisation des entités OR-address par des organisations multinationales.....	88
G.1 Principes d'adressage.....	88
G.2 Exemples de configuration.....	88
G.2.1 Domaines PRMD multiples indépendants .....	89
G.2.2 Un seul domaine PRMD désigné d'après un pays "natal" .....	89
G.2.3 Un seul domaine PRMD doté de noms de pays et de domaine multiples .....	90
G.3 Entités OR-address pseudonymes .....	91
Annexe H – Utilisation de mots de passe protégés pour l'accès à la mémoire de messages.....	92
Annexe I – Différences entre l'ISO/CEI 10021-2 et la Rec. UIT-T X.402 .....	95
Annexe J – Résumé des modifications apportées aux versions précédentes .....	96
J.1 Différences entre l'ISO/CEI 10021-2:1990 et la Rec. CCITT X.402 (1992) .....	96
J.2 Différences entre la Rec. CCITT X.402 (1992) et la Rec. UIT-T X.402 (1995)   ISO/CEI 10021-2:1996 .....	96
J.3 Différences entre la Rec. UIT-T X.402 (1995)   ISO/CEI 10021-2: 1996 et la Rec. UIT-T X.402 (1999)   ISO/CEI 10021-2:1999 .....	96
Annexe K – Index.....	97

## Introduction

La présente Spécification s'inscrit dans une série de Recommandations | Normes internationales consacrées à la messagerie. La série complète donne un schéma d'ensemble d'un système de messagerie (MHS, *message handling system*) réalisé à l'aide d'un nombre quelconque de systèmes ouverts associés.

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

La présente Spécification porte sur l'architecture globale du système MHS et lui sert d'introduction technique.

La présente Spécification a été mise au point conjointement par l'UIT-T et par l'ISO/CEI; elle est publiée comme texte commun formant la Rec. UIT-T X.402 | ISO/CEI 10021-2.

**NORME INTERNATIONALE  
RECOMMANDATION UIT-T**

**Technologies de l'information – Systèmes de messagerie:  
architecture globale**

**SECTION 1 – INTRODUCTION**

**1 Domaine d'application**

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

D'autres aspects de la messagerie sont spécifiés dans d'autres Recommandations UIT-T | parties de l'ISO/CEI 10021. Un aperçu non technique de la messagerie est donné dans la Rec. UIT-T X.400 | ISO/CEI 10021-1. Les essais de conformité des composantes du système MHS sont décrits dans la Rec. UIT-T X.403. Les règles détaillées suivant lesquelles le système MTS convertit le contenu de messages d'un type d'information codée (EIT) en un autre sont définies dans la Rec. UIT-T X.408. Le service abstrait assuré par le système MTS et les procédures qui en régissent le fonctionnement décentralisé sont définis dans la Rec. UIT-T X.411 | ISO/CEI 10021-4. Le service abstrait assuré par la mémoire MS est défini dans la Rec. UIT-T X.413 | ISO/CEI 10021-5. Les protocoles d'application qui régissent les interactions des composantes du système MHS sont spécifiés dans la Rec. UIT-T X.419 | ISO/CEI 10021-6. Le système de messagerie de personne à personne qui est une application de la messagerie, est défini dans la Rec. UIT-T X.420 | ISO/CEI 10021-7. L'accès télématique au système de messagerie de personne à personne est spécifié dans la Recommandation T.330. Le service de messagerie avec échange informatisé de données (EDI) est décrit par la Rec. CCITT F.435 | ISO/CEI 10021-8; le système de messagerie avec échange informatisé de données, qui est une des applications de messagerie, est défini par la Rec. CCITT X.435 | ISO/CEI 10021-9. Le moyen par lequel les messages peuvent être acheminés à travers le système de messagerie est spécifié par l'ISO/CEI 10021-10. L'information de gestion relative aux composantes du système de messagerie est définie par les Recommandations de la série X.460 | ISO/CEI 11588.

Le Tableau 1 récapitule les Recommandations UIT-T et Normes internationales ISO/CEI relatives à la messagerie.

**Tableau 1 – Spécifications concernant les systèmes de messagerie**

ISO/CEI	UIT-T	SUJETS
+-- Introduction		
10021-1	X.400	Services de messagerie et aperçu général du système
10021-2	X.402	Architecture globale
+-- Aspects divers		
-	X.408	Règles de conversion entre différents types d'informations codées
+-- Services abstraits		
10021-4	X.411	Définition et procédures du service
10021-5	X.413	abstrait MTS
+-- Protocoles		
10021-6	X.419	Spécifications des protocoles
+-- Système de messagerie de personne à personne		
10021-7	X.420	Système de messagerie de personne à personne
-	T.330	Accès télématique aux systèmes IPMS
+-- Système de messagerie avec échange informatisé de données		
10021-8	F.435	Service de messagerie avec échange informatisé de données
10021-9	X.435	Système de messagerie avec échange informatisé de données
+-- Routage		
10021-10	X.412	Routage MHS
10021-11	X.404	Routage MHS: Guide pour les gestionnaires
+-- Gestion des systèmes de messagerie		
11588-1	X.460	Gestion: modèle et architecture
11588-3	X.462	Informations de journalisation
11588-8	X.467	Gestion des agents de transfert de messages

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

**Tableau 2 – Spécifications concernant les annuaires**

ISO/CEI	UIT-T	SUJETS
9594-1	X.500	Aperçu général
9594-2	X.501	Modèles
9594-3	X.511	Définition du service abstrait
9594-4	X.518	Procédures régissant le fonctionnement réparti
9594-5	X.519	Spécifications du protocole
9594-6	X.520	Types d'attributs sélectionnés
9594-7	X.521	Classes d'objets sélectionnées
9594-8	X.509	Cadre d'authentification
9594-9	X.525	Duplication
9594-10	X.530	Gestion-systèmes pour l'administration

Les bases architecturales de la messagerie font l'objet d'autres Recommandations | Normes internationales. Le modèle de référence OSI est défini dans la Rec. UIT-T X.200 | ISO/CEI 7498. La notation permettant de spécifier les structures de données des services abstraits et des protocoles d'application, ASN.1, ainsi que les règles de codage correspondantes, sont définies dans les Rec. UIT-T X.680 | ISO/CEI 8824-1, Rec. UIT-T X.681 | ISO/CEI 8824-2, Rec. UIT-T X.682 | ISO/CEI 8824-3, Rec. UIT-T X.683 | ISO/CEI 8824-4 et Rec. UIT-T X.690 | ISO/CEI 8825-1. Le moyen qui permet d'établir et de libérer des associations, l'élément de service de contrôle d'association ACSE, est défini dans la Rec. UIT-T X.217 | ISO/CEI 8649 et dans la Rec. UIT-T X.227 | ISO/CEI 8650-1. Le moyen qui permet d'acheminer de manière fiable les unités APDU pendant les associations, l'élément de service de transfert fiable RTSE, est défini dans la Rec. UIT-T X.218 et ISO/CEI 9066-1 et dans la Rec. X.228 du CCITT | ISO/CEI 9066-2. Le moyen qui permet d'adresser des demandes d'autres systèmes ouverts, l'élément de service d'opérations distantes ROSE, est défini dans la Rec. UIT-T X.880 | ISO/CEI 13712-1, dans la Rec. UIT-T X.881 | ISO/CEI 13712-2 et dans la Rec. UIT-T X.882 | ISO/CEI 13712-3.

Le Tableau 3 présente un état récapitulatif des Recommandations UIT-T et des Normes internationales ISO/CEI sur lesquelles repose la messagerie.

**Tableau 3 – Spécifications concernant les bases du MHS**

ISO/CEI	UIT-T	SUJETS
+- Modèle -----		
7498-1	X.200	Modèle de référence OSI
+- ASN.1 -----		
8824-1	X.680	Notation de syntaxe abstraite numéro un
8824-2	X.681	Objets d'information ASN.1
8824-3	X.682	Spécification des contraintes ASN.1
8824-4	X.683	Paramétrage ASN.1
8825-1	X.690	Règles de codage de base
+- Contrôle d'association -----		
8649	X.217	Définition des services
8650	X.227	Spécification du protocole
+- Transfert fiable -----		
9066-1	X.218	Définition des services
9066-2	X.228	Spécification du protocole
+- Opérations distantes -----		
13712-1	X.880	Concepts, modèle et notation
13712-2	X.881	Définition du service
13712-3	X.882	Spécification du protocole

La présente Recommandation | Norme internationale est structurée comme suit. La section 1 est un aperçu général. La section 2 présente des modèles abstraits de messagerie. La section 3 spécifie comment on peut configurer les systèmes MHS pour répondre à l'une quelconque des spécifications fonctionnelles, physiques et organisationnelles. La section 4 décrit la dénomination et l'adressage des utilisateurs et des listes de distribution et le routage des objets d'information jusqu'à eux. La section 5 décrit les utilisations possibles de l'annuaire par le système MHS. La section 6 décrit comment

le système MHS est réalisé à l'aide de l'OSI. Les conventions utilisées dans la définition des services abstraits sont définies à la section 7. Les annexes donnent d'importants renseignements complémentaires.

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

## 2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

### 2.1 Interconnexion des systèmes ouverts

La présente Spécification et d'autres de cette série citent les spécifications OSI suivantes.

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base: Le modèle de référence de base.*
- Recommandation CCITT X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'application du CCITT.*  
ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: architecture de sécurité.*
- Recommandation UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Définition du service de présentation.*
- Recommandation UIT-T X.217 (1995) | ISO/CEI 8649:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition de service applicable à l'élément de service de contrôle d'association.*
- Recommandation UIT-T X.218 (1993), *Transfert fiable: modèle et définition du service.*  
ISO/CEI 9066-1:1989, *Systèmes de traitement de l'information – Communication de texte – Transfert fiable – Partie 1: modèle et définition du service.*
- Recommandation UIT-T X.227 (1995) | ISO/CEI 8650-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: spécification du protocole.*
- Recommandation CCITT X.228 (1988), *Transfert fiable: spécification du protocole.*  
ISO/CEI 9066-2:1989, *Systèmes de traitement de l'information – Communication de texte – Transfert fiable – Partie 2: spécification du protocole.*
- Recommandation UIT-T X.666 (1997) | ISO/CEI 9834-7:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – Procédures d'exploitation pour les organismes d'enregistrement de l'OSI: attribution de noms internationaux pour emploi dans des contextes spécifiques.*
- Recommandation UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*
- Recommandation UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*
- Recommandation UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*
- Recommandation UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*
- Recommandation UIT-T X.690 (1997) | ISO/CEI 8825-1:1998, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*
- Recommandation UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Technologies de l'information – Opérations distantes: concepts, modèle et notation.*

## ISO/CEI 10021-2:2003 (F)

- Recommandation UIT-T X.881 (1994) | ISO/CEI 13712-2:1995, *Technologies de l'information – Opérations distantes: réalisations OSI – Définition du service de l'élément de service d'opérations distantes.*
- Recommandation UIT-T X.882 (1994) | ISO/CEI 13712-3:1995, *Technologies de l'information – Opérations distantes: réalisations OSI – Spécification du protocole de l'élément de service d'opérations distantes.*

### 2.2 Systèmes d'annuaire

La présente Spécification et d'autres de cette série citent les spécifications de système d'annuaire suivantes.

- Recommandation UIT-T X.500 (1997) | ISO/CEI 9594-1:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services.*
- Recommandation UIT-T X.501 (1997) | ISO/CEI 9594-2:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.*
- Recommandation UIT-T X.509 (1997) | ISO/CEI 9594-8:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification.*
- Recommandation UIT-T X.511 (1997) | ISO/CEI 9594-3:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition du service abstrait.*
- Recommandation UIT-T X.518 (1997) | ISO/CEI 9594-4:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti.*
- Recommandation UIT-T X.519 (1997) | ISO/CEI 9594-5:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification du protocole.*
- Recommandation UIT-T X.520 (1997) | ISO/CEI 9594-6:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés.*
- Recommandation UIT-T X.521 (1997) | ISO/CEI 9594-7:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées.*
- Recommandation UIT-T X.525 (1997) | ISO/CEI 9594-9:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication.*
- Recommandation UIT-T X.530 (1997) | ISO/CEI 9594-10:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: utilisation de la gestion-systèmes pour l'administration de l'annuaire.*

### 2.3 Systèmes de messagerie

La présente Spécification et d'autres de cette série citent les spécifications de système de messagerie suivantes.

- Recommandation CCITT T.330 (1988), *Accès télématique aux systèmes de messagerie de personne à personne.*
- Recommandation UIT-T F.400/X.400 (1999), *Services de messagerie: aperçu général du système et du service de messagerie.*  
ISO/CEI 10021-1:2003, *Technologies de l'information – Systèmes de messagerie (MHS) – Partie 1: Présentation générale du système et des services.*
- Recommandation CCITT X.408 (1988), *Systèmes de messagerie: règles de conversion entre différents types d'informations codées.*
- Recommandation UIT-T X.411 (1999) | ISO/CEI 10021-4:2003, *Technologies de l'information – Systèmes de messagerie: système de transfert de messages: définition et procédures du service abstrait.*
- Recommandation UIT-T X.413 (1999) | ISO/CEI 10021-5:1999, *Technologies de l'information – Systèmes de messagerie: mémoire de messages – Définition du service abstrait.*
- Recommandation UIT-T X.419 (1999) | ISO/CEI 10021-6:2003, *Technologies de l'information – Systèmes de messagerie: spécification des protocoles.*
- Recommandation UIT-T X.420 (1999) | ISO/CEI 10021-7:2003, *Technologies de l'information – Systèmes de messagerie: système de messagerie de personne à personne.*
- Recommandation UIT-T F.435 (1999), *Services de messagerie: service de messagerie avec échange informatisé de données.*  
ISO/CEI 10021-8:1999, *Technologies de l'information – Systèmes de messagerie (MHS) – Partie 8: Service de messagerie par échange informatisé de données.*

- Recommandation UIT-T X.435 (1999) | ISO/CEI 10021-9:1999, *Technologies de l'information – Systèmes de messagerie: système de messagerie par échange informatisé de données.*
- Recommandation UIT-T X.412 (1999) | ISO/CEI 10021-10:1999, *Technologies de l'information – Systèmes de messagerie: routage.*
- Recommandation UIT-T X.404 (1999) | ISO/CEI TR 10021-11:1999, *Technologies de l'information – Systèmes de messagerie: routage – Guide pour les gestionnaires des systèmes de messagerie.*
- Recommandation UIT-T X.460 (1995) | ISO/CEI 11588-1:1996, *Technologies de l'information – Gestion des systèmes de messagerie: modèle et architecture.*
- Recommandation UIT-T X.462 (1996) | ISO/CEI 11588-3:1997, *Technologies de l'information – Gestion des systèmes de messagerie: informations de journalisation.*
- Recommandation UIT-T X.467 (1996) | ISO/CEI 11588-8:1997, *Technologies de l'information – Gestion des systèmes de messagerie: gestion des agents de transfert de messages.*

## 2.4 Codes de pays

La présente Spécification cite les spécifications suivantes, relatives aux codes de pays:

- ISO 3166-1:1997, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1 Codes pays.*
- Recommandation UIT-T X.121 (1996), *Plan de numérotage international pour les réseaux publics pour données.*

## 2.5 Adresses dans le réseau

La présente Spécification cite la spécification suivante relative aux adresses du réseau:

- Recommandation CCITT E.164 (1991), *Plan de numérotage pour l'ère du RNIS.*

## 2.6 Code de langue

La présente Spécification cite la spécification suivante relative au code de langue:

- ISO 639-2:1998, *Codes pour la représentation des noms de langue.*

## 2.7 Jeux de caractères

La présente Spécification cite la spécification suivante relative aux jeux de caractères:

- ISO 10646-1:1993, *Technologies de l'information – Jeu universel de caractères codés à plusieurs octets – Partie 1: Architecture et table multilingue.*

## 3 Définitions

Pour les besoins de la présente Spécification et d'autres de cette série, les définitions suivantes s'appliquent.

### 3.1 Interconnexion des systèmes ouverts

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1, ainsi que les noms des sept couches du modèle de référence:

- a) syntaxe abstraite;
- b) entité d'application (AE, *application entity*);
- c) processus d'application;
- d) unité de données protocolaire d'application (APDU, *application protocol data unit*);
- e) élément de service d'application (ASE, *application service element*);
- f) tâche de traitement réparti de l'information;
- g) couche;
- h) système ouvert;
- i) interconnexion des systèmes ouverts (OSI, *open systems interconnection*);

## ISO/CEI 10021-2:2003 (F)

- j) homologue;
- k) contexte de présentation;
- l) protocole;
- m) modèle de référence;
- n) syntaxe de transfert;
- o) élément utilisateur (UE, *user element*).

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans les Rec. UIT-T X.680 | ISO/CEI 8824-1, Rec. ITU-T X.681 | ISO/CEI 8824-2, Rec. ITU-T X.682 | ISO/CEI 8824-3 et Rec. UIT-T X.683 | ISO/CEI 8824-4, ainsi que les noms des types de données et des valeurs de l'ASN.1:

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

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans la Rec. UIT-T X.217 | ISO/CEI 8649:

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

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans la Rec. UIT-T X.218 | ISO/CEI 9066-1:

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

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans la Rec. UIT-T X.880 | ISO/CEI 13712-1:

- a) argument;
- b) asynchrone;
- c) rattachement;
- d) paramètre;
- e) erreur distante;
- f) opération distante;
- g) opérations distantes (RO, *remote operations*);
- h) élément du service d'opérations distantes (ROSE, *remote operations service element*);
- i) résultat;
- j) synchrone;
- k) détachement.

### 3.2 Systèmes d'annuaire

La présente Spécification et d'autres de cette série utilisent les termes ci-dessous qui sont définis dans les Recommandations de la série X.500 | ISO/CEI 9594:

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

### 3.3 Systèmes de messagerie

Pour les besoins de la présente Spécification, les définitions répertoriées dans l'Annexe K s'appliquent.

## 4 Abréviations

Pour les besoins de la présente Spécification, les abréviations répertoriées dans l'Annexe K s'appliquent.

## 5 Conventions

La présente Spécification utilise les conventions descriptives identifiées ci-dessous.

### 5.1 ASN.1

La présente Spécification utilise plusieurs conventions descriptives fondées sur la notation ASN.1 dans ses Annexes A et C, pour définir les informations spécifiques à la messagerie que l'annuaire peut contenir. La notation ASN.1 est définie dans les Rec. UIT-T X.680 | ISO/CEI 8824-1, Rec. UIT-T X.681 | ISO/CEI 8824-2, Rec. UIT-T X.682 | ISO/CEI 8824-3 et Rec. UIT-T X.683 | ISO/CEI 8824-4. Elle utilise notamment les classes d'objets d'information OBJECT-CLASS et ATTRIBUTE de la Rec. UIT-T X.501 | ISO/CEI 9594-2 pour définir les classes d'objets et les attributs propres à la messagerie.

La notation 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.

Les étiquettes de la notation ASN.1 sont implicites dans le module de la notation ASN.1 qui est défini dans l'Annexe C; ce module est définitif à cet égard.

Bien que la syntaxe abstraite de cette définition du service contienne des marqueurs d'extension, il n'a pas été établi avec certitude que ceux-ci sont présents dans toutes les instances requises pour permettre l'utilisation en toute sécurité des règles de codage condensé.

## 5.2 Catégorie

Chaque fois que la présente Spécification décrit une classe de structure de données (entités OR-address, par exemple) ayant des composantes (attributs, par exemple), chaque composante est classée dans l'une des catégories suivantes:

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

## 5.3 Termes

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

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

# SECTION 2 – MODÈLES ABSTRAITS

## 6 Aperçu général

La présente section présente des modèles abstraits de *messagerie* qui fournissent la base architecturale pour les spécifications plus détaillées qui figurent dans d'autres spécifications du système MHS.

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

- a) transfert de messages: acheminement (différé) d'objets d'information entre des parties qui utilisent des ordinateurs comme intermédiaires;
- b) enregistrement de messages: enregistrement automatique d'objets d'information acheminés par le transfert de message, en vue de leur extraction ultérieure.

La présente section porte sur les sujets suivants:

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

NOTE – La messagerie a diverses applications; l'une d'entre elles, la messagerie de personne à personne, est décrite dans la Rec. UIT-T X.420 | ISO/CEI 10021-7.

## 7 Modèle fonctionnel

Un modèle fonctionnel de messagerie est présenté dans le présent paragraphe. La réalisation concrète de ce modèle fait l'objet d'autres Spécifications concernant le système MHS.

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

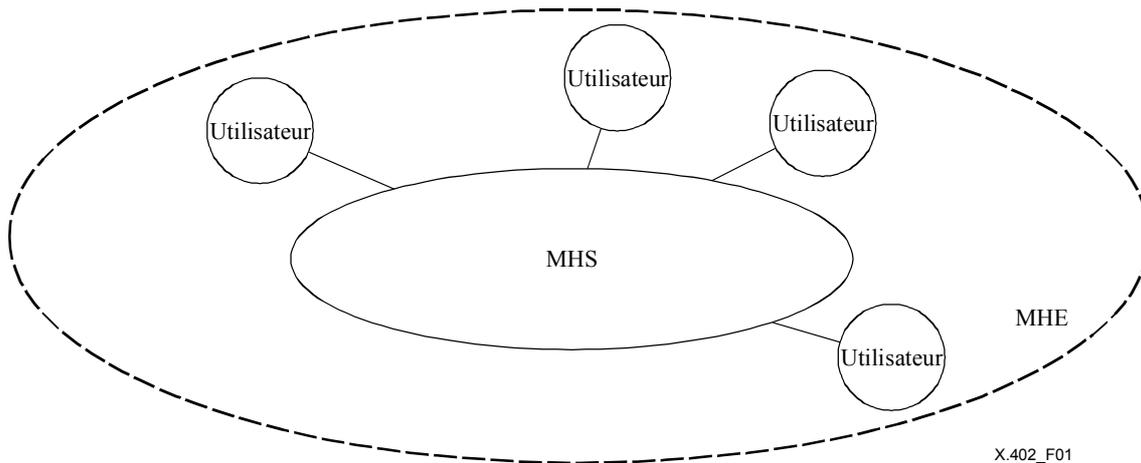
Comme précisé ci-après, les objets fonctionnels sont parfois spécialement adaptés à une ou plusieurs applications de messagerie, par exemple la messagerie de personne à personne (voir la Rec. UIT-T X.420 | ISO/CEI 10021-7 et la Rec. CCITT T.330). Un objet fonctionnel qui a été spécialement adapté à une 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 Spécification ou dans d'autres spécifications concernant le système MHS. En particulier, un *agent d'utilisateur* type assure des fonctions non normalisées de préparation, de présentation et d'enregistrement des messages.

## 7.1 Objets fonctionnels primaires

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

La situation est représentée à la Figure 1.



X.402\_F01

Figure 1 – L'environnement du système de messagerie

### 7.1.1 Système de messagerie

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

L'environnement MHE comprend un seul système MHS.

### 7.1.2 Utilisateurs

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

On distingue les sortes d'utilisateurs suivantes:

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

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

### 7.1.3 Listes de distribution

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

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

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

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

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

## 7.2 Objets fonctionnels secondaires

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

La situation est représentée à la Figure 2.

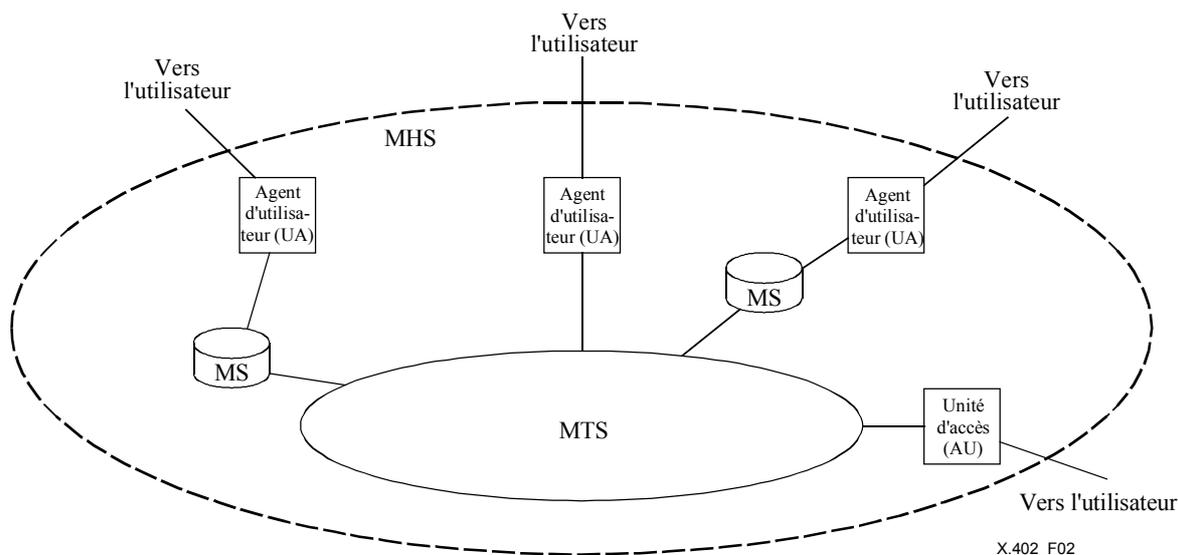


Figure 2 – Système de messagerie

### 7.2.1 Système de transfert de messages

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

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

Le système MHS comprend un seul système MTS.

### 7.2.2 Agents d'utilisateurs

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

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

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

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

### 7.2.3 Mémoires de message

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

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

Le système MHS comporte un nombre quelconque de mémoires MS.

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

#### 7.2.4 Unités d'accès

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

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

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

### 7.3 Objets fonctionnels tertiaires

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

La situation est représentée à la Figure 3.

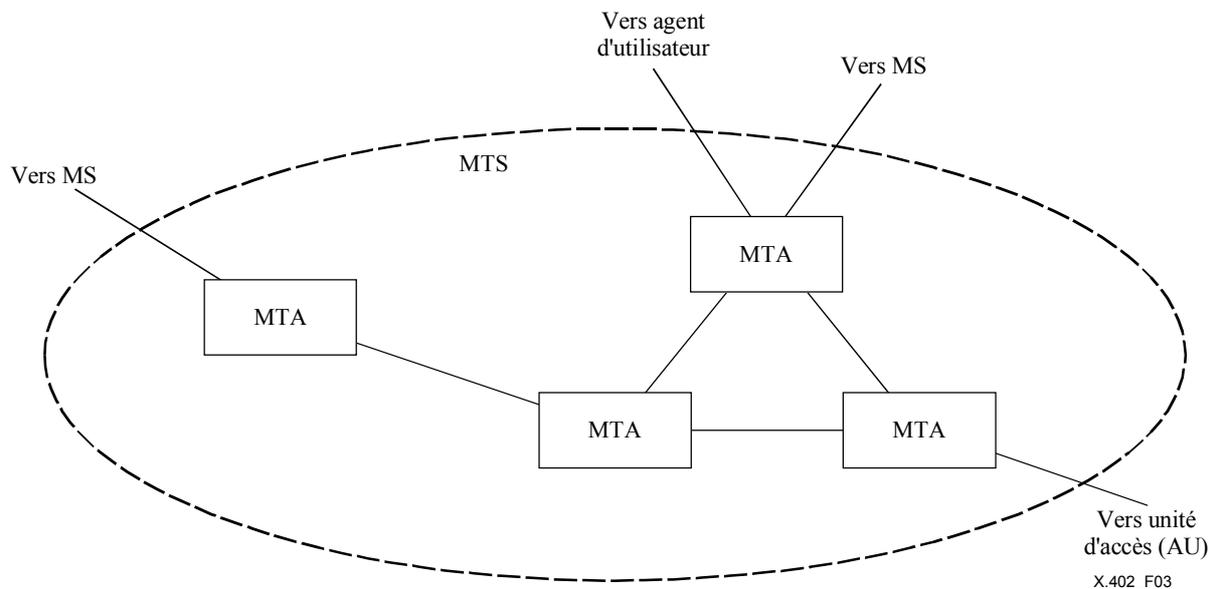


Figure 3 – Système de transfert de messages

#### 7.3.1 Agents de transfert de messages

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

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

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

#### 7.4 Types d'unités AU choisies

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

### 7.4.1 Remise physique

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

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

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

Parmi les applications de messagerie qu'assure chaque unité PDAU, signalons la messagerie de personne à personne (voir la Rec. UIT-T X.420 | ISO/CEI 10021-7).

### 7.4.2 Télématique

Les unités d'accès télématique, qui assurent exclusivement la messagerie de personne à personne, sont présentées dans la Rec. UIT-T X.420 | ISO/CEI 10021-7.

### 7.4.3 Téléx

Les unités d'accès téléx, qui assurent exclusivement la messagerie de personne à personne, sont présentées dans la Rec. UIT-T X.420 | ISO/CEI 10021-7.

## 8 Modèle informationnel

Le présent article décrit un modèle informationnel de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres spécifications du service MHS.

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

**Tableau 4 – Objets informationnels acheminables**

Objet informa- tionnel	Objet fonctionnel				
	utilisateur	UA	MS	MTA	AU
Message	SD	-	-	-	-
Envoi-test	S	-	-	D	-
Rapport	D	-	-	S	-

+ - Légende -----+

S	origine première
D	destination finale

-----+

Les objets informationnels résumés dans le tableau sont définis et décrits un par un dans les paragraphes qui suivent.

### 8.1 Messages

L'objectif principal du transfert de message est de transmettre des objets informationnels appelés messages d'un utilisateur à d'autres utilisateurs. Comme indiqué à la Figure 4, un message comporte les parties suivantes:

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

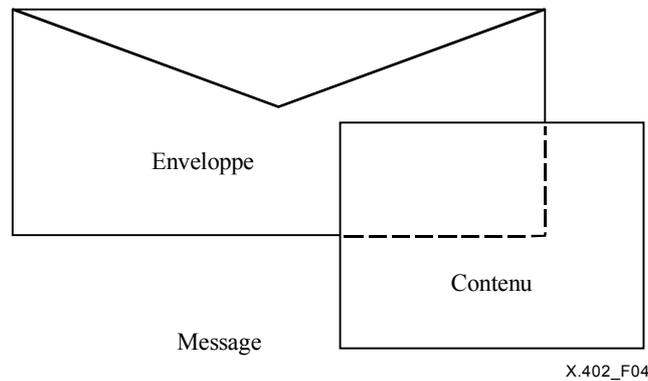


Figure 4 – Enveloppe et contenu d'un message

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

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

## 8.2 Envois-tests

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

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

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

Le *dépôt* d'un envoi-test entraîne essentiellement le même comportement du système MTS que le *dépôt* d'un message décrit, sauf que, dans ce cas, on renonce *au développement de la liste DL* et à la *remise*. En particulier, et si on excepte les conséquences de la suppression du *développement de la liste DL*, l'envoi-test donne lieu aux mêmes *rapports* que n'importe quel message décrit. C'est ce qui confère aux envois-tests 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 système MTS, un rapport rend compte des résultats ou du déroulement de la *transmission* d'un message ou d'un envoi-test à un ou plusieurs *destinataires potentiels*.

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

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

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

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

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

## 9 Modèle opérationnel

Le présent paragraphe décrit un modèle opérationnel de messagerie. La réalisation concrète de ce modèle fait l'objet d'autres spécifications du service MHS.

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

### 9.1 Transmission

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

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

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

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

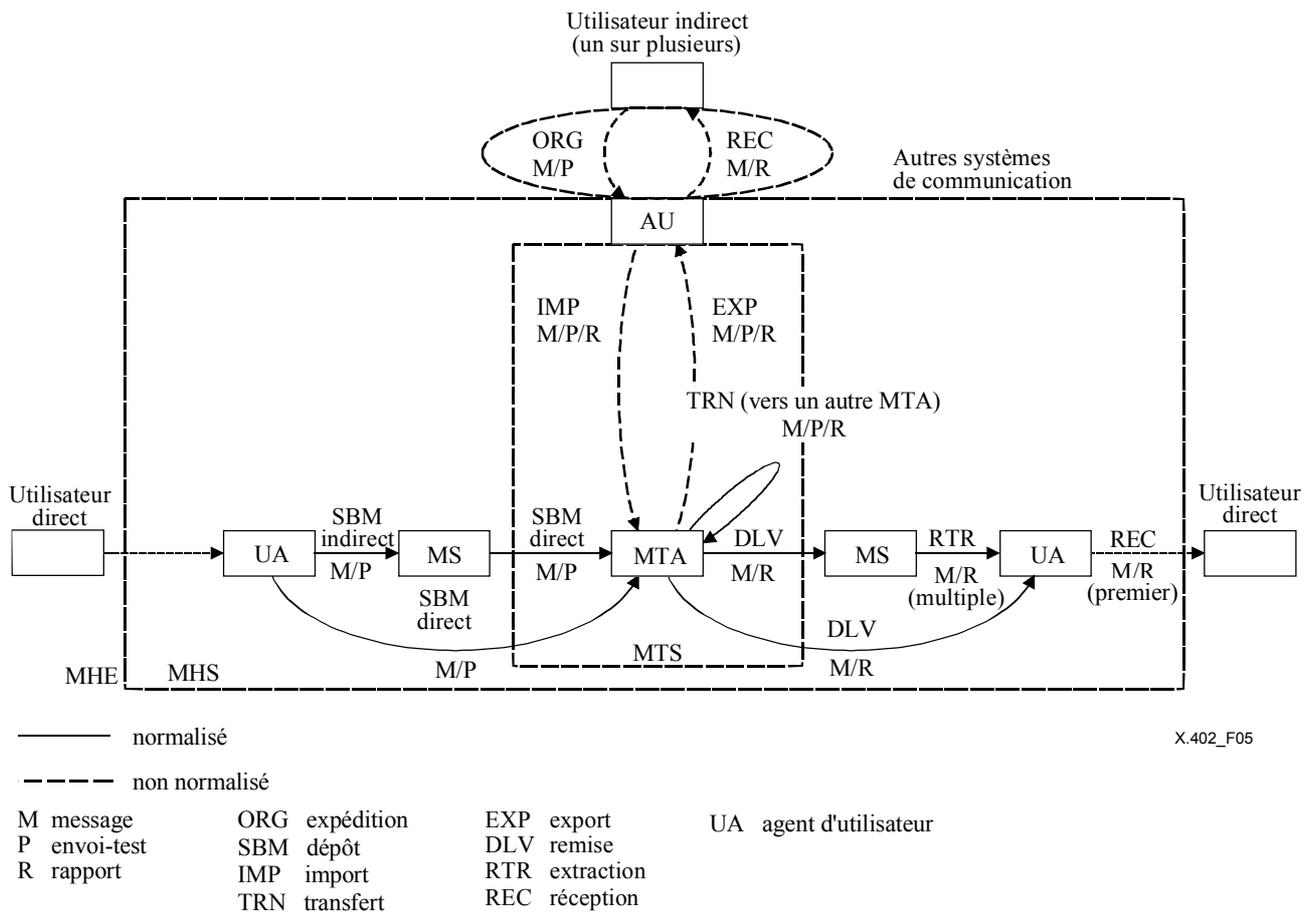


Figure 5 – Cheminement de l'information pendant la transmission

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

## 9.2 Rôles de transmission

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

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

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

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

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

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

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

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

### 9.3 Etapes de la transmission

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

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

**Tableau 5 – Etapes de transmission**

Etape de transmission	Norma- lisée?	Objets informationnels			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	-	-	-

+- Légende		
M message	S source	x permis
P envoi-test	D destination	
R rapport		

Les différentes étapes de transmission, résumées dans le tableau, sont définies et décrites une par une dans les paragraphes qui suivent.

#### 9.3.1 Expédition

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

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

### 9.3.2 Dépôt

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

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

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

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

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

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

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

### 9.3.3 Import

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

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

### 9.3.4 Transfert

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

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

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

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

### 9.3.5 Export

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

Au cours de cette étape, l'agent MTA peut produire un rapport de remise. Selon les conditions à remplir pour le type d'unité d'accès précisées dans les spécifications de messagerie qui s'appliquent, un rapport de remise positif indique que l'unité d'accès a accepté le message (ou l'envoi-test) ou qu'elle a poursuivi avec succès l'acheminement du message (ou de l'envoi-test).

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

### 9.3.6 Remise

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

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

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

**9.3.7 Extraction**

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

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

**9.3.8 Réception**

Dans une étape de réception, un agent UA transmet un message ou un rapport à son utilisateur direct, ou le système de communication qui dessert un utilisateur indirect transmet un tel objet informationnel à cet utilisateur. Dans l'un et l'autre cas, cette étape achemine l'objet jusqu'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 informationnel par le système de communication qui dessert l'utilisateur. Dans l'un et l'autre cas, l'utilisateur est un destinataire potentiel (et, dans le cas d'un utilisateur direct, un destinataire effectif) du message en question, ou l'expéditeur du message ou de l'envoi-test sujet.

**9.4 Evénements de transmission**

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

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

**Tableau 6 – Evénements de transmission**

Evénement de transmission	Objets Informationnels			Objets Fonctionnels				
	M	P	R	Utilisateur	UA	MS	MTA	AU
fractionnement	x	x	-	-	-	-	x	-
groupage	x	x	x	-	-	-	x	-
résolution de nom	x	x	-	-	-	-	x	-
développement de liste DL	x	-	-	-	-	-	x	-
réacheminement	x	x	-	-	-	-	x	-
conversion	x	x	-	-	-	-	x	-
non-remise	x	-	x	-	-	-	x	-
non-affirmation	-	x	-	-	-	-	x	-
affirmation	-	x	-	-	-	-	x	-
acheminement	x	x	x	-	-	-	x	-

+- Légende -----+  
 | M message           x permis |  
 | P envoi-test        |  
 | R rapport            |  
 +-----+

Les différents événements de transmission résumés dans le Tableau 6 sont définis et décrits un par un dans les paragraphes qui suivent.

**9.4.1 Fractionnement**

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

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

#### 9.4.2 Groupage

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

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

#### 9.4.3 Résolution du nom

Dans un événement de résolution du nom, un agent MTA ajoute l'entité *OR-address* correspondant à l'entité *OR-name* qui identifie un des destinataires immédiats d'un message ou d'un envoi-test.

#### 9.4.4 Développement de liste DL

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

Une liste DL particulière fait toujours l'objet d'un développement à un emplacement préétabli à l'intérieur du système MTS. Cet emplacement est appelé point de développement de la liste DL et est identifié par une entité *OR-address*.

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

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

#### 9.4.5 Réacheminement

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

#### 9.4.6 Conversion

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

Selon la façon dont on choisit le type EIT de l'information à convertir et celui qui résultera de la conversion, on distingue les types de conversion suivants:

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

#### 9.4.7 Non-remise

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

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

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

#### 9.4.8 Non-affirmation

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

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

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

#### **9.4.9 Affirmation**

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

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

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

#### **9.4.10 Acheminement**

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

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

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

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

## **10 Modèle de sécurité**

Le présent paragraphe décrit un modèle de sécurité abstrait pour le transfert de message. La réalisation concrète de ce modèle fait l'objet d'autres spécifications du système MHS. Le modèle de sécurité offre un cadre pour décrire les services de sécurité destinés à faire face aux éventuelles menaces (voir Annexe D) visant le système MTS et les éléments de sécurité qui sont à la base de ces services.

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

NOTE 1 – Malgré ces fonctions de sécurité, certaines perturbations peuvent atteindre une communication entre un utilisateur et le système MHS ou entre utilisateurs (par exemple dans le cas d'utilisateurs accédant au système MHS par une unité d'accès ou d'utilisateurs accédant à distance à leurs agents UA). Les solutions de ces problèmes impliquent une extension des présents modèles et services de sécurité, qui seront normalisés ultérieurement.

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

Les services de sécurité sont assurés grâce à l'utilisation d'éléments de service de l'enveloppe de message du service de transfert de messages. Cette enveloppe contient des arguments relatifs à la sécurité, comme indiqué dans la Rec. UIT-T X.411 | ISO/CEI 10021-4. La description des services de sécurité a la forme générale suivante. Les services énumérés au § 10.2 sont accompagnés, dans chaque cas, d'une définition du service et d'une indication de la manière dont celui-ci peut être assuré à l'aide des éléments de sécurité indiqués dans la Rec. UIT-T X.411 | ISO/CEI 10021-4. Les éléments de sécurité décrits un par un au § 10.3 sont accompagnés, dans chaque cas, d'une définition de l'élément de service et des références à ses arguments constitutifs figurant dans la Rec. UIT-T X.411 | ISO/CEI 10021-4.

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

NOTE 2 – Les termes "service de sécurité" et "élément de sécurité" utilisés dans le présent article ne doivent pas être confondus avec les termes "service" et "élément de service" au sens qui leur est donné dans la Rec. UIT-T X.400 | ISO/CEI 10021-1. Les premiers de ces termes sont utilisés dans le présent article dans un souci de conformité avec l'ISO 7498-2.

## 10.1 Politiques de sécurité

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

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

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

## 10.2 Services de sécurité

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

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

Tableau 7 – 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 DE L'ORIGINE -----							
Authentification de l'origine du message	*	*	-	*	-	-	-
Authentification de l'origine de l'envoi-test	-	-	*	*	-	-	-
Authentification de l'origine du rapport	-	-	-	*	*	*	-
Preuve du dépôt	-	-	-	-	-	*	-
Preuve de remise	*	-	-	-	-	-	Note
+ GESTION DE LA SÉCURITÉ DE L'ACCÈS -----							
Authentification de l'entité homologue	-	*	*	*	*	*	*
Contexte de sécurité	-	*	*	*	*	*	*
+ CONFIDENTIALITÉ DES DONNÉES -----							
Confidentialité de la connexion	-	*	*	*	*	*	*
Confidentialité du contenu	*	-	-	-	-	-	-
Confidentialité du cheminement du message	*	-	-	-	-	-	-
+ SERVICE D'INTÉGRITÉ DES DONNÉES -----							
Intégrité de la connexion	-	*	*	*	*	*	*
Intégrité du contenu	*	-	-	-	-	-	-
Intégrité de la séquence de message	*	-	-	-	-	-	-
+ NON-RÉPUDIATION -----							
Non-répudiation d'origine	*	-	-	*	-	-	-
Non-répudiation de dépôt	-	-	-	-	-	*	-
Non-répudiation de remise	*	-	-	-	-	-	Note
+ ÉTIQUETAGE DE SÉCURITÉ DU MESSAGE -----							
Étiquetage de sécurité du message	*	*	*	*	*	*	*
+ SERVICES DE GESTION DE LA SÉCURITÉ -----							
Modifications des pouvoirs	-	*	-	*	*	*	-
Enregistrement	-	*	-	*	-	-	-
Enregistrement de la mémoire MS	-	*	-	-	-	-	-

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

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

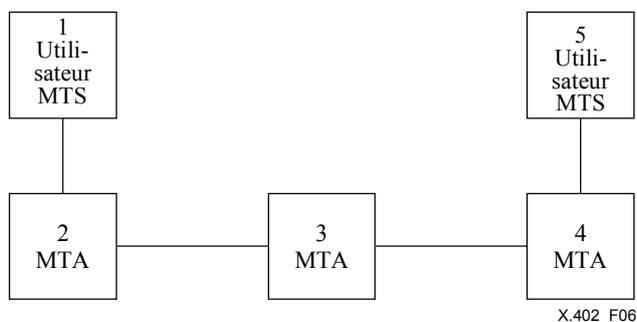


Figure 6 – Modèle fonctionnel du système MHS simplifié

**10.2.1 Services de sécurité Authentification de l'origine**

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

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

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

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

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

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

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

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

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

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

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

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

#### **10.2.1.2 Service de sécurité Preuve du dépôt**

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

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

#### **10.2.1.3 Service de sécurité Preuve de remise**

Ce service de sécurité permet à l'expéditeur d'un message d'obtenir confirmation que son message a été remis par le système MTS au ou aux destinataires prévus.

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

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

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

#### **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 connexion pour confirmer l'identité de l'entité qui établit la connexion. Il peut être utilisé sur les liaisons 1-2, 2-3, 3-4 ou 4-5 de la Figure 6 et garantit, au moment de l'utilisation uniquement, qu'une entité ne tente pas un piratage par usurpation d'identité ou par réexécution non autorisée des codes d'échange d'une connexion antérieure.

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

#### **10.2.2.2 Service de sécurité Contexte de sécurité**

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

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

### **10.2.3 Services de sécurité Confidentialité des données**

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

### 10.2.3.1 Service de sécurité Confidentialité de la connexion

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

### 10.2.3.2 Service de sécurité Confidentialité du contenu

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

Il peut être assuré par 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, le contenu du message étant inintelligible pour les agents MTA.

### 10.2.3.3 Service de sécurité Confidentialité du cheminement du message

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

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

## 10.2.4 Services de sécurité Intégrité des données

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

### 10.2.4.1 Service de sécurité Intégrité de la connexion

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

### 10.2.4.2 Service de sécurité Intégrité du contenu

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

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

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

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

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

Ce service de sécurité protège l'expéditeur et le destinataire d'une séquence de messages contre tout réarrangement de cette séquence et, ainsi, contre toute réexécution des messages.

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

Ces éléments de sécurité fournissent ce service aux communications entre les utilisateurs MTS 1 jusqu'à MTS 5 de la Figure 6, mais non avec les agents MTA intermédiaires.

### **10.2.5 Services de sécurité Non-répudiation**

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

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

Ce service de sécurité apporte au ou aux destinataires d'un message la preuve irréfutable de l'origine du message, du contenu de celui-ci et de l'Étiquette de sécurité associée.

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

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

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

#### **10.2.5.2 Service de sécurité Non-répudiation de dépôt**

Ce service de sécurité apporte à l'expéditeur du message la preuve irréfutable que ce message a été déposé dans le système MTS pour être remis au ou aux destinataires spécifiés au départ.

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

#### **10.2.5.3 Service de sécurité Non-répudiation de remise**

Ce service de sécurité apporte à l'expéditeur du message la preuve irréfutable que ce message a été remis au ou aux destinataires spécifiés au départ.

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

### **10.2.6 Service de sécurité Etiquetage de sécurité du message**

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

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

### **10.2.7 Services de gestion de la sécurité**

Le système MHS nécessite un certain nombre de services de gestion de la sécurité. Les seuls services de gestion prévus dans la Rec. UIT-T X.411 | ISO/CEI 10021-4 concernent la modification des pouvoirs et l'enregistrement des étiquettes de sécurité des utilisateurs du MTS.

#### **10.2.7.1 Service de sécurité Modification des pouvoirs**

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

#### **10.2.7.2 Service de sécurité Enregistrement**

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

#### **10.2.7.3 Service de sécurité Enregistrement de la mémoire MS**

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

### **10.3 Eléments de sécurité**

Les paragraphes qui suivent décrivent les éléments de sécurité disponibles dans les protocoles décrits dans la Rec. UIT-T X.411 | ISO/CEI 10021-4 pour prendre en charge les services de sécurité du système MHS. Ces éléments de sécurité se rapportent directement aux arguments de divers services décrits dans la Rec. UIT-T X.411 | ISO/CEI 10021-4. L'objectif du présent paragraphe est de séparer chaque élément des définitions de service de la Rec. UIT-T X.411 | ISO/CEI 10021-4 concernant la sécurité et de définir la fonction de chacun des éléments de sécurité ainsi identifiés.

#### **10.3.1 Eléments de sécurité Authentification**

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

##### **10.3.1.1 Élément de sécurité Echange d'authentification**

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

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.

Lorsque les mots de passe sont utilisés pour l'authentification, ceux-ci peuvent être de simples mots de passe ou des mots de passe protégés. L'utilisation des mots de passe protégés, entre l'agent UA et la mémoire MS, est décrite en détail dans l'Annexe H.

NOTE – Bien que l'Annexe H décrive l'authentification entre l'agent UA et la mémoire MS, cette authentification s'applique également, outre le mécanisme de protection pour changer le mot de passe, entre l'agent UA et l'agent MTA.

##### **10.3.1.2 Eléments de sécurité Authentification de l'origine des données**

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

###### **10.3.1.2.1 Élément de sécurité Authentification de l'origine du message**

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

Cet élément de sécurité suppose la transmission, dans le message, d'un Contrôle d'authentification de l'origine du message, calculé en fonction du contenu du message, de l'Identificateur du contenu du message et de l'Étiquette de

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

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

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

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

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

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

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

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

#### **10.3.1.3 Élément de sécurité Preuve de dépôt**

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

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

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

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

#### **10.3.1.4 Élément de sécurité Preuve de remise**

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

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

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

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

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

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

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

### **10.3.2.1 Élément de sécurité Contexte de sécurité**

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

Le Contexte de sécurité lui-même se compose d'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 de rattachement au système MTS et de rattachement à l'agent MTA.

### **10.3.2.2 Élément de sécurité Enregistrement**

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

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

### **10.3.2.3 Élément de sécurité Enregistrement de la mémoire MS**

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

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

## **10.3.3 Éléments de sécurité Confidentialité des données**

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

### **10.3.3.1 Élément de sécurité Confidentialité du contenu**

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

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

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

### **10.3.3.2 Élément de sécurité Confidentialité de l'argument du message**

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

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

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

## **10.3.4 Éléments 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 Élément de sécurité Intégrité de contenu**

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

Cet élément de sécurité fonctionne à l'aide d'un ou de plusieurs algorithmes cryptographiques. La spécification de cet ou de ces algorithmes, le ou les codes utilisés et toutes les autres données d'initialisation sont acheminés à l'aide des éléments de sécurité Confidentialité de l'argument du message et Intégrité de l'argument du message. Le résultat de l'application des algorithmes et du code est le Contrôle de l'intégrité du contenu, qui est envoyé dans l'enveloppe du message. Cet élément de sécurité n'est accessible qu'au ou aux destinataires du message du fait qu'il agit sur le texte en clair du contenu de message.

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

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

#### **10.3.4.2 Élément de sécurité Intégrité de l'argument du message**

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

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

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

#### **10.3.4.3 Élément de sécurité Intégrité de la séquence du message**

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

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

### **10.3.5 Éléments de sécurité Non-répudiation**

Aucun élément de sécurité Non-répudiation spécifique n'est défini dans la Rec. UIT-T X.411 | ISO/CEI 10021-4. Les services de Non-répudiation peuvent être assurés à l'aide d'une combinaison d'autres éléments de sécurité.

### **10.3.6 Éléments de sécurité Etiquette de sécurité**

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

#### **10.3.6.1 Élément de sécurité Etiquette de sécurité du message**

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

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

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

### **10.3.7 Éléments de sécurité Gestion de la sécurité**

#### **10.3.7.1 Élément de sécurité Modification des pouvoirs**

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

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

### 10.3.8 Technique de double enveloppe

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

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

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

### 10.3.9 Chiffrement et adressage calculé

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

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

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

## SECTION 3 – CONFIGURATIONS

### 11 Aperçu général

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

Elle traite des sujets suivants:

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

### 12 Configurations fonctionnelles

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

#### 12.1 Annuaire

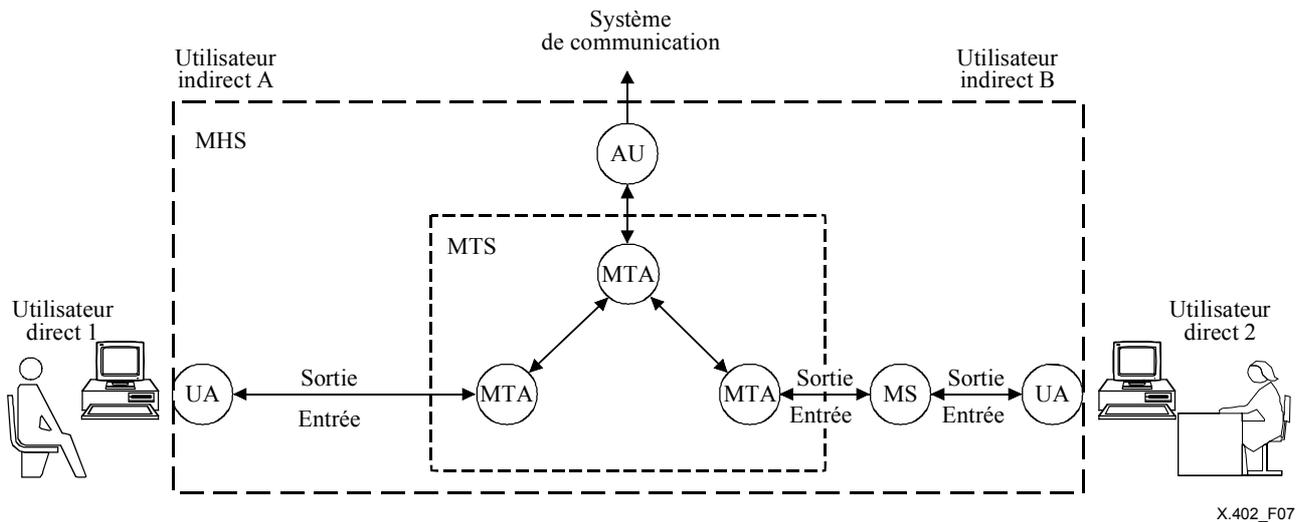
En ce qui concerne l'annuaire, le système MHS peut être configuré pour un utilisateur particulier ou pour un groupe d'utilisateurs (voir par exemple § 14.1) avec ou sans l'annuaire. Un utilisateur qui n'a pas accès à l'annuaire peut ne pas disposer des fonctions décrites dans la section 5.

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

#### 12.2 Mémoire de messages

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

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



NOTE – 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 – Configurations fonctionnelles concernant la mémoire MS

### 13 Configurations physiques

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

#### 13.1 Systèmes de messagerie

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

Les différents types de systèmes de messagerie sont décrits à la Figure 8.

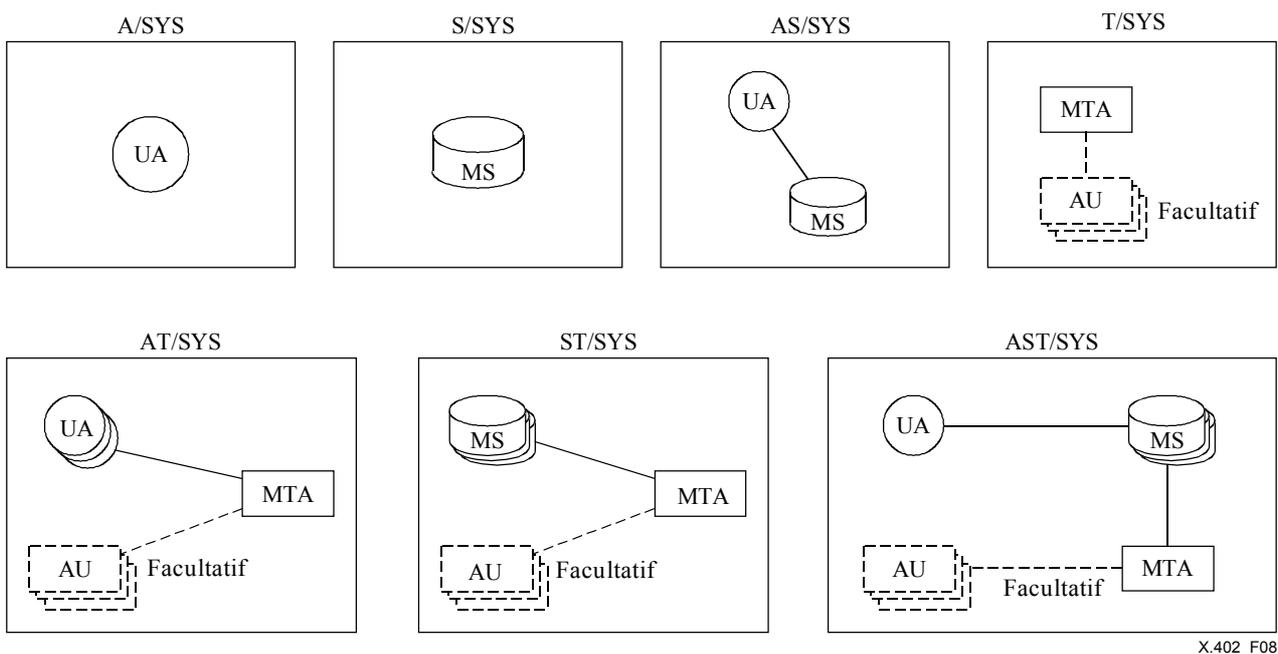


Figure 8 – Types de systèmes de messagerie

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

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

**Tableau 8 – Systèmes de messagerie**

Système de messagerie	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]

+- Légende -----+  
 | M Multiple [...] Facultatif |  
 +-----+

Les types de systèmes de messagerie résumés dans le Tableau 8 sont définis et décrits individuellement ci-dessous.

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

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

### 13.1.1 Systèmes d'accès

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

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

### 13.1.2 Systèmes de mémorisation

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

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

### 13.1.3 Systèmes d'accès et de mémorisation

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

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

### 13.1.4 Systèmes de transfert

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

Un système T/SYS peut desservir plusieurs utilisateurs.

### 13.1.5 Systèmes d'accès et de transfert

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

Un système AT/SYS peut desservir plusieurs utilisateurs.

### 13.1.6 Systèmes de mémorisation et de transfert

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

Un système ST/SYS peut desservir plusieurs utilisateurs.

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

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

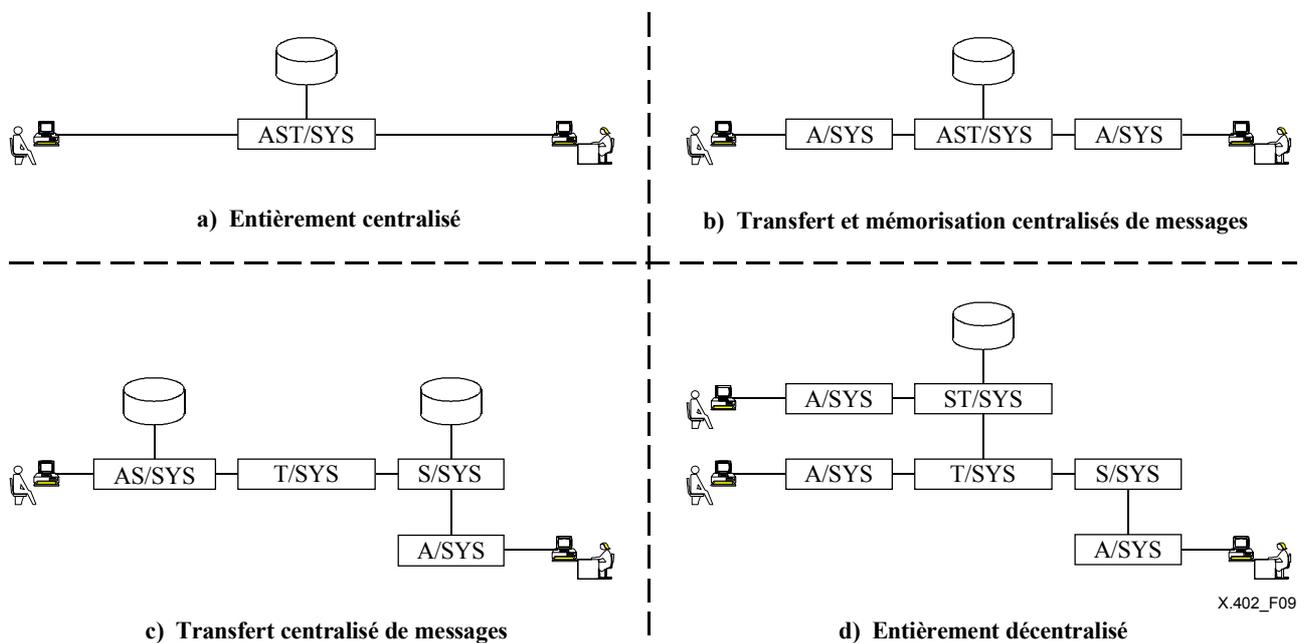
Un système AST/SYS peut desservir plusieurs utilisateurs.

## 13.2 Configurations représentatives

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

### 13.2.1 Système MHS entièrement centralisé

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



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

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

Figure 9 – Configurations physiques représentatives

### 13.2.2 Transfert et mémorisation centralisés de messages

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

### 13.2.3 Transfert centralisé de messages

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

### 13.2.4 Système MHS entièrement décentralisé

Le MHS peut décentraliser le transfert de messages (partie *d* de la Figure 9). Cette conception fait intervenir plusieurs systèmes ST/SYS ou T/SYS.

## 14 Configurations organisationnelles

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

### 14.1 Domaines de gestion

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

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

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

#### 14.1.1 Domaines de gestion d'administration

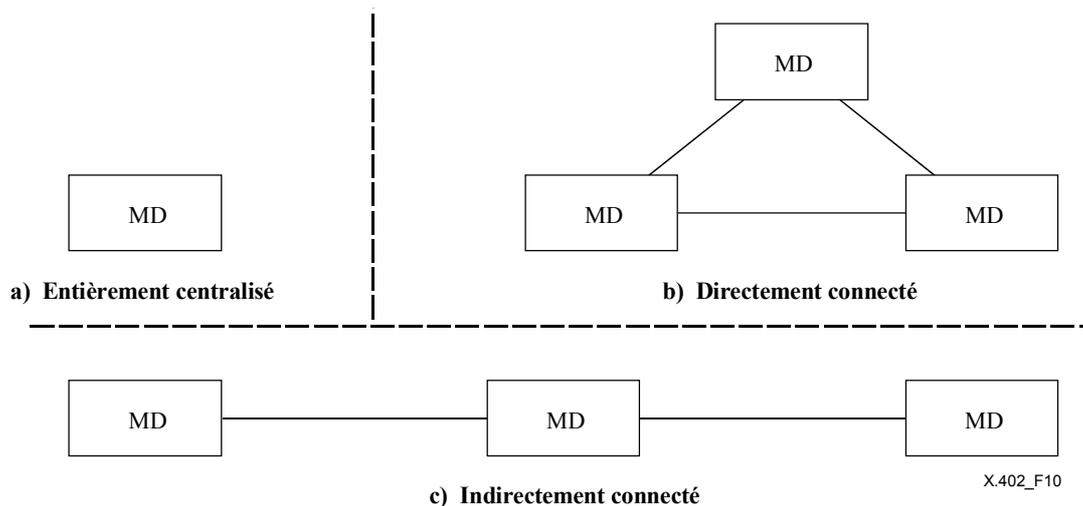
Un domaine de gestion d'administration (ADMD, *administration management domain*) offre des services de messagerie publics aux domaines PRMD et/ou aux utilisateurs individuels. Un domaine ADMD a des responsabilités de gestion par lesquelles il doit assurer que ses clients peuvent communiquer avec tout autre domaine MD rattaché au *système MHS mondial*.

#### 14.1.2 Domaines de gestion privés

Un domaine de gestion privé (PRMD, *private management domain*) comprend les systèmes de messagerie gérés par une organisation privée. Bien qu'aucune restriction ne soit imposée à un domaine PMRD offrant des services de messagerie publique, ce domaine n'a pas accepté les responsabilités d'Administration qui garantiraient à ses clients de communiquer avec tout autre domaine de gestion rattaché au *système MHS mondial*.

### 14.2 Configurations représentatives

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



**Figure 10 – Configurations représentatives organisationnelles**

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

#### 14.2.1 Système MHS entièrement centralisé

L'ensemble du système MHS peut être géré par une organisation (partie *a* de la Figure 10). Cette conception s'effectue avec un seul domaine MD.

#### 14.2.2 Système MHS connecté directement

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

#### 14.2.3 Système MHS connecté indirectement

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

## 15 Le système MHS mondial

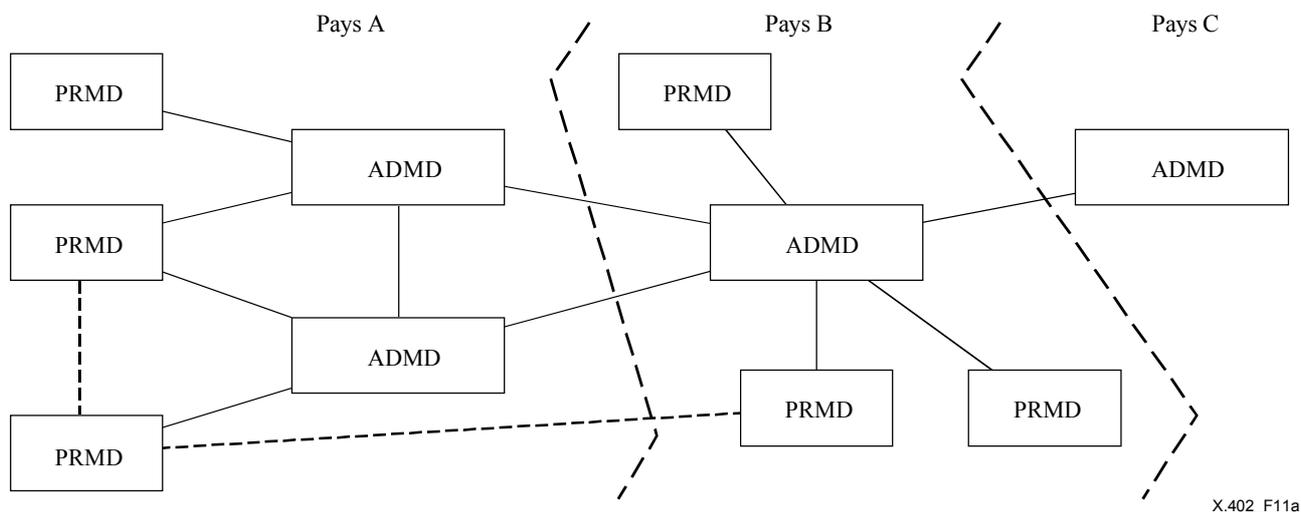
Un des principaux buts des Spécifications concernant le système MHS est de permettre l'élaboration du système MHS mondial, un système MHS fournissant à l'échelle mondiale un service de messagerie à la fois à l'intérieur d'une organisation et entre organisations, et au niveau national et international.

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

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

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

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



X.402\_F11a

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

Figure 11 – Le système MHS mondial

## SECTION 4 – DÉNOMINATION, ADRESSAGE ET ACHEMINEMENT

### 16 Aperçu général

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

Elle traite des sujets suivants:

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

### 17 Dénomination

Le présent paragraphe spécifie comment les utilisateurs et les listes DL sont nommés aux fins de messagerie en général et du transfert de messages en particulier. Il définit les *entités OR-name* et décrit le rôle que les noms d'annuaire jouent dans ces noms.

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

#### 17.1 Noms d'annuaire

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

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

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

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

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

## 17.2 Entités OR-name

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

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

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

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

NOTE – Un réacheminement ou un développement de la liste DL peut obliger le système MTS à transmettre à un agent UA ou une mémoire MS, au moment de la remise, des entités OR-name que l'agent UA ou la mémoire MS n'a pas fournies en dépôt direct.

Pour obtenir des informations sur les organisations opérant dans deux pays ou plus, voir l'Annexe G, ainsi que le § 7.3.2 de la Rec. UIT-T X.400 | ISO/CEI 10021-1.

## 18 Adressage

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

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

### 18.1 Listes d'attributs

Les *entités OR-address* des utilisateurs et des listes DL sont des listes d'attributs. Une liste d'attributs est un ensemble ordonné d'*attributs*.

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

Un attribut est composé des parties suivantes:

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

Les attributs sont de deux sortes, à savoir:

- a) Attribut normalisé: attribut dont le type est lié par la présente Spécification à une classe d'information.  
La valeur de chaque attribut normalisé, à l'exception du type de terminal, est soit une chaîne, soit un ensemble de chaînes.
- b) Attribut défini-par-domaine: attribut dont le type est lié à une classe d'information par un domaine MD. Par conséquent, le type et la valeur d'un attribut défini-par-domaine sont définis par un domaine MD. Le domaine MD est identifié par un *nom de domaine privé*, par un *nom de domaine d'Administration*, ou par les deux.

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

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

## 18.2 Jeux de caractères

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

- a) le type ou la valeur d'un attribut défini-par-domaine particulier peut être une chaîne imprimable, une chaîne télétexte, une chaîne universelle, ou toute combinaison de celles-ci. Le même choix ou les mêmes choix doivent être effectués pour le type et la valeur;
- b) les types des chaînes à partir desquelles les valeurs d'attributs normalisés peuvent être constituées et leur constitution (par exemple en une seule chaîne ou en plusieurs) varient d'un attribut à l'autre (voir § 18.3).

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

- a) pour le *nom de domaine d'administration*, le *nom de domaine privé* et le *code postal*, la même valeur numérique peut être représentée par une chaîne numérique ou imprimable;
- b) lorsque les chaînes imprimable et télétexte sont toutes deux autorisées, des chaînes de l'une de ces catégories ou des deux à la fois peuvent être fournies. Si à la fois des chaînes imprimables et des chaînes télétexte sont fournies, elles doivent toutes identifier sans ambiguïté le même utilisateur;
- c) partout où les chaînes imprimables, télétexte et universelles sont autorisées, un, deux ou l'ensemble des trois types, peut être fourni. Lorsque plus d'un type est proposé pour un attribut, chaque valeur devrait identifier de façon non ambiguë le même utilisateur. De nombreux systèmes ne seront pas en mesure d'interpréter tous les caractères possibles pouvant être représentés par les chaînes universelles (en étant, par exemple, limités au sous-ensemble des chaînes universelles satisfaisant les besoins nationaux), et certains systèmes seront totalement incapables d'interpréter les chaînes universelles. Par conséquent, les chaînes universelles seules ne devraient être utilisées que lorsque l'on sait que tous les destinataires possibles peuvent traiter les caractères concernés (par exemple, au sein d'une communauté régionale ou nationale d'utilisateurs).

Lorsqu'une chaîne universelle est fournie, un code de langue, défini dans l'ISO 639, peut être ajouté pour faciliter l'interprétation de la chaîne universelle; par exemple, lorsqu'un caractère est interprété différemment dans différentes langues, cela peut provoquer la sélection d'une police appropriée. Le code de langue comprend un code de deux caractères spécifié par l'ISO 639, suivi, de façon facultative, par un espace et, s'il est nécessaire d'identifier une utilisation nationale spécifique de la langue (par exemple, "en" identifie la langue anglaise, "en GB" identifie l'anglais utilisé au Royaume-Uni, et "en US" identifie l'anglais utilisé aux Etats-Unis d'Amérique), un code de pays ISO 3166 sur deux caractères (voir le § 4.4 de l'ISO 639).

Lorsqu'une chaîne universelle contient uniquement des caractères de la Table multilingue de base (voir l'ISO/CEI 10646-1), elle peut être codée en notation ASN.1 comme une chaîne UniversalString ou comme une chaîne BMPString.

Aux fins de comparaison des valeurs des adresses d'OR, on ne tient pas compte des codes de langue pouvant figurer dans la chaîne.

*UIT-T seulement:*

La longueur de chaque chaîne et de chaque séquence de chaînes d'un attribut doit être limitée selon les indications fournies dans la spécification plus détaillée des attributs (à savoir, l'ASN.1) contenue dans la Rec. UIT-T X.411.

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

NOTE 2 – Les règles d'adaptation vers le bas énoncées dans l'Annexe B de la Rec. UIT-T X.419 | ISO/CEI 10021-6 stipulent qu'il est impossible d'adapter vers le bas une entité OR-address si seule une chaîne universelle ou une chaîne télétext (ou les deux) a (ont) été fournie(s) et contient (contiennent) des caractères n'appartenant pas au répertoire de la chaîne imprimable.

NOTE 3 – La syntaxe ASN.1 permet de coder les chaînes de télétext en utilisant (entre autres) les répertoires de caractères 102, 103, 6 et 156 qui offrent deux possibilités de codage pour de nombreux caractères latins. A des fins de compatibilité avec les systèmes antérieurs, il est recommandé de coder toujours les caractères des répertoires 102 et 103 à l'aide de ces répertoires et de ne pas utiliser les répertoires 6 et 156 pour coder une chaîne qui ne contient que des caractères disponibles dans les répertoires 102 et 103. Cette même condition s'applique à toutes les instances de chaîne de télétext dans les protocoles du système MHS.

### 18.3 Attributs normalisés

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

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

Tableau 9 – Attributs normalisés

Type d'attribut normalisé	Jeux de caractères		
	Numérique	Imprimable	Universel ou Télétext
<b>Généraux</b>			
Nom de domaine d'administration ( <i>administration-domain-name</i> )	x	x	–
Nom courant ( <i>common-name</i> )	–	x	x
Nom de pays ( <i>country-name</i> )	x	x	–
Adresse réseau ( <i>network-address</i> )	x*	–	–
Identificateur numérique d'utilisateur ( <i>numeric-user-identifier</i> )	x	–	–
Nom d'organisation ( <i>organization-name</i> )	–	x	x
Noms d'unités organisationnelles ( <i>organizational-unit-names</i> )	–	x	x
Nom personnel ( <i>personal-name</i> )	–	x	x
Nom de domaine privé ( <i>private-domain-name</i> )	x	x	–
Identificateur de terminal ( <i>terminal-identifier</i> )	–	x	–
Type de terminal ( <i>terminal-type</i> )	–	–	–
<b>Acheminement postal</b>			
Nom de système de remise physique ( <i>pds-name</i> )	–	x	–
Nom de pays de remise physique ( <i>physical-delivery-country-name</i> )	x	x	–
Code postal ( <i>postal-code</i> )	x	x	–
<b>Adresse postale</b>			
Extension des composantes d'entité OR-address postale ( <i>extension-postal-OR-address-components</i> )	–	x	x
Extension des composantes d'adresse de remise physique ( <i>extension-physical-delivery-address-components</i> )	–	x	x
Attributs postaux locaux ( <i>local-postal-attributes</i> )	–	x	x
Nom de bureau de remise physique ( <i>physical-delivery-office-name</i> )	–	x	x
Numéro de bureau de remise physique ( <i>physical-delivery-office-number</i> )	–	x	x

Tableau 9 – Attributs normalisés

Type d'attribut normalisé	Jeux de caractères		
	Numérique	Imprimable	Universel ou Télétex
Nom d'organisation de remise physique ( <i>physical-delivery-organization-name</i> )	–	x	x
Nom personnel de remise physique ( <i>physical-delivery-personal-name</i> )	–	x	x
Adresse de boîte postale ( <i>post-office-box-address</i> )	–	x	x
Adresse de poste restante ( <i>poste-restante-address</i> )	–	x	x
Adresse de rue ( <i>street-address</i> )	–	x	x
Adresse postale non formatée ( <i>unformatted-postal-address</i> )	–	x	x
Nom postal unique ( <i>unique-postal-name</i> )	–	x	x
x permis * Séquence de chaînes d'octets dans certaines circonstances.			

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

### 18.3.1 Nom de domaine d'administration

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

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

NOTE 1 – La valeur d'attribut comprenant un simple espace (" ") doit être réservée aux fins suivantes. Si cela est autorisé par le pays représenté par l'attribut nom de pays, un seul espace doit désigner n'importe quel domaine ADMD (c'est-à-dire tous les domaines ADMD) existant dans ce pays. Cela concerne à la fois l'identification des utilisateurs dans le pays et l'acheminement des messages, envois-tests et rapports vers les domaines ADMD de ce pays et entre eux. Pour ce qui est de l'identification des utilisateurs, cela implique que les entités OR-address des utilisateurs du pays soient choisies de façon à ne comporter aucune ambiguïté, même en l'absence des noms effectifs des domaines ADMD des utilisateurs. Du point de vue de la deuxième fonction, cette valeur d'attribut permet à la fois aux domaines PRMD situés à l'intérieur du pays et aux domaines ADMD installés à l'extérieur de ce pays, d'acheminer des messages, des envois-tests et des rapports vers l'un des domaines ADMD situés à l'intérieur du pays et implique que ceux-ci s'interconnectent de sorte que les messages, les envois-tests et les rapports soient transmis à leurs destinataires.

La valeur d'attribut comprenant un seul zéro ("0"), codée comme une chaîne imprimable ou comme une chaîne numérique, doit être réservée aux domaines PRMD qui ne sont connectés à aucun domaine ADMD et qui ne sont atteignables depuis aucun domaine ADMD. Un domaine PRMD qui est connecté à un ou plusieurs domaines ADMD n'utilisera pas la valeur à un seul zéro. Un domaine PRMD connecté indirectement à un domaine ADMD (autrement dit, là où existent des accords à la fois avec un domaine ADMD et des domaines PRMD intermédiaires pour acheminer les messages indirectement entre le domaine ADMD et le domaine PRMD en question) n'utilisera pas la valeur à un seul zéro. La valeur à un seul zéro, qui fournit une partie appropriée de l'espace d'entité OR-address pour de tels domaines PRMD, permet aussi à des domaines ADMD et d'autres domaines PRMD (n'ayant pas d'accords d'acheminement avec le domaine PRMD en question) de déterminer que les messages, les envois-tests et les rapports ne peuvent être acheminés jusqu'au domaine PRMD en question. La présence d'une entité OR-address ayant un nom de domaine d'administration à un seul zéro parmi les destinataires pour lesquels la responsabilité est mise à "non", ou pour le destinataire d'un message ou d'un rapport qui a subi un développement DL ou qui a été réacheminé, est permise et ne doit pas empêcher la remise.

NOTE 2 – Le nom de domaine d'administration à un seul zéro ne sous-entend pas que l'application doit entreprendre une action particulière, mais elle lui permet de faire des économies sur les frais de transmission en détectant à l'avance que la remise ne sera pas possible.

### 18.3.2 Nom courant (*common-name*)

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

La valeur d'un nom commun (*common-name*) est une chaîne imprimable, une chaîne télétex, une chaîne universelle, ou une combinaison de ces types. Quel que soit le type utilisé, la valeur est choisie parmi cet ensemble de chaînes, administré à cette fin (et éventuellement à d'autres) par l'entité mentionnée ci-dessus.

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

### 18.3.3 Nom de pays (*Country-name*)

Un nom de pays (*country-name*) est un attribut normalisé qui identifie un pays (ou, exceptionnellement, une autorité internationale d'enregistrement de domaine MD).

La valeur d'un nom de pays (*country-name*) est une chaîne imprimable (*Printable String*) qui indique la paire de caractères affectée au pays par l'ISO 3166, ou une chaîne numérique (*Numeric String*) qui indique l'un des numéros affecté au pays (ou à la région géographique, ou au service non localisé) par la Rec. CCITT X.121.

La valeur d'attribut chaîne imprimable comprenant les caractères "XX" doit être réservée pour indiquer l'autorité internationale d'enregistrement des noms de domaines de gestion conformément à la Rec. UIT-T X.666 | ISO/CEI 9834-7.

NOTE 1 – La valeur "XX" fait partie des valeurs réservées dans l'ISO 3166 au profit des utilisateurs de cette norme; il n'y aura ainsi pas de contradiction possible entre un nouveau code de pays alloué dans l'ISO 3166 et cette valeur réservée.

NOTE 2 – Quelques utilisateurs ont, avant l'existence d'une procédure formelle d'enregistrement, utilisé la valeur "WW" comme nom de pays pour arriver à un résultat similaire à la valeur "XX". Cependant, l'ISO 3166 n'a pas actuellement affecté la valeur "WW" à cette fin.

### 18.3.4 Extension des composantes d'entité OR-address postale (*extension-postal-OR-address-components*)

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

La valeur d'une extension des composantes d'adresse OR postale (*extension-postal-OR-address-components*) est une chaîne imprimable, une chaîne télétexte, une chaîne universelle, ou une combinaison de ces types.

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

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

La valeur d'une extension des composantes d'adresse de remise physique (*extension-physical-delivery-address-components*) est une chaîne imprimable, une chaîne télétexte, une chaîne universelle, ou une combinaison de ces types.

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

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

La valeur des attributs postaux locaux (*local-postal-attributes*) est une chaîne imprimable, une chaîne télétexte, une chaîne universelle, ou une combinaison de ces types.

### 18.3.7 Adresse réseau (*network-address*)

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

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

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

NOTE 1 – Parmi les chaînes admises par la Rec. CCITT X.121, on note des numéros de télex et de téléphone précédés d'un chiffre d'échappement.

NOTE 2 – Les protocoles du système MHS permettent de transporter 16 chiffres dans la composante adresse X.121 de l'adresse de réseau, donc d'utiliser un chiffre d'échappement plus un numéro de téléphone ou de RNIS complet à 15 chiffres. D'autres protocoles peuvent avoir une limite de 14 chiffres ou un mécanisme différent pour le codage de numéros à 15 chiffres; le mappage entre ces protocoles et les protocoles MHS relève, si il est nécessaire, des autorités locales.

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

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

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

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

La valeur du nom d'organisation (*organization-name*) est une chaîne imprimable, une chaîne télétexte, une chaîne universelle, ou une combinaison de ces types.

Lorsqu'elles apparaissent dans une *entité OR-address mnémotechnique* (voir § 18.5.1), sur le plan national, les organisations peuvent être identifiées soit par rapport au pays désigné par un nom de pays (de sorte que les noms d'organisation soient uniques dans ce pays), soit par rapport au domaine MD désigné par un *nom de domaine privé*, par un nom de domaine d'Administration, ou par les deux. Quel que soit le type de chaîne utilisé, la chaîne est sélectionnée dans un ensemble de chaînes de ce type régi à cette fin (et éventuellement à d'autres fins) par le pays ou par le domaine MD précité.

NOTE – Dans les pays qui choisissent des noms d'organisation uniques pour tout le pays, un organisme national d'enregistrement des noms d'organisation est nécessaire.

Lorsqu'il apparaît dans une *entité OR-address de terminal* (voir § 18.5.4), le nom d'organisation est une valeur à structure non imposée, sans spécification d'enregistrement.

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

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

La valeur d'un attribut noms d'unité organisationnelle est une séquence ordonnée de chaînes imprimables, de chaînes télétexte, une séquence ordonnée de chaînes universelles, ou toute combinaison de ces trois options. Quel que soit le type de chaîne utilisé, chaque chaîne est sélectionnée dans un ensemble de chaînes de ce type régi à cette fin (et éventuellement à d'autres fins) par l'organisation (ou l'unité englobante) précitée.

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

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

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

### **18.3.12 Nom personnel (*personal-name*)**

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

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

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

Les informations ci-dessus sont fournies sous forme de chaînes imprimables, de chaînes télétexte, de chaînes universelles ou de toute combinaison de ces types.

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

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

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

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

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

La valeur du nom de bureau de remise physique "physical-delivery-office-name" est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

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

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

La valeur du numéro de bureau de remise physique "physical-delivery-office-number" est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

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

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

La valeur du nom d'organisation de remise physique "physical-delivery-organization-name" est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

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

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

La valeur du nom personnel de remise physique "physical-delivery-personal-name" est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

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

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

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

#### **18.3.19 Code postal (*postal-code*)**

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

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

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

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

La valeur d'adresse de poste restante "post-restante-address" est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

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

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

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

NOTE – Dans les pays qui choisissent des noms de domaines PRMD uniques pour tout le pays, un organisme national d'enregistrement des noms de domaine privé est nécessaire.

#### **18.3.22 Adresse de rue (*street-address*)**

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

La valeur d'une adresse de rue est une chaîne imprimable, une chaîne télétext, une chaîne universelle, ou toute combinaison de ces types.

### 18.3.23 Identificateur de terminal (*terminal-identifier*)

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

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

### 18.3.24 Type de terminal (*terminal-type*)

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

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

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

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

La valeur d'une adresse postale non formatée est soit une séquence de chaînes imprimables, chacune représentant une ligne de texte, soit une seule chaîne universelle ou une chaîne télétext, les lignes étant séparées par des commandes CR LF ou des LF CR (jusqu'à un maximum de cinq) ou les deux à la fois.

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

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

La valeur du nom postal unique (*unique-postal-name*) est une chaîne imprimable, une chaîne télétext, une chaîne universelle ou une combinaison de ces types.

## 18.4 Equivalence entre les listes d'attributs

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

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

NOTE 1 – Cette règle s'applique même à l'attribut normalisé nom de pays lorsque le choix entre les formes de la Rec. X.121 ou de l'ISO 3166 doit être considéré comme non significatif. Lorsque la Rec. X.121 attribue plusieurs numéros à un pays, la signification du numéro utilisé n'a pas été normalisée par la présente Spécification.

- c) lorsque la valeur d'un attribut normalisé peut être une chaîne imprimable, une chaîne télétext, une chaîne universelle ou une combinaison, le choix parmi les sept possibilités doit être considéré comme non significatif;
- d) lorsque le type ou la valeur d'un attribut défini par domaine, ou la valeur d'un attribut normalisé, comporte des caractères du répertoire Chaîne imprimable, le choix, lorsqu'il est autorisé, entre un codage en chaîne télétext et un codage en chaîne imprimable, doit être considéré comme non significatif;
- e) lorsque le type ou la valeur d'un attribut défini par domaine (domain-defined), ou lorsque la valeur d'un attribut normalisé, comprend des caractères issus du répertoire Chaînes télétext, le choix, lorsqu'il est autorisé, entre un codage en chaîne télétext et un codage en chaîne universelle doit être considéré comme non significatif;
- f) lorsque la valeur d'un attribut normalisé peut contenir des lettres, les types de caractères de ces lettres doivent être considérés comme non significatifs;
- g) dans un type ou une valeur d'attribut défini par domaine, ou dans une valeur d'attribut normalisé, tous caractères d'espacement placés au début et à la fin du texte, ainsi que, au-delà du premier, tous les caractères d'espacement consécutifs placés entre deux mots, doivent être considérés comme non significatifs;

- h) dans une chaîne télétexte, le caractère graphique de soulignement à chasse nulle doit être considéré comme non significatif, de même que toutes les fonctions de commande, à l'exception de la fonction d'espacement et des fonctions utilisées pour les procédures d'extension de code;
- i) dans une chaîne télétexte, le choix du codage pour le même caractère doit être considéré comme non significatif;
- j) dans une chaîne universelle, le choix entre différents codages du même caractère (par exemple, l'ordre dans lequel les composants des caractères constitutifs sont codés) doit être considéré comme non significatif.

NOTE 2 – Un domaine MD peut imposer des règles d'équivalence supplémentaires aux attributs qu'il affecte à ses propres utilisateurs et listes DL. Il peut définir, par exemple, des règles concernant les caractères de ponctuation dans les valeurs d'attributs, le type de caractères des lettres dans ces valeurs, ou l'ordre relatif des attributs définis par domaine.

### 18.5 Formes d'entités OR-address

A chaque utilisateur ou liste DL sont attribuées une ou plusieurs entités OR-address. Une entité OR-address est une liste d'attributs qui distingue un utilisateur d'un autre et qui identifie le point d'accès de l'utilisateur au MHS ou le point de développement de la liste DL.

Une entité OR-address peut prendre l'une quelconque des formes résumées dans le Tableau 10. La première colonne de ce tableau définit les attributs disponibles pour l'élaboration des entités OR-address. Pour chaque forme d'entité OR-address, la deuxième colonne indique les attributs pouvant apparaître dans ces entités OR-address et leurs degrés (voir également § 18.6).

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

Tableau 10 – Formes d'entité OR-address

Type d'attribut	Formes d'entité OR-address						
	MNEM	NUMR	POST		TERM		
Généraux							
Nom de domaine d'administration (administration-domain-name)	M	M	M	M	C		
Nom courant (common-name)	C	-	-	-	C*		
Nom de pays (country-name)	M	M	M	M	C		
Adresse réseau (network-address)	-	-	-	-	M		
Identificateur numérique d'utilisateur (numeric-user-identifiant)	-	M	-	-	-		
Nom d'organisation (organization-name)	C	-	-	-	C*		
Noms d'unités organisationnelles (organizational-unit-names)	C	-	-	-	C*		
Nom personnel (personal-name)	C	-	-	-	C*		
Nom de domaine privé (private-domain-name)	C	C	C	C	C		
Identificateur de terminal (terminal-identifiant)	-	-	-	-	C		
Type de terminal (terminal-type)	-	-	-	-	C		
Acheminement postal							
Nom de système de remise physique (pds-name)	-	-	C	C	-		
Nom de pays de remise physique (physical-delivery-country-name)	-	-	M	M	-		
Code postal (postal-code)	-	-	M	M	-		
Adresse postale							
Extension des composantes d'entité OR-address postale (extension-postal-OR-address-components)	-	-	C	-	-		
Extension des composantes d'adresse de remise physique (extension-physical-delivery-address-components)	-	-	C	-	-		
Attributs postaux locaux (local-postal-attributes)	-	-	C	-	-		
Nom de bureau de remise physique (physical-delivery-office-name)	-	-	C	-	-		
Numéro de bureau de remise physique (physical-delivery-office-number)	-	-	C	-	-		
Nom d'organisation de remise physique (physical-delivery-organization-name)	-	-	C	-	-		
Nom personnel de remise physique (physical-delivery-personal-name)	-	-	C	-	-		
Adresse de boîte postale (post-office-box-address)	-	-	C	-	-		
Adresse de poste restante (poste-restante-address)	-	-	C	-	-		
Adresse de rue (street-address)	-	-	C	-	-		
Adresse postale non formatée (unformatted-postal-address)	-	-	-	M	C*		
Nom postal unique (unique-postal-name)	-	-	C	-	-		
Défini par domaine							
Défini par domaine (un ou plus) (domain-defined)	C	C	-	-	C		
Légende							
MNEM	Mnémotechnique	NUMR	Numérique	POST	Postal	TERM	Terminal
F	Formaté	U	Non formaté	M	Obligatoire	C	Conditionnel
C*	Conditionnel, à utiliser à des fins de restitution mais pas pour l'adressage ou l'acheminement dans le système MHS						

Les formes d'entité OR-address, résumées dans le Tableau 10, sont définies et décrites individuellement ci-dessous. La représentation des entités OR-address en vue de leur emploi par l'utilisateur est donnée à l'Annexe F.

### 18.5.1 Entité OR-address mnémotechnique

L'entité OR-address mnémotechnique fournit une identification facile à mettre en mémoire, tant pour un utilisateur que pour une liste DL. Elle identifie un domaine MD et un utilisateur ou une liste DL s'y rapportant.

Une entité OR-address mnémotechnique comprend les attributs suivants:

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

### 18.5.2 Entité OR-address numérique

L'entité OR-address numérique est une adresse qui identifie de façon numérique un utilisateur par rapport à un domaine MD.

Une entité OR-address numérique comprend les attributs suivants:

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

NOTE – Seul l'identificateur numérique d'utilisateur doit être numérique.

### 18.5.3 Entité OR-address postale

L'entité OR-address postale est celle qui identifie un utilisateur au moyen de son adresse postale. Elle identifie le système PDS par lequel l'utilisateur doit être atteint et fournit l'adresse postale de l'utilisateur.

On distingue deux types d'entités OR-address postales:

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

Une entité OR-address postale, formatée ou non, comprend les attributs suivants:

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

Une entité OR-address postale formatée comprend en outre un exemplaire de chacun des attributs d'adresse postale conditionnels (énumérés dans le Tableau 10) nécessaires au système PDS, mais elle ne contient pas l'attribut d'adresse postale non formatée.

Une entité OR-address postale non formatée comprend, en outre, un attribut d'adresse postale non formatée.

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

### 18.5.4 Entité OR-address du terminal

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

Une entité OR-address du terminal comprend les attributs suivants:

- a) une adresse réseau;

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

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

#### 18.5.5 Détermination des formes d'adresse

La forme d'une entité OR-address doit être déterminée de la manière suivante:

- si elle contient un identificateur numérique d'utilisateur, elle est une entité OR-address numérique;
- si elle contient une adresse réseau, elle est une entité OR-address du terminal;
- si elle contient un nom de pays de remise physique, elle est une entité OR-address postale;
- toute autre entité OR-address est une entité OR-address mnémotechnique.

Si une entité OR-address postale contient une adresse postale non formatée, elle est une entité OR-address postale non formatée; sinon il s'agit d'une entité OR-address postale.

#### 18.6 Attributs conditionnels

La présence ou l'absence dans une entité OR-address particulière des attributs indiqués comme conditionnels au Tableau 10 sont déterminées ci-après.

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

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

### 19 Acheminement

*Version de l'UIT-T:*

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

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

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

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

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

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

*Version de l'ISO/CEI:*

Pour acheminer un message, un envoi-test ou un rapport vers un utilisateur ou vers le point de développement d'une liste DL, un agent MTA doit non seulement localiser l'utilisateur ou la liste DL (c'est-à-dire obtenir son entité OR-address), mais également sélectionner une voie d'acheminement vers cet emplacement. L'acheminement est donc le processus consistant à sélectionner, pour une entité OR-address donnée, l'agent MTA auquel il y a lieu de transférer le message, l'envoi-test ou le rapport.

Le présent paragraphe est de nature didactique; il est prévu que la Rec. UIT-T X.412 | ISO/CEI 10021-10 normalise des mécanismes de diffusion et d'utilisation des informations nécessaires aux décisions à prendre en matière d'acheminement. La Rec. UIT-T X.404 | ISO/CEI TR 10021-11 donne des conseils à l'intention des gestionnaires de système de messagerie sur l'emploi de ces mécanismes d'acheminement.

En l'absence d'autres considérations, la solution optimale consiste à transférer le message aussi directement que possible à l'agent MTA auquel est connecté l'agent UA du destinataire. Toutefois, certains facteurs peuvent rendre plus appropriée une voie d'acheminement moins directe; il s'agit par exemple des voies d'acheminement moins directes utilisant des liaisons entre agents MTA ayant des largeurs de bande plus grandes, l'emploi d'une sortance récente pour optimiser les coûts des transmissions, l'accès à un agent MTA intermédiaire pour un service tel qu'une conversion. Les coûts de diffusion et d'enregistrement des informations d'acheminement, éventuellement combinés à la volonté de certains domaines de ne pas divulguer leur structure interne, signifient qu'il ne sera souvent pas possible de faire l'acheminement directement à l'agent MTA de destination, même si cela est souhaitable.

La première décision que doit prendre l'agent MTA est de déterminer si le destinataire se trouve dans son propre domaine MD. Pour cela, il doit connaître toutes les combinaisons de nom de pays, de nom de domaine d'administration et de nom de domaine privé qui identifient son propre domaine. Un domaine PRMD peut avoir autant de combinaisons de ces attributs qu'il y a de points d'entrée depuis les domaines ADMD vers ce domaine PRMD bien que, pour les domaines PRMD se trouvant entièrement dans un pays qui adopte des noms de domaine privé uniques au plan national, une simple paire de valeurs formée du nom de pays et du nom de domaine privé soit suffisante pour identifier le domaine PRMD de manière interne, que l'absence sémantique du nom de domaine d'administration au point d'entrée depuis les domaines ADMD soit permise ou non.

Si on constate que le destinataire se trouve dans le même domaine MD, les valeurs d'autres attributs de l'entité OR address du destinataire sont examinées afin de déterminer si ce destinataire est un agent UA desservi par cet agent MTA, auquel cas la remise sera locale, ou s'il est un agent MTA approprié dans le domaine MD auquel peut être relayé le message. Si les deux possibilités échouent, un événement de non-remise doit survenir.

Il n'est pas nécessaire que tous les agents MTA relevant d'un domaine MD soient configurés avec la capacité de relayer vers d'autres domaines MD ou de recevoir depuis eux, mais il faut qu'au moins un agent MTA faisant partie du domaine ait ces capacités afin que le domaine MD ne soit pas isolé des autres. Chaque agent MTA faisant partie d'un domaine MD (non isolé) doit avoir la capacité d'acheminer vers un agent MTA situé à l'intérieur du domaine qui a la capacité de relayer vers d'autres MD, à moins qu'il n'ait lui-même cette capacité. Aussi, même si le destinataire est identifié comme étant à l'extérieur du domaine MD, il peut encore être nécessaire de relayer vers un autre agent MTA à l'intérieur du domaine MD.

Si l'on constate que le domaine MD extérieur est un domaine avec lequel une connexion directe existe, celle-ci sera souvent utilisée. Le domaine MD extérieur peut également être identifié comme un domaine atteint par relais via un ou plusieurs domaines intermédiaires. Si ces domaines MD intermédiaires sont des domaines PRMD, cette option peut être utilisée par accord bilatéral. Une autre possibilité est que le domaine MD extérieur soit inconnu: dans ce cas, il faudra recourir aux services d'un domaine ADMD.

Le rôle d'un domaine ADMD à l'intérieur du système MHS consiste à assurer le relais, directement ou indirectement, avec tous les autres domaines ADMD et à relayer des messages vers tous les domaines PRMD directement connectés à ce domaine ADMD. Un domaine PRMD a donc toujours la possibilité d'utiliser les services d'un domaine ADMD pour l'acheminement vers d'autres domaines PRMD.

Quand on identifie plusieurs points d'entrée d'un domaine MD extérieur, on peut utiliser des attributs d'entités OR-address additionnelles ou d'autres considérations pour déterminer le point d'entrée le plus approprié. Dans le cas extrême du domaine MD d'origine disposant de toutes les informations concernant le domaine MD du destinataire, cela permettrait la communication directe entre l'agent MTA de l'expéditeur et l'agent MTA du destinataire.

## SECTION 5 – UTILISATION DE L'ANNUAIRE

### 20 Aperçu général

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

La présente section couvre les sujets suivants:

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

### 21 Authentification

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

### 22 Résolution de nom

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

Pour obtenir l'adresse (les adresses) OR-address d'un utilisateur ou d'une liste DL dont il possède le nom d'annuaire, un objet présente ce nom à l'annuaire et demande à l'entrée d'annuaire les attributs suivants:

- a) *entités OR-address du système MHS;*
- b) *méthodes préférées de remise.*

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

L'objet fonctionnel cherche ensuite à déterminer une entité OR-address qui répond à une méthode de remise préférée. Pour les méthodes autres que la remise mhs-delivery, l'objet fonctionnel doit éventuellement construire une adresse au moyen d'autres attributs de l'entrée d'annuaire et au moyen des informations de configuration locale.

### 23 Développement d'une liste DL

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

L'objet présente à l'annuaire le nom d'annuaire d'une liste DL et demande à l'entrée d'annuaire les attributs suivants:

- a) *membres de la liste DL du système MHS;*
- b) *politique de liste DL du système MHS;*
- c) *autorisations de dépôt de la liste DL du système MHS.*

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

### 24 Evaluation des capacités

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

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

- a) *types de contenus pouvant être remis dans le système MHS;*
- b) *types EIT pouvant être remis dans le système MHS;*
- c) *longueur de contenu maximale dans le système MHS;*
- d) *adresses OR du système MHS avec capacités offertes;*

- e) *types EIT ne pouvant être remis dans le système MHS;*
- f) *méthodes de remise préférées.*

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

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

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

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

## SECTION 6 – RÉALISATION OSI

### 25 Aperçu général

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

Elle traite des sujets suivants:

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

### 26 Éléments de service d'application

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

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

NOTE – Outre les éléments ASE étudiés dans la présente section, le système MHS compte sur l'élément de service d'accès à l'annuaire défini dans la Rec. UIT-T X.519 | ISO/CEI 9594-5. Cependant, cet élément ASE ne figurant pas dans les contextes d'application *AC* concernant la messagerie (voir la Rec. UIT-T X.419 | ISO/CEI 10021-6), il n'est pas étudié ici.

#### 26.1 Concept d'élément ASE

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

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

Un élément ASE joue le rôle principalement mécanique de traduire les demandes et les réponses formulées par ses éléments UE en provenance et à destination de la forme prescrite par le protocole d'application régissant l'interaction de l'élément ASE avec son homologue dans le système ouvert auquel l'association le relie. L'élément ASE réalise un service abstrait, ou une partie de ce service, aux fins d'une communication OSI (voir les paragraphes 28-30).

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

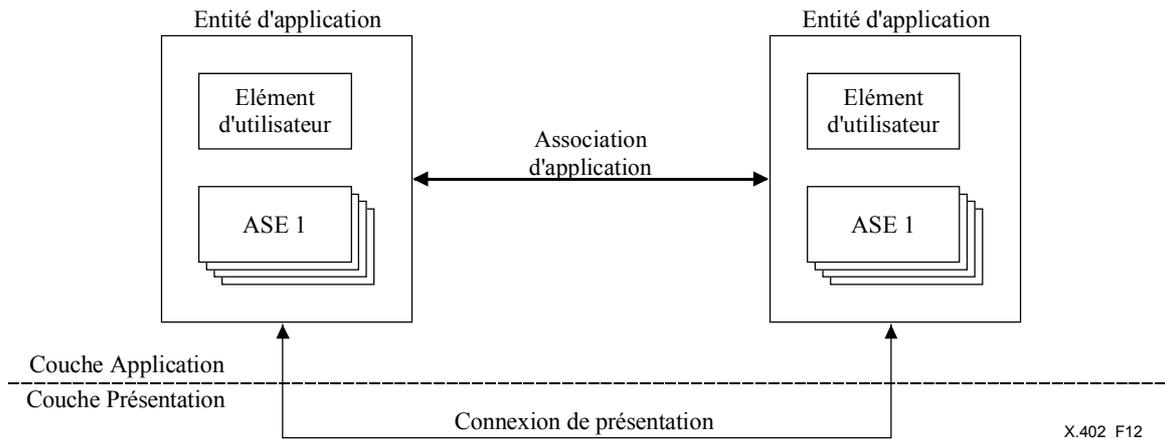


Figure 12 – Le concept d'élément ASE

## 26.2 Éléments ASE symétriques et asymétriques

On peut distinguer deux types d'éléments ASE, illustrés sur la Figure 13:

- symétrique: se dit d'un élément ASE grâce auquel un élément UE à la fois assure et utilise un service. Par exemple, l'élément ASE destiné au transfert de messages est symétrique car les deux systèmes ouverts, qui comprennent chacun un agent MTA, offrent et peuvent utiliser, grâce à lui, le service de transfert de messages;
- asymétrique: se dit d'un élément ASE grâce auquel un élément UE assure ou utilise un service, selon la configuration de l'élément ASE, mais n'effectue pas les deux. Par exemple, l'élément ASE destiné à la remise de messages est asymétrique car seul le système ouvert comprenant un agent MTA offre le service associé et seul l'autre système ouvert, qui comprend un agent UA ou une mémoire MS, l'utilise.

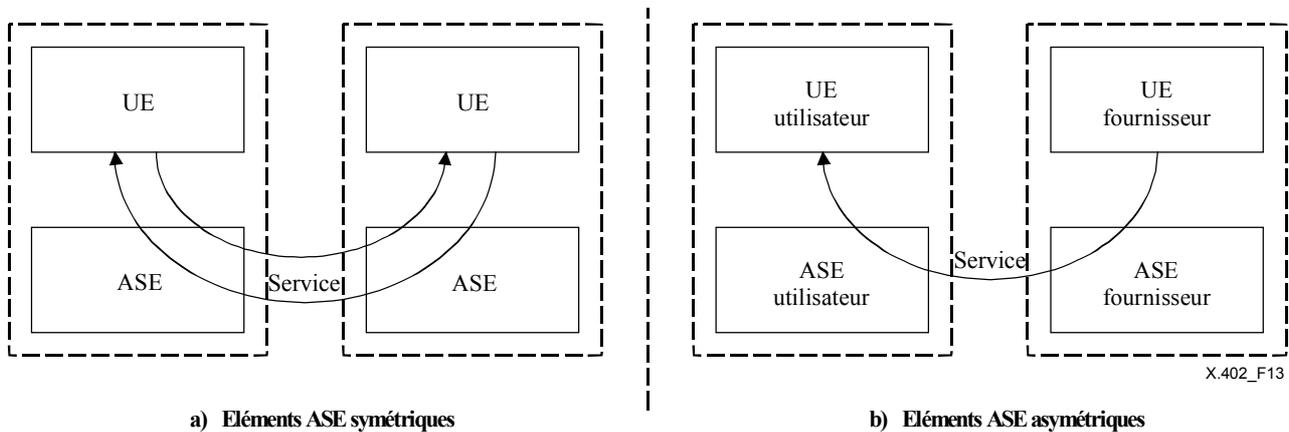
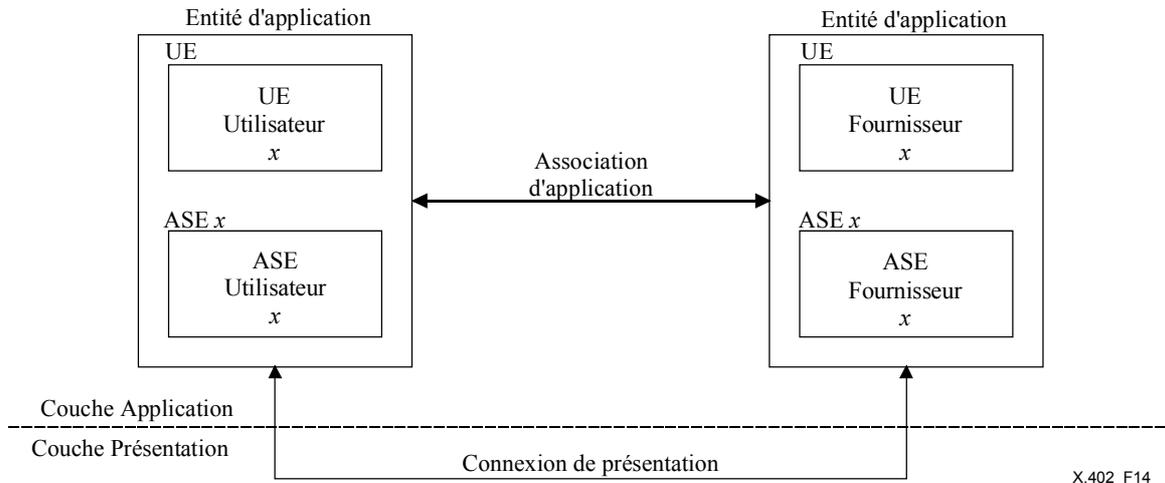


Figure 13 – Éléments ASE symétriques et asymétriques

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

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

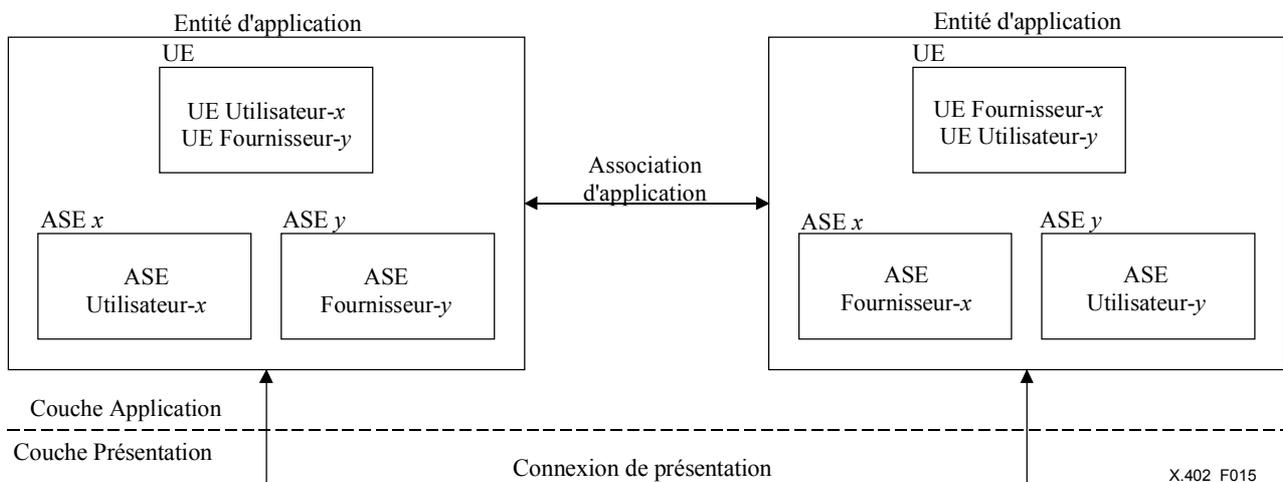
- c) élément UE utilisateur-*x*: processus d'application qui utilise le service représenté par l'élément ASE asymétrique *x*;
- d) élément ASE utilisateur-*x*: élément ASE asymétrique conçu pour être installé au même emplacement qu'un élément UE utilisateur-*x*.



X.402\_F14

Figure 14 – Terminologie relative aux éléments ASE asymétriques

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



X.402\_F015

Figure 15 – Éléments ASE asymétriques multiples

### 26.3 Éléments ASE de messagerie

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

**Tableau 11 – Eléments 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	-

+- Légende -----+	
SY	Symétrique C Utilisateur
ASY	Asymétrique S Fournisseur

Les éléments ASE de messagerie, résumés dans le Tableau 11, sont présentés individuellement ci-dessous. Chacun d'eux est défini dans la Rec. UIT-T X.419 | ISO/CEI 10021-6.

**26.3.1 Transfert de messages**

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

**26.3.2 Dépôt de messages**

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

**26.3.3 Remise de messages**

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

**26.3.4 Retrait de messages**

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

**26.3.5 Gestion de messages**

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

**26.4 Eléments ASE supports**

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

**Tableau 12 – Eléments ASE supports**

ASE	Forme
ROSE	SY
RTSE	SY
ACSE	SY

+- Légende -----+	
SY	Symétrique
ASY	Asymétrique

Les éléments ASE supports, résumés dans le Tableau 12, sont présentés individuellement ci-dessous.

#### 26.4.1 Opérations distantes

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

L'élément ROSE est défini dans la Rec. UIT-T X.880 | ISO/CEI 13712-1.

#### 26.4.2 Transfert fiable

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

L'élément RTSE est défini dans la Rec. UIT-T X.218 | ISO/CEI 9066-1.

#### 26.4.3 Contrôle d'association

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

L'élément ACSE est défini dans la Rec. UIT-T X.217 | ISO/CEI 8649.

## 27 Contextes d'application

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

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

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

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

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

Les contextes AC permettant d'assurer les divers services de messagerie sont spécifiés dans la Rec. UIT-T X.419 | ISO/CEI 10021-6. Ces protocoles sont appelés P1, P3 et P7.

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

## SECTION 7 – CONVENTIONS POUR LA DÉFINITION DU SERVICE ABSTRAIT

**28 Aperçu général**

On peut avoir intérêt, quand on décrit une tâche complexe de traitement réparti de l'information, à spécifier la tâche en termes abstraits plutôt qu'en termes concrets, car cela permet d'être certain que les impératifs fonctionnels de la tâche sont stipulés indépendamment de la réalisation pratique. Tout en permettant que la spécification se développe par un processus d'affinement progressif, cette séparation est importante étant donné que chaque aspect de la tâche peut donner lieu à diverses réalisations pratiques. Dans un système de messagerie comprenant, par exemple, trois agents de transfert de message, le premier et le deuxième peuvent interagir au moyen de la communication OSI alors que le deuxième et le troisième peuvent le faire par des moyens non normalisés.

La présente section spécifie les conventions pour la description abstraite des services fournis par une tâche de traitement réparti de l'information, le service abstrait, au moyen d'un modèle abstrait. La réalisation du service abstrait au moyen de services de communication OSI est également décrite.

NOTE – La présente section remplace et rend caduques les conventions pour la définition du service abstrait contenues dans la Rec. X.407 du CCITT (1988) | ISO/CEI 10021-3:1990.

La Rec. UIT-T X.880 | ISO/CEI 13712-1 définit plusieurs classes d'objets informationnels qui sont utiles dans la spécification des protocoles d'application fondés sur les opérations distantes ROS comme celles qui sont définies pour le système MHS.

**29 Composantes du modèle abstrait****29.1 Objets abstraits**

Un objet abstrait (objet MHS) est une entité fonctionnelle, éventuellement l'une de plusieurs entités qui interagissent entre elles. Un objet abstrait d'un type donné peut représenter un système; les objets abstraits multiples d'un autre type peuvent représenter des utilisateurs. Ces objets abstraits n'interagissent que s'ils sont reliés pour former une association qui définit les services offerts et le contexte de leur interaction en termes de contrat abstrait.

Un objet MHS est spécifié comme une instance d'une classe d'objets informationnels de système MHS. Sa définition est identique à celle de la classe d'objets informationnels ROS-OBJECT-CLASS des opérations distantes. Cette définition indique les capacités d'un objet abstrait en termes des contrats (d'association) qu'il prend en charge en tant que demandeur ou en tant que répondeur, ou les deux.

MHS-OBJECT ::= ROS-OBJECT-CLASS

**29.2 Contrats abstraits**

Un contrat abstrait (contrat) définit un contexte dans lequel une paire d'objets abstraits peut interagir. Cela inclut la spécification de la manière dont deux objets abstraits établissent une association (rattachement), libèrent une association (détachement), identifient les accès abstraits rattachés pendant la durée de l'association. La spécification d'un contrat spécifie les accès où l'initiateur de l'association assume le rôle de "consommateur", les accès où il assume le rôle de "fournisseur" et les accès qui peuvent être symétriques ou dans lesquels l'initiateur de l'association peut occuper simultanément les rôles de "consommateur" et de "fournisseur".

Un contrat est défini comme une instance de la classe d'objets informationnels CONTRACT des opérations distantes.

**29.3 Paquets de connexion**

Un paquet de connexion spécifie la partie d'un contrat qui est concernée par l'établissement et la libération dynamiques d'une association. Il spécifie l'opération de rattachement abstrait utilisée pour établir l'association et l'opération de détachement abstrait utilisée pour la libérer.

Un paquet de connexion est défini comme une instance de la classe d'objets informationnels CONNECTION-PACKAGE des opérations distantes.

## 29.4 Accès abstraits

Un accès abstrait (accès) est un point où l'objet abstrait interagit avec un autre objet abstrait quand ces deux objets sont rattachés conformément aux termes d'un contrat. Il définit la série d'opérations qui peuvent être invoquées par un objet abstrait jouant le rôle de "consommateur", les opérations qui peuvent être invoquées par un objet abstrait jouant le rôle de "fournisseur" et les opérations qui peuvent être invoquées par chacun des deux objets abstraits.

Un accès est défini comme étant symétrique si toutes les instances de cet accès sont identiques (c'est-à-dire sans distinction des rôles de consommateur et de fournisseur). Un accès est défini comme étant asymétrique si chaque instance de cet accès est de l'une ou de l'autre nature, fournisseur ou consommateur (c'est-à-dire s'il y a distinction entre les rôles).

Un accès est spécifié comme étant une instance d'une classe d'objets informationnels PORT. Cette définition est identique à la classe d'objets informationnels OPERATION-PACKAGE des opérations distantes.

PORT ::= OPERATION-PACKAGE

## 29.5 Opérations abstraites et erreurs abstraites

Une opération abstraite est une procédure qu'un objet abstrait (le demandeur) peut demander à un autre objet (l'exécuteur) au niveau d'une paire d'accès rattachée aux termes d'un contrat. Si les accès sont symétriques, chacun des deux objets abstraits peut invoquer l'opération. Si les accès sont asymétriques, la définition de l'accès prescrit quelles opérations peuvent être invoquées par l'objet abstrait agissant comme consommateur au niveau de l'accès et celles qui peuvent être invoquées par l'objet agissant comme fournisseur.

Une erreur abstraite est une situation exceptionnelle qui peut survenir au cours de l'exécution d'une opération abstraite, dont elle provoque la défaillance. En cas de signalisation d'une erreur abstraite, l'exécutant transmet au demandeur l'identité de l'erreur abstraite et si possible un objet informationnel unique appelé son paramètre.

Les opérations abstraites et les erreurs abstraites sont spécifiées comme étant des instances des classes d'objets informationnels ABSTRACT-OPERATION et ABSTRACT-ERROR.

Leurs définitions sont identiques aux classes d'objets informationnels OPERATION et ERROR des opérations distantes.

ABSTRACT-OPERATION ::= OPERATION

ABSTRACT-ERROR ::= ERROR

## 30 Réalisation du service ROS

Dès qu'une tâche de traitement réparti de l'information a été décrite et spécifiée en termes abstraits, il faut prescrire la manière dont chaque aspect de la tâche doit être réalisé concrètement. Chaque aspect peut admettre plusieurs réalisations pratiques.

La réalisation pratique des composantes du service abstrait MHS est souvent banale quand elle est accomplie au moyen des opérations distantes. Il en est ainsi étant donné qu'il existe, pour un service abstrait donné, un protocole d'application fondé sur le service ROS qui est fonctionnellement identique. Cela résulte du fait que le cadre de la spécification des services abstraits est isomorphe à celui de la spécification des protocoles d'application fondés sur le service ROS. Les correspondances propres à cet isomorphisme sont énumérées dans le Tableau 13.

**Tableau 13 – Correspondance entre les composants de services abstraits et les classes d'objets informationnels du service ROS**

Composantes des services abstraits	Classe d'objets informationnels ROS
Objet MHS Accès Opération abstraite Erreur abstraite	ROS-OBJECT-CLASS OPERATION-PACKAGE OPERATION ERROR

Les classes d'objets informationnels CONTRACT et CONNECTION-PACKAGE du service ROS sont utilisées directement dans le modèle abstrait du service MHS.

## Annexe A

## Classes d'objets et attributs d'annuaire

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

Plusieurs classes d'objets, attributs, syntaxes d'attributs, contextes et variantes nominatives d'entité de certificat d'annuaire sont spécifiques à la messagerie. Ces classes sont définies dans la présente annexe à l'aide des classes d'objets informationnels OBJECT-CLASS, ATTRIBUTE et CONTEXT de la Rec. UIT-T X.501 | ISO/CEI 9594-2 ainsi qu'à l'aide des classes d'objets informationnels OTHER-NAME de la Rec. UIT-T X.509 | ISO/CEI 9594-8, selon le cas.

## A.1 Classes d'objets

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

NOTE – Les classes d'objets d'annuaire décrites dans la présente annexe peuvent être combinées avec d'autres classes d'objets, par exemple celles qui sont définies dans la Rec. UIT-T X.521 | ISO/CEI 9594-7. Voir également le § 12 de la Rec. UIT-T X.501 | ISO/CEI 9594-2 pour une explication montrant comment des classes d'objets d'annuaire peuvent être combinées en une entrée d'annuaire. L'Annexe B de la Rec. UIT-T X.521 | ISO/CEI 9594-7 donne quelques informations complémentaires relatives aux formes de nom d'annuaire et aux structures arborescentes possibles d'informations d'annuaire.

## A.1.1 Liste de distribution du système MHS

Un objet **liste de distribution du système MHS** est une liste de distribution. Ses attributs identifient ses: nom courant, autorisations de dépôt et adresses OR-address et, dans la mesure où les attributs correspondants sont présents, décrivent la liste de distribution, identifient son organisation, ses unités organisationnelles et son propriétaire; citent les objets apparentés; identifient sa longueur de contenu maximale, les types de contenu pouvant être remis, les types d'informations codées (EIT) acceptables, exclusivement acceptables et inacceptables; et identifient sa politique de développement, ses adresses d'abonnement, ses adresses d'archivage, ses listes et membres apparentés.

```
mhs-distribution-list OBJECT-CLASS ::= {
  SUBCLASS OF   { top }
  MUST CONTAIN  { commonName |
                 mhs-dl-submit-permissions |
                 mhs-or-addresses }
  MAY CONTAIN   { description |
                 organizationName |
                 organizationalUnitName |
                 owner |
                 seeAlso |
                 mhs-maximum-content-length |
                 mhs-deliverable-content-types |
                 mhs-acceptable-eits |
                 mhs-exclusively-acceptable-eits |
                 mhs-unacceptable-eits |
                 mhs-dl-policy |
                 mhs-dl-subscription-service |
                 mhs-dl-archive-service |
                 mhs-dl-related-lists |
                 mhs-dl-members }
  ID            id-oc-mhs-distribution-list }
```

## A.1.2 Mémoire de message du système MHS

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

```
mhs-message-store OBJECT-CLASS ::= {
  SUBCLASS OF   { applicationEntity }
  MAY CONTAIN   { owner |
                 mhs-supported-attributes |
                 mhs-supported-automatic-actions |
                 mhs-supported-matching-rules |
                 mhs-supported-content-types |
                 protocolInformation }
  ID            id-oc-mhs-message-store }
```

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

Un objet **agent de transfert de message du système MHS** est une entité d'application (AE) qui implémente un agent MTA. Les attributs contenus dans son entrée, dans la mesure où ils sont présents, décrivent l'agent MTA et identifient son propriétaire, sa longueur de contenu maximale et ses protocoles de réseau pris en charge.

```
mhs-message-transfer-agent OBJECT-CLASS ::= {
    SUBCLASS OF    { applicationEntity }
    MAY CONTAIN    { owner |
                    mhs-maximum-content-length |
                    protocolInformation }
    ID             id-oc-mhs-message-transfer-agent }
```

### A.1.4 Utilisateur du système MHS

Un objet **utilisateur du système MHS** est un utilisateur générique du système MHS. (L'utilisateur MHS générique peut avoir, par exemple, une adresse professionnelle, une adresse résidentielle, ou les deux.) Les attributs de l'entrée identifient l'adresse OR-address de l'utilisateur et, dans la mesure où les attributs correspondants sont présents, la longueur de contenu maximale, les types de contenu et les types d'informations codées (EIT); sa mémoire MS; et ses méthodes de remise préférées.

```
mhs-user OBJECT-CLASS ::= {
    SUBCLASS OF    { top }
    KIND           auxiliary
    MUST CONTAIN   { mhs-or-addresses }
    MAY CONTAIN    { mhs-maximum-content-length |
                    mhs-deliverable-content-types |
                    mhs-acceptable-eits |
                    mhs-exclusively-acceptable-eits |
                    mhs-unacceptable-eits |
                    mhs-or-addresses-with-capabilities |
                    mhs-message-store-dn }
    ID             id-oc-mhs-user }
```

Si l'utilisateur du système MHS dispose de plusieurs adresses OR-address avec différentes capacités de remise, les attributs `mhs-deliverable-content-types`, `mhs-deliverable-eits` et `mhs-undeliverable-eits` devraient représenter la réunion logique de ces capacités de remise; l'attribut `mhs-maximum-content-length` doit contenir la plus grande des valeurs de cet attribut. La capacité de chaque adresse OR-address peut ensuite être déterminée selon les besoins à partir de l'attribut `mhs-or-addresses-with-capabilities`.

NOTE – Les informations de méthode de remise préférée `preferredDeliveryMethod` de l'utilisateur du système MHS sont héritées, dans l'ensemble d'attributs de télécommunication `telecommunicationAttributeSet`, de la classe d'objets de dénomination de l'utilisateur de l'annuaire.

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

Un objet **agent d'utilisateur du système MHS** est une entité d'application qui réalise un agent d'utilisateur (UA). Les attributs de l'entrée, dans la mesure où ils sont présents, identifient le propriétaire de l'agent UA; sa longueur de contenu maximale, ses types de contenu et les types d'informations codées (EIT); ses classes de possibilité de remise; son adresse OR-address et ses protocoles de réseau pris en charge.

```
mhs-user-agent OBJECT-CLASS ::= {
    SUBCLASS OF    { applicationEntity }
    MAY CONTAIN    { owner |
                    mhs-maximum-content-length |
                    mhs-deliverable-content-types |
                    mhs-acceptable-eits |
                    mhs-exclusively-acceptable-eits |
                    mhs-unacceptable-eits |
                    mhs-deliverable-classes |
                    mhs-or-addresses |
                    protocolInformation }
    ID             id-oc-mhs-user-agent }
```

## A.2 Attributs

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

### A.2.1 Types d'informations codées acceptables (*mhs-acceptable-eits*)

Cet attribut identifie un ensemble de types d'informations codées; la présence de l'un quelconque de ces types dans un message fait qu'un utilisateur en acceptera la remise ou que la liste de distribution en sera développée, selon la définition du § 8.4.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. L'ordre de préséance entre cet attribut et ceux des § A.2.10 et A.2.19 est défini dans le § 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

Cet attribut prend pour valeur un identificateur d'objet.

```
mhs-acceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedEncodedInformationType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-acceptable-eits }
```

### A.2.2 Classes livrables (*mhs-deliverable-classes*)

Cet attribut identifie les classes de messages dont l'agent d'utilisateur acceptera la remise (voir § 8.4.1.1.3 de la Rec. UIT-T X.411 | ISO/CEI 10021-4).

Cet attribut prend pour valeur une capacité (voir § A.3.4).

```
mhs-deliverable-classes ATTRIBUTE ::= {
    WITH SYNTAX                Capability
    EQUALITY MATCHING RULE     capabilityMatch
    ID                          id-at-mhs-deliverable-classes }
```

### A.2.3 Types de contenu livrables (*mhs-deliverable-content-types*)

Cet attribut identifie les types de contenu des messages dont l'utilisateur acceptera la remise ou dont la liste DL sera développée. L'absence de cet attribut indique que tout type de contenu peut être remis (ou développé).

Cet attribut prend pour valeur un identificateur d'objet.

```
mhs-deliverable-content-types ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedContentType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-deliverable-content-types }
```

### A.2.4 Service d'archives DL (*mhs-dl-archive-service*)

Cet attribut identifie un service auquel l'utilisateur peut demander des copies de messages précédemment distribués par cette liste DL. La spécification détaillée d'un tel service (par exemple le format des demandes) sort du cadre de la présente Norme internationale.

Cet attribut prend pour valeur un nom OR-name.

```
mhs-dl-archive-service ATTRIBUTE ::= {
    WITH SYNTAX                ORName
    EQUALITY MATCHING RULE     oRNameExactMatch
    -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
    --                            oRNameSubstringElementsMatch |
    --                            oRNameSingleElementMatch }--
    ID                          id-at-mhs-dl-archive-service }
```

### A.2.5 Membres de liste DL (*mhs-dl-members*)

Cet attribut identifie les membres d'une liste DL. Quand une telle liste est développée, chacune des valeurs de cet attribut devient un destinataire du message.

Cet attribut prend pour valeur un nom OR-name.

```
mhs-dl-members ATTRIBUTE ::= {
    WITH SYNTAX                ORName
    EQUALITY MATCHING RULE     oRNameExactMatch
    -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
    --                            oRNameSubstringElementsMatch |
    --                            oRNameSingleElementMatch }--
    ID                          id-at-mhs-dl-members }
```

Une valeur de cet attribut peut avoir une annotation attachée afin de fournir les informations à utiliser dans le cadre de l'administration d'une liste DL (voir § A.4.1), peut avoir une indication attachée indiquant que ce membre est lui-même une liste DL afin de permettre une évaluation efficace de la permission de dépôt de liste DL (voir § A.4.2) ou peut avoir une indication attachée indiquant que ce membre utilise un système non normalisé (voir § A.4.3).

#### A.2.6 Politique de liste DL (*mhs-dl-policy*)

Cet attribut identifie les choix en matière de politique qu'il y a lieu d'appliquer lors du développement de la liste DL.

Cet attribut prend pour valeur une politique de liste DL.

```
mhs-dl-policy ATTRIBUTE ::= {
    WITH SYNTAX                DLPolicy
    SINGLE VALUE                TRUE
    ID                          id-at-mhs-dl-policy }
```

#### A.2.7 Listes apparentées à la liste DL (*mhs-dl-related-lists*)

Cet attribut identifie d'autres listes de distribution qui sont, d'une manière non précisée, apparentées à cette liste DL.

Cet attribut prend pour valeur un nom distinctif.

```
mhs-dl-related-lists ATTRIBUTE ::= {
    SUBTYPE OF                  distinguishedName
    EQUALITY MATCHING RULE      distinguishedNameMatch
    ID                          id-at-mhs-dl-related-lists }
```

#### A.2.8 Autorisations de dépôt de liste DL (*mhs-dl-submit-permissions*)

Cet attribut identifie les utilisateurs et les listes de distribution qui peuvent adresser des messages (ou des envois-tests) à une liste DL. Il n'intervient pas dans le traitement des rapports aux points de développement des listes.

Cet attribut prend pour valeur une autorisation de dépôt de liste.

```
mhs-dl-submit-permissions ATTRIBUTE ::= {
    WITH SYNTAX                  DLSubmitPermission
    ID                          id-at-mhs-dl-submit-permissions }
```

#### A.2.9 Service d'abonnement de liste DL (*mhs-dl-subscription-service*)

Cet attribut identifie un service auquel l'utilisateur peut demander d'apporter des modifications aux membres de la DL (adjonction d'un utilisateur à la liste DL par exemple). La spécification détaillée d'un tel service (le format des demandes par exemple) sort du cadre de la présente Norme internationale.

Cet attribut prend pour valeur un nom OR-name.

```
mhs-dl-subscription-service ATTRIBUTE ::= {
    WITH SYNTAX                  ORName
    EQUALITY MATCHING RULE      ORNameExactMatch
    -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
    --                            ORNameSubstringElementsMatch |
    --                            ORNameSingleElementMatch }--
    ID                          id-at-mhs-dl-subscription-service }
```

#### A.2.10 Types EIT exclusivement acceptables (*mhs-exclusively-acceptable-eits*)

Cet attribut identifie un ensemble de types d'informations codées (EIT); la présence de tous ces types dans un message fait que l'utilisateur en acceptera la remise ou qu'une liste DL le développera, conformément au § 8.4.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. L'ordre de préséance entre cet attribut et ceux des § A.2.1 et A.2.19 est défini au § 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

NOTE – Une conversion implicite peut avoir lieu dans le système de transfert de messages avant la remise du message; un type d'informations codées présent dans le message d'origine et ne faisant pas partie des types exclusivement acceptables peut se trouver alors converti en un des types acceptables, rendant ainsi possible la remise du message (ou le développement de la liste).

Cet attribut prend pour valeur un identificateur d'objet.

```
mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                  ExtendedEncodedInformationType
    EQUALITY MATCHING RULE      objectIdentifierMatch
    ID                          id-at-mhs-exclusively-acceptable-eits }
```

**A.2.11 Longueur maximale de contenu (*mhs-maximum-content-length*)**

Cet attribut identifie la longueur maximale du contenu des messages qu'un utilisateur acceptera de recevoir, qu'une liste DL acceptera de développer, ou qu'un agent MTA acceptera de recevoir.

Cet attribut prend pour valeur un entier.

```
mhs-maximum-content-length ATTRIBUTE ::= {
    WITH SYNTAX                ContentLength
    EQUALITY MATCHING RULE     integerMatch
    SINGLE VALUE               TRUE
    ID                          id-at-mhs-maximum-content-length }
```

**A.2.12 Nom d'annuaire d'une mémoire de message (*mhs-message-store-directory-name*)**

Cet attribut identifie la mémoire MS d'un utilisateur par son nom.

Il prend pour valeur un nom distinctif d'annuaire.

```
mhs-message-store-dn ATTRIBUTE ::= {
    SUBTYPE OF                 distinguishedName
    EQUALITY MATCHING RULE     distinguishedNameMatch
    SINGLE VALUE               TRUE
    ID                          id-at-mhs-message-store-dn }
```

**A.2.13 Adresses OR-address (*mhs-OR-addresses*)**

Cet attribut spécifie les adresses OR-address d'un utilisateur ou d'une liste DL. L'utilisateur de l'annuaire peut choisir n'importe quelle valeur utilisable comme adresse OR-address pour cet utilisateur.

Cet attribut prend pour valeur une adresse OR-address.

```
mhs-or-addresses ATTRIBUTE ::= {
    WITH SYNTAX                ORAddress
    EQUALITY MATCHING RULE     oRAddressMatch
    -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch |
    --                          oRAddressSubstringElementsMatch |
    --                          oRNameSingleElementMatch } --
    ID                          id-at-mhs-or-addresses }
```

Lorsque l'attribut *mhs-OR-addresses-with-capabilities* est présent dans une entrée, l'attribut *mhs-OR-addresses* ne doit contenir que l'adresse préférée de l'utilisateur.

**A.2.14 Adresses OR-address avec capacités (*mhs-OR-addresses-with-capabilities*)**

Cet attribut identifie les capacités de remise de chacune des adresses OR-address de l'utilisateur.

Il prend pour valeur une adresse OR-address avec capacités.

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
    WITH SYNTAX                AddressCapabilities
    EQUALITY MATCHING RULE     addressCapabilitiesMatch
    ID                          id-at-mhs-or-addresses-with-capabilities }
```

Cet attribut peut servir à indiquer les capacités de chacune des adresses OR de l'utilisateur lorsque ces capacités varient selon l'adresse. Il peut être également utilisé lorsqu'une même adresse a, par exemple, différentes capacités selon le type de contenu. En l'absence de capacités différentes à distinguer, la présence du seul attribut *mhs-OR-addresses* suffit.

**A.2.15 Attributs pris en charge (*mhs-supported-attributes*)**

Cet attribut identifie les attributs qu'une mémoire MS prend entièrement en charge.

Il prend pour valeur un identificateur d'objet.

```
mhs-supported-attributes ATTRIBUTE ::= {
    WITH SYNTAX                ATTRIBUTE.&id({AttributeTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-attributes
}
```

**A.2.16 Actions automatiques prises en charge (*mhs-supported-automatic-actions*)**

Cet attribut identifie les actions automatiques qu'une mémoire MS prend entièrement en charge.

Il prend pour valeur un identificateur d'objet.

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
    WITH SYNTAX                AUTO-ACTION.&id ({AutoActionTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-automatic-actions }
```

**A.2.17 Types de contenus pris en charge (*mhs-supported-content-types*)**

Cet attribut identifie les types de contenu des messages dont la syntaxe et la sémantique sont entièrement pris en charge par une mémoire MS.

Il prend pour valeur un identificateur d'objet.

```
mhs-supported-content-types ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedContentType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-content-types }
```

**A.2.18 Règles de correspondance prises en charge (*mhs-supported-matching-rules*)**

Cet attribut identifie les règles de correspondance que la mémoire MS prend entièrement en charge.

Il prend pour valeur un identificateur d'objet.

```
mhs-supported-matching-rules ATTRIBUTE ::= {
    WITH SYNTAX                MATCHING-RULE.&id ({MatchingRuleTable})
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-supported-matching-rules }
```

**A.2.19 Types d'informations codées inacceptables (*mhs-unacceptable-eits*)**

Cet attribut identifie un ensemble de types d'informations codées (EIT); la présence de l'un quelconque de ces types dans le message fera que le destinataire n'en acceptera pas la remise ou qu'une liste DL ne le développera pas, conformément à la définition donnée au § 8.4.1.1.3.1 de la Rec. UIT-T X.411 | ISO/CEI 10021-4. L'ordre de préséance entre cet attribut et ceux des § A.2.1 et A.2.10 est défini au § 14.3.4.4 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

NOTE – Une conversion implicite peut avoir lieu dans le système de messagerie avant la remise du message, tout type d'information codée inacceptable figurant dans le message d'origine étant converti en un type acceptable, autorisant ainsi la remise du message (ou le développement de sa liste de distribution).

Cet attribut prend pour valeur un identificateur d'objet.

```
mhs-unacceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX                ExtendedEncodedInformationType
    EQUALITY MATCHING RULE     objectIdentifierMatch
    ID                          id-at-mhs-unacceptable-eits }
```

**A.3 Syntaxes d'attributs**

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

**A.3.1 Autorisation de dépôt de liste DL (DL Submit Permission)**

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

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

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

- a) *Individual* (individuel): l'utilisateur ou la liste DL (non développée) dont l'une quelconque des entités OR-name est égale à l'entité OR-name spécifiée.
- b) *Member-of-dl* (membre de liste dl): chaque membre de la liste DL, dont l'une quelconque des entités OR-name est égale à l'entité OR-name spécifiée, ou de chaque liste DL imbriquée, de manière récurrente.
- c) *Pattern-match* (correspondance de structure): chaque utilisateur ou liste DL (non développée) dont l'une quelconque des entités OR-name correspond à la structure de l'entité OR-name spécifiée.

ORNamePattern ::= ORName

Une structure d'entité OR-name vide (c'est-à-dire une entité OR-name contenant une séquence d'attributs intégrés built-in-standard-attributes) signifie que tout utilisateur a l'autorisation de dépôt.

```
any-user-may-submit DLSubmitPermission ::=
    pattern-match: { built-in-standard-attributes { } }
```

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

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

### A.3.1.1 Procédure d'évaluation de l'autorisation de dépôt de liste DL

Quand on utilise l'attribut autorisation de dépôt de liste DL dans le système MHS pour déterminer si un message donné peut être développé par une liste DL, on applique la procédure suivante: si le message contient la chronologie du développement de liste DL, c'est l'entité OR-name de la dernière liste DL de la chronologie du développement qui est comparée avec les valeurs d'attribut d'autorisation de dépôt; sinon c'est l'entité OR-name de l'expéditeur du message.

La comparaison porte tour à tour sur chacune des valeurs jusqu'à ce que survienne la première correspondance par laquelle le message obtient l'autorisation de dépôt, ou jusqu'à ce qu'il n'y ait plus de valeurs à comparer, situation dans laquelle le message n'obtient pas l'autorisation de dépôt.

NOTE – L'annuaire ne tient pas à jour de classement des valeurs d'attribut. Généralement, on agira de manière efficace en considérant d'abord les valeurs de *correspondance des structures (Pattern-match)*, en commençant par les plus courtes, suivies par les valeurs *individuelles (Individual)*.

La procédure appropriée ci-dessous est appliquée à chaque valeur d'attribut:

- a) *Individual* (individuel)

L'entité OR-name du message est comparée à l'entité OR-name de cette valeur d'attribut au moyen de la procédure spécifiée au § A.3.1.2.

- b) *Member-of-dl* (membre de liste dl)

Cette valeur d'attribut est l'entité OR-name d'une liste DL. On obtient les membres MHS DL de cette liste DL. Si une entité OR-name de membre ou de composante d'entité OR-address manque, on l'obtient à partir de l'attribut d'entités OR-address de l'entrée d'annuaire du membre. L'entité OR-name du message est comparée avec chaque entité OR-name de membre, tour à tour, au moyen de la procédure spécifiée dans le § A.3.1.2, jusqu'à ce qu'il y ait correspondance.

A défaut de correspondance, une recherche dans l'annuaire est effectuée pour chaque entité OR-name de membre afin de déterminer si elle-même est une autre liste DL. On applique pour chaque liste DL imbriquée la procédure *Member-of-dl* (membre de liste dl) de manière récurrente.

- c) *Pattern-match* (correspondance de structure)

Cette valeur d'attribut contient des éléments d'entité OR-name; autrement dit, elle peut contenir certaines composantes d'entité OR-address, certaines composantes RDN d'un nom d'annuaire, ou les deux. Si la valeur de l'attribut est une structure d'entité OR-name vide, l'autorisation de dépôt est accordée à tout utilisateur.

Une entité OR-name ne contenant pas de types d'attribut qui sont absents de la structure est construite par rejet d'autres attributs d'entité OR-name du message. Le nom ainsi construit est comparé à l'entité OR-name type de cette valeur d'attribut au moyen de la procédure spécifiée dans la règle OR-name-elements-match du § 12.4.5 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

d) *Member-of-group* (membre de groupe)

Cette valeur d'attribut est le nom d'annuaire d'un groupe de noms (voir § 6.10 de l'ISO/CEI 9594-7). On détermine les membres de ce groupe de noms et l'on construit une entité OR-name pour chaque entité OR-address de chaque membre à partir du nom d'annuaire de ce membre et de l'attribut OR-addresses MHS de ce membre. L'entité OR-name du message est comparée tout à tour avec l'entité OR-name de chaque membre au moyen de la procédure spécifiée au § A.3.1.2, jusqu'à ce qu'il y ait correspondance.

En l'absence de correspondance, une recherche dans l'annuaire est effectuée pour le nom d'annuaire de chaque membre afin de déterminer si celui-ci est lui-même un groupe de noms. On applique la procédure *Member-of-group*, de manière récurrente, à chaque groupe de noms imbriqué qui est trouvé.

Quand un membre d'une liste DL ou un groupe dispose de plus d'une valeur dans l'attribut des entités OR-address de ce membre, une entité OR-name individuelle est construite pour chacune des entités OR-address.

### A.3.1.2 Procédure pour déterminer l'équivalence des entités OR-name

L'entité OR-name qui provient du message contient toujours une entité OR-address et peut également contenir un nom d'annuaire. L'entité OR-name provenant de l'attribut peut comprendre un nom d'annuaire ou une entité OR-address, voire les deux; l'entité OR-address sera présente si elle est également présente dans la valeur de l'attribut, mais elle peut également être obtenue de l'annuaire pour les membres d'une liste DL ou des groupes.

Les entités OR-name sont comparées à l'aide de la règle OR-name-match définie au § 12.4.4 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

### A.3.2 Politique des listes DL

La syntaxe d'attribut **DL Policy** caractérise l'attribut dont la valeur est une politique de liste DL.

```
DLPolicy ::= SET {
    report-propagation [0] INTEGER {
        previous-dl-or-originator (0),
        dl-owner (1),
        both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,
    report-from-dl [1] INTEGER {
        whenever-requested (0),
        when-no-propagation (1) } DEFAULT whenever-requested,
    originating-MTA-report [2] INTEGER {
        unchanged (0),
        report (2),
        non-delivery-report (3),
        audited-report (4) } DEFAULT unchanged,
    originator-report [3] INTEGER {
        unchanged (0),
        no-report (1),
        report (2),
        non-delivery-report (3) } DEFAULT unchanged,
    return-of-content [4] ENUMERATED {
        unchanged (0),
        content-return-not-requested (1),
        content-return-requested (2) } DEFAULT unchanged,
    priority [5] INTEGER {
        unchanged (0),
        normal (1),
        non-urgent (2),
        urgent (3) } DEFAULT unchanged,
    disclosure-of-other-recipients [6] ENUMERATED {
        unchanged (0),
        disclosure-of-other-recipients-prohibited (1),
        disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,
    implicit-conversion-prohibited [7] ENUMERATED {
        unchanged (0),
        implicit-conversion-allowed (1),
        implicit-conversion-prohibited (2) } DEFAULT unchanged,
    conversion-with-loss-prohibited [8] ENUMERATED {
        unchanged (0),
        conversion-with-loss-allowed (1),
        conversion-with-loss-prohibited (2) } DEFAULT unchanged,
    further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,
    originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,
    proof-of-delivery [11] INTEGER {
        dl-expansion-point (0),
        dl-members (1),
        both (2),
        neither (3) } DEFAULT dl-members,
    requested-delivery-method [12] CHOICE {
        unchanged [0] NULL,
```

```

        removed [1] NULL,
        replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,
token-encryption-algorithm-preference [13] SEQUENCE OF
        AlgorithmInformation OPTIONAL,
token-signature-algorithm-preference [14] SEQUENCE OF
        AlgorithmInformation OPTIONAL,
... }
AlgorithmInformation ::= SEQUENCE {
    algorithm-identifiant [0] AlgorithmIdentifier,
    originator-certificate-selector [1] CertificateAssertion OPTIONAL,
    recipient-certificate-selector [2] CertificateAssertion OPTIONAL}

```

Une politique de liste DL peut spécifier les valeurs correspondant aux options suivantes:

- a) *propagation des rapports*: si les rapports reçus au point de développement de liste DL doivent être envoyés à la liste DL précédente (ou en l'absence de celle-ci, à l'expéditeur), au propriétaire de la liste DL ou aux deux;
- b) *rapport émanant de la liste DL*: si le point de développement DL envoie un rapport confirmant la remise quand il développe un message qui en demande un, ou si de tels rapports sont envoyés uniquement quand la propagation du rapport relève du propriétaire de la liste DL ou quand le rapport originator-report a la valeur correspondant à "pas de rapport" ou "rapport de non-remise";
- c) *rapport de l'agent MTA de l'expéditeur*: si la demande de rapport de l'agent MTA est inchangée ou si elle a la valeur correspondant au rapport de remise et de non-remise, la valeur correspondant au rapport de non-remise seulement ou la valeur correspondant au rapport de remise contrôlé;
- d) *rapport de l'expéditeur*: si la demande de rapport de l'expéditeur est inchangée ou si elle a la valeur correspondant à pas de rapport, la valeur correspondant aux rapports de remise et de non-remise ou la valeur demandant uniquement les rapports de non-remise;
- e) *retour du contenu*: si la demande de l'expéditeur concernant le retour du contenu est inchangée ou si elle a la valeur correspondant à pas de demande de retour ou la valeur correspondant à retour avec les rapports de non-remise;
- f) *priorité*: si la valeur correspondant à la priorité de l'expéditeur est inchangée ou si elle a la valeur "normale", la valeur "non urgent" ou la valeur "urgent";
- g) *divulcation d'autres destinataires*: si le réglage de l'expéditeur est inchangé ou s'il a la valeur empêchant la divulgation ou la valeur permettant la divulgation;
- h) *conversion implicite interdite*: si le réglage de l'expéditeur est inchangé ou s'il a la valeur permettant la conversion implicite ou la valeur interdisant la conversion implicite;
- i) *conversion avec perte interdite*: si le réglage de l'expéditeur est inchangé ou s'il a la valeur permettant la conversion avec perte ou la valeur interdisant la conversion avec perte;
- j) *poursuite du développement de liste DL permise*: si le développement d'une liste DL imbriquée est autorisé ou interdit;
- k) *retrait de destinataire suppléant désigné par l'expéditeur*: si le destinataire suppléant désigné par l'expéditeur est inchangé ou annulé;
- l) *production de la preuve de remise*: si la preuve de remise, quand elle est demandée, est produite au point de développement de la liste DL, par les membres de la liste DL, par les deux ou n'est pas produite;
- m) *méthode de remise demandée*: si le réglage de l'expéditeur est inchangé, supprimé ou remplacé par une valeur donnée;
- n) *préférence d'algorithme de chiffrement de jeton*: cette option spécifie l'ordre de préférence des algorithmes de chiffrement asymétrique à utiliser pour rechiffrer les données correspondant à chaque membre de la liste DL dans un jeton, lorsque le message en cours de développement contient des données chiffrées dans un jeton pour le destinataire de la liste DL;
- o) *préférence d'algorithme de signature de jeton*: cette option spécifie l'ordre de préférence des algorithmes de signature à utiliser pour signer les données lorsque cela est nécessaire pour créer un nouveau jeton pour chaque membre de la liste DL, par exemple lorsque le message en cours de développement contient des données chiffrées dans un jeton de message pour le destinataire de la liste DL.

Les renseignements détaillés sur ces options de politique figurent au § 14.3.10 de la Rec. UIT-T X.411 | ISO/CEI 10021-4.

### A.3.3 Entité OR-address (OR-Address)

La syntaxe de l'entité OR-address est définie dans la Rec. UIT-T X.411 | ISO/CEI 10021-4 et sa sémantique au § 18 de la présente Spécification.

La valeur présentée d'une entité OR-address est égale à une valeur cible d'entité OR-address aux conditions spécifiées au § 18.4. Les règles de correspondance pour OR-address-match, OR-address-elements-match, OR-address-substring-elements-match et OR-name-single-elements-match sont définies aux § 12.4.1, 12.4.2, 12.4.3 et 12.4.7 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

### A.3.4 Adresse OR-address avec capacités

La syntaxe de l'attribut d'adresse OR-address avec capacités caractérise un attribut dont la valeur identifie la capacité de remise de chacune des entités OR-address de l'utilisateur. En cas de choix automatique parmi plusieurs adresses de capacités appropriées, la manière d'effectuer la sélection est du ressort local. En cas de choix manuel, la description peut contribuer à une meilleure sélection.

Cet attribut prend pour valeur une adresse OR-address avec capacités.

```
AddressCapabilities ::= SEQUENCE {
    description GeneralString,
    address ORAddress,
    capabilities SET OF Capability }
Capability ::= SET {
    content-types [0] SET OF ExtendedContentType OPTIONAL,
    maximum-content-length [1] ContentLength OPTIONAL,
    encoded-information-types-constraints [2] EncodedInformationTypesConstraints
                                                OPTIONAL,
    security-labels [3] SecurityContext OPTIONAL,
    ... }
```

La règle d'équivalence address-capabilities-match permet d'établir l'identité entre une valeur présentée et une valeur d'attribut d'adresse OR avec capacités. Cette règle de correspondance n'est utilisée que pour la maintenance de l'annuaire.

```
addressCapabilitiesMatch MATCHING-RULE ::= {
    SYNTAX AddressCapabilities
    ID id-mr-address-capabilities-match }
```

La règle renvoie la valeur *Vrai* si et seulement si:

- a) les éléments de description contiennent des chaînes équivalentes;
- b) les éléments d'adresse se correspondent selon la règle d'équivalence d'adresses définie au § 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5;
- c) les éléments de capacité contiennent des composantes identiques.

Compte tenu du caractère complexe de la composante de capacité, il n'est pas envisagé que l'annuaire puisse servir à déterminer si une quelconque valeur d'attribut satisfait à une prescription présentée en matière de capacité de remise. Il est donc prévu que toutes les valeurs d'attribut soient obtenues de l'annuaire et que l'évaluation soit effectuée par l'utilisateur (par exemple par l'agent MTA).

La règle d'équivalence capability-match permet d'établir l'identité entre une valeur présentée et une valeur d'attribut des classes de remise MHS. Cette règle d'équivalence n'est utilisée que pour la maintenance de l'annuaire.

```
capabilityMatch MATCHING-RULE ::= {
    SYNTAX Capability
    ID id-mr-capability-match }
```

La règle renvoie la valeur *Vrai* si et seulement si les capacités contiennent des composantes équivalentes.

### A.3.5 Entité OR-name (OR-Name)

La syntaxe de l'entité OR-name est définie dans la Rec. UIT-T X.411 | ISO/CEI 10021-4 et sa sémantique dans le § 17 de la présente Spécification.

## ISO/CEI 10021-2:2003 (F)

La règle de la correspondance exacte OR-name-exact-match détermine si les composantes nom de répertoire et entité OR-address d'une entité OR-name correspondent l'une à l'autre. Chacune des composantes doit correspondre si elle est présente soit dans la valeur proposée soit dans la valeur cible. Une valeur d'entité OR-name proposée est égale à une valeur d'entité OR-name cible si les composantes de l'entité OR-address sont équivalentes conformément aux règles spécifiées au § 18.4 et si les composantes du nom de répertoire sont équivalentes conformément aux règles spécifiées dans les Recommandations de la série X.500 | ISO/CEI 9594. Toutefois, la correspondance peut être déclarée sous d'autres conditions, selon l'application.

```
oRNameExactMatch MATCHING-RULE ::= {  
    SYNTAX      ORName  
    ID          id-mr-orname-exact-match }
```

La règle renvoie une valeur *Vrai* uniquement dans les conditions suivantes:

- si la valeur présentée ne contient qu'une adresse OR, la règle n'établit la correspondance qu'avec une valeur d'attribut sans nom de répertoire lorsque cette correspondance est conforme à la règle définie au § 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5;
- si la valeur présentée ne contient qu'un nom de répertoire, la règle n'établit la correspondance qu'avec une valeur d'attribut sans adresse OR, lorsque cette correspondance est conforme à la règle définie au § 12.5.2 de la Rec. UIT-T X.501 | ISO/CEI 9594-2;
- si la valeur présentée contient à la fois une adresse OR et un nom de répertoire, la règle n'établit la correspondance qu'avec une valeur d'attribut contenant ces deux composantes lorsque la correspondance de l'adresse OR est conforme à la règle définie au § 12.4.1 de la Rec. UIT-T X.413 | ISO/CEI 10021-5 et que la correspondance du nom de répertoire est conforme à la règle définie au § 12.5.2 de la Rec. UIT-T X.501 | ISO/CEI 9594-2.

NOTE – La règle de la correspondance exacte OR-name-exact-match ne nécessite pas de codage des valeurs proposée et cible.

Les règles de correspondance pour OR-name-match, OR-name-elements-match, OR-name-substring-elements-match et OR-name-single-elements-match sont définies aux § 12.4.4, 12.4.5, 12.4.6 et 12.4.7 de la Rec. UIT-T X.413 | ISO/CEI 10021-5.

## A.4 Contextes

Les contextes spécifiques à la messagerie sont spécifiés ci-dessous.

### A.4.1 Annotation d'administrateur de liste DL (DL-Administrator-Annotation)

Le contexte Annotation d'Administrateur de liste DL (DL-Administrator-Annotation) associe à une valeur de l'attribut des membres de liste DL une annotation textuelle affectée par, ou à utiliser par, l'administrateur de liste DL.

```
dl-administrator-annotation CONTEXT ::= {  
    WITH SYNTAX CHOICE{  
        bmpstring                BMPString,  
        universalstring          UniversalString}  
    ID id-con-dl-administrator-annotation }
```

Une valeur présentée est considérée comme correspondant à une valeur stockée si la valeur présentée est une sous-chaîne de la valeur stockée.

```
}  
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {  
    ATTRIBUTE TYPE                mhs-dl-members.&id OPTIONAL  
    CONTEXTS                      {dl-administrator-annotation} }
```

Une annotation textuelle peut être associée à chaque membre de la liste DL. Elle n'est utilisée que pour permettre à l'administrateur d'associer des informations au membre afin d'aider l'administrateur dans l'administration de la liste DL. Cela peut être utile, par exemple, lorsqu'un attribut des membres de liste DL du système MHS omet le composant Nom d'Annuaire et comprend seulement une adresse d'OR numérique.

#### A.4.2 Liste DL imbriquée dans liste DL (DL Nested DL)

Le contexte Liste DL imbriquée dans liste DL (DL Nested DL) associée à une valeur d'attribut des membres de liste DL du système MHS une indication selon laquelle ce membre est lui-même une liste DL.

```
dl-nested-dl CONTEXT ::= {
    WITH SYNTAX          NULL
    ID                   id-con-dl-nested-dl }

dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE      mhs-dl-members.&id OPTIONAL
    CONTEXTS           {dl-nested-dl} }
```

Lorsque ce contexte est associé à une valeur d'attribut des membres de liste DL du système MHS, il indique que ce membre est lui-même une liste DL (imbriquée). Ce contexte peut-être ajouté par un agent d'utilisateur d'annuaire (DUA) administratif pour faciliter l'évaluation efficace de l'option permission de dépôt de liste DL pour membre de liste DL.

#### A.4.3 Réinitialisation de l'expéditeur de la liste DL (DL-Reset-Originator)

Le contexte Réinitialisation de l'expéditeur de la liste DL (DL-Reset-Originator) associée à une valeur d'attribut des membres de la liste DL une indication selon laquelle ce membre utilise un, ou est atteint au travers d'un, système qui n'envoie pas de rapport de (non)-remise à la dernière liste DL identifiée dans l'Historique de Développement de liste (comme cela est requis pour la conformité à la Rec. UIT-T X.400 | ISO/CEI 10021).

```
dl-reset-originator CONTEXT ::= {
    WITH SYNTAX          NULL
    ID                   id-con-dl-reset-originator }

dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE      mhs-dl-members.&id
    OPTIONAL CONTEXTS  {dl-reset-originator} }
```

Lorsque ce contexte est associé à une valeur d'attribut des membres de liste DL du système MHS, si l'élément de rapport de propagation de la Politique de liste DL est (seulement) propriétaire de la liste DL, le point de développement de la liste DL remplace, dans l'enveloppe de la copie du message pour membre de la liste DL, l'expéditeur par le nom OR du propriétaire de la liste DL. Cela peut être utile lorsque, par exemple, ce membre de liste DL utilise un système conforme à la Rec. UIT-T X.400 (1984), ou un système utilisant un protocole de type autre que X.400 | ISO/CEI 10021.

### A.5 Variantes nominatives d'entité de certificat

Les autres formes nominatives propres à la messagerie, à utiliser le champ de variante nominative d'entité d'un certificat (voir le § 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8) sont spécifiées ci-dessous.

#### A.5.1 Nom d'agent de transfert de messages

La variante nominative du nom d'agent MTA d'une entité de certificat permet à une autorité de certification de délivrer des certificats attestant la conformité de l'association entre ce nom d'agent MTA et la clé publique.

```
mta-name OTHER-NAME ::= { SEQUENCE {
                                domain          GlobalDomainIdentifier,
                                mta-name        MTAName }
    IDENTIFIED BY      id-san-mta-name }
```

## Annexe B

## Définition de référence des identificateurs d'objets

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

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

Tous les identificateurs d'objets traités par la présente Spécification sont affectés dans la présente annexe, laquelle est définitive pour tous les identificateurs à l'exception de ceux des modules ASN.1 et du système MHS lui-même. L'affectation définitive des identificateurs de modules s'effectue dans les modules eux-mêmes; il y est fait référence dans les déclarations d'importation. L'identificateur du système MHS est fixe.

-----

```

MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0) object-identifiers(0)
                        version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Prologue

-- Export tout.

IMPORTS -- néant -- ;

ID ::= OBJECT IDENTIFIER

-- Eléments généraux relatifs au système MHS

id-mhs-protocols ID ::= {joint-iso-itu-t mhs(6) protocols (0)}
-- Contextes d'application et protocoles du système MHS
-- Voir Rec. UIT-T X.419 | ISO/CEI 10021-6.
id-ipms ID ::= {joint-iso-itu-t mhs(6) ipms (1)}
-- Messagerie de personne à personne
-- Voir Rec. UIT-T X.420 | ISO/CEI 10021-7.
-- La valeur {joint-iso-itu-t mhs(6) 2} n'est plus définie
id-mts ID ::= {joint-iso-itu-t mhs(6) mts (3)}
-- Système de transfert de message
-- Voir Rec. UIT-T X.411 | ISO/CEI 10021-4.
id-ms ID ::= {joint-iso-itu-t mhs(6) ms (4)}
-- Mémoire de messages
-- Voir Rec. UIT-T X.413 | ISO/CEI 10021-5.
id-arch ID ::= {joint-iso-itu-t mhs(6) arch (5)}
-- Architecture globale
-- Voir la présente Spécification.
id-group ID ::= {joint-iso-itu-t mhs(6) group (6)}
-- Réservé.
id-edims ID ::= {joint-iso-itu-t mhs(6) edims (7)}
-- Messagerie avec échange des données informatisé
-- Voir Rec. UIT-T X.435 | ISO/CEI 10021-9.
id-management ID ::= {joint-iso-itu-t mhs(6) management (9)}
-- Gestion MHS
-- Voir Recommandations UIT-T X.460 – X.467 | ISO/CEI 11588.
id-routing ID ::= {joint-iso-itu-t mhs(6) routing (10)}
-- Acheminement MHS
-- Voir Rec. UIT-T Rec. X.412 | ISO/CEI 10021-10.

-- Catégories

id-mod ID ::= {id-arch 0} -- modules; non définitive
id-oc ID ::= {id-arch 1} -- classes d'objets
id-at ID ::= {id-arch 2} -- types d'attribut
-- La valeur {id-arch 3} n'est plus définie
id-mr ID ::= {id-arch 4} -- règles de correspondance
id-con ID ::= {id-arch 5} -- contextes
id-san ID ::= {id-arch 6} -- variantes nominatives d'entité de certificat

```

*-- Modules*

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

*-- Classes d'objets*

```
id-oc-mhs-distribution-list      ID ::= {id-oc 0}
id-oc-mhs-message-store         ID ::= {id-oc 1}
id-oc-mhs-message-transfer-agent ID ::= {id-oc 2}
id-oc-mhs-user                  ID ::= {id-oc 3}
id-oc-mhs-user-agent            ID ::= {id-oc 4}
```

*-- Attributs*

```
id-at-mhs-maximum-content-length      ID ::= {id-at 0}
id-at-mhs-deliverable-content-types   ID ::= {id-at 1}
id-at-mhs-exclusively-acceptable-eits ID ::= {id-at 2}
id-at-mhs-dl-members                  ID ::= {id-at 3}
id-at-mhs-dl-submit-permissions       ID ::= {id-at 4}
id-at-mhs-message-store-dn           ID ::= {id-at 5}
id-at-mhs-or-addresses                ID ::= {id-at 6}
-- La valeur {id-at 7} n'est plus définie
id-at-mhs-supported-automatic-actions  ID ::= {id-at 8}
id-at-mhs-supported-content-types     ID ::= {id-at 9}
id-at-mhs-supported-attributes        ID ::= {id-at 10}
id-at-mhs-supported-matching-rules    ID ::= {id-at 11}
id-at-mhs-dl-archive-service          ID ::= {id-at 12}
id-at-mhs-dl-policy                   ID ::= {id-at 13}
id-at-mhs-dl-related-lists            ID ::= {id-at 14}
id-at-mhs-dl-subscription-service      ID ::= {id-at 15}
id-at-mhs-or-addresses-with-capabilities ID ::= {id-at 16}
id-at-mhs-acceptable-eits             ID ::= {id-at 17}
id-at-mhs-unacceptable-eits           ID ::= {id-at 18}
id-at-mhs-deliverable-classes         ID ::= {id-at 19}
id-at-encrypted-mhs-maximum-content-length ID ::= {id-at 0 2}
id-at-encrypted-mhs-deliverable-content-types ID ::= {id-at 1 2}
id-at-encrypted-mhs-exclusively-acceptable-eits ID ::= {id-at 2 2}
id-at-encrypted-mhs-dl-members        ID ::= {id-at 3 2}
id-at-encrypted-mhs-dl-submit-permissions ID ::= {id-at 4 2}
id-at-encrypted-mhs-message-store-dn  ID ::= {id-at 5 2}
id-at-encrypted-mhs-or-addresses      ID ::= {id-at 6 2}
id-at-encrypted-mhs-supported-automatic-actions ID ::= {id-at 8 2}
id-at-encrypted-mhs-supported-content-types ID ::= {id-at 9 2}
id-at-encrypted-mhs-supported-attributes ID ::= {id-at 10 2}
id-at-encrypted-mhs-supported-matching-rules ID ::= {id-at 11 2}
id-at-encrypted-mhs-dl-archive-service ID ::= {id-at 12 2}
id-at-encrypted-mhs-dl-policy         ID ::= {id-at 13 2}
id-at-encrypted-mhs-dl-related-lists  ID ::= {id-at 14 2}
id-at-encrypted-mhs-dl-subscription-service ID ::= {id-at 15 2}
id-at-encrypted-mhs-or-addresses-with-capabilities ID ::= {id-at 16 2}
id-at-encrypted-mhs-acceptable-eits   ID ::= {id-at 17 2}
id-at-encrypted-mhs-unacceptable-eits ID ::= {id-at 18 2}
id-at-encrypted-mhs-deliverable-classes ID ::= {id-at 19 2}
```

*-- Règles de correspondance*

```
id-mr-orname-exact-match          ID ::= {id-mr 0}
id-mr-address-capabilities-match  ID ::= {id-mr 1}
id-mr-capability-match            ID ::= {id-mr 2}
```

*-- Contextes*

```
id-con-dl-administrator-annotation  ID ::= {id-con 0}
id-con-dl-nested-dl                 ID ::= {id-con 1}
id-con-dl-reset-originator          ID ::= {id-con 2}
```

*-- Variantes nominatives d'entité de certificat*

```
id-san-mta-name                    ID ::= {id-san 0}
```

END -- fin du module MHSObjectIdentifiers

## Annexe C

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

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

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 propres à la messagerie. Elle utilise les classes d'objets informationnels OBJECT-CLASS et ATTRIBUTE de la Rec. UIT-T X.501 | ISO/CEI 9594-2.

-----

```
MHSDirectoryObjectsAndAttributes { joint-iso-itu-t mhs(6) arch(5) modules(0) directory(1)
    version-1999(1) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
-- Prologue
```

```
-- Exporte tout.
```

```
IMPORTS
```

```
-- Identificateurs d'objets du système MHS
```

```
id-at-mhs-acceptable-eits, id-at-mhs-deliverable-classes,
id-at-mhs-deliverable-content-types, id-at-mhs-dl-archive-service,
id-at-mhs-dl-members, id-at-mhs-dl-policy, id-at-mhs-dl-related-lists,
id-at-mhs-dl-submit-permissions, id-at-mhs-dl-subscription-service,
id-at-mhs-exclusively-acceptable-eits, id-at-mhs-maximum-content-length,
id-at-mhs-message-store-dn, id-at-mhs-or-addresses,
id-at-mhs-or-addresses-with-capabilities, id-at-mhs-supported-attributes,
id-at-mhs-supported-automatic-actions, id-at-mhs-supported-content-types,
id-at-mhs-supported-matching-rules, id-at-mhs-unacceptable-eits,
id-con-dl-administrator-annotation, id-con-dl-nested-dl, id-con-dl-reset-originator,
id-mr-address-capabilities-match, id-mr-capability-match, id-mr-orname-exact-match,
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, id-san-mta-name
```

```
----
FROM MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0)
    object-identifiers(0) version-1999(1) }
```

```
-- Service abstrait de transfert de message MTS
```

```
ContentLength, EncodedInformationTypesConstraints, ExtendedContentType,
ExtendedEncodedInformationType, GlobalDomainIdentifier, MTAName, ORAddress, ORName,
RequestedDeliveryMethod, SecurityContext
```

```
----
FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
    mts-abstract-service(1) version-1999(1) }
```

```
-- Service abstrait de mémoire de messages MS
```

```
ATTRIBUTE, AUTO-ACTION
```

```
----
FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
    abstract-service(1) version-1999(1) }
```

```
-- Types généraux d'attribut de mémoire de messages MS
```

```
AttributeTable
```

```
----
FROM MSGGeneralAttributeTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
    general-attribute-types(2) version-1999(1) }
```

*-- Types généraux d'action automatique de memoire de messages MS*

```

AutoActionTable
-----
FROM MSGGeneralAutoActionTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
    general-auto-action-types(3) version-1994(0) }

```

*-- Règles de correspondance*

```

MatchingRuleTable, oRAddressMatch, oRAddressElementsMatch,
oRAddressSubstringElementsMatch, oRNameMatch, oRNameElementsMatch,
oRNameSingleElementMatch, oRNameSubstringElementsMatch
-----
FROM MSMatchingRules { joint-iso-itu-t mhs(6) ms(4) modules(0)
    general-matching-rules(5) version-1999(1) }

```

*-- Cadre général d'information*

```

ATTRIBUTE, CONTEXT, distinguishedNameMatch, DIT-CONTEXT-USE-RULE,
objectIdentifierMatch, MATCHING-RULE, Name, OBJECT-CLASS, top
-----
FROM InformationFramework { joint-iso-itu-t ds(5) module(1)
    informationFramework(1) 3 }

```

*-- Classes d'objets sélectionnées*

```

applicationEntity
-----
FROM SelectedObjectClasses { joint-iso-itu-t ds(5) module(1)
    selectedObjectClasses(6) 3 }

```

*-- Types d'attributs sélectionnés*

```

commonName, description, distinguishedName, integerMatch, organizationName,
organizationalUnitName, owner, protocolInformation, seeAlso
-----
FROM SelectedAttributeTypes { joint-iso-itu-t ds(5) module(1)
    selectedAttributeTypes(5) 3 }

```

*-- Cadre général d'authentification*

```

AlgorithmIdentifier
-----
FROM AuthenticationFramework { joint-iso-itu-t ds(5) module(1)
    authenticationFramework(7) 3 }

```

*-- Extensions de certificat*

```

CertificateAssertion, OTHER-NAME
-----
FROM CertificateExtensions { joint-iso-itu-t ds(5) module(1)
    certificateExtensions(26) 0 };

```

*-- CLASSES D'OBJETS**-- Liste de distribution du système de messagerie MHS*

```

mhs-distribution-list OBJECT-CLASS ::= {
    SUBCLASS OF { top }
    MUST CONTAIN { commonName |
        mhs-dl-submit-permissions |
        mhs-or-addresses }
    MAY CONTAIN { description |
        organizationName |
        organizationalUnitName |
        owner |
        seeAlso |
        mhs-maximum-content-length |
        mhs-deliverable-content-types |
        mhs-acceptable-eits |
        mhs-exclusively-acceptable-eits |
        mhs-unacceptable-eits |
        mhs-dl-policy |
        mhs-dl-subscription-service |

```

```

        mhs-dl-archive-service |
        mhs-dl-related-lists |
        mhs-dl-members }
ID      id-oc-mhs-distribution-list }

```

-- Mémoire du système de messagerie MHS

```

mhs-message-store OBJECT-CLASS ::= {
  SUBCLASS OF { applicationEntity }
  MAY CONTAIN { owner |
               mhs-supported-attributes |
               mhs-supported-automatic-actions |
               mhs-supported-matching-rules |
               mhs-supported-content-types |
               protocolInformation }
  ID          id-oc-mhs-message-store }

```

-- Agent de transfert de message MHS

```

mhs-message-transfer-agent OBJECT-CLASS ::= {
  SUBCLASS OF { applicationEntity }
  MAY CONTAIN { owner |
               mhs-maximum-content-length |
               protocolInformation }
  ID          id-oc-mhs-message-transfer-agent }

```

-- Utilisateur MHS

```

mhs-user OBJECT-CLASS ::= {
  SUBCLASS OF { top }
  KIND        auxiliary
  MUST CONTAIN { mhs-or-addresses }
  MAY CONTAIN { mhs-maximum-content-length |
               mhs-deliverable-content-types |
               mhs-acceptable-eits |
               mhs-exclusively-acceptable-eits |
               mhs-unacceptable-eits |
               mhs-or-addresses-with-capabilities |
               mhs-message-store-dn }
  ID          id-oc-mhs-user }

```

-- Agent d'utilisateur MHS

```

mhs-user-agent OBJECT-CLASS ::= {
  SUBCLASS OF { applicationEntity }
  MAY CONTAIN { owner |
               mhs-maximum-content-length |
               mhs-deliverable-content-types |
               mhs-acceptable-eits |
               mhs-exclusively-acceptable-eits |
               mhs-unacceptable-eits |
               mhs-deliverable-classes |
               mhs-or-addresses |
               protocolInformation }
  ID          id-oc-mhs-user-agent }

```

-- ATTRIBUTS

-- Types d'informations codées acceptables dans le système MHS

```

mhs-acceptable-eits ATTRIBUTE ::= {
  WITH SYNTAX      ExtendedEncodedInformationType
  EQUALITY MATCHING RULE objectIdentifierMatch
  ID              id-at-mhs-acceptable-eits }

```

-- Classes pouvant être remises dans le système MHS

```

mhs-deliverable-classes ATTRIBUTE ::= {
  WITH SYNTAX      Capability
  EQUALITY MATCHING RULE capabilityMatch
  ID              id-at-mhs-deliverable-classes }

```

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

```
mhs-deliverable-content-types ATTRIBUTE ::= {
  WITH SYNTAX          ExtendedContentType
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                    id-at-mhs-deliverable-content-types }
```

-- Service d'archives de liste de distribution DL dans le système MHS

```
mhs-dl-archive-service ATTRIBUTE ::= {
  WITH SYNTAX          ORName
  EQUALITY MATCHING RULE  ORNameExactMatch
  -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
  --                           ORNameSubstringElementsMatch | ORNameSingleElementMatch }--
  ID                    id-at-mhs-dl-archive-service }
```

-- Membres de liste de distribution DL dans le système MHS

```
mhs-dl-members ATTRIBUTE ::= {
  WITH SYNTAX          ORName
  EQUALITY MATCHING RULE  ORNameExactMatch
  -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
  --                           ORNameSubstringElementsMatch | ORNameSingleElementMatch }--
  ID                    id-at-mhs-dl-members }
```

-- Politique de liste de distribution DL dans le système MHS

```
mhs-dl-policy ATTRIBUTE ::= {
  WITH SYNTAX          DLPolicy
  SINGLE VALUE         TRUE
  ID                    id-at-mhs-dl-policy }
```

-- Listes liées à la liste de distribution DL dans le système MHS

```
mhs-dl-related-lists ATTRIBUTE ::= {
  SUBTYPE OF          distinguishedName
  EQUALITY MATCHING RULE  distinguishedNameMatch
  ID                    id-at-mhs-dl-related-lists }
```

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

```
mhs-dl-submit-permissions ATTRIBUTE ::= {
  WITH SYNTAX          DLSubmitPermission
  ID                    id-at-mhs-dl-submit-permissions }
```

-- Service d'abonnement à la liste DL dans le système MHS

```
mhs-dl-subscription-service ATTRIBUTE ::= {
  WITH SYNTAX          ORName
  EQUALITY MATCHING RULE  ORNameExactMatch
  -- EXTENSIBLE MATCHING RULE { ORNameMatch | ORNameElementsMatch |
  --                           ORNameSubstringElementsMatch | ORNameSingleElementMatch }--
  ID                    id-at-mhs-dl-subscription-service }
```

-- Types d'informations codées exclusivement acceptables dans le système MHS

```
mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
  WITH SYNTAX          ExtendedEncodedInformationType
  EQUALITY MATCHING RULE  objectIdentifierMatch
  ID                    id-at-mhs-exclusively-acceptable-eits }
```

-- Longueur maximale du contenu dans le système MHS

```
mhs-maximum-content-length ATTRIBUTE ::= {
  WITH SYNTAX          ContentLength
  EQUALITY MATCHING RULE  integerMatch
  SINGLE VALUE         TRUE
  ID                    id-at-mhs-maximum-content-length }
```

-- Nom d'annuaire de mémoire de messages dans le système MHS

```
mhs-message-store-dn ATTRIBUTE ::= {
    SUBTYPE OF          distinguishedName
    EQUALITY MATCHING RULE distinguishedNameMatch
    SINGLE VALUE
    ID                  id-at-mhs-message-store-dn }
```

-- Adresses OR dans le système MHS

```
mhs-or-addresses ATTRIBUTE ::= {
    WITH SYNTAX          ORAddress
    EQUALITY MATCHING RULE oRAddressMatch
    -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch | oRNameSingleElementMatch |
    --                          oRAddressSubstringElementsMatch } --
    ID                  id-at-mhs-or-addresses }
```

-- Adresses OR avec capacités dans le système MHS

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
    WITH SYNTAX          AddressCapabilities
    EQUALITY MATCHING RULE addressCapabilitiesMatch
    ID                  id-at-mhs-or-addresses-with-capabilities }
```

-- Attributs pris en charge par le système MHS

```
mhs-supported-attributes ATTRIBUTE ::= {
    WITH SYNTAX          ATTRIBUTE.&id({AttributeTable})
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                  id-at-mhs-supported-attributes
}
```

-- Actions automatiques prises en charge par le système MHS

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
    WITH SYNTAX          AUTO-ACTION.&id ({AutoActionTable})
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                  id-at-mhs-supported-automatic-actions }
```

-- Types de contenu pris en charge par le système MHS

```
mhs-supported-content-types ATTRIBUTE ::= {
    WITH SYNTAX          ExtendedContentType
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                  id-at-mhs-supported-content-types }
```

-- Règles de correspondance prises en charge par le système MHS

```
mhs-supported-matching-rules ATTRIBUTE ::= {
    WITH SYNTAX          MATCHING-RULE.&id ({MatchingRuleTable})
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                  id-at-mhs-supported-matching-rules }
```

-- Types d'informations codées inacceptables

```
mhs-unacceptable-eits ATTRIBUTE ::= {
    WITH SYNTAX          ExtendedEncodedInformationType
    EQUALITY MATCHING RULE objectIdentifierMatch
    ID                  id-at-mhs-unacceptable-eits }
```

-- SYNTAXES D'ATTRIBUTS

-- Autorisation de dépôt de liste de distribution DL

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

ORNamePattern ::= ORName

any-user-may-submit DLSubmitPermission ::= pattern-match: { built-in-standard-attributes { } }

*-- Politique de liste de distribution DL*

DLPolicy ::= SET {  
 report-propagation [0] INTEGER {  
   previous-dl-or-originator (0),  
   dl-owner (1),  
   both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,  
 report-from-dl [1] INTEGER {  
   whenever-requested (0),  
   when-no-propagation (1) } DEFAULT whenever-requested,  
 originating-MTA-report [2] INTEGER {  
   unchanged (0),  
   report (2),  
   non-delivery-report (3),  
   audited-report (4) } DEFAULT unchanged,  
 originator-report [3] INTEGER {  
   unchanged (0),  
   no-report (1),  
   report (2),  
   non-delivery-report (3) } DEFAULT unchanged,  
 return-of-content [4] ENUMERATED {  
   unchanged (0),  
   content-return-not-requested (1),  
   content-return-requested (2) } DEFAULT unchanged,  
 priority [5] INTEGER {  
   unchanged (0),  
   normal (1),  
   non-urgent (2),  
   urgent (3) } DEFAULT unchanged,  
 disclosure-of-other-recipients [6] ENUMERATED {  
   unchanged (0),  
   disclosure-of-other-recipients-prohibited (1),  
   disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,  
 implicit-conversion-prohibited [7] ENUMERATED {  
   unchanged (0),  
   implicit-conversion-allowed (1),  
   implicit-conversion-prohibited (2) } DEFAULT unchanged,  
 conversion-with-loss-prohibited [8] ENUMERATED {  
   unchanged (0),  
   conversion-with-loss-allowed (1),  
   conversion-with-loss-prohibited (2) } DEFAULT unchanged,  
 further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,  
 originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,  
 proof-of-delivery [11] INTEGER {  
   dl-expansion-point (0),  
   dl-members (1),  
   both (2),  
   neither (3) } DEFAULT dl-members,  
 requested-delivery-method [12] CHOICE {  
   unchanged [0] NULL,  
   removed [1] NULL,  
   replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,  
 token-encryption-algorithm-preference [13] SEQUENCE OF AlgorithmInformation OPTIONAL,  
 token-signature-algorithm-preference [14] SEQUENCE OF AlgorithmInformation OPTIONAL,  
 ... }

AlgorithmInformation ::= SEQUENCE {  
 algorithm-identifier [0] AlgorithmIdentifier,  
 originator-certificate-selector [1] CertificateAssertion OPTIONAL,  
 recipient-certificate-selector [2] CertificateAssertion OPTIONAL}

*-- Adresses OR avec capacités*

AddressCapabilities ::= SEQUENCE {  
 description GeneralString OPTIONAL,  
 address ORAddress,  
 capabilities SET OF Capability }

Capability ::= SET {  
 content-types [0] SET OF ExtendedContentType OPTIONAL,  
 maximum-content-length [1] ContentLength OPTIONAL,  
 encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,  
 security-labels [3] SecurityContext OPTIONAL,  
 ... }

-- RÈGLES DE CORRESPONDANCE

-- Correspondance d'adresse OR avec capacités

```
addressCapabilitiesMatch MATCHING-RULE ::= {
    SYNTAX    AddressCapabilities
    ID        id-mr-address-capabilities-match }
```

-- Correspondance de capacités

```
capabilityMatch MATCHING-RULE ::= {
    SYNTAX    Capability
    ID        id-mr-capability-match }
```

-- Correspondance exacte de nom OR

```
ORNameExactMatch MATCHING-RULE ::= {
    SYNTAX    ORName
    ID        id-mr-orname-exact-match }
```

-- CONTEXTES

-- Annotation d'Administrateur de liste DL

```
dl-administrator-annotation CONTEXT ::= {
    WITH SYNTAX CHOICE{
        bmpstring      BMPString,
        universalstring UniversalString}
    ID id-con-dl-administrator-annotation
}
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE          mhs-dl-members.&id OPTIONAL
    CONTEXTS                {dl-administrator-annotation} }
```

-- Liste DL imbriquée dans la liste DL

```
dl-nested-dl CONTEXT ::= {
    WITH SYNTAX          NULL
    ID                   id-con-dl-nested-dl }
dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE          mhs-dl-members.&id OPTIONAL
    CONTEXTS                {dl-nested-dl} }
```

-- Réinitialisation de l'expéditeur de la liste DL

```
dl-reset-originator CONTEXT ::= {
    WITH SYNTAX          NULL
    ID                   id-con-dl-reset-originator }
dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {
    ATTRIBUTE TYPE          mhs-dl-members.&id
    OPTIONAL CONTEXTS      {dl-reset-originator} }
```

-- VARIANTES NOMINATIVES D'ENTITÉ DE CERTIFICAT

-- Nom d'agent de transfert de message MTA

```
mta-name OTHER-NAME ::= { SEQUENCE {
                                domain      GlobalDomainIdentifier,
                                mta-name    MTAName }
    IDENTIFIED BY id-san-mta-name }
```

END -- fin du module MHSDirectory

## Annexe D

### Menaces concernant la sécurité

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

Un aperçu général des risques auxquels le système MHS est exposé est donné au § 15.1 de la Rec. UIT-T X.400 | ISO/CEI 10021-1, où sont examinés les risques rencontrés dans un système MHS à différents niveaux: à l'accès, entre les messages, à l'intérieur même des messages et dans la mémoire de message. Ces risques peuvent prendre les différentes formes suivantes:

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

En outre, ces incidents peuvent survenir par accident ou être causés dans une intention malveillante et peuvent être actifs ou passifs. Les tentatives d'agression visant ce système MHS seront dirigées sur ses éventuels points faibles et pourront 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 indique comment ces risques peuvent être évités à l'aide des services de sécurité du système MHS. La liste des risques présentée ici est donnée à titre indicatif et n'est pas définitive.

#### D.1 Usurpation d'identité

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

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

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

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

#### D.2 Mise en séquence d'un message

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

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

- a) réexécution de messages;
- b) réarrangement de messages;
- c) exécution anticipée de messages;
- d) retard de messages.

Tableau D.1 – Utilisation des services de sécurité du système MHS

RISQUE	SERVICES
<b>USURPATION D'IDENTITÉ</b>	
Usurpation d'identité et usage abusif du système MTS	Authentification de l'origine du message Authentification de l'origine de l'envoi-test Gestion de la sécurité de l'accès Preuve de la remise
Accusé de réception mensonger Prétendue expédition d'un message	Authentification de l'origine du message
Usurpation de l'identité d'un agent MTA vis-à-vis d'un utilisateur du système MTS	Preuve du dépôt Authentification de l'origine du rapport Gestion de la sécurité de l'accès
Usurpation de l'identité d'un agent MTA vis-à-vis d'un autre agent MTA	Authentification de l'origine du rapport Gestion de la sécurité de l'accès
<b>MISE EN SÉQUENCE DES MESSAGES</b>	
Réexécution des messages Réarrangement de messages Exécution anticipée de messages Retard de messages	Intégrité de la séquence du message Intégrité de la séquence du message
<b>MODIFICATION DES INFORMATIONS</b>	
Modification de messages	Intégrité de la connexion Intégrité du contenu Intégrité de la séquence du message
Destruction de messages Modification de l'information d'acheminement ou d'une autre information de gestion	
<b>REFUS DE SERVICE</b>	
Refus de communications Adressage sous forme avalanche d'un agent MTA Adressage sous forme avalanche du système MTS	
<b>RÉPUDIATION</b>	
Refus d'origine Refus de dépôt Refus de remise	Non-répudiation d'origine Non-répudiation de dépôt Non-répudiation de remise
<b>FUITE D'INFORMATIONS</b>	
Perte de confidentialité	Confidentialité de la connexion Confidentialité du contenu Confidentialité du cheminement du message
Perte d'anonymat Détournement de messages Analyse du trafic	Gestion de la sécurité de l'accès Confidentialité du cheminement du message
<b>AUTRES RISQUES</b>	
Expéditeur non autorisé pour l'Étiquette de sécurité de Message Agent MTA/utilisateur MTS non autorisé pour le contexte de sécurité Acheminement erroné	Gestion de la sécurité de l'accès Étiquetage de sécurité de message Gestion de la sécurité de l'accès
Politiques d'étiquetage différentes	Gestion de la sécurité de l'accès Étiquetage de sécurité de message

### D.3 Modification des informations

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

Les risques de modification des informations sont les suivants:

- a) modification de messages;
- b) destruction de messages;
- c) modification des informations d'acheminement ou d'autres informations de gestion.

#### D.4 Refus de service

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

Les risques de refus de service sont les suivants:

- a) refus de communications;
- b) défaillance d'un agent MTA;
- c) inondation du système MTS.

#### D.5 Répudiation

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

Les risques de répudiation sont les suivants:

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

#### D.6 Fuite d'informations

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

Les risques de fuite d'informations sont les suivants:

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

#### D.7 Autres risques

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

Les risques visés dans ce paragraphe sont les suivants:

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

## Annexe E

## Prestation de services de sécurité décrits dans la Rec. UIT-T X.411 | ISO/CEI 10021-4

(Cette annexe fait partie intégrante de la présente Recommandation | Norme internationale)

Le Tableau E.1 indique les éléments de service tirés de la Rec. UIT-T X.411 | ISO/CEI 10021-4 qui peuvent être utilisés pour assurer les services de sécurité décrits au § 10.2.

Tableau E.1 – Prestation des services de sécurité dans le système MHS

SERVICE	ARGUMENTS/SERVICES DU SYSTÈME MTS
+-- SERVICES DE SÉCURITÉ D'AUTHENTIFICATION DE L'ORIGINE -----	
Authentification de l'origine du message	Contrôle d'authentification de l'origine du message Jeton de message
Authentification de l'origine de l'envoi-test	Contrôle d'authentification de l'origine de l'envoi-test
Authentification de l'origine du rapport	Contrôle d'authentification de l'origine du rapport
Demande de preuve du dépôt	Demande de preuve du dépôt
Preuve de remise	Preuve du dépôt Demande de preuve de la remise Preuve de la remise
+-- SERVICES DE SÉCURITÉ DE GESTION DE LA SÉCURITÉ DE L'ACCÈS -----	
Authentification de l'entité homologue	Pouvoirs du demandeur Pouvoirs du demandé
Contexte de sécurité	Contexte de sécurité
+-- SERVICES DE SÉCURITÉ DE CONFIDENTIALITÉ DES DONNÉES -----	
Confidentialité de la connexion	Non assurée
Confidentialité du contenu	Identificateur de l'algorithme de confidentialité du contenu Jeton de message
Confidentialité du cheminement du message	Type de contenu
+-- SERVICES DE SÉCURITÉ D'INTÉGRITÉ DES DONNÉES -----	
Intégrité de la connexion	Non assurée
Intégrité du contenu	Contrôle d'intégrité du contenu Jeton de message
Intégrité de la séquence du message	Contrôle d'authentification de l'origine du message Numéro de séquence de message Jeton de message
+-- SERVICES DE SÉCURITÉ DE NON-RÉPUDIATION -----	
Non-répudiation d'origine	Contrôle d'intégrité du contenu Jeton de message
Non-répudiation de dépôt	Contrôle d'authentification de l'origine du message Demande de preuve du dépôt Preuve du dépôt
Non-répudiation de remise	Preuve de la demande de remise Preuve de la remise
Etiquetage de sécurité du message	Etiquette de sécurité du message Jeton de message Contrôle d'authentification de l'origine du message
+-- SERVICES DE SÉCURITÉ DE GESTION DE LA SÉCURITÉ -----	
Modification des pouvoirs	Modification des pouvoirs
Enregistrement	Enregistrement

## Annexe F

### Représentation des entités OR-address pour l'utilisateur

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

Le texte qui suit est l'Annexe B/F.401; il ne fait pas partie de la Recommandation UIT-T.

#### F.1 Objet

L'entité OR-address (spécifiée au § 18) est constituée d'une série de valeurs d'attributs de la liste du Tableau F.1. Pour représenter visuellement une adresse à l'intention de l'utilisateur et pour lui permettre d'introduire l'adresse dans une interface d'utilisateur, chaque valeur d'attribut doit être associée avec le type d'attribut correct. Beaucoup de noms des types d'attribut représentés dans le Tableau F.1 sont trop longs pour en faire une utilisation pratique sur papier ou sur un écran. Aussi faut-il un format permettant de représenter des attributs de manière concise, comme c'est le cas, par exemple, sur une carte de visite.

La présente annexe spécifie la manière dont les adresses peuvent être énoncées de manière concise au moyen d'étiquettes représentant les types d'attribut. Il y a trois catégories d'attribut: les attributs mnémotechniques standard, qui sont le plus susceptible d'être trouvés dans les entités OR-address dans leur représentation pour l'utilisateur (par exemple sur une carte de visite), ceux utilisés dans les adresses de remise physique, et d'autres attributs spécialisés (y compris les attributs définis par le domaine). Pour obtenir un format qui soit aussi concis que possible, beaucoup d'étiquettes sont formées d'un caractère unique. Cela les rend par ailleurs moins dépendantes de la langue.

Le § F.3 spécifie le format de représentation des adresses et le § F.4 spécifie les caractéristiques que devront présenter les interfaces d'utilisateur qui seront utilisées avec ce format.

#### F.2 Domaine d'application

Un format étiqueté pour la communication des entités OR-address aux utilisateurs a été spécifié. Le format est constitué d'une série de paires d'étiquettes et de valeurs d'attributs. Les caractéristiques que doit présenter une interface d'utilisateur pour accepter les adresses ayant ce format ont également été spécifiées.

Par ailleurs, on a spécifié un format explicite pouvant être utilisé quand il y a davantage d'espace, par exemple dans les documents imprimés et dans l'interface d'utilisateur.

#### F.3 Format

##### F.3.1 Généralités

Le but du format étiqueté est de permettre aux entités OR-address d'être représentées sous une forme concise qui peut être transcrite de manière exacte par les utilisateurs. Cela peut être fait en choisissant avec soin les attributs et les valeurs utilisés pour former une entité OR-address.

Si les attributs d'une entité OR-address comportent des caractères provenant d'un jeu de caractères étendu, les utilisateurs qui n'utilisent normalement pas le jeu en question peuvent avoir des difficultés à écrire l'entité OR-address ou à l'entrer dans leur système de messagerie. Dans une telle situation, il y a lieu de fournir un pseudonyme formé de caractères sous forme de chaînes imprimables.

NOTE 1 – La politique de structuration des entités OR-address doit être examinée avec soin. Les entités OR-address individuelles doivent être attribuées au sein d'une division appropriée de l'espace d'adresse afin de ramener à un niveau acceptable la probabilité que deux utilisateurs aient la même entité OR-address. Généralement, le prénom ou les initiales suffisent pour faire la distinction entre les utilisateurs. Il ne serait guère approprié de faire apparaître une granularité excessive dans les nom-unité-organisation, surtout si la structure de l'organisation est sujette à de fréquents changements ou si les utilisateurs se déplacent entre les unités de l'organisation.

NOTE 2 – Il peut y avoir incompatibilité entre les avantages que présente l'utilisation de valeurs longues pour les attributs explicites (le nom complet d'une organisation, par exemple) et ceux que présentent les valeurs plus courtes (le format destiné aux cartes de visite, par exemple). On peut remédier à ce problème en fournissant une valeur d'attribut courte (telle que les initiales de l'organisation) en tant que variante de la valeur longue.

NOTE 3 – Pour les utilisateurs ayant des doutes au sujet des espaces dans une valeur d'attribut (surtout en caractères composés), on peut proposer des variantes avec et sans espace (par exemple "SNOMAIL400" comme variante de "SNOMAIL 400" et "Mac Donald" comme variante de "MacDonald").

NOTE 4 – S'il existe, pour une entité OR-address, une variante courte et une variante longue (la variante préférée), cette dernière sera de préférence produite pour tous les messages émanant de l'utilisateur.

Quand il est possible, au plan national, d'utiliser un espace unique comme valeur pour le nom-domaine-administration de l'adresse, cet espace est représenté dans l'adresse soit par omission de l'attribut nom-domaine-administration, soit par représentation de l'attribut nom-domaine-administration sans valeur ou avec la valeur d'un espace. La valeur "XX" d'un nom de pays (country-name) peut être représentée dans une adresse par omission de l'attribut nom de pays (country-name).

### F.3.2 Format étiqueté

#### F.3.2.1 Syntaxe

Les entités OR-address au format étiqueté sont constituées de paires délimitées d'étiquettes et de valeurs de la syntaxe <label> "=" <value>. Les étiquettes correspondant à chaque attribut sont spécifiées dans les Tableaux F.1, F.2 et F.3 (les attributs de remise physique du Tableau F.2 sont inclus pour des raisons d'exhaustivité). L'étiquette et sa valeur sont séparées soit par le caractère "=", soit par l'espace entre les deux colonnes d'un tableau. Les étiquettes peuvent être représentées en minuscules ou en majuscules, mais ces dernières sont recommandées étant donné leur plus grande clarté.

Si des paires d'étiquettes/valeurs apparaissent en séquence sur une ligne, elles sont séparées par des délimiteurs. Ceux-ci peuvent être facultativement suivis d'un ou de plusieurs espaces. Le caractère délimiteur peut être ";" ou "/", mais un seul des deux peut être utilisé dans une même entité OR-address. Quand le délimiteur est "/", la première étiquette a le préfixe "/". L'utilisation d'un délimiteur à la fin de la ligne est facultative. Si la valeur d'un attribut quelconque contient un caractère délimiteur, celui-ci doit être représenté par une paire de caractères délimiteurs.

Si un identificateur est nécessaire comme préface à l'adresse étiquetée, il est recommandé d'utiliser "X.400".

Si une adresse est entièrement composée d'attributs contenus dans le Tableau F.1, il est recommandé d'utiliser la séquence d'attributs d'adresse donnée dans le Tableau F.1. Si cette séquence est incompatible avec des habitudes locales, on peut adopter une autre séquence qui sera essentiellement utilisée dans le cadre de ces habitudes.

**Tableau F.1 – Attributs normalisés de la forme adresse mnémorique**

Type d'attribut	Défini au paragraphe	Abréviation (si nécessaire)	Etiquette
Prénom	18.3.12	Prénom	G
Initiales	18.3.12	Initiales	I
Nom de famille	18.3.12	Nom	S
Qualificateur de génération	18.3.12	Génération	Q
Nom courant	18.3.2	Nom courant	CN
Organisation	18.3.9	Organisation	O
Unité 1 d'organisation	18.3.10	Unité org.1	OU1
Unité 2 d'organisation	18.3.10	Unité org.2	OU2
Unité 3 d'organisation	18.3.10	Unité org.3	OU3
Unité 4 d'organisation	18.3.10	Unité org.4	OU4
Nom de domaine privé	18.3.21	PRMD	P
Nom de domaine d'administration	18.3.1	ADMD	A
Pays	18.3.3	Pays	C

Tableau F.2 – Attributs de remise physique

Type d'attribut	Défini au paragraphe	Abréviation (si nécessaire)	Etiquette
Nom personnel de remise physique	18.3.17	Personne PD	PD-PN
Composants d'entité OR-address – Extension postale	18.3.4	Extension adr. PD	PD-EA
Développement de composants d'adresse de remise physique	18.3.5	Dévl. adr. PD	PD-ED
Numéro du bureau de remise physique	18.3.15	Numéro bureau PD	PD-OFN
Nom du bureau de remise physique	18.3.14	Nom bureau PD	PD-OF
Nom de l'organisation de remise physique	18.3.16	Organisation PD	PD-O
Adresse-rue	18.3.22	Rue PD	PD-S
Adresse postale non formatée	18.3.25	Adresse PD	PD-A1 PD-A2 PD-A3 PD-A4 PD-A5 PD-A6
(il y a des étiquettes individuelles pour chaque ligne de l'adresse)			
Nom postal unique	18.3.26	PD unique	PD-U
Attributs postaux locaux	18.3.6	PD local	PD-L
Adresse poste restante	18.3.20	PD restante	PD-R
Adresse de case postale	18.3.18	Boîte PD	PD-B
Code postal	18.3.19	Code PD	PD-PC
Nom du service de remise physique	18.3.11	Service PD	PD-SN
Nom du pays de remise physique	18.3.13	Pays PD	PD-C

Tableau F.3 – Autres attributs

Type d'attribut	Défini au paragraphe	Abréviation (si nécessaire)	Etiquette
Adresse réseau X.121	18.3.7	X.121	X.121
Adresse réseau E.164	18.3.7	RNIS	RNIS
Adresse réseau PSAP	18.3.7	PSAP	PSAP
Identificateur numérique d'utilisateur	18.3.8	N-ID	N-ID
Identificateur de terminal	18.3.23	T-ID	T-ID
Type de terminal	18.3.24	T-TY	T-TY
Attribut défini par le domaine	18.1	DDA:<type>	DDA:<type>

Où la notation <type> identifie le type d'attribut défini par le domaine.

## EXEMPLE

X.400: G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

L'adresse ci-dessus peut également être écrite sous forme de tableau:

```
G John
S Smith
O A Bank Ltd
P ABL
A Snomail
C AQ
```

## F.3.2.2 Type de terminal

Six types de terminal sont actuellement définis au § 18.3.24 et si l'homogénéité internationale est requise, les abréviations spécifiques suivantes devront être utilisées pour représenter les valeurs correspondant à ces types: tlx, ttx, g3fax, g4fax, ia5 et vtx.

## F.3.2.3 Attribut défini par le domaine

L'étiquette d'un attribut défini par le domaine consiste en "DDA:" suivi du type d'attribut défini par le domaine. Si une adresse comporte plus d'un attribut défini par le domaine de même type, on part de l'hypothèse que les attributs définis par le domaine sont prévus d'être traités dans l'ordre où ils sont représentés.

EXEMPLE

DDA:RFC-822=fred(a)widget.co.uk; O=gateway; P=abc; C=gb

Si le type de l'attribut défini par le domaine comporte le caractère "=", il est représenté par "\=". Si le type d'un attribut défini par le domaine comporte le caractère "\", il est représenté par "\\\". Aucune représentation spéciale n'est requise si le type d'un attribut défini par le domaine inclut le caractère délimiteur ";" ou "/".

**F.3.3 Format explicite**

Le format explicite peut être utilisé quand l'espace disponible est suffisant. Il est constitué d'une liste des types d'attribut, représentés in extenso ou par des abréviations. Les types d'attributs ou abréviations peuvent être exprimés dans n'importe quelle langue, mais doivent être suivis de l'étiquette spécifiée dans le Tableau F.1, F.2 ou F.3. Si l'on utilise les abréviations anglaises, il y a lieu d'utiliser celles données dans les Tableaux F.1, F.2 et F.3.

Si une adresse est entièrement composée d'attributs figurant dans le Tableau F.1, il est recommandé que les séquences d'attributs soient celles qui sont données dans le Tableau F.1. Si la séquence est incompatible avec les habitudes locales, on peut utiliser une autre séquence qui sera essentiellement utilisée dans le cadre de ces habitudes.

EXEMPLE 1 – Utilisation des types d'attribut en langue norvégienne:

Fornavn (G)	Per
Etternavn (S)	Hansen
Organisasjon (O)	Teledir
Organisasjonsenhet (OU1)	Forskning
Privat domene (P)	Tele
Administrasjonsdomene (A)	Telemax
Land (C) NO	

EXEMPLE 2 – Utilisation des types d'attribut et abréviations en langue anglaise:

Given name (G)	John
Surname (S)	Smith
Organisation (O)	A Bank Ltd
Org. Unit (OU1)	IT Dept
Org. Unit (OU2)	MSG Group
PRMD (P)	ABL
ADMD (A)	Snomail
Country (C)	AQ

**F.4 Interface d'utilisateur**

Le présent paragraphe spécifie les caractéristiques que doivent présenter les interfaces d'utilisateur pour que l'utilisateur puisse introduire les entités OR-address représentées dans l'un des formats spécifiés au § F.3.

L'interface d'utilisateur doit pouvoir accepter toute combinaison valable d'attributs des Tableaux F.1, F.2 et F.3 qui auront été introduits.

Si l'interface d'utilisateur énumère les attributs donnés dans le Tableau F.1, il est recommandé d'utiliser la séquence du Tableau F.1 ou, si elle est incompatible avec les habitudes locales, une autre séquence utilisée dans le cadre de ces habitudes.

Si l'utilisateur fournit une valeur pour l'attribut nom de domaine privé mais qu'il omette l'attribut nom de domaine d'administration ou la valeur correspondant à l'attribut nom de domaine d'administration, la valeur du nom de domaine d'administration à utiliser est un espace unique.

Si l'utilisateur fournit une valeur pour l'attribut nom de domaine privé (private-domain-name) ou l'attribut nom de domaine d'administration (administration-domain-name) mais qu'il omette l'attribut nom de pays (country-name), la valeur de nom de pays (country-name) à utiliser est "XX".

Une entité OR-address qui est introduite sous forme de chaîne unique (par exemple dans une interface à ligne de commande), doit être acceptée dans tout format étiqueté valable permettant à l'utilisateur d'introduire les deux délimiteurs. Il ne faut pas nécessairement que les attributs soient spécifiés dans un ordre particulier. L'interface doit accepter les étiquettes en caractères minuscules ou majuscules.

NOTE 1 – Pour certaines interfaces à ligne de commande actuelles, il faut joindre toute l'adresse au format étiqueté entre guillemets.

Dans tout autre type d'interface (par exemple une interface à invite ou à grille), il convient de fournir un moyen permettant à l'utilisateur d'associer aisément l'identité de chaque attribut aux étiquettes spécifiées dans les Tableaux F.1, F.2 et F.3.

NOTE 2 – Une manière d'associer l'identité de chaque attribut aux étiquettes consiste à faire suivre le type d'attribut (ou abréviation) pour chaque attribut de l'étiquette entre parenthèses; par exemple:

Prénom (G)  
 Initiales (I)  
 Nom de famille (S)  
 Qualificateur de génération (Q)  
 Nom courant (CN)  
 Organisation (O)  
 Unité 1 d'organisation (OU1)  
 Unité 2 d'organisation (OU2)  
 Unité 3 d'organisation (OU3)  
 Unité 4 d'organisation (OU4)  
 Nom de domaine de gestion privé (P)  
 Nom de domaine de gestion d'administration (A)  
 Pays (C)

NOTE 3 – Nombre d'utilisateurs auront sans doute des difficultés à transcrire une adresse présentée sous forme de tableau (soit au format étiqueté, soit au format explicite) dans une interface à ligne de commande qui utilise des délimiteurs.

NOTE 4 – Dans le cas des interfaces de type à grille, on obtient les meilleurs résultats quand l'interface se rapproche le plus possible du format de l'adresse fournie avec la même suite d'attributs utilisant les mêmes types d'attributs ou d'étiquettes.

## EXEMPLES D'APPLICATION

1 – L'utilisateur norvégien d'une interface à ligne de commande reçoit une carte de visite comportant l'entité OR-address suivante:

G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

L'interface à ligne de commande permet à l'utilisateur de taper l'adresse exactement comme elle est présentée sur la carte de visite.

2 – L'utilisateur norvégien d'une interface à grille reçoit la même carte de visite. Le formulaire à l'écran comporte les champs suivants:

Fornavn (G)  
 Etternavn (S)  
 Organisasjon (O)  
 Privat domene (P)  
 Administrasjonsdomene (A)  
 Land (C)

L'utilisateur peut remplir le formulaire en associant les étiquettes formées de lettres uniques figurant sur la carte de visite aux mêmes étiquettes entre parenthèses suivant les noms en norvégien des attributs affichés à l'écran (les délimiteurs ne sont pas utilisés pour l'entrée de ce type).

3 – L'utilisateur de langue anglaise d'une interface à ligne de commande reçoit un document comportant l'entité OR-address suivante:

Fornavn (G)	Per
Etternavn (S)	Hansen
Organisasjon (O)	Teledir
Organisasjonsenhet (OU1)	Forskning
Privat domene (P)	Tele
Administrasjonsdomene (A)	Telex
Land (C)	NO

L'utilisateur sait comment transformer l'adresse du format explicite en format étiqueté. Il peut entrer au choix l'adresse avec le délimiteur, c'est-à-dire:

g=per;s=hansen;o=teledir;ou1=forskning;p=tele;a=telex;c=no

ou:

/g=per/s=hansen/o=teledir/ou1=forskning/p=tele/a=telex/c=no

## Annexe G

### Utilisation des entités OR-address par des organisations multinationales

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

Voir également l'Annexe E de la Rec. UIT-T F.400.

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

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

#### G.1 Principes d'adressage

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

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

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

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

#### G.2 Exemples de configuration

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

### G.2.1 Domaines PRMD multiples indépendants

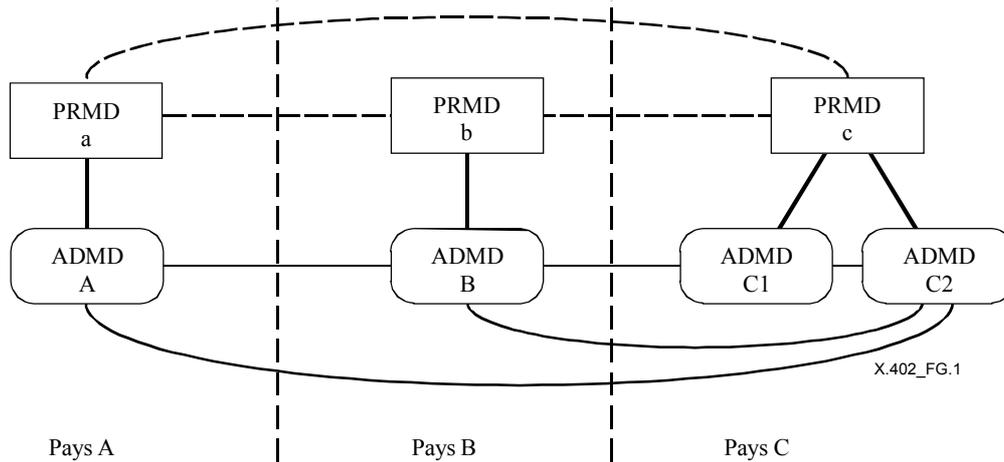


Figure G.1 – Domaines PRMD multiples indépendants

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

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

NOTE 1 – Le choix d'un pseudonyme entraîne un certain nombre de conséquences; voir § G.3.

NOTE 2 – Il faudra peut-être réviser les procédures MTS pour pouvoir prendre en charge les domaines PRMD multinationaux dans un environnement mondial de messagerie.

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

Cette configuration tient compte des réglementations différentes dans plusieurs pays et prévoit également l'attribution d'entités OR-address uniques.

### G.2.2 Un seul domaine PRMD désigné d'après un pays "natal"

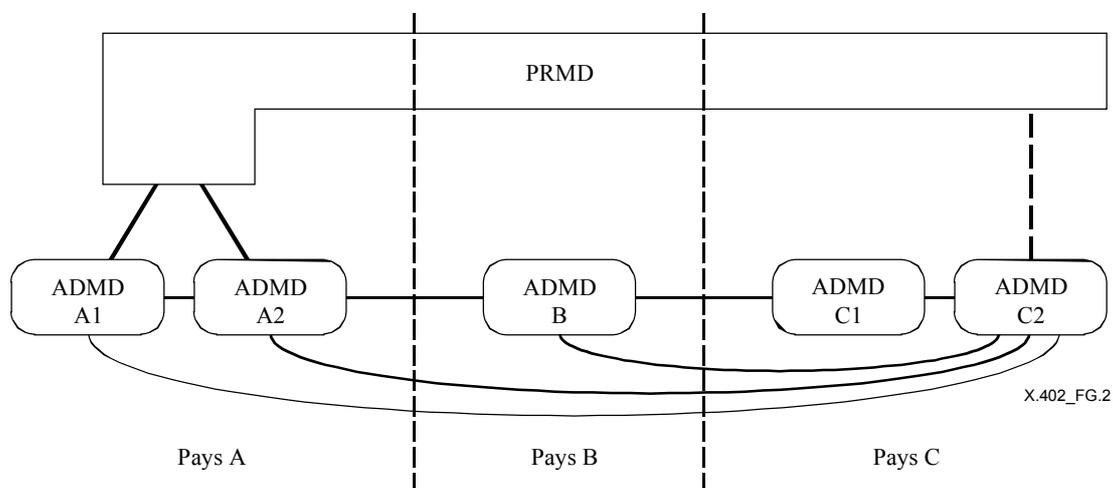


Figure G.2 – Un seul domaine PRMD doté d'un seul nom

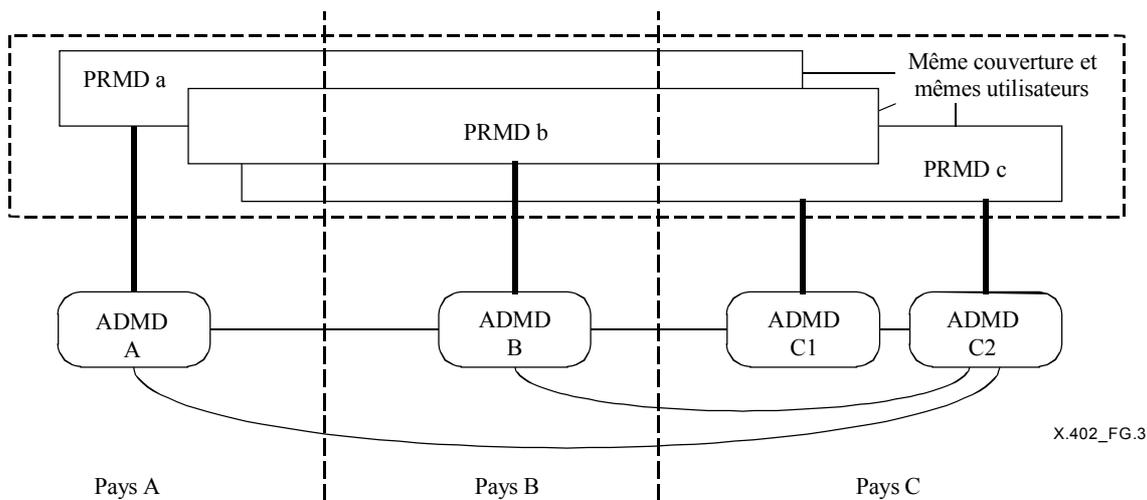
L'organisation multinationale peut utiliser un seul domaine de gestion physiquement implanté dans plus d'un pays. Un seul pays est choisi comme pays natal aux fins d'adressage. Dans ce cas, les adresses de tous les agents UA situés dans ce domaine MD ont les mêmes valeurs de nom de pays, de nom de domaine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

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

Il se peut que l'utilisation conséquente du nom d'un pays, dans l'entité OR-address, ne convienne pas à des utilisateurs de ces domaines PRMD, parce qu'ils n'appartiennent peut-être pas à ce pays.

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

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



**Figure G.3 – Un seul domaine PRMD doté de noms de pays et de domaine multiples**

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

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

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

NOTE 1 – Le choix d'un nom de pseudonyme entraîne un certain nombre de conséquences; voir § G.3.

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

NOTE 2 – Il peut être nécessaire de réexaminer les procédures dans le système MTS pour prendre en charge les domaines PRMD multinationaux dans un environnement de messagerie mondial.

### G.3 Entités OR-address pseudonymes

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

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

Un utilisateur individuel peut choisir un domaine ADMD préféré parmi ceux qui sont disponibles et indiquer entre guillemets les: nom de pays, nom de domaine d'administration et nom de domaine privé correspondants lorsqu'il communique son entité OR-address, par exemple sur une carte professionnelle ou dans l'entité OR-address de l'expéditeur des messages.

Un utilisateur peut également rencontrer quelques difficultés pour utiliser les services d'autres domaines ADMD auxquels le domaine PRMD est connecté. Dans certaines conditions, l'utilisateur (ou l'agent d'utilisateur) peut avoir la possibilité de sélectionner une autre combinaison du nom ADMD et du nom PRMD qui correspond au domaine ADMD avec lequel il veut alors correspondre et modifier en conséquence l'entité OR-address de l'expéditeur. Cependant, cela n'est possible que dans le cas où le même domaine ADMD sert à atteindre tous les destinataires d'un message et le choix de ce domaine ADMD est alors connu au moment du dépôt. Il n'est pas possible de modifier l'entité OR-address de l'expéditeur après le dépôt, car ce serait incompatible avec les services de sécurité. Les utilisateurs peuvent également être induits en erreur en recevant des messages provenant du même expéditeur mais comportant des entités OR-address différentes.

Toutes ces raisons font qu'il peut être plus intéressant pour l'utilisateur de n'employer qu'une seule entité OR-address et, pour certains domaines ADMD, d'accepter des messages pour lesquels l'entité OR-address de l'expéditeur ne correspond pas à ce nom de pays et à ce nom de domaine d'administration. Il se peut également que les entités OR-address de l'expéditeur ne correspondent pas au domaine PRMD local si les services de listes de distribution et de réacheminement (par exemple, le service destinataire suppléant désigné par le destinataire) sont implémentés. Des accords bilatéraux conclus entre les exploitants des domaines ADMD doivent tenir compte de l'utilisation de ces capacités (entre autres) en cas de transit par plus d'un domaine. Une accessibilité mondiale est réalisable, du moins en principe.

L'entité OR-address de l'expéditeur utilisée pour envoyer des messages peut influencer le trajet emprunté par des messages envoyés en réponse. En général, les messages de réponse sont acheminés via le pays et le domaine ADMD spécifiés dans l'entité OR-address. Des accords bilatéraux conclus entre les domaines PRMD ou entre le domaine PRMD et des domaines ADMD peuvent permettre l'utilisation d'autres trajets. Ces facteurs peuvent influencer le choix, par l'utilisateur, d'un nom de domaine pouvant être utilisé dans l'entité OR-address. Il convient de garder à l'esprit que des entités OR-address multiples pour le même utilisateur influencent également les destinataires potentiels. Cette source de confusion peut gêner l'établissement d'une communication ouverte satisfaisante.

## Annexe H

**Utilisation de mots de passe protégés pour l'accès à la mémoire de messages**

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

Le but du mécanisme de mot de passe protégé dans MS-Bind est de permettre aux utilisateurs, lorsqu'ils utilisent un réseau non sécurisé, de s'identifier auprès de la mémoire de messages sans courir le risque que quelqu'un puisse obtenir le mot de passe utilisé en analysant le trafic sur le réseau. Ce problème survient dans les environnements de réseaux locaux (tels que Ethernet), où toute station connectée au réseau peut analyser tout le trafic traversant le réseau. De même, les administrateurs des réseaux publics longue distance peuvent ne pas être fiables.

La solution évidente consiste à chiffrer tout le trafic traversant les réseaux non fiables, mais le temps de traitement ou d'administration supplémentaire requis par un tel système peut ne pas être considéré comme rentable. En outre, l'utilisation du chiffrement fort est légalement limitée dans beaucoup de régions. Le mécanisme du mot de passe protégé peut être mis en œuvre pour un coût minimal, et permet d'éviter, grâce à l'utilisation d'algorithmes de hachage plutôt qu'un chiffrement total, la plupart des problèmes légaux. Bien que les données restent non protégées, le risque est limité à la quantité de données rapatriées depuis la mémoire de messages durant une session, alors que l'obtention d'un mot de passe permettrait à l'intrus d'accéder à la totalité du contenu de la mémoire MS et lui permettrait également de mettre en œuvre des attaques de refus de service ou d'usurpation d'identité. Le mot de passe protégé est donc un compromis utile, offrant une sécurité notablement accrue pour un coût réduit.

Le fondement du mécanisme de mot de passe protégé repose sur l'utilisation d'algorithmes de hachage cryptographique. Ce sont des algorithmes mathématiques produisant un résultat lié aux données d'entrée, mais qui ont la propriété de rendre infaisable la détermination informatique de la valeur d'entrée qui produit un résultat donné, ainsi que la détermination de toute autre valeur d'entrée qui produirait le même résultat.

Le plus simple algorithme de mot de passe protégé possible consisterait à prendre le mot de passe introduit par l'utilisateur, à le faire passer à travers l'algorithme de hachage et à transmettre le résultat. L'intrus serait seulement en mesure de voir la valeur hachée et ne serait pas capable de retrouver le mot de passe initial. Malheureusement, cela ne fournit pas beaucoup plus de sécurité car l'intrus n'a pas besoin de connaître le mot de passe en clair puisque le mot de passe haché fournira toujours la même valeur. L'intrus a simplement besoin de construire un agent UA pouvant réexécuter la valeur du mot de passe haché enregistré et la mémoire MS l'acceptera.

La solution à ce problème consiste à ajouter un nombre aléatoire au mot de passe avant de calculer la valeur hachée. L'agent UA envoie alors le mot de passe haché à la mémoire MS, accompagné de la valeur choisie pour le nombre aléatoire. La mémoire MS connaît le vrai mot de passe et peut effectuer le même calcul en utilisant la valeur aléatoire fournie par l'agent UA: si le calcul de hachage donne le même résultat que celui qui a été fourni par l'agent UA, alors l'utilisateur doit avoir introduit le mot de passe correct. Cela peut être mathématiquement représenté comme suit:

Définition:  $\text{protection} = F(\text{mot de passe} + \text{aléatoire})$

L'agent UA envoie à la mémoire MS:  $\text{protection}, \text{aléatoire}$

La mémoire MS stocke:  $\text{protection}, \text{toutes les valeurs utilisées pour le nombre aléatoire}$

L'intrus peut obtenir la valeur de  $\text{protection}$  et également la valeur du nombre aléatoire utilisé, mais ne peut toujours pas retrouver la valeur originale du mot de passe. De plus, si la mémoire MS garde trace de toutes les valeurs de nombres aléatoires utilisées précédemment et n'autorise pas de nouvelle utilisation de la même valeur, l'intrus ne pourra même pas obtenir l'accès en renvoyant les mêmes données qu'il aura précédemment vues fonctionner.

Etant donné qu'il est assez peu pratique pour la mémoire MS de conserver une liste de toutes les valeurs de nombre aléatoire qui ont été précédemment utilisés (il peut y en avoir un très grand nombre), il est préférable d'utiliser la date courante et l'heure au lieu du (ou en plus du) nombre aléatoire. La mémoire MS enregistre simplement la date la plus récente qui a été utilisée et requiert que toute nouvelle tentative de connexion utilise une date ultérieure à celle qui est enregistrée<sup>1)</sup>. Cela assure également que chaque connexion utilisera une nouvelle valeur de  $\text{protection}$  et évite que l'intrus obtienne l'accès. Cette version devient:

Définition:  $\text{protection} = F(\text{mot de passe} + \text{aléatoire} + \text{temps})$

L'agent UA envoie à la mémoire MS:  $\text{protection}, \text{aléatoire}, \text{temps}$

La mémoire MS stocke:  $\text{mot de passe}, \text{dernière valeur de temps}$

<sup>1)</sup> La mémoire MS peut également valider le fait que le temps est approximativement correct pour l'heure du jour courante dans le monde réel. Cela n'est pas requis pour l'authentification mais cela évite qu'un utilisateur soit bloqué en utilisant, par inadvertance, une machine dont l'horloge est très en avance ou très en retard.

Cette version fournit une bonne protection contre une attaque externe, mais elle présente l'inconvénient que la mémoire MS doit stocker la version en clair du mot de passe de l'utilisateur. Cela est considéré comme non souhaitable, puisque les mots de passe peuvent être dévoilés par inadvertance lors d'une maintenance du système, et car il est extrêmement facile pour un administrateur de système corrompu de dévoiler les mots de passe. La procédure du mot de passe protégé spécifiée pour le système MHS ajoute un niveau de hachage supplémentaire de telle sorte que la mémoire MS ne stocke plus les mots de passe en clair<sup>2)</sup>:

Définition:  $protection1 = F1(\text{mot de passe} + \text{aléatoire1} + \text{temps1})$

Définition:  $protection2 = F2(\text{protection1} + \text{temps2} + \text{aléatoire2})$

L'agent UA stocke:  $temps1, \text{aléatoire1}$

L'agent UA envoie à la mémoire MS:  $protection2, \text{temps2}$ , et/ou  $\text{aléatoire2}$ , et, facultativement,  $temps1$  et/ou  $\text{aléatoire1}$

La mémoire MS stocke:  $protection1$ , dernier  $temps2$  utilisé, facultativement,  $temps1, \text{aléatoire1}$

Dans ce mécanisme, l'agent UA calcule d'abord  $protection1$  en utilisant une valeur connue (préconfigurée) de  $temps1$  et de  $\text{aléatoire1}$  et le mot de passe d'utilisateur. Il sélectionne ensuite  $\text{aléatoire2}$ , lit l'horloge pour obtenir  $temps2$  et calcule  $protection2$ . Les données envoyées à la mémoire MS incluent au moins  $protection2, \text{temps2}$  et  $\text{aléatoire2}$ . La mémoire MS prend alors la valeur stockée de  $protection1$  plus la valeur de  $temps2$  fournie et le nombre  $\text{aléatoire2}$  afin de calculer une autre version de  $protection2$ : si tout cela correspond à  $protection2$  de l'agent UA, l'utilisateur est authentifié.

Le protocole offre un large choix d'algorithmes, autorisant différents algorithmes pour  $F1()$  et  $F2()$  et autorisant l'omission de n'importe quel élément  $temps1, \text{temps2}, \text{aléatoire1}, \text{aléatoire2}$ . L'utilisation exacte des paramètres temps et nombre aléatoire dépendra des algorithmes utilisés et de la politique de sécurité. Toutefois, il sera normalement nécessaire d'utiliser au moins un des deux paramètres  $temps2/\text{aléatoire2}$  afin d'assurer que la valeur de hachage est différente à chaque fois; la mémoire MS doit stocker suffisamment d'informations concernant les valeurs précédentes des paramètres  $temps2/\text{aléatoire2}$  pour éviter l'utilisation future de la même combinaison (le temps est particulièrement pratique pour cela). La protection élémentaire du mot de passe utilise  $temps1/\text{aléatoire1}$  pour garantir que deux utilisateurs ayant choisi le même mot de passe aient des valeurs de  $protection1$  différentes (cela rend des attaques de type "dictionnaire" moins efficaces); toutefois des politiques de sécurité peuvent utiliser ces champs à des fins additionnelles comme obsolescence/expiration du mot de passe ou pour effectuer un choix parmi différents mots de passe.

La gamme des possibilités peut être illustrée par trois exemples:

- si les mots de passe en clair sont acceptables au niveau de la mémoire MS, la fonction  $F1()$  peut être rendue transparente (une fonction retournant ses entrées inchangées) et les paramètres  $temps1, \text{aléatoire1}$  peuvent être omis – donnant un simple niveau de hachage. Le paramètre  $\text{aléatoire1}$  peut être également omis;
- une implémentation typique pourrait utiliser la même fonction de hachage à la fois pour  $F1()$  et  $F2()$  et ignorer  $\text{aléatoire2}$  et  $temps1$ , en transmettant seulement  $protection$  et  $temps2$  dans l'argument de liaison et en prenant  $\text{aléatoire1}$  dans la configuration;
- une implémentation plus complexe pourrait nécessiter que la mémoire MS stocke plus d'un mot de passe (par exemple la valeur  $protection1$ ) pour chaque utilisateur, et transmettrait ainsi les valeurs  $temps1/\text{aléatoire1}$  pour indiquer celle que l'agent UA utilise.

La mémoire MS n'a pas besoin de stocker  $temps1/\text{aléatoire1}$  si des mots de passe protégés sont utilisés pour chaque connexion. Toutefois, le mécanisme de mot de passe protégé peut interagir avec l'authentification par mot de passe simple si la mémoire MS stocke également  $temps1/\text{aléatoire1}$ . Dans le cas où l'agent UA a fourni un mot de passe simple à la mémoire MS conçue pour le mot de passe protégé, la mémoire MS calcule simplement une valeur du paramètre  $protection1$  à partir du mot de passe fourni et des paramètres  $temps1, \text{aléatoire1}$  stockés puis compare le résultat avec le paramètre  $protection1$  stocké. De même, si l'utilisateur change le mot de passe avec le changement normalisé de justificatif d'identité, la mémoire MS peut calculer un nouveau paramètre  $protection1$  à partir du mot de passe fourni et des paramètres  $temps1/\text{aléatoire1}$  stockés.

2) Il convient de noter que, bien que la protection contre une attaque externe soit très forte, la protection contre une attaque interne (par exemple, des administrateurs de système lisant les fichiers dans lesquels la mémoire MS stocke les mots de passe) est, par nature, plus superficielle. Bien que les mots de passe ne soient plus stockés en clair, seul le paramètre  $protection1$  stocké est théoriquement nécessaire pour obtenir, au moyen d'un agent UA convenablement adapté, l'accès à la mémoire MS. Cependant, un intrus pouvant lire le fichier des mots de passe de la mémoire MS peut aussi, très probablement, lire les fichiers des boîtes à lettres. La protection nécessite donc de se prémunir contre les divulgations par inadvertance plutôt que contre une attaque délibérée.

La fourniture d'un mécanisme protégé pour changer le mot de passe est plus difficile. Il est inutile de fournir le nouveau mot de passe sous la forme d'une valeur de `protection2`, puisque la mémoire MS doit stocker `protection1` et qu'il est fondamental que, pour l'ensemble du mécanisme, le paramètre `protection1` ne puisse pas être calculé à partir de `protection2`. Le nouveau paramètre `protection1` ne peut pas non plus être envoyé directement, puisque exposer le nouveau paramètre `protection1` à un intrus est presque aussi néfaste que dévoiler le nouveau mot de passe. Cependant, la mémoire MS et l'agent UA ont un secret partagé sous la forme de l'ancienne valeur du paramètre `protection1`. Le nouveau paramètre `protection1` peut être exprimé sous la forme d'une modification devant être appliquée à l'ancien paramètre `protection1` pour produire le nouveau paramètre `protection1`. Etant donné que seule l'information de changement est transmise, un intrus ne connaissant pas l'ancien paramètre `protection1` ne pourra toujours pas connaître le nouveau paramètre `protection1`. Si l'algorithme de hachage `F1()` a la caractéristique de produire un résultat de taille fixe (ainsi que le font la plupart des algorithmes), le changement peut alors être spécifié comme une chaîne de bits (bit-string) à combiner par un OU-exclusif avec l'ancien paramètre `protection1` afin de produire le nouveau paramètre `protection1`. Le nombre de bits modifiés ne donne à l'intrus aucune information utile, puisqu'un bon algorithme de hachage se caractérisera par le fait qu'un petit changement au niveau de l'entrée peut susciter un changement important à la sortie. Pour les algorithmes de hachage avec une sortie de longueur variable, une description de changement plus complexe sera nécessaire, mais les mêmes principes s'appliquent.

## Annexe I

### Différences entre l'ISO/CEI 10021-2 et la Rec. UIT-T X.402

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

La présente annexe donne les différences techniques entre la Rec. UIT-T X.402 et l'ISO/CEI 10021-2.

Ces différences sont les suivantes:

- a) dans la Recommandation UIT-T, l'interconnexion directe de domaines PRMD peut être "influencée par les règlements", ce qui n'est pas le cas dans l'ISO/CEI (voir la Figure 11);
- b) dans l'ISO/CEI et dans la Recommandation UIT-T, les adresses sont structurées de manière hiérarchique; dans la Recommandation UIT-T, la gestion de cette hiérarchie est confiée aux domaines ADMD, tandis que dans l'ISO/CEI, la gestion est faite de manière indépendante (par exemple par les organismes nationaux d'enregistrement) (voir § 14.1.1, 14.1.2 et 15);  
 Dans la Recommandation UIT-T, le routage entre les domaines respecte cette hiérarchie (de telle manière que tout le routage des messages entre les domaines PRMD fait obligatoirement intervenir les services d'un ou de plusieurs domaines ADMD), alors que l'ISO/CEI permet en plus la connexion directe des domaines PRMD (par exemple par accord bilatéral) (voir § 19);
- c) au § 18.3.1, l'alinéa définissant le nom de domaine d'administration à un seul espace est une partie normative de l'ISO/CEI alors qu'elle est une Note dans la Recommandation UIT-T. L'alinéa définissant le nom de domaine d'administration à un zéro est une partie normative de l'ISO/CEI qui n'apparaît pas dans la Rec. UIT-T;
- d) la représentation des entités OR-address pour l'utilisateur (Annexe F) est une annexe informative de l'ISO/CEI. Elle est aussi une annexe informative (Annexe B) de la Rec. UIT-T F.401 mais non de la Rec. UIT-T X.402.

## Annexe J

### Résumé des modifications apportées aux versions précédentes

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

#### J.1 Différences entre l'ISO/CEI 10021-2:1990 et la Rec. CCITT X.402 (1992)

Les différences techniques sont les suivantes:

- a) adjonction d'une Annexe G sur l'utilisation des adresses OR par les organisations multinationales;
- b) utilisation d'attributs normalisés additionnels dans les adresses OR-address des terminaux.

#### J.2 Différences entre la Rec. CCITT X.402 (1992) et la Rec. UIT-T X.402 (1995) | ISO/CEI 10021-2:1996

Les différences techniques sont les suivantes:

- a) adjonction d'une Annexe F sur la représentation des adresses OR pour un utilisateur humain;
- b) neuf nouvelles définitions d'attribut d'annuaire (voir A.2.1, A.2.2, A.2.4, A.2.6, A.2.7, A.2.9, A.2.14, A.2.18 et A.2.19);
- c) nouvelle section 7 sur les conventions relatives à la définition du service abstrait (voir 28-30).

Les autres modifications sont d'ordre rédactionnel et concernent l'utilisation de la notation ASN.1 révisée telle que celle-ci est définie dans les Recommandations UIT-T X.680 à X.684 (1994) | ISO/CEI 8824:1994 et utilisée dans les Recommandations UIT-T X.500 à X.525 (1993) | ISO/CEI 9596:1994.

#### J.3 Différences entre la Rec. UIT-T X.402 (1995) | ISO/CEI 10021-2:1996 et la Rec. UIT-T X.402 (1999) | ISO/CEI 10021-2:1999

Les différences techniques sont les suivantes:

- a) utilisation du jeu universel de caractères codés sur plusieurs octets à l'intérieur des attributs d'adresse OR (voir § 18.2 à 18.4);
- b) nouvelles définitions de contexte d'annuaire (voir § A.4) et variante nominative d'entité de certificat pour les agents MTA (voir § A.5);
- c) adjonction d'une Annexe H sur l'utilisation de mots de passe protégés pour l'accès à la mémoire de messages.

## Annexe K

## Index

(cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

Cette annexe constitue un index de cette Spécification. Elle indique le(s) numéro(s) de page de la version anglaise où se trouve la définition de chacun des items répartis en plusieurs catégories, lesquelles sont couvertes de façon exhaustive.

Cette annexe renvoie aux items figurant (le cas échéant) dans les catégories suivantes:

- a) abrégations;
- b) termes;
- c) items d'information;
- d) modules ASN.1;
- e) classes d'objets informationnels ASN.1;
- f) types ASN.1;
- g) valeurs ASN.1.

-----

<i>Abbreviations</i>			
A/SYS	30	PDS	11
AC	6	PRMD	32
ACs	51	RO	6
ACSE	6, 51	ROSE	6, 50
ADMD	32	RT	6
AE	5	RTSE	6, 51
APDU	5	S/SYS	30
AS/SYS	30	ST/SYS	30
ASE	5	T/SYS	30
ASEs	47	UA	10
ASN.1	6	UE	5
AST/SYS	30		
AT/SYS	30	<i>Terms</i>	
AU	10	access and storage system	30
C	7	access and transfer system	30
COMPUSEC	19	access system	30
D	7	access unit	10
DL	9	access, storage, and transfer system	30
DSA	5	actual recipient	15
EIT	13	administration management domain	32
M	7	administration-domain-name	37
MASE	50	affirmation	18
MD	31	asymmetric	48
MDSE	50	attribute	35
MHE	8	attribute list	35
MHS	9	attribute type	35
MRSE	49	attribute value	35
MS	10	common-name	37
MSSE	49	conditional	7
MTA	11	consuming ASE	48
MTS	10	consuming UE	48
MTSE	49	content	12
O	7	content type	12
OSI	5	conversion	18
P1	51	country-name	37
P3	51	defaultable	7
P7	51	delivery	16
PDAU	11	delivery agent	16

**ISO/CEI 10021-2:2003 (F)**

delivery report	13	Physical delivery	11
described message	12	physical delivery access unit	11
direct submission	16	physical delivery system	11
direct user	9	physical message	11
distribution list	9	physical rendition	11
DL expansion	18	physical-delivery-country-name	39
domain	31	physical-delivery-office-name	39
domain-defined attribute	35	physical-delivery-office-number	39
encoded information type	12	physical-delivery-organization-name	39
envelope	12	physical-delivery-personal-name	39
event	14	postal OR-address	43
expansion point	18	postal-code	40
explicit conversion	18	poste-restante-address	40
export	16	post-office-box-address	40
extension-physical-delivery-address-components	38	potential recipient	15
external routing	19	private management domain	32
external transfer	16	private-domain-name	40
formatted	43	probe	12
Global MHS	32	receipt	17
grade	7	recipient	15
immediate recipient	14	recipient-assigned alternate recipient	15
implicit conversion	18	redirection	18
import	16	report	13
indirect submission	16	retrieval	16
indirect user	9	routing	19
intended recipient	15	security policy	19
internal routing	19	splitting	17
internal transfer	16	standard attribute	35
joining	17	step	14
local-postal-attributes	38	storage and transfer system	30
management domain	31	storage system	30
mandatory	7	street-address	40
member recipient	15	subject message	13
members	9	subject probe	13
message	12	submission	16
Message Handling	8	submission agent	16
Message Handling Environment	8	submit permission	9
Message Handling System	9	supplying ASE	48
Message Storage	8	supplying UE	48
message store	10	symmetric	48
Message Transfer	8	terminal OR-address	43
message transfer agent	11	terminal-identifier	40
Message Transfer System	10	terminal-type	40
messaging system	29	transfer	16
mnemonic OR-address	42	transfer system	30
name resolution	18	transmittal	13
nested	9	transmittal event	14
network-address	38	transmittal step	14
non-affirmation	18	type	35
non-delivery	18	unformatted	43
non-delivery report	13	unformatted-postal-address	40
numeric OR-address	42	unique-postal-name	41
numeric-user-identifier	38	user	9
optional	7	user agent	10
OR-address	41	value	35
organizational-unit-names	39		
organization-name	38	<i>Information items</i>	
origination	15	address-capabilities-match	62
originator	14	capability-match	63
originator-specified alternate recipient	15	DL Administrator Annotation	63
OR-name	34	DL Nested DL	64
pds-name	39	DL Policy	60
personal-name	39	DL Reset Originator	64

DL Submit Permission	59	EncodedInformationTypesConstraints	- see ISO/IEC 10021-4
MHS Acceptable EITs	55	ExtendedContentType	- see ISO/IEC 10021-4
MHS Deliverable Classes	56	ExtendedEncodedInformationType	- see ISO/IEC 10021-4
MHS Deliverable Content Types	56	GlobalDomainIdentifier	- see ISO/IEC 10021-4
MHS Distribution List	54	ID	65
MHS DL Archive Service	56	MatchingRuleTable	- see ISO/IEC 10021-5
MHS DL Members	56	MTAName	- see ISO/IEC 10021-4
MHS DL Policy	56	Name	- see ISO/IEC 9594-2
MHS DL Related Lists	57	ORAddress	- see ISO/IEC 10021-4
MHS DL Submit Permissions	57	ORName	- see ISO/IEC 10021-4
MHS DL Subscription Service	57	ORNamePattern	59, 71
MHS Exclusively Acceptable EITs	57	RequestedDeliveryMethod	- see ISO/IEC 10021-4
MHS Maximum Content Length	57	SecurityContext	- see ISO/IEC 10021-4
MHS Message Store	54		
MHS Message Store Directory Name	57	<i>ASN.1 values</i>	
MHS Message Transfer Agent	54	addressCapabilitiesMatch	62, 73
MHS OR-Addresses	58	any-user-may-submit	59, 71
MHS OR-Addresses with Capabilities	58	applicationEntity	- see ISO/IEC 9594-7
MHS Supported Attributes	58	capabilityMatch	63, 73
MHS Supported Automatic Actions	58	commonName	- see ISO/IEC 9594-6
MHS Supported Content Types	58	description	- see ISO/IEC 9594-6
MHS Supported Matching Rules	59	distinguishedName	- see ISO/IEC 9594-6
MHS Unacceptable EITs	59	distinguishedNameMatch	- see ISO/IEC 9594-2
MHS User	55	dl-administrator-annotation	63, 73
MHS User Agent	55	dl-administrator-annotation-use-rule	63, 73
MTA Name	54	dl-nested-dl	64, 73
OR-Address	62	dl-nested-dl-use-rule	64, 73
OR-Address with Capabilities	62	dl-reset-originator	64, 73
OR-name	63	dl-reset-originator-use-rule	64, 73
		id-arch	65
<i>ASN.1 modules</i>		id-at	65
MHSDirectoryObjectsAndAttributes	67	id-at-encrypted-mhs-acceptable-eits	66
MHSObjectIdentifiers	65	id-at-encrypted-mhs-deliverable-classes	66
		id-at-encrypted-mhs-deliverable-content-types	66
<i>ASN.1 information object classes</i>		id-at-encrypted-mhs-dl-archive-service	66
ABSTRACT-ERROR	52	id-at-encrypted-mhs-dl-members	66
ABSTRACT-OPERATION	52	id-at-encrypted-mhs-dl-policy	66
ATTRIBUTE	67	id-at-encrypted-mhs-dl-related-lists	66
ATTRIBUTE (Directory)	- see ISO/IEC 9594-2	id-at-encrypted-mhs-dl-submit-permissions	66
ATTRIBUTE (MS)	- see ISO/IEC 10021-5	id-at-encrypted-mhs-dl-subscription-service	66
AUTO-ACTION	- see ISO/IEC 10021-5	id-at-encrypted-mhs-exclusively-acceptable-eits	66
CONTEXT	- see ISO/IEC 9594-2	id-at-encrypted-mhs-maximum-content-length	66
DIT-CONTEXT-USE-RULE	- see ISO/IEC 9594-2	id-at-encrypted-mhs-message-store-dn	66
MATCHING-RULE	- see ISO/IEC 9594-2	id-at-encrypted-mhs-or-addresses	66
MHS-OBJECT	51	id-at-encrypted-mhs-or-addresses-with-capabilities	66
MS-ATTRIBUTE	67	id-at-encrypted-mhs-supported-attributes	66
OBJECT-CLASS	- see ISO/IEC 9594-2	id-at-encrypted-mhs-supported-automatic-actions	66
OTHER-NAME	- see ISO/IEC 9594-8	id-at-encrypted-mhs-supported-content-types	66
PORT	52	id-at-encrypted-mhs-supported-matching-rules	66
		id-at-encrypted-mhs-unacceptable-eits	66
<i>ASN.1 types</i>		id-at-mhs-acceptable-eits	66
AddressCapabilities	62, 72	id-at-mhs-deliverable-classes	66
AlgorithmIdentifier	- see ISO/IEC 9594-8	id-at-mhs-deliverable-content-types	66
AlgorithmInformation	61, 72	id-at-mhs-dl-archive-service	66
AttributeTable	- see ISO/IEC 10021-5	id-at-mhs-dl-members	66
AutoActionTable	- see ISO/IEC 10021-5	id-at-mhs-dl-policy	66
Capability	62, 72	id-at-mhs-dl-related-lists	66
CertificateAssertion	- see ISO/IEC 9594-8	id-at-mhs-dl-submit-permissions	66
ContentLength	- see ISO/IEC 10021-4	id-at-mhs-dl-subscription-service	66
DLPolicy	61, 72	id-at-mhs-exclusively-acceptable-eits	66
DLSubmitPermission	59, 71		

## ISO/CEI 10021-2:2003 (F)

id-at-mhs-maximum-content-length	66	mhs-distribution-list	54, 68
id-at-mhs-message-store-dn	66	mhs-dl-archive-service	56, 70
id-at-mhs-or-addresses	66	mhs-dl-members	56, 70
id-at-mhs-or-addresses-with-capabilities	66	mhs-dl-policy	56, 70
id-at-mhs-supported-attributes	66	mhs-dl-related-lists	57, 70
id-at-mhs-supported-automatic-actions	66	mhs-dl-submit-permissions	57, 70
id-at-mhs-supported-content-types	66	mhs-dl-subscription-service	57, 70
id-at-mhs-supported-matching-rules	66	mhs-exclusively-acceptable-eits	57, 70
id-at-mhs-unacceptable-eits	66	mhs-maximum-content-length	57, 70
id-con	65	mhs-message-store	54, 69
id-con-dl-administrator-annotation	66	mhs-message-store-dn	58, 70
id-con-dl-nested-dl	66	mhs-message-transfer-agent	55, 69
id-con-dl-reset-originator	66	mhs-or-addresses	58, 71
id-directory-objects-and-attributes	65	mhs-or-addresses-with-capabilities	58, 71
id-edims	65	mhs-supported-attributes	58, 71
id-group	65	mhs-supported-automatic-actions	58, 71
id-ipms	65	mhs-supported-content-types	58, 71
id-management	65	mhs-supported-matching-rules	59, 71
id-mhs-protocols	65	mhs-unacceptable-eits	59, 71
id-mod	65	mhs-user	55, 69
id-mr	65	mhs-user-agent	55, 69
id-mr-address-capabilities-match	66	mta-name	64, 73
id-mr-capability-match	66	objectIdentifierMatch	- see ISO/IEC 9594-2
id-mr-orname-exact-match	66	oRAddressElementsMatch	- see ISO/IEC 10021-5
id-ms	65	oRAddressMatch	- see ISO/IEC 10021-5
id-mts	65	oRAddressSubstringElementsMatch	- see ISO/IEC 10021-5
id-object-identifiers	65	organizationalUnitName	- see ISO/IEC 9594-6
id-oc	65	organizationName	- see ISO/IEC 9594-6
id-oc-mhs-distribution-list	66	oRNameElementsMatch	- see ISO/IEC 10021-5
id-oc-mhs-message-store	66	oRNameExactMatch	63, 73
id-oc-mhs-message-transfer-agent	66	oRNameMatch	- see ISO/IEC 10021-5
id-oc-mhs-user	66	oRNameSingleElementMatch	- see ISO/IEC 10021-5
id-oc-mhs-user-agent	66	oRNameSubstringElementsMatch	- see ISO/IEC 10021-5
id-routing	65	owner	- see ISO/IEC 9594-6
id-san	65	protocolInformation	- see ISO/IEC 9594-6
id-san-mta-name	66	seeAlso	- see ISO/IEC 9594-6
integerMatch	- see ISO/IEC 9594-6	top	- see ISO/IEC 9594-2
mhs-acceptable-eits	55, 69		
mhs-deliverable-classes	56, 69		
mhs-deliverable-content-types	56, 69		



## 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	Réseaux câblés et 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, circuits téléphoniques, télégraphie, télécopie 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
<b>Série X</b>	<b>Réseaux de données et communication entre systèmes ouverts</b>
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication