UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.411

(06/1999)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Systèmes de messagerie

Technologies de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait

Recommandation UIT-T X.411

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
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
INTERCONNEXION DES SYSTÈMES OUVERTS	
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
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	**X.400–X.499**
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
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
GESTION OSI	
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
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

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

NORME INTERNATIONALE ISO/CEI 10021-4
RECOMMANDATION UIT-T X.411

Technologies de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait

Résumé

La présente Recommandation | Norme internationale contient une version améliorée de l'opération d'enregistrement *Register* du protocole P3 qui permet la prise en charge de l'élément de service de remise restreinte *Restricted Delivery* et confère une extensibilité universelle à l'opération d'enregistrement. Les déclarations ASN.1 ont été complètement révisées et prennent en compte les nouvelles versions des Recommandations X.680 et X.880, tout en restant entièrement compatibles avec les versions de 1988 et de 1992 des protocoles P1 et P3. La présente Recommandation | Norme internationale contient des améliorations relatives à l'utilisation des caractères de l'ISO/CEI 10646 dans les adresses OR, de nouvelles valeurs des codes d'erreur afin d'assurer la sécurité et de résoudre les défauts de sécurité au moyen de certificats en version 3, d'extensions de messagerie de classe commerciale, d'une page de couverture de télécopie et au moyen de l'annuaire de 1997.

Source

La Recommandation UIT-T X.411, a été approuvée le 18 juin 1999. Un texte identique est également publié comme Norme internationale ISO/CEI 10021-4.

Conformément à la décision de l'UIT-T visant à publier de nouvelles éditions de l'ensemble des Recommandations relatives à la messagerie, la présente édition de la Rec. UIT-T X.411 intègre la Rec. X.411 (11/1995), le Corrigendum technique 1 (08/1997), l'Amendement 1 (12/1997), le Corrigendum technique 2 (12/1997) et le Corrigendum technique 3 (09/1998).

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.

TABLE DES MATIÈRES

Page

SECTION 1 – INTRODUCTION 1

1 Domaine d'application 1

2 Références normatives 2
- 2.1 Interconnexion des systèmes ouverts 2
- 2.2 Systèmes de messagerie 2
- 2.3 Systèmes d'annuaires 2
- 2.4 Indicatifs de pays 3
- 2.5 Services de télématique 3

3 Définitions 3

4 Abréviations 3

5 Conventions 3
- 5.1 Termes 3
- 5.2 Présence des paramètres 4
- 5.3 Définitions de syntaxe abstraite 4
- 5.4 Interprétation des valeurs de type UTCTime 4

SECTION 2 – SERVICE ABSTRAIT DE SYSTEME DE TRANSFERT DE MESSAGES 5

6 Modèle de système de transfert de messages 5

7 Service abstrait du système de transfert de messages MTS: aperçu général 6
- 7.1 Rattachement et détachement MTS 6
- 7.2 Point d'accès de dépôt 6
- 7.3 Point d'accès de remise 7
- 7.4 Point d'accès d'administration 7

8 Définition du service abstrait de système de transfert de messages (MTS) 7
- 8.1 Rattachement MTS-bind et détachement MTS-unbind 7
  - 8.1.1 Opérations abstraites de rattachement et de détachement 7
  - 8.1.2 Erreurs de rattachement bind-errors 11
- 8.2 Point d'accès de dépôt submission-port 11
  - 8.2.1 Opérations abstraites abstract-operations 11
  - 8.2.2 Erreurs abstraites abstract-errors 34
- 8.3 Point d'accès de remise delivery-port 37
  - 8.3.1 Opérations abstraites abstract-operations 37
  - 8.3.2 Erreurs abstraites abstract-errors 54
- 8.4 Accès d'administration 56
  - 8.4.1 Opérations abstraites abstract-operations 56
  - 8.4.2 Erreurs abstraites abstract-errors 62
- 8.5 Types de paramètre commun 63
  - 8.5.1 Identificateur MTS-identifier 63
  - 8.5.2 Identificateur global de domaine global-domain-identifier 63
  - 8.5.3 Nom MTA-name 64
  - 8.5.4 Heure (time) 64
  - 8.5.5 Nom OR-name 64
  - 8.5.6 Types d'informations codées encoded-information-types 64
  - 8.5.7 Certificat (certificate) 65
  - 8.5.8 Jeton 67
  - 8.5.9 Etiquette de sécurité security-label 68
  - 8.5.10 Identificateur d'algorithme algorithm-identifier 69
  - 8.5.11 Mot de passe password 69

9 Définition de syntaxe abstraite du système de transfert de messages MTS 69
- 9.1 Mécanisme d'extension 70
- 9.2 Mécanisme de criticité 70

Page

SECTION 3 – SERVICE ABSTRAIT D'AGENT DE TRANSFERT DE MESSAGES 114

10 Modèle affiné de système de transfert de messages (MTS) 114

11 Présentation du service abstrait d'agent de transfert de messages MTA 115
11.1 Rattachement MTA-bind et détachement MTA-unbind 115
11.2 Opérations abstraites de l'accès de transfert 115

12 Définition du service abstrait d'agent de transfert des messages MTA 115
12.1 Rattachement MTA-bind et détachement MTA-unbind 116
12.1.1 Rattachement abstrait et détachement abstrait 116
12.1.2 Erreurs de rattachement bind-errors 118
12.2 Accès de transfert 119
12.2.1 Opérations abstraites abstract-operations 119
12.2.2 Erreurs abstraites abstract-errors 125
12.3 Types de paramètres communs 125
12.3.1 Information de trace trace-information et information de trace interne internal-trace-information 125

13 Définition de syntaxe abstraite de l'agent de transfert des messages MTA 127

SECTION 4 – PROCÉDURES DE FONCTIONNEMENT RÉPARTI DU SYSTÈME MTS 137

14 Procédures de fonctionnement réparti du système MTS 137
14.1 Aperçu général du modèle MTA 137
14.1.1 Organisation et technique de modélisation 137
14.2 Module de remise différée 139
14.2.1 Procédure de remise différée Deferred-delivery 140
14.3 Module principal 140
14.3.1 Procédure de commande (Control) 143
14.3.2 Procédure de face-avant (Front-end) 145
14.3.3 Procédure de décision d'acheminement et de conversion (Routing-and-conversion-decision) 146
14.3.4 Procédure de décision d'acheminement Routing-decision 147
14.3.5 Procédure de décision de conversion Conversion-decision 150
14.3.6 Procédure de traitement d'erreurs Error-processing 151
14.3.7 Procédure de réacheminement (Redirection) 152
14.3.8 Procédure de duplication (Splitter) 153
14.3.9 Procédure de conversion 154
14.3.10 Procédure de conversion 154
14.3.11 Algorithme de détection de boucle (loop detection) et d'acheminement (routing) 157
14.3.12 Procédure de résolution de nom d'annuaire (Directory Name Resolution) 158
14.3.13 Mise sous double enveloppe 159
14.3.14 Procédure de l'extracteur double-envelope-extractor 160
14.4 Module de rapport (Report) 160
14.4.1 Procédure de commande (Control) 161
14.4.2 Procédure de face avant de rapport (Report-front-end) 162
14.4.3 Procédure de production de rapport 162
14.4.4 Procédure d'acheminement du rapport (Report-routing) 163
14.4.5 Procédure de mise sous double enveloppe 165
14.5 Rattachement MTS-bind et détachement MTS-unbind 165
14.5.1 Procédure de rattachement MTS-bind demandée par l'utilisateur MTS 165
14.5.2 Procédure de détachement MTS-unbind demandée par l'utilisateur MTS 166
14.5.3 Procédure de rattachement MTS-bind demandée par l'agent MTA 167
14.5.4 Procédure de détachement MTS-unbind demandée par l'agent MTA 168
14.6 Point d'accès de dépôt submission-port 168
14.6.1 Procédure de dépôt de message Message-submission 168
14.6.2 Procédure de dépôt d'envoi-test Probe-submission 169
14.6.3 Procédure d'annulation de remise différée Cancel-deferred-delivery 170
14.6.4 Procédure de commande de dépôt Submission-control 171

Page

14.7 Point d'accès de remise ... 171
14.7.1 Procédure de remise de message Message-delivery ... 171
14.7.2 Procédure d'essai de remise d'envoi-test Probe-delivery-test ... 174
14.7.3 Procédure de remise de rapport Report-delivery ... 174
14.7.4 Procédure de commande de remise Delivery-control ... 175
14.8 Accès d'administration ... 176
14.8.1 Procédure enregistrement (Register) ... 176
14.8.2 Procédure de modification des pouvoirs Change-credentials à l'initiative de l'utilisateur MTS ... 176
14.8.3 Procédure de modification des pouvoirs à l'initiative de l'agent MTA ... 177
14.9 Rattachement MTA-bind et détachement MTA-unbind ... 178
14.9.1 Procédure de rattachement en entrée MTA-bind-in ... 178
14.9.2 Procédure de détachement en entrée MTA-unbind-in ... 178
14.9.3 Procédure de rattachement en sortie MTA-bind-out ... 179
14.9.4 Procédure de détachement en sortie MTA-unbind-out ... 180
14.10 Accès de transfert ... 180
14.10.1 Procédure de message entrant Message-in ... 180
14.10.2 Procédure d'envoi-test entrant Probe-in ... 180
14.10.3 Procédure de rapport entrant Report-in ... 181
14.10.4 Procédure de message sortant Message-out ... 181
14.10.5 Procédure d'envoi-test sortant Probe-out ... 182
14.10.6 Procédure de rapport sortant Report-out ... 183

Annexe A – Définition de référence des identificateurs d'objet MTS ... 184

Annexe B – Définition de référence des limites supérieures des paramètres MTS ... 186

Annexe C – Définition du service abstrait pour le système de transfert de messages de 1988 ... 189
C.1 Enregistrement-88 Register-88 ... 189
C.1.1 Arguments ... 189
C.1.2 Résultats ... 191
C.1.3 Erreurs abstraites abstract-errors ... 191
C.2 Commande de remise-88 Delivery-control-88 ... 191
C.2.1 Arguments ... 191
C.2.2 Résultats ... 192
C.2.3 Erreurs abstraites ... 192

Annexe D – Différences entre la Norme ISO/CEI 10021-4 et la Recommandation UIT-T X.411 ... 196

Annexe E – Index ... 197

Introduction

La présente Définition de service fait partie d'une série de Recommandations | Normes internationales définissant le système de messagerie dans un environnement de systèmes ouverts répartis.

Les services de messagerie permettent aux abonnés d'échanger des messages en mode différé (enregistrement et retransmission). Un message envoyé par un usager (l'*expéditeur*) est transféré par l'intermédiaire du système de transfert de messages (MTS, *message transfer system*) et remis à un ou plusieurs autres usagers (les *destinataires*).

Le système MTS comprend un certain nombre d'agents de transfert de messages (MTA, *message-transfer-agents*), qui transfèrent les messages et les remettent à leurs destinataires prévus.

La présente Définition de service a été élaborée conjointement par l'UIT-T et par l'ISO/CEI. Elle est publiée sous forme de texte commun formant la Rec. UIT-T X.411 | ISO/CEI 10021-4.

NORME INTERNATIONALE ISO/CEI 10021-4
RECOMMANDATION UIT-T X.411

Technologies de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait

SECTION 1 – INTRODUCTION

1 Domaine d'application

La présente Recommandation | Norme internationale définit le service abstrait assuré par le système de transfert de messages ou système MTS (service abstrait MTS) et spécifie les procédures que doivent exécuter les agents de transfert de messages ou agents MTA pour assurer un fonctionnement réparti correct du système MTS.

La Rec. UIT-T X.402 | ISO/CEI 10021-2 identifie les autres Recommandations | Normes internationales qui définissent d'autres aspects des systèmes de messagerie.

L'accès au service abstrait MTS défini dans la présente Recommandation | Norme internationale peut être assuré par le protocole d'accès MTS (P3) que définit la Rec. UIT-T X.419 | ISO/CEI 10021-6. Le fonctionnement réparti du système MTS, exposé dans la présente Recommandation | Norme internationale, peut être assuré par l'utilisation du protocole de transfert MTS (P1), également défini dans la Rec. UIT-T X.419 | ISO/CEI 10021-6. Les moyens par lesquels les messages sont acheminés à travers le système MTS sont spécifiés dans l'ISO/CEI 10021-10.

La Section 2 de la présente Recommandation | Norme internationale définit le service abstrait MTS. L'article 6 décrit le modèle de système de transfert de messages. L'article 7 donne un aperçu général de ce service abstrait MTS, l'article 8 définit la sémantique des paramètres de ce service et l'article 9 définit sa syntaxe abstraite.

La Section 3 définit le service abstrait d'agent MTA. L'article 10 affine le modèle du système MTS déjà décrit à l'article 6 et montre que le système MTS comprend un certain nombre d'agents MTA dont l'interfonctionnement assure le service abstrait MTS. L'article 11 donne un aperçu général du service abstrait d'agent MTA, l'article 12 définit la sémantique des paramètres de ce service et l'article 13 définit sa syntaxe abstraite.

La Section 4 spécifie les procédures effectuées par les agents MTA pour assurer le fonctionnement réparti correct du système MTS.

L'Annexe A fournit une définition de référence des identificateurs d'objets MTS cités dans les modules ASN.1 contenus dans le corps de la présente Recommandation | Norme internationale.

L'Annexe B fournit une définition de référence des limites supérieures des contraintes de taille imposées aux types de données de longueur variable définis dans les modules ASN.1 du corps de la présente Recommandation | Norme internationale.

L'Annexe C donne la définition du service abstrait pour le système de transfert de messages de 1988.

L'Annexe D indique les différences techniques entre les versions de l'ISO/CEI et de l'UIT-T de la Rec. UIT-T X.411 et de l'ISO | CEI 10021-4.

L'Annexe E contient un index des termes utilisés dans la présente Recommandation | Norme internationale, rangés dans les catégories suivantes: définitions des paramètres du système MTS; abréviations; termes; modules ASN.1; classes d'objets informationnels ASN.1; types ASN.1 et valeurs ASN.1.

2 Références normatives

Les Recommandations et les 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 Définition de service cite les spécifications OSI suivantes.

- 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.880 (1994) | ISO/CEI 13712-1:1995, *Technologies de l'information – Opérations distantes: concepts, modèle et notation.*

2.2 Systèmes de messagerie

La présente Définition de service cite les spécifications suivantes relatives aux systèmes de messagerie.

- 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 UIT-T X.402 (1999) | ISO/CEI 10021-2:2003, *Technologies de l'information – Systèmes de messagerie: architecture globale.*
- Recommandation UIT-T X.412 (1999) | ISO/CEI 10021-10:1999, *Technologies de l'information – Systèmes de messagerie: routage.*
- 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: spécifications 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 X.408 du CCITT (1988), *Systèmes de messagerie: règles de conversion entre différents types d'informations codées.*

2.3 Systèmes d'annuaires

La présente Définition de service cite les spécifications suivantes relatives au système d'annuaire.

- 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.*

2.4 Indicatifs de pays

La présente Définition de service cite les spécifications suivantes, relatives aux indicatifs 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 Services de télématique

La présente Définition de service cite les spécifications suivantes relatives aux services de télématique:

- Recommandation F.170 du CCITT (1992), *Dispositions relatives à l'exploitation du service public international de télécopie entre bureaux publics (Bureaufax).*
- Recommandation UIT-T T.30 (1993), *Procédures pour la transmission de documents par télécopie sur le réseau téléphonique public commuté.*

3 Définitions

Pour les besoins de la présente Définition de service, les définitions données dans la Rec. UIT-T X.402 | ISO/CEI 10021-2 s'appliquent.

4 Abréviations

Pour les besoins de la présente Définition de service, les abréviations données dans la Rec. UIT-T X.402 | ISO/CEI 10021-2 sont utilisées.

5 Conventions

La présente Définition de service utilise les conventions descriptives exposées ci-dessous.

5.1 Termes

Dans la présente Définition de service, le libellé des termes définis ainsi que les noms et valeurs des paramètres du service abstrait MTS et du service abstrait d'agent MTA commencent par une lettre minuscule et sont reliés par un trait d'union, à moins qu'il ne s'agisse d'un nom propre; exemple: terme-défini. Les noms propres commencent par une lettre majuscule et ne sont pas reliés par un trait d'union; exemple: Nom Propre. Les noms et valeurs des paramètres du service abstrait MTS et du service abstrait d'agent MTA (y compris les éléments d'adresse OR définis dans l'ISO/CEI 10021-2) sont imprimés en **gras**.

5.2 Présence des paramètres

Dans les tableaux de paramètres des articles 8 et 12, la présence de chaque paramètre est qualifiée comme suit:

Obligatoire (M, *mandatory*): un paramètre obligatoire est toujours présent.

Facultatif (O, *optional*): la présence d'un argument facultatif est laissée au choix de l'agent qui appelle l'opération abstraite; la présence d'un résultat facultatif est laissée au choix de l'agent qui effectue l'opération abstraite.

Conditionnel (C): les conditions de présence d'un paramètre conditionnel sont spécifiées dans la présente Définition de service.

Lorsque la présence d'un paramètre conditionnel est rendue nécessaire par une action du système MTS sur le message, message d'essai ou rapport, cela est explicitement défini. La présence d'autres paramètres conditionnels dépend de la présence de ces paramètres dans d'autres opérations abstraites (par exemple, la présence d'un argument conditionnel d'opération abstraite de transfert de message *Message-transfer* dépend de sa présence dans l'opération abstraite de dépôt de message *Message-submission* correspondante.

5.3 Définitions de syntaxe abstraite

La présente Définition de service décrit la syntaxe abstraite du service abstrait MTS et du service abstrait d'agent MTA en utilisant la notation de syntaxe abstraite ASN.1 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 ainsi que les conventions de notation des services abstraits décrites dans la Rec. UIT-T X.402 | ISO/CEI 10021-2 qui utilise la notation pour les opérations distantes définie dans la Rec. UIT-T X.880 | ISO/CEI 13712-1.

Lorsqu'il en découle des modifications de protocoles décrits dans la Recommandation X.411 du CCITT (1984), ces modifications sont mises en évidence par soulignement dans les définitions de syntaxe abstraite.

Bien que la syntaxe abstraite décrite dans la présente Définition de service contienne des marqueurs d'extension, il n'a pas été vérifié que ceux-ci étaient présents dans toutes les instances où la présence d'un tel marqueur est nécessaire pour pouvoir utiliser en toute sécurité les règles de codage compact.

5.4 Interprétation des valeurs de type UTCTime

Les dates et les heures des protocoles MHS sont représentées à l'aide du type ASN.1 *UTCTime* (temps UTC) qui n'utilise que des nombres à deux chiffres pour symboliser l'année, le siècle n'étant pas spécifié. Puisque les systèmes MHS doivent traiter les dates du passé (par exemple heures de dépôt d'anciens messages pouvant être stockés dans des mémoires locales ou retransmis) et celles de l'avenir (heure d'expiration, heure de remise différée), il est important de respecter une convention normalisée pour éviter un affichage de valeurs inexactes ou un mauvais fonctionnement des protocoles MHS lorsqu'on compare les dates de siècles différents.

Avec ces nombres à deux chiffres, on peut représenter 100 années différentes; il faut donc mettre en œuvre un mécanisme qui permette d'associer chacune de ces valeurs à un siècle donné. La convention choisie est la suivante: les dix années précédant la date actuelle correspondront au siècle actuel et les quarante années suivant cette date correspondront au siècle suivant, l'interprétation des 49 années restantes dépendant de la mise en œuvre. Par exemple, pour un système fonctionnant en 1996, on interprétera les valeurs "86" à "99" comme étant les années 1986 à 1999, les valeurs "00" à "36" comme étant les années 2000 à 2036 et l'interprétation des valeurs "37" à "85" dépendra de l'implémentation.

NOTE – Cette convention permet l'application de deux stratégies différentes. Avec la première, on peut choisir une interprétation fixe de toutes les valeurs des années: la convention est respectée pendant la durée de vie prévue pour le produit. Avec la seconde, on peut choisir une interprétation dynamique fondée sur la date actuelle, l'implémentation restant ainsi valide indéfiniment. Par exemple, on pourrait choisir l'implémentation pour laquelle les dates utilisables iraient de 1970 à 2069, ce qui obligerait à procéder à une révision du système en 2029, si celui-ci fonctionne encore cette année-là.

SECTION 2 – SERVICE ABSTRAIT DE SYSTEME DE TRANSFERT DE MESSAGES

6 Modèle de système de transfert de messages

Un système de messagerie permet l'échange de messages entre utilisateurs, par enregistrement et retransmission. Le message déposé par un utilisateur (*expéditeur*) est transféré par le système de transfert de messages (MTS) puis remis à un ou plusieurs autres utilisateurs (*destinataires*).

Le système MTS est décrit au moyen d'un modèle abstrait qui permet de définir les services qu'il fournit, regroupés sous l'appellation générique service abstrait MTS.

Le système MTS est modélisé sous forme d'*objet*, dont le comportement général peut être décrit sans référence à sa structure interne. Les services fournis par l'objet MTS sont disponibles aux *points d'accès*. Un type de point d'accès représente une vue spécifique des services fournis par l'objet MTS.

L'utilisateur du système MTS est également modélisé sous forme d'un objet qui obtient les services fournis par le système MTS par l'intermédiaire d'un point d'accès apparié avec un point d'accès MTS de même type.

Un type de point d'accès correspond à un ensemble d'*opérations abstraites* (*abstract-operations*) qui peuvent intervenir en ce point: celles qui peuvent être effectuées par l'objet MTS (appelées par l'objet utilisateur MTS) et celles qui peuvent être appelées par l'objet MTS (effectuées par l'objet utilisateur MTS).

Un point d'accès peut être symétrique, auquel cas l'ensemble des opérations effectuées par l'objet MTS peut également être appelé par lui, et inversement. Sinon, le point d'accès est asymétrique et l'objet est réputé *fournisseur* ou *consommateur* par rapport à ce type de point d'accès. Les termes *fournisseur* et *consommateur* ne servent qu'à établir une distinction entre les rôles d'un couple de points d'accès au niveau de l'appel d'une opération ou de son exécution. L'affectation des termes est en général intuitive lorsqu'un objet fournit un service utilisé par un autre objet; l'objet serveur (par exemple le système MTS) est en général considéré comme *fournisseur*, et l'objet utilisateur (par exemple un objet utilisateur MTS) comme *consommateur*.

Avant que des objets puissent se demander mutuellement d'effectuer des opérations, il est nécessaire de les relier en une *association* abstraite. La constitution de cette association crée une liaison entre ces objets qui n'est rompue que lorsque l'association est libérée. L'association est toujours libérée par celui qui a pris l'initiative de la constituer. La constitution d'une association établit les *pouvoirs* de l'interaction des objets ainsi que le *contexte d'application* (*application-context*) et le *contexte de sécurité* (*security-context*) de l'association. Le *contexte d'application* (*application-context)* d'une association peut être constitué par un ou plusieurs types de points d'accès appariés entre les deux objets.

Le modèle présenté est abstrait: un observateur extérieur n'est pas toujours en mesure d'identifier les limites entre les objets ou de décider du moment de l'opération ou des moyens qu'elle utilisera. Toutefois, dans certains cas, le modèle abstrait sera *réalisé*. Par exemple, un couple d'objets communiquant par des points d'accès appariés peuvent être situés dans des systèmes ouverts distincts. Dans ce cas, la limite entre les objets est visible, les points d'accès sont exposés et les opérations peuvent être prises en charge par les instances de communication OSI.

L'objet MTS prend en charge trois types de points d'accès différents: *points d'accès de dépôt (submission-port)*, *de remise (delivery-port)* et *d'administration (administration-port)*.

Le point d'accès de dépôt submission-port permet à l'utilisateur MTS de déposer des messages que le système, après transfert, remettra à un ou plusieurs utilisateurs MTS destinataires; il permet également de tester la capacité du système MTS à remettre un message sujet (*subject-message*).

Le point d'accès de remise delivery-port permet à l'utilisateur MTS de réceptionner les messages qui lui parviennent, ainsi que les rapports de remise ou de non-remise des messages et des envois-tests.

Le point d'accès d'administration administration-port permet à l'utilisateur MTS de modifier des paramètres à long terme, consignés par le système MTS et associés à la remise de message, et permet également au système MTS et à l'utilisateur MTS de modifier leurs *pouvoirs* réciproques.

Un message déposé par un utilisateur MTS en un point d'accès de dépôt submission-port est normalement remis à un ou plusieurs utilisateurs MTS destinataires par les points d'accès de remise delivery-port. L'utilisateur MTS expéditeur peut demander à recevoir notification de la remise ou de la non-remise d'un message via son point d'accès de remise delivery-port.

La Figure 1 représente le modèle du système MTS (système de transfert de messages).

L'article 7 donne un aperçu général du service abstrait de système MTS.

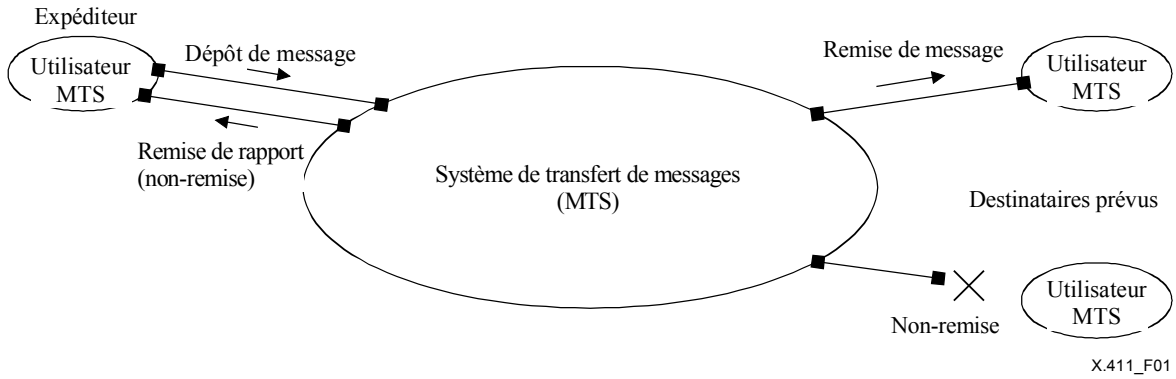


Figure 1 – Modèle du système de transfert de messages

7 Service abstrait du système de transfert de messages MTS: aperçu général

La présente Définition de service définit les services suivants, qu'offre le service abstrait de système MTS:

Rattachement et détachement MTS

a) rattachement (MTS-bind);

b) détachement (MTS-unbind);

Opérations abstraites du point d'accès de dépôt

c) dépôt de message (Message-submission);

d) dépôt d'envoi-test (Probe-submission);

e) annulation de remise différée (Cancel-deferred-delivery);

f) commande de dépôt (Submission-control);

Opérations abstraites du point d'accès de remise

g) remise de message (Message-delivery);

h) remise de rapport (Report-delivery);

i) commande de remise (Delivery-control);

Opérations abstraites du point d'accès d'administration

j) enregistrement (Register);

k) modification des pouvoirs (Change-credentials).

7.1 Rattachement et détachement MTS

Le service de rattachement **MTS-bind** permet à l'utilisateur MTS d'établir une association avec le système MTS ou à celui-ci d'établir une association avec un utilisateur MTS. Les opérations abstraites autres que de rattachement MTS-bind ne peuvent être demandées que dans le contexte d'une association établie.

Le détachement **MTS-unbind** permet au demandeur d'une association établie de la libérer.

7.2 Point d'accès de dépôt

L'opération abstraite de dépôt de message **Message-submission** permet à un utilisateur MTS de déposer un message auprès du système MTS pour transfert et remise à un ou plusieurs utilisateurs MTS destinataires.

L'opération abstraite de dépôt d'envoi-test **Probe-submission** permet à un utilisateur MTS de déposer un envoi-test afin de déterminer si un éventuel message peut être ou non transféré et remis à un ou plusieurs utilisateurs MTS destinataires.

L'opération abstraite d'annulation de remise différée **Cancel-deferred-delivery** permet à un utilisateur MTS de demander l'annulation d'un message précédemment déposé (pour remise différée) par appel de l'opération abstraite de dépôt de message Message-submission.

L'opération abstraite de commande de dépôt **Submission-control** permet au système MTS d'imposer des contraintes à l'utilisation des opérations abstraites de point d'accès de dépôt submission-port par l'utilisateur MTS.

Les opérations abstraites de dépôt de message **Message-submission** et de dépôt d'envoi-test **Probe-submission** peuvent entraîner l'appel ultérieur par le système MTS d'une opération abstraite de remise de rapport Report-delivery.

7.3 Point d'accès de remise

L'opération abstraite de remise de message **Message-delivery** permet au système MTS de remettre un message à un utilisateur MTS.

L'opération abstraite de remise de rapport **Report-delivery** permet au système MTS de rendre compte à l'utilisateur MTS du résultat d'une opération abstraite antérieurement appelée de dépôt de message Message-submission ou de dépôt d'envoi-test Probe-submission. Dans le cas du dépôt de message Message-submission, l'opération abstraite de remise de rapport Report-delivery indique la remise ou la non-remise du message déposé. Dans le cas du dépôt d'envoi-test Probe-submission, l'opération abstraite de remise de rapport Report-delivery indique si un message éventuellement déposé pourrait être remis. L'opération abstraite de remise de rapport Report-delivery peut également acheminer une notification de remise physique par un système de remise physique PDS.

L'opération abstraite de commande de remise **Delivery-control** permet à un utilisateur MTS d'imposer des contraintes à l'utilisation par le système MTS des opérations abstraites de point d'accès de remise delivery-port.

7.4 Point d'accès d'administration

L'opération abstraite d'enregistrement **Register** permet à un utilisateur MTS de modifier les paramètres à long terme d'utilisateur MTS consignés par le système MTS et associés à la remise de message.

L'opération abstraite de modification des pouvoirs **Change-credentials** permet à un utilisateur MTS de modifier ses pouvoirs auprès du système MTS ou à celui-ci de modifier ses pouvoirs auprès de l'utilisateur MTS.

8 Définition du service abstrait de système de transfert de messages (MTS)

Le présent article définit la sémantique des paramètres du service abstrait MTS.

Le § 8.1 définit les opérations de rattachement MTS-bind et de détachement MTS-unbind. Le § 8.2 définit les opérations du point d'accès de dépôt submission-port. Le § 8.3 définit les opérations du point d'accès de remise delivery-port. Le § 8.4 définit les opérations du point d'accès d'administration administration-port. Le § 8.5 définit certains types de paramètres communs.

La syntaxe abstraite du service abstrait MTS est définie à l'article 9.

8.1 Rattachement MTS-bind et détachement MTS-unbind

Le présent paragraphe définit les opérations de rattachement MTS-bind et de détachement MTS-unbind, qui permettent d'établir et de libérer des associations entre un utilisateur MTS et le système MTS.

8.1.1 Opérations abstraites de rattachement et de détachement

Le présent paragraphe définit les opérations abstraites suivantes de rattachement et de détachement:

a) rattachement MTS-bind;

b) détachement MTS-unbind.

8.1.1.1 Rattachement MTS-bind

Le rattachement MTS-bind permet à un utilisateur MTS d'établir une association avec le système MTS ou à ce dernier d'établir une association avec le premier.

Le rattachement MTS-bind établit les pouvoirs **credentials** de l'utilisateur MTS et du système MTS en interaction, ainsi que le contexte d'application **application-context** et le **credentials-context** de sécurité security-context de l'association. Une association ne peut être libérée que par son demandeur (par l'opération détachement MTS-unbind).

Les opérations abstraites autres que le rattachement MTS-bind ne peuvent être appelées que dans le contexte d'une association établie.

Le succès du rattachement MTS-bind signifie que l'association est établie.

L'interruption d'un rattachement MTS-bind par une erreur de rattachement bind-error indique que l'association n'a pas été établie.

8.1.1.1.1 Arguments

Le Tableau 1 fournit la liste des arguments de l'opération de rattachement MTS-bind, qualifie leur présence et indique le paragraphe dans lequel ils sont définis.

Tableau 1 – Arguments de l'opération de rattachement MTS-bind

Argument	Présence	Paragraphe
Arguments de rattachement		
Nom du demandeur *initiator-name*	M	8.1.1.1.1.1
Pouvoirs du demandeur *initiator-credentials*	M	8.1.1.1.1.2
Contexte de sécurité *security-context*	O	8.1.1.1.1.3
Messages en attente *messages-waiting*	O	8.1.1.1.1.4

8.1.1.1.1.1 Nom du demandeur initiator-name

Cet argument comprend un nom de demandeur de l'association. Il est produit par le demandeur de l'association.

Si le demandeur est un utilisateur MTS, il s'agit du nom **OR-name** de l'utilisateur MTS tel qu'il est enregistré auprès du système MTS (voir § 8.4.1.1.1.1). Le nom du demandeur **initiator-name** contient l'adresse **OR-address** et peut facultativement comprendre le nom d'annuaire **directory-name** de l'utilisateur MTS (**OR-address-and-optional-directory-name**). Le nom du demandeur **initiator-name** indiquera aussi si le demandeur est un agent d'usager (UA) ou une mémoire de messages (MS).

Si le demandeur est le système MTS (ou un agent de transfert de message MTA – voir l'article 11), le nom est un nom **MTA-name**, connu de l'utilisateur MTS.

8.1.1.1.1.2 Pouvoirs du demandeur initiator-credentials

Cet argument contient les pouvoirs **credentials** du demandeur de l'association. Il est produit par ce dernier.

Les pouvoirs du demandeur **initiator-credentials** permettent au demandé d'authentifier l'identité du demandeur (voir Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si on n'utilise qu'une authentification simple, les pouvoirs du demandeur **initiator-credentials** comprennent un simple mot de passe **password** associé au nom du demandeur **initiator-name**.

Si on utilise une authentification protégée, les pouvoirs du demandeur **initiator-credentials** comprennent un mot de passe **password** protégé comme le décrit l'article 6 de la Rec. UIT-T X.509 | ISO/CEI 9594-8 (protection1 ou protection2) ainsi qu'à titre facultatif des arguments pour ce procédé de protection (temps1, temps2, aléatoire1 et aléatoire2) dont le sens est précisé par accord mutuel. La description, dans l'Annexe H de la Rec. UIT-T X.402 | ISO/CEI 10021-2, de l'authentification protégée s'applique également à l'opération MTS-Bind (outre le mécanisme protégé pour changer le mot de passe).

Si on utilise une authentification renforcée, les pouvoirs du demandeur **initiator-credentials** comprennent un jeton de rattachement de demandeur **initiator-bind-token** et, à titre facultatif, un certificat de demandeur **initiator-certificate** ou un sélecteur de certificat **certificate-selector**.

Le jeton de rattachement du demandeur **initiator-bind-token** est produit par le demandeur de l'association. S'il s'agit d'un jeton asymétrique **asymmetric-token**, les données signées **signed-data** comprennent un nombre aléatoire **random-number**. Les données chiffrées **encrypted-data** d'un jeton asymétrique **asymmetric-token** peuvent servir à acheminer des informations secrètes relatives à la sécurité (par exemple une ou plusieurs clés symétriques de chiffrement) servant à sécuriser l'association; elles peuvent également être absentes du jeton de rattachement du demandeur **initiator-bind-token**.

Des algorithmes symétriques peuvent être utilisés dans le cadre du jeton asymétrique **asymmetric-token** ci-dessus (voir § 8.5.8).

Le certificat du demandeur **initiator-certificate** est un certificat du demandeur de l'association produit par une source de confiance (une autorité de certification par exemple) et, facultativement des certificats additionnels indiquant un trajet de certification pour le certificat du demandeur. Il peut être fourni par le demandeur de l'association si le jeton de rattachement **initiator-bind-token** est un jeton asymétrique **asymmetric-token**. Si le demandeur est un utilisateur du système MTS, le certificat **initiator-certificate** doit contenir l'adresse **OR-address** du demandeur dans la composante

x400Address de son champ de variante nominative d'entité (voir § 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), à moins que la politique de sécurité ne propose une autre possibilité de rattachement du certificat à l'utilisateur du système MTS. Si le demandeur est le système MTS, le certificat **initiator-certificate** doit contenir le nom **MTA-name** du demandeur dans un nom *mta-name* (voir § A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) de la composante *otherName* de son champ de variante nominative d'entité, à moins que la politique de sécurité ne propose une autre possibilité de rattachement du certificat à l'agent MTA demandeur. Le certificat de demandeur **initiator-certificate** peut servir à acheminer une copie certifiée de la clé publique de chiffrement asymétrique public-asymmetric-encryption-key (clé publique de sujet **subject-public-key**) du demandeur de l'association. La clé publique public-asymmetric-encryption-key du demandeur peut être utilisée par le demandé pour valider le jeton de rattachement de demandeur **initiator-bind-token** et pour calculer les données chiffrées **encrypted-data** dans le jeton de rattachement de demandé **responder-bind-token**. Si on sait que le demandé dispose du certificat de demandeur **initiator-certificate** ou qu'il y a accès (par l'annuaire par exemple), le certificat **initiator-certificate** peut être omis et, lorsque le demandeur a plusieurs certificats, le sélecteur **certificate-selector** peut être fourni pour identifier le certificat au moyen de tout critère de sélection spécifié pour la correspondance de certificat (voir le § 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

8.1.1.1.1.3 Contexte de sécurité security-context

Cet argument identifie le contexte de sécurité **security-context** que le demandeur de l'association propose d'appliquer. Il peut être produit par ce demandeur.

Le contexte de sécurité **security-context** comporte une ou plusieurs étiquettes de sécurité **security-labels** définissant, au vu de la politique de sécurité en vigueur, la sensibilité des interactions qui peuvent se produire entre l'utilisateur MTS et le système MTS pendant la durée de l'association. Le contexte de sécurité **security-context** doit être recevable au niveau des étiquettes de sécurité utilisateur **user-security-labels** de l'utilisateur MTS telles qu'elles sont enregistrées, et au niveau des étiquettes de sécurité **security-labels** associées à l'agent MTA du système MTS.

Une fois établis, les contextes de sécurité **security-context** des points d'accès de dépôt submission-port et de remise delivery-port peuvent être temporairement restreints respectivement par l'opération abstraite de commande de dépôt Submission-control (voir § 8.2.1.4.5) et de commande de remise Delivery-control (voir 8.3.1.3.1.7).

Si aucun contexte de sécurité **security-context** n'a été établi entre l'utilisateur MTS et le système MTS, la sensibilité des interactions entre l'utilisateur MTS et le système MTS peut être choisie par l'appelant d'une opération abstraite.

8.1.1.1.1.4 Messages en attente messages-waiting

Cet argument indique le nombre de messages et le nombre total d'octets en instance de remise par le système MTS à l'utilisateur MTS, ventilés par niveau de priorité **priority**. Il peut être produit par le demandeur de l'association.

Cet argument n'est présent que lorsque le service MTS demande une association avec un utilisateur MTS et lorsque ce dernier a souscrit à l'élément de service "Mise en instance" (défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1).

8.1.1.1.2 Résultats

Le Tableau 2 énumère les résultats du rattachement MTS-bind, en qualifie la présence et spécifie le paragraphe dans lequel ils sont définis.

Tableau 2 – Résultats de rattachement MTS-bind

Résultat	Présence	Paragraphe
Résultats de rattachement		
Nom du demandé *responder-name*	M	8.1.1.1.2.1
Pouvoirs du demandé *responder-credentials*	M	8.1.1.1.2.2
Messages en attente *messages-waiting*	O	8.1.1.1.2.3

8.1.1.1.2.1 Nom du demandé responder-name

Cet argument comprend un nom identifiant le demandé de l'association. Il est produit par lui.

Si le demandé est un utilisateur MTS, le nom en question est son nom **OR-name** tel qu'il est enregistré auprès du système MTS (voir 8.4.1.1.1.1). Le nom du demandé **responder-name** contient l'adresse **OR-address** et, à titre facultatif, le nom d'annuaire **directory-name** de l'utilisateur MTS (**OR-address-and-optional-directory-name**). Le nom du demandé **responder-name** indiquera aussi si le demandé est un agent (UA) ou une mémoire de messages (MS).

Lorsque le demandé est le système MTS lui-même (ou un agent MTA – voir l'article 11), le nom est un nom **MTA-name** connu de l'utilisateur MTS.

8.1.1.1.2.2 Pouvoirs du demandé responder-credentials

Cet argument contient les pouvoirs **credentials** du demandé de l'association, et il est produit par lui.

Les pouvoirs du demandé **responder-credentials** peuvent être utilisés par le demandeur de l'association pour authentifier l'identité du demandé (voir la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Lorsqu'on utilise une authentification simple, les pouvoirs du demandé **responder-credentials** comprennent un mot de passe simple **password** associé au nom du demandé **responder-name**.

Si on utilise une authentification protégée, les pouvoirs du demandé **responder-credentials** comprennent un mot de passe protégé comme le décrit l'article 6 de la Rec. UIT-T X.509 | ISO/CEI 9594-8 (protection1 ou protection2) ainsi qu'à titre facultatif, des arguments de ce procédé de protection (temps1, temps2, aléatoire1 et aléatoire2) dont le sens est précisé par accord mutuel.

Lorsqu'on utilise une authentification renforcée, les pouvoirs du demandé **responder-credentials** comprennent un jeton de rattachement de demandé **responder-bind-token** et, facultativement, un certificat **responder-certificate** ou un sélecteur **certificate-selector**. Il s'agit d'un jeton produit par le demandé de l'association. Il est du même type que le jeton de rattachement de demandeur **initiator-bind-token**. Si le jeton de rattachement de demandé **responder-bind-token** est asymétrique, les données signées **signed-data** comprennent un nombre aléatoire **random-number** (qui peut être lié au nombre aléatoire fourni dans le jeton de rattachement de demandeur). Les données chiffrées **encrypted-data** d'un jeton asymétrique peuvent servir à acheminer des informations secrètes relevant de la sécurité (une ou plusieurs clés symétriques de chiffrement par exemple) servant à sécuriser l'association, ou être absentes du jeton de rattachement de demandé **responder-bind-token**.

On peut utiliser des algorithmes symétriques dans le cadre du jeton asymétrique **asymmetric-token** ci-dessus (voir § 8.5.8).

Le certificat du demandé **responder-certificate** est un certificat **certificate** du demandeur de l'association, produit par une source de confiance (par exemple l'autorité de certification) et, facultativement, de certificats additionnels indiquant un trajet de certification pour le certificat du demandeur. Il peut être fourni par le demandé de l'association si le jeton de rattachement du demandé **responder-bind-token** est un jeton asymétrique**, asymmetric-token**. Si le demandé est un utilisateur du système MTS, le certificat du demandé **responder-certificate** doit contenir l'adresse **OR-address** du demandé dans la composante *x400Address* de son champ de variante nominative d'entité (voir le § 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), à moins que la politique de sécurité ne propose une autre possibilité de rattachement du certificat à l'utilisateur du systéme MTS. Si le demandé est le système MTS, le certificat du demandé **responder-certificate** doit contenir le nom **MTA-name** du demandé dans un nom *mta-name* (voir § A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) de la composante *otherName* de son champ de variante nominative d'entité, à moins que la politique de sécurité ne fournisse une autre possibilité de rattachement des certificats à l'agent MTA demandé. Le certificat du demandé **responder-certificate** peut être utilisé pour acheminer une copie vérifiée de la clé publique de chiffrement asymétrique (**subject-public-key**) du demandé de l'association. Cette clé de certification peut être utilisée par le demandeur pour valider le jeton **responder-bind-token**. Si le demandeur est réputé avoir le **certificate** ou y avoir accès (via l'annuaire), le certificat du demandé **responder-certificate** peut être omis et, si le demandé a plusieurs certificats, un sélecteur de certificat **certificate-selector** peut être fourni pour identifier le certificat au moyen des critères de sélection spécifiés pour la correspondance de certificat (voir § 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

8.1.1.1.2.3 Messages en attente messages-waiting

Cet argument indique le nombre de messages et le nombre total d'octets en instance de remise à l'utilisateur MTS par le système MTS, ventilés par niveau de priorité **priority**. Il peut être produit par le demandé de l'association.

Cet argument n'est présent que lorsque le système MTS est le demandé de l'association et que l'utilisateur MTS souscrit à l'élément de service de mise en instance de remise Hold for Delivery (défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1).

8.1.1.1.3 Erreurs de rattachement bind-errors

Les erreurs de rattachement bind-errors qui peuvent perturber le rattachement MTS-bind sont définies au § 8.1.2.

8.1.1.2 Détachement MTS-unbind

Le détachement MTS-unbind permet au demandeur d'une association établie de la libérer.

8.1.1.2.1 Arguments

Le détachement MTS-unbind ne comporte pas d'arguments.

8.1.1.2.2 Résultats

Le détachement MTS-unbind renvoie un résultat vide qui indique la libération de l'association.

8.1.1.2.3 Erreurs de détachement unbind-errors

Aucune erreur de détachement unbind-error ne peut perturber le détachement MTS-unbind.

8.1.2 Erreurs de rattachement bind-errors

Ce paragraphe définit les erreurs de rattachement bind-errors suivantes:

a) erreur d'authentification authentication-error;

b) occupé busy;

c) mode de dialogue non acceptable unacceptable-dialogue-mode;

d) contexte de sécurité non acceptable unacceptable-security-context;

e) confidentialité d'association inadaptée inadequate-association-confidentiality.

8.1.2.1 Erreur d'authentification authentication-error

L'erreur de rattachement authentication-error (erreur d'authentification) signale l'impossibilité d'établir une association par suite d'une d'erreur d'authentification; les pouvoirs **credentials** du demandeur ne sont pas acceptables ou sont incorrectement spécifiés.

L'erreur de rattachement authentication-error n'a pas de paramètres.

8.1.2.2 Occupé busy

L'erreur de rattachement busy (occupé) signale l'impossibilité d'établir une association, le demandé étant occupé.

L'erreur de rattachement busy (occupé) n'a pas de paramètres.

8.1.2.3 Mode de dialogue non acceptable unacceptable-dialogue-mode

L'erreur de rattachement unacceptable-dialogue-mode (mode de dialogue non acceptable) signale que le mode de dialogue proposé par le demandeur de l'association n'est pas acceptable pour le demandé (voir la Rec. UIT-T X.419 | ISO/CEI 10021-6).

L'erreur de rattachement unacceptable-dialogue-mode (mode de dialogue non acceptable) n'a pas de paramètres.

8.1.2.4 Contexte de sécurité non acceptable unacceptable-security-context

L'erreur de rattachement unacceptable-security-context (contexte de sécurité non acceptable) signale que le contexte de sécurité **security-context** proposé par le demandeur de l'association n'est pas acceptable pour le demandé.

L'erreur de rattachement unacceptable-security-context (contexte de sécurité non acceptable) n'a pas de paramètres.

8.1.2.5 Confidentialité d'association inadaptée Inadequate-association-confidentiality

L'erreur de rattachement Inadequate-association-confidentiality (confidentialité d'association inadaptée) signale qu'une association ne peut pas être établie car la connexion sous-jacente ne fournit pas la confidentialité nécessaire.

8.2 Point d'accès de dépôt submission-port

Le présent paragraphe définit les opérations abstraites et les erreurs abstraites qui se produisent au point d'accès de dépôt submission-port.

8.2.1 Opérations abstraites abstract-operations

Le présent paragraphe définit les opérations abstraites suivantes du point d'accès de dépôt (*submission-port*):

a) dépôt de message *message-submission*;

b) dépôt d'envoi-test *probe-submission*;

c) annulation de remise différée *cancel-deferred-delivery*;

d) commande de dépôt *submission-control*.

8.2.1.1 Dépôt de message Message-submission

L'opération abstraite de dépôt de message Message-submission permet à un utilisateur MTS de déposer un message auprès du système MTS pour transfert et remise à un ou plusieurs utilisateurs MTS destinataires.

L'achèvement avec succès de l'opération abstraite signifie que le système MTS a accepté la responsabilité du message (mais non qu'il l'a déjà remis aux destinataires prévus).

La perturbation de cette opération abstraite abstract-operation par une erreur abstraite abstract-error indique que le système MTS ne peut assumer la responsabilité du message.

8.2.1.1.1 Arguments

Le Tableau 3 énumère les arguments de l'opération abstraite de dépôt de message Message-submission, en qualifie la présence et spécifie le paragraphe dans lequel ils sont définis.

8.2.1.1.1.1 Nom d'expéditeur originator-name

Cet argument contient le nom **OR-name** de l'expéditeur du message. Il est produit par l'utilisateur MTS expéditeur. Si l'adresse **OR-address** n'est pas incluse dans le nom d'expéditeur **originator-name**, il sera inséré par l'agent MTA expéditeur. Le nom d'expéditeur **originator-name** restera inchangé tout le temps de l'acheminement du message à travers le système MTS. Lorsque des arguments de sécurité utilisent le nom d'expéditeur **originator-name**, son adresse **OR-address** sera produite par l'utilisateur MTS expéditeur.

Le nom d'expéditeur **originator-name** contient le nom **OR-name** d'un expéditeur individuel et ne doit pas contenir celui d'une liste DL.

8.2.1.1.1.2 Nom de destinataire recipient-name

Cet argument contient le nom **OR-name** d'un destinataire du message. Il est produit par l'expéditeur. Une valeur de cet argument doit être spécifiée pour chaque destinataire du message.

Le nom de destinataire **recipient-name** contient le nom **OR-name** d'un destinataire individuel ou d'une liste DL.

8.2.1.1.1.3 Destinataire suppléant autorisé *alternate-recipient-allowed*

Cet argument précise si le message peut être remis à un destinataire suppléant désigné par le domaine de gestion MD destinataire, lorsque le nom de destinataire **recipient-name** n'identifie pas un utilisateur du système MTS. Il peut être produit par l'expéditeur du message.

Cet argument peut prendre l'une des valeurs suivantes: **alternate-recipient-allowed** (destinataire suppléant autorisé) ou **alternate-recipient-prohibited** (destinataire suppléant interdit).

Si l'argument a la valeur **alternate-recipient-allowed** (autorisé) et si le nom de destinataire **recipient-name** (spécifié par l'expéditeur du message, ajouté par développement de liste DL, ou remplacé par réacheminement vers un destinataire suppléant désigné par le destinataire (**recipient-assigned-alternate-recipient**) ou par l'expéditeur (**originator-requested-alternate-recipient**), ou présent en vertu d'une combinaison quelconque de réacheminement et de développement de liste) n'identifie pas d'utilisateur MTS, le message peut être réacheminé vers un destinataire suppléant désigné à cette fin par le domaine de gestion destinataire. Si aucun destinataire suppléant alternate-recipient n'a été désigné par le domaine de gestion destinataire, ou si cet argument a la valeur **alternate-recipient-prohibited** (interdit), un rapport de non-remise doit être produit.

En l'absence de cet argument, la valeur **alternate-recipient-prohibited** (destinataire suppléant interdit) est adoptée par défaut.

Tableau 3 – Arguments de l'opération de dépôt de message Message-submission

Argument	Présence	Paragraphe
Argument d'expéditeur		
Nom d'expéditeur *originator-name*	M	8.2.1.1.1.1
Arguments de destinataire		
Nom de destinataire *recipient-name*	M	8.2.1.1.1.2
Autorisation de destinataire suppléant *alternate-recipient-allowed*	O	8.2.1.1.1.3
Interdiction de réassignation de destinataire *recipient-reassignment-prohibited*	O	8.2.1.1.1.4
Destinataire suppléant désigné par l'expéditeur *originator-requested-alternate-recipient*	O	8.2.1.1.1.5
Interdiction de développement de liste DL *DL-expansion-prohibited*	O	8.2.1.1.1.6
Divulgation des autres destinataires *disclosure-of-other-recipients*	O	8.2.1.1.1.7
Destinataires exemptés de liste DL *DL-exempted-recipients*	O	8.2.1.1.1.40
Argument de priorité		
Priorité priority	O	8.2.1.1.1.8
Arguments de conversion		
Interdiction de conversion implicite *Implicit-conversion-prohibited*	O	8.2.1.1.1.9
Interdiction de conversion avec perte *conversion-with-loss-prohibited*	O	8.2.1.1.1.10
Conversion explicite *explicit-conversion*	O	8.2.1.1.1.11
Arguments de date et heure de remise		
Heure de remise différée *deferred-delivery-time*	O	8.2.1.1.1.12
Heure limite de remise *latest-delivery-time*	O	8.2.1.1.1.13
Argument de méthode de remise		
Méthode de remise demandée *requested-delivery-method*	O	8.2.1.1.1.14
Arguments de remise physique		
Interdiction de retransmission physique *physical-forwarding-prohibited*	O	8.2.1.1.1.15
Demande d'adresse de retransmission physique *physical-forwarding-address-request*	O	8.2.1.1.1.16
Modes de remise physique *physical-delivery-modes*	O	8.2.1.1.1.17
Type de courrier recommandé *registered-mail-type*	O	8.2.1.1.1.18
Numéro de destinataire pour avis *recipient-number-for-advice*	O	8.2.1.1.1.19
Attributs de restitution physique *physical-rendition-attributes*	O	8.2.1.1.1.20
Adresse de renvoi à l'expéditeur *originator-return-address*	O	8.2.1.1.1.21
Arguments de demande de rapport		
Demande de rapport par l'expéditeur *originator-report-request*	M	8.2.1.1.1.22
Demande de retour de contenu *content-return-request*	O	8.2.1.1.1.23
Demande de rapport de remise physique *physical-delivery-report-request*	O	8.2.1.1.1.24
Arguments de sécurité		
Certificat d'expéditeur *originator-certificate*	O	8.2.1.1.1.25
Jeton de message *message-token*	O	8.2.1.1.1.26
Identificateur d'algorithme de confidentialité de contenu *content-confidentiality-algorithm-identifier*	O	8.2.1.1.1.27
Vérification d'intégrité de contenu *content-integrity-check*	O	8.2.1.1.1.28
Contrôle d'authentification d'origine de message *message-origin-authentication-check*	O	8.2.1.1.1.29
Etiquette de sécurité de message *message-security-label*	O	8.2.1.1.1.30
Demande de preuve de dépôt *proof-of-submission-request*	O	8.2.1.1.1.31
Demande de preuve de remise *proof-of-delivery-request*	O	8.2.1.1.1.32
Certificats d'expéditeurs multiples *multiple-originator-certificates*	O	8.2.1.1.1.41
Certificats de destinataires *recipient-certificate*	O	8.2.1.1.1.42
Sélecteurs de certificats *certificate-selectors*	O	8.2.1.1.1.43
Violation des sélecteurs de certificats *certificate-selectors-override*	O	8.2.1.1.1.44

Tableau 3 – Arguments de l'opération de dépôt de message Message-submission

Argument	Présence	Paragraphe
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	O	8.2.1.1.1.33
Type de contenu *content-type*	M	8.2.1.1.1.34
Identificateur de contenu *content-identifier*	O	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	O	8.2.1.1.1.36
Contenu *content*	M	8.2.1.1.1.37
Type de notification *notification-type*	O	8.2.1.1.1.38
Message de service *service-message*	O	8.2.1.1.1.39

8.2.1.1.1.4 Interdiction de réassignation de destinataire recipient-reassignment-prohibited

Cet argument indique si le message peut être réassigné à un autre utilisateur MTS enregistré par le destinataire prévu comme destinataire suppléant **recipient-assigned-alternate-recipient**. Il peut être produit par l'expéditeur du message.

Cet argument peut prendre l'une des valeurs suivantes: **recipient-reassignment-prohibited** (réassignation de destinataire interdite) ou **recipient-reassignment-allowed** (réassignation de destinataire autorisée).

Si cet argument a la valeur **recipient-reassignment-allowed** (autorisé) et si le destinataire prévu a enregistré un destinataire suppléant valide **recipient-assigned-alternate-recipient**, le message est réacheminé vers ce dernier.

Si cet argument a la valeur **recipient-reassignment-prohibited** (interdit) et si le destinataire prévu a enregistré un destinataire suppléant valide **recipient-assigned-alternate-recipient**, et que l'expéditeur ait spécifié un destinataire suppléant **originator-requested-alternate-recipient**, c'est vers ce dernier que le message est réacheminé; si aucun destinataire suppléant n'a été spécifié par l'expéditeur, un rapport de non-remise non-delivery-report doit être produit.

En l'absence de cet argument, la valeur **recipient-reassignment-allowed** (autorisé) est adoptée par défaut.

8.2.1.1.1.5 Destinataire suppléant désigné par l'expéditeur originator-requested-alternate-recipient

Cet argument contient le nom **OR-name** du destinataire suppléant désigné par l'expéditeur du message. Il peut être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

Le destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient** contient le nom **OR-name** d'un destinataire suppléant individuel ou d'une liste DL.

Si cet argument est présent et qu'il s'avère impossible de remettre le message au nom de destinataire **recipient-name** (spécifié par l'expéditeur, ou ajouté par développement de liste DL, ou encore remplacé par réacheminement vers le destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient**), le message est réacheminé vers le destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient** spécifié par cet argument.

Si un destinataire suppléant **originator-requested-alternate-recipient** a été spécifié par l'expéditeur, le message est réacheminé vers ce destinataire suppléant de préférence à celui qui a été assigné par le domaine de gestion destinataire.

8.2.1.1.1.6 Interdiction de développement de liste DL-expansion-prohibited

Cet argument indique si les noms de destinataire correspondant à une liste de distribution DL doivent être développés dans le système MTS. Il peut être produit par l'expéditeur.

Cet argument peut prendre l'une des valeurs suivantes: **DL-expansion-prohibited** (développement de liste DL interdit) ou **DL-expansion-allowed** (développement de liste DL autorisé).

En l'absence de cet argument, la valeur **DL-expansion-allowed** (autorisé) est adoptée par défaut.

8.2.1.1.1.7 Divulgation d'autres destinataires disclosure-of-other-recipients

Cet argument indique si le nom **recipient-name** de tous les destinataires doit être indiqué à chaque utilisateur MTS destinataire à la remise du message. Il peut être produit par l'expéditeur du message.

Cet argument peut prendre l'une des valeurs suivantes: **disclosure-of-other-recipients-requested** (divulgation demandée) ou **disclosure-of-other-recipients-prohibited** (divulgation interdite).

En l'absence de cet argument, la valeur **disclosure-of-other-recipients-prohibited** (interdit) est adoptée par défaut.

8.2.1.1.1.8 Priorité priority

Cet argument spécifie la priorité relative du message: **normal**, **non urgent** ou **urgent**. Il peut être produit par l'expéditeur.

En l'absence de cet argument, la valeur **priority** (priorité) "**normal**" est adoptée par défaut.

8.2.1.1.1.9 Interdiction de conversion implicite implicit-conversion-prohibited

Cet argument indique si une conversion implicite peut être effectuée sur le contenu **content** du message. Il peut être produit par l'expéditeur.

Cet argument peut prendre l'une des valeurs suivantes: **implicit-conversion-prohibited** (conversion implicite interdite) ou **implicit-conversion-allowed** (conversion implicite autorisée).

En l'absence de cet argument, la valeur **implicit-conversion-allowed** (autorisé) est adoptée par défaut.

Voir également § 8.2.1.1.1.10.

8.2.1.1.1.10 Interdiction de conversion avec perte conversion-with-loss-prohibited

Cet argument indique si des conversions de type d'information codée **encoded-information-type** peuvent être effectuées sur le contenu **content** du message, au cas où cela entraînerait une perte d'information. La perte d'information est définie dans la Rec. X.408 du CCITT. Cet argument peut être produit par l'expéditeur.

Cet argument peut prendre l'une des valeurs suivantes: **conversion-with-loss-prohibited** (conversion avec perte interdite) ou **conversion-with-loss-allowed** (conversion avec perte autorisée).

En l'absence de cet argument, la valeur **conversion-with-loss-allowed** (autorisé) est adoptée par défaut.

L'effet combiné des arguments d'interdiction de conversion implicite **implicit-conversion-prohibited** et d'interdiction de conversion avec perte **conversion-with-loss-prohibited** est défini au Tableau 4.

Tableau 4 – Effet combiné des arguments de conversion

Conversion implicite	Conversion avec perte	Effet combiné
autorisée	autorisée avec perte	autorisé
autorisée	interdite avec perte	interdit avec perte
interdite	autorisée avec perte	interdit
interdite	interdite avec perte	interdit

8.2.1.1.1.11 Conversion explicite explicit-conversion

Cet argument indique le type de conversion du contenu **content** du message demandé explicitement par l'expéditeur pour le destinataire. Il peut être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes: **ia5-text-to-teletex** (IA5/télétex), **ia5-text-to-g3-facsimile** (IA5/télécopie G3), **ia5-text-to-g4-class-1** (IA5/télécopie G4 classe 1), **ia5-text-to-videotex** (IA5/vidéotex), **teletex-to-ia5-text** (télétex/IA5), **teletex-to-g3-facsimile** (télétex/télécopie G3), **teletex-to-g4-class-1** (télétex/télécopie G4 classe 1), **teletex-to-videotex** (télétex/vidéotex), **videotex-to-ia5-text** (vidéotex/IA5) ou **videotex-to-teletex** (vidéotex/télétex). D'autres types de conversion explicite **explicit-conversion** pourront être définis par des addenda ou de futures versions de la présente Recommandation | Norme internationale. La conversion explicite **explicit-conversion** sera effectuée conformément aux spécifications de la Rec. X.408 du CCITT.

En l'absence de cet argument, aucune conversion explicite ne sera effectuée.

NOTE – Lorsqu'elle est spécifiée pour une liste DL destinataire, la conversion explicite **explicit-conversion** s'applique à tous les membres de cette liste.

8.2.1.1.1.12 Heure de remise différée deferred-delivery-time

Cet argument spécifie la date et l'heure **Time** avant lesquelles le message ne doit pas être remis à ses destinataires. Il peut être produit par l'expéditeur.

8.2.1.1.1.13 Heure limite de remise latest-delivery-time

Cet argument contient la date et l'heure **Time** après lesquelles le message ne doit pas être remis à ses destinataires. Il peut être produit par l'expéditeur.

Le traitement de la non-remise pour cause de dépassement de l'heure limite **latest-delivery-time** de remise est décrit au § 14.3.2.4.

8.2.1.1.1.14 Méthode de remise demandée requested-delivery-method

Cet argument indique la méthode préférée de remise du message à son destinataire. Il peut être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre une ou plusieurs des valeurs suivantes: **any-delivery-method** (méthode de remise indifférente), **mhs-delivery** (remise par messagerie), **physical-delivery** (remise physique), **telex-delivery** (remise télex), **teletex-delivery** (remise télétex), **g3-facsimile-delivery** (remise par télécopie G3), **g4-facsimile-delivery** (remise par télécopie G4), **ia5-terminal-delivery** (remise sur terminal IA5), **videotex-delivery** (remise vidéotex) ou **telephone-delivery** (remise téléphonique).

Lorsque plusieurs valeurs de cet argument sont spécifiées pour un destinataire donné, la séquence des valeurs est censée refléter l'ordre de préférence de l'expéditeur concernant les méthodes de remise.

En l'absence de cet argument, la valeur **any-delivery-method** (méthode indifférente) est adoptée par défaut.

Si le nom de destinataire **recipient-name** produit par l'expéditeur du message contient un nom d'annuaire **directory-name** mais en omet l'adresse **OR-address**, le système MTS peut utiliser la méthode de remise demandée **requested-delivery-method** comme indication du type d'adresse **OR-address** auquel le nom d'annuaire **directory-name** doit être associé par le système MTS (en utilisant l'annuaire par exemple). S'il n'est pas possible de trouver d'adresse **OR-address**, on renverra à l'expéditeur un message d'erreur abstraite de spécification incorrecte de destinataire **recipient-improperly-specified** ou un rapport de non-remise.

S'il y a incompatibilité entre la méthode de remise demandée **requested-delivery-method** fournie par l'expéditeur et la méthode de remise préférée par le destinataire (telle qu'elle est par exemple enregistrée dans l'annuaire dans l'attribut de méthode de remise préférée mhs), c'est la méthode de remise demandée par l'expéditeur qui prime. Si la méthode de remise demandée par l'expéditeur est incompatible avec ses spécifications de conversion (voir du § 8.2.1.1.1.9 au § 8.2.1.1.1.11), un rapport de non-remise lui sera renvoyé.

8.2.1.1.1.15 Interdiction de retransmission physique en renvoi physical-forwarding-prohibited

Cet argument indique l'interdiction éventuelle de la retransmission physique du message. Il peut être produit par l'expéditeur du message lorsque l'argument de méthode de remise demandée **requested-delivery-method** spécifie une remise physique au destinataire ou lorsque l'expéditeur du message a fourni une adresse postale **postal-OR-address** de destinataire. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre une des valeurs suivantes: **physical-forwarding-allowed** (retransmission physique autorisée) ou **physical-forwarding-prohibited** (retransmission physique interdite).

En l'absence de cet argument, la valeur **physical-forwarding-allowed** (autorisé) est adoptée par défaut.

8.2.1.1.1.16 Demande d'adresse de retransmission physique physical-forwarding-address-request

Cet argument indique si l'adresse de retransmission physique **physical-forwarding-address** du destinataire doit être renvoyée dans le rapport. Il peut être produit par l'expéditeur du message lorsque l'argument de méthode de remise demandée **requested-delivery-method** spécifie une remise physique au destinataire ou lorsque l'expéditeur fournit une adresse postale **postal-OR-address** de destinataire. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes: **physical-forwarding-address-requested** (adresse de retransmission physique demandée) ou **physical-forwarding-address-not-requested** (adresse de retransmission physique non demandée).

En l'absence de cet argument, la valeur **physical-forwarding-address-not-requested** (non demandée) est adoptée par défaut.

Une adresse de retransmission physique physical-forwarding-address peut être spécifiée, que la retransmission physique soit interdite ou autorisée (voir § 8.2.1.1.1.15).

8.2.1.1.1.17 Modes de remise physique physical-delivery-modes

Cet argument indique le mode de remise physique à adopter. Il peut être produit par l'expéditeur du message si l'argument de méthode de remise demandée **requested-delivery-method** spécifie la remise physique au destinataire ou si l'expéditeur du message fournit l'adresse postale **postal-OR-address** du destinataire. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

La valeur de cet argument est la combinaison de deux éléments indépendants. S'il est présent, le premier élément prend l'une des valeurs suivantes: **ordinary-mail** (courrier ordinaire), **special-delivery** (remise spéciale), **express-mail** (courrier express), **counter-collection** (retrait au guichet), **counter-collection-with-telephone-advice** (retrait au guichet avec avis téléphonique), **counter-collection-with-telex-advice** (retrait au guichet avec avis télex), ou **counter-collection-with-teletex-advice** (retrait au guichet avec avis télétex). S'il est présent, le second élément peut prendre la valeur **bureau-fax-delivery** (remise par Bureaufax). Si la remise par Bureaufax est demandée et si le premier élément est également présent, celui-ci est alors activé par le service Bureaufax.

La remise par Bureaufax **bureau-fax-delivery** comprend l'ensemble des modes de remise de A à H définis dans la Rec. F.170 du CCITT, à savoir: A – Courrier ordinaire, B – Porteur spécial, C – Courrier express, D – Retrait au guichet, E – Retrait au guichet avec avis téléphonique, F – Télécopie, G – Retrait au guichet avec avis télex et H – Retrait au guichet avec avis télétex.

En l'absence de cet argument, la valeur **ordinary-mail** (courrier ordinaire) est adoptée par défaut.

8.2.1.1.1.18 Type de courrier recommandé registered-mail-type

Cet argument indique le type de service de courrier recommandé à utiliser pour remettre physiquement le message au destinataire. Il peut être produit par l'expéditeur du message lorsque l'argument méthode de remise demandée **requested-delivery-method** spécifie que le message doit être physiquement remis au destinataire ou lorsque l'expéditeur fournit une adresse postale **postal-OR-address** de destinataire. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes: **non-registered-mail** (courrier non recommandé), **registered-mail** (courrier recommandé), **registered-mail-to-addressee-in-person** (courrier recommandé à remettre en mains propres).

En l'absence de cet argument, la valeur **non-registered-mail** (courrier non recommandé) est adoptée par défaut.

8.2.1.1.1.19 Numéro de destinataire pour avis recipient-number-for-advice

Cet argument contient le numéro de téléphone, de télex ou de télétex du destinataire, destiné à être utilisé avec les modes de remise physique **counter-collection-with-advice** (retrait au guichet avec avis) et **bureau-fax-delivery**. Il peut être produit par l'expéditeur du message si l'argument de méthode de remise demandée **requested-delivery-method** spécifie que le message doit être physiquement remis au destinataire ou si l'expéditeur du message fournit une adresse postale **postal-OR-address** de destinataire et si l'argument modes de remise physique **physical-delivery-modes** spécifie le mode **counter-collection-with-advice** (retrait au guichet avec avis) ou **bureau-fax-delivery**. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

8.2.1.1.1.20 Attributs de restitution physique physical-rendition-attributes

Cet argument indique les attributs de restitution physique **physical-rendition-attributes** à appliquer lorsque le message est restitué sous forme physique. Il peut être produit par l'expéditeur du message si le message nécessite probablement une restitution, par exemple si l'adresse de destinataire désigne une unité d'accès ou si la méthode de remise demandée **requested-delivery-method** spécifie une méthode de remise mettant en jeu une unité physique. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

Cet argument est spécifié comme un Identificateur d'Objet. Les valeurs suivantes sont définies dans la présente spécification:

> **basic** (élémentaire) Aucune restitution spéciale n'est requise – la restitution normale offerte par l'unité AU devrait être appliquée;
>
> **no-cover-page** (pas de page de couverture) Le message devrait être restitué sans qu'aucune page de couverture fournie par l'AU soit ajoutée. Cette valeur est particulièrement appropriée pour les unités d'accès de télécopie.

D'autres valeurs de cet argument peuvent être enregistrées de façon privée et utilisées dans le cadre d'un accord. Des ajouts ou de futures versions de la présente Recommandation | Norme Internationale peuvent définir d'autres valeurs normalisées.

En l'absence de cet argument, la valeur **basic** doit être adoptée par défaut.

8.2.1.1.1.21 Adresse de retour à l'expéditeur originator-return-address

Cet argument contient l'adresse **postal-OR-address** de l'expéditeur du message. Il peut être produit par l'expéditeur lorsque l'argument de méthode de remise demandée **requested-delivery-method** spécifie une remise physique du message à un ou plusieurs destinataires ou lorsque l'expéditeur a fourni une ou plusieurs adresses **postal-OR-addresses** de destinataire. Il peut également être produit par l'expéditeur lorsqu'une liste DL destinataire comporte ou risque de comporter un ou plusieurs éléments pour lesquels une remise physique est demandée.

L'adresse de retour à l'expéditeur **originator-return-address** doit contenir l'adresse **postal-OR-address** d'un expéditeur individuel (adresse **OR-address**) et non le nom d'annuaire **directory-name** de l'expéditeur ou d'une liste DL.

8.2.1.1.1.22 Demande de rapport par l'expéditeur originator-report-request

Cet argument indique le type de rapport requis par l'expéditeur du message. Il doit être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes:

no-report (pas de rapport): l'expéditeur du message demande la suppression des rapports de non-remise non-delivery-reports;

non-delivery-report (rapport de non-remise): un rapport n'est fourni qu'en cas de non-remise;

report (rapport): un rapport est renvoyé en cas de remise ou de non-remise.

La valeur de cet argument peut être modifiée en un point de développement de liste DL conformément à la politique de présentation de rapport de la liste DL. Une telle modification peut affecter le nombre et le type de rapports que peut recevoir l'expéditeur au sujet de la remise à la liste DL.

8.2.1.1.1.23 Demande de renvoi de contenu content-return-request

Cet argument indique si le contenu **content** du message doit être renvoyé avec un éventuel rapport de non-remise. Il peut être produit par l'expéditeur.

Cet argument peut prendre l'une des valeurs suivantes: **content-return-requested** (renvoi de contenu demandé) ou **content-return-not-requested** (renvoi de contenu non demandé).

En l'absence de cet argument, la valeur **content-return-not-requested** (renvoi de contenu non demandé) est adoptée par défaut.

La suppression des rapports de non-remise non-delivery-reports par l'expéditeur (voir § 8.2.1.1.1.22) a priorité sur toute demande de renvoi du contenu.

Si des rapports de non-remise sont remis au titulaire d'une liste DL (voir § 8.3.1.2.1.4), le contenu du message n'est pas présent.

8.2.1.1.1.24 Demande de rapport de remise physique physical-delivery-report-request

Cet argument indique le type de rapport de remise physique demandé par l'expéditeur du message. Il peut être produit par l'expéditeur du message si l'argument de méthode de remise demandée **requested-delivery-method** spécifie que le message doit être physiquement remis au destinataire ou si l'expéditeur a fourni une adresse **postal-OR-address** de destinataire. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

Cet argument peut prendre l'une des valeurs suivantes: **return-of-undeliverable-mail-by-PDS** (retour du courrier non remis par distribution physique PDS), **return-of-notification-by-PDS** (retour de notification par PDS), **return-of-notification-by-MHS** (retour de notification par MHS) ou **return-of-notification-by-MHS-and-PDS** (retour de notification par MHS et PDS).

En l'absence de cet argument, la valeur **return-of-undeliverable-mail-by-PDS** (retour du courrier non remis par PDS) est adoptée par défaut.

8.2.1.1.1.25 Certificat d'expéditeur originator-certificate

Cet argument contient le certificat **certificate** de l'expéditeur du message. Il est produit par une source de confiance (par exemple par une autorité de certification) et peut être fourni par l'expéditeur lui-même.

Le certificat d'expéditeur **originator-certificate** peut servir à acheminer une copie certifiée de la clé publique de codage asymétrique (*public-asymmetric-encryption-key*) (**subject-public-key**) (clé publique de sujet) de l'expéditeur du message.

NOTE – Si plusieurs certificats d'expéditeur doivent être transmis à tous les destinataires, le certificat pour le message **message-origin-authentication-check** est véhiculé dans cet argument et les autres certificats dans l'argument **multiple-originator-certificates** (certificats d'expéditeur multiple). Si des certificats dédiés sont requis pour chaque destinataire, les certificats dédiés sont identifiés dans l'argument **certificates-selectors-override** (voir le § 8.2.1.1.1.44).

Lorsque le même algorithme et la même clé secrète ont été utilisés pour calculer les signatures numériques véhiculées dans un ou plusieurs des arguments suivants: **message-origin-authentication-check** (contrôle d'authentification d'origine de message), **content-integrity-check** (vérification d'intégrité de contenu) ou **message-token** (jeton de message), la clé publique public-asymmetric-encryption-key correspondante de l'expéditeur peut être utilisée par les destinataires du message afin de valider les signatures numériques véhiculées dans l'argument **content-integrity-check** (vérification d'intégrité de contenu) et, si le jeton asymétrique **asymmetric-token** est utilisé avec un algorithme asymétrique (voir § 8.5.8*)*, véhiculées dans l'argument **message-token** (jeton de message). Il peut également être utilisé par les destinataires du message et par n'importe quel agent MTA au travers duquel le message est transféré, afin de valider la vérification d'authentification d'origine de message **message-origin-authentication-check**.

8.2.1.1.1.26 Jeton de message message-token

Cet argument contient le jeton associé au message. Il peut être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Si le jeton **message-token** est asymétrique (**asymmetric-token**), les données signées **signed-data** peuvent comprendre:

l'un quelconque des arguments suivants: **content-confidentiality-algorithm-identifier** (identificateur d'algorithme de confidentialité de contenu), **content-integrity-check** (vérification d'intégrité de contenu), **message-security-label** (étiquette de sécurité de message), **proof-of-delivery-request** (demande de preuve de remise);

un numéro de séquence **message-sequence-number** qui identifie la position du message dans une séquence de messages envoyés par l'expéditeur au destinataire auquel le jeton **message-token** se rapporte (pour fournir l'élément de service d'intégrité de séquence de messages Message Sequence Integrity, selon la définition donnée dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). La première occurrence d'un numéro de séquence peut être un nombre aléatoire.

Si le jeton **message-token** est asymétrique (**asymmetric-token**), les données chiffrées **encrypted-data** peuvent comprendre:

une clé de confidentialité de contenu **content-confidentiality-key**: clé de codage symétrique utilisée par l'expéditeur en même temps que l'identificateur d'algorithme de confidentialité de contenu **content-confidentiality-algorithm-identifier** pour chiffrer le contenu du message et par le destinataire pour déchiffrer le contenu du message;

la vérification d'intégrité de contenu **content-integrity-check**: qui peut être insérée dans les données chiffrées **encrypted-data** lorsqu'il est nécessaire d'assurer la confidentialité de la vérification d'intégrité de contenu **content-integrity-check** ou lorsque l'étiquette de sécurité **message-security-label** est incluse dans les données chiffrées **encrypted-data** (pour en assurer la confidentialité) et qu'il faut maintenir l'association entre la vérification d'intégrité de contenu content-integrity-check et l'étiquette de sécurité de message message-security-label;

l'étiquette de sécurité de message **message-security-label**: peut être incluse dans les données chiffrées **encrypted-data** s'il est nécessaire d'en assurer la confidentialité;

une clé d'intrégrité de contenu **content-integrity-key**: clé de chiffrement symétrique utilisée avec l'identificateur d'algorithme d'intégrité de contenu **content-integrity-algorithm-identifier** par l'expéditeur pour calculer la vérification d'intégrité de contenu **content-integrity-check** et par le destinataire pour valider ce dernier argument;

un numéro de séquence de message **message-sequence-number**: tel qu'il est défini pour les données signées **signed-data** ci-dessus, mais qui peut être inclus dans les données chiffrées **encrypted-data** s'il faut assurer la confidentialité de la séquence. La première occurrence d'un numéro de séquence peut être un nombre aléatoire.

Si le jeton **message-token** est asymétrique (**asymmetric-token**) et si les données signées **signed-data** du jeton **message-token** comprennent la vérification d'intégrité de contenu **content-integrity-check**, le jeton de message peut assurer la non-répudiation d'origine du contenu du message, sous réserve de la disponibilité d'une infrastructure appropriée de clés publiques (élément de service de non-répudiation d'origine, tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Si les données signées **signed-data** du jeton **message-token** comprennent à la fois la vérification d'intégrité de contenu **content-integrity-check** et l'étiquette de sécurité de message **message-security-label**, le jeton de message fournit une preuve d'association entre l'étiquette de sécurité **message-security-label** et le contenu du message.

Des algorithmes symétriques peuvent être utilisés dans les jetons asymétriques **asymmetric-token** ci-dessus (voir § 8.5.8). Si des algorithmes symétriques sont utilisés à la fois pour le jeton **message-token** et pour la vérification d'intégrité de contenu **content-integrity-check**, alors ce jeton ne peut prendre en charge l'élément de service de non-répudiation d'origine que si la politique de sécurité en vigueur prévoit l'implication d'une tierce partie tenant le rôle de notaire.

NOTE 1 – Si plusieurs certificats doivent être échangés pour traiter le jeton de message **message-token**, ces certificats peuvent être transportés dans l'argument **multiple-originator-certificates** (certificats d'expéditeur multiple), dans l'argument **recipient-certificate** (certificats par destinataire), ou dans les deux arguments à la fois.

NOTE 2 – Un certificat requis pour mettre en œuvre un accord de clé pour les données chiffrées du jeton, peut utiliser un certificat d'expéditeur dans l'argument **multiple-originator-certificates** (certificats d'expéditeur multiple), ainsi que le certificat de destinataire dans l'argument **recipient-certificates** (certificat par destinataire). Le certificat approprié peut être identifié au moyen de la version 3 des certificats qui contient, pour cela, des extensions de certificat; cette identification peut être acheminée dans les **arguments certificate-selectors** et **certificate-selectors-override**. (Par exemple, le champ **key usage** peut être utilisé pour indiquer que le certificat doit être utilisé pour un accord de clé et le champ **certificate policies** peut être utilisé pour indiquer la politique sous laquelle l'accord clé doit fonctionner).

8.2.1.1.1.27 Identificateur d'algorithme de confidentialité de contenu content-confidentiality-algorithm-identifier

Cet argument contient un identificateur d'algorithme **algorithm-identifier**, qui identifie l'algorithme qu'utilise l'expéditeur du message pour chiffrer le contenu du message (pour assurer l'élément de service de confidentialité du contenu tel que défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur du message.

Le ou les destinataires peuvent utiliser cet algorithme pour déchiffrer le contenu **content** du message.

L'algorithme de confidentialité de contenu peut être un algorithme de chiffrement symétrique ou asymétrique.

Lorsqu'on utilise un algorithme de chiffrement symétrique, la clé de confidentialité de contenu **content-confidentiality-key** que l'expéditeur utilise pour chiffrer le contenu du message et que le destinataire peut utiliser pour déchiffrer ce contenu, peut être obtenue à partir du jeton **message-token** envoyé avec le message. Une autre façon de faire consiste à distribuer la clé de confidentialité **content-confidentiality-key** par d'autres moyens.

Lorsqu'on utilise un algorithme de chiffrement asymétrique, l'expéditeur du message peut utiliser la clé publique de chiffrement asymétrique public-asymmetric-encryption-key du destinataire prévu pour chiffrer le contenu du message. Le destinataire peut utiliser sa clé secrète de chiffrement asymétrique secret-asymmetric-encryption-key pour déchiffrer ce contenu. Lorsqu'on utilise un algorithme de chiffrement asymétrique, le message ne peut être adressé qu'à un seul destinataire ou à un ensemble de destinataires partageant le même couple de clés de chiffrement asymétrique.

8.2.1.1.1.28 Vérification d'intégrité de contenu content-integrity-check

Cet argument fournit au destinataire du message un moyen de valider le fait que le contenu du message n'a pas été modifié (afin de fournir l'élément de service d'intégrité de contenu comme cela est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur du message. Une valeur différente de cet argument peut être définie pour chaque destinataire du message.

Si la valeur de cet argument est spécifique à un destinataire, parce qu'un algorithme ou une clé spécifique a été utilisé pour produire cette valeur (par exemple lorsque différentes valeurs de l'argument sont définies pour chaque destinataire du message), les certificats appropriés peuvent être véhiculés dans l'argument **multiple-originator-certificates** et identifiés par l'argument **certificate-selectors-override**.

Si le même algorithme et la même clé ont été utilisés pour produire cet argument pour tous les destinataires (c'est-à-dire que la même valeur de l'argument est spécifiée pour chaque destinataire du message), le certificat approprié peut être véhiculé par l'argument **originator-certificates** (certificats de l'expéditeur) ou, si plus d'un certificat d'expéditeur doit être transporté, l'argument **multiple-originator-certificates (**certificats d'expéditeur multiple) doit être utilisé et le certificat approprié doit être identifié par les arguments **certificate-selectors** et **certificate-selectors-override**.

Cet argument permet au destinataire du message de valider l'intégrité du contenu du message reçu ainsi que l'authentification de l'expéditeur du message.

La vérification d'intégrité de message **content-integrity-check** permet de valider l'intégrité du contenu pour un destinataire en utilisant soit un algorithme de chiffrement symétrique soit un algorithme de chiffrement asymétrique.

NOTE 1 – La vérification d'authentification d'origine de message **message-origin-authentication-check** fournit un moyen de valider l'intégrité du contenu par message en utilisant un algorithme de chiffrement asymétrique.

La vérification d'intégrité de contenu **(content-integrity-check)** peut également être incluse dans les données signées (**signed-data)** ou dans les données chiffrées **encrypted-data** du jeton de message **message-token** pour assurer la non-répudiation de l'origine du contenu du message, et constituer une preuve d'association entre l'étiquette de sécurité **message-security-label** et le contenu du message.

NOTE 2 – Ainsi, il y a trois arguments distincts de vérification d'intégrité de contenu **content-integrity-check**, un par argument de destinataire et deux dans le jeton de message**.**

La vérification d'intégrité de contenu **content-integrity-check** est calculée au moyen de l'algorithme identifié par l'identificateur d'algorithme d'intégrité de contenu **content-integrity-algorithm-identifier** (un identificateur d'algorithme **algorithm-identifier**).

NOTE 3 – Les différents arguments de vérification d'intégrité de contenu **CONTENT-INTEGRITY-CHECK** peuvent être calculés au moyen d'algorithmes différents. La vérification d'intégrité de contenu **CONTENT-INTEGRITY-CHECK**, en particulier lorsqu'elle est incluse dans les données signées **SIGNED-DATA** ou dans les données chiffrées **ENCRYPTED-DATA** du jeton de message **MESSAGE-TOKEN**, peut être calculée au moyen d'un algorithme différent de l'argument de vérification d'intégrité de contenu **content-integrity-check** par destinataire.

La vérification d'intégrité de contenu **content-integrity-check** contient l'identificateur d'algorithme **algorithm-identifier** d'intégrité de contenu et une signature numérique produite au moyen d'une ou de plusieurs fonctions chiffrées (par exemple en version comprimée, en version hachée simple ou en version hachée double) appliquée(s) au contenu du message et, de façon conditionnelle, l'identificateur d'algorithme d'intégrité de contenu **content-integrity-algorithm-identifier.**

NOTE 4 – La vérification d'intégrité de contenu **content-integrity-check** pourrait être calculée au moyen du contenu en clair (c'est-à-dire non chiffré) ou du contenu chiffré. Ce choix peut être effectué indépendamment pour chaque occurrence de la vérification d'intégrité de contenu du message. Ce choix est dicté par la politique de sécurité en vigueur et peut également être indiqué par l'identificateur d'algorithme d'intégrité de contenu **content-integrity-algorithm-identifier**.

L'identificateur **content-integrity-algorithm-identifier** spécifiera:

1) si la vérification **content-integrity-check** est calculée au moyen du contenu en clair (c'est-à-dire non chiffré) ou du contenu chiffré, si elle n'est pas imposée par la politique de sécurité;
2) la présence ou l'absence de l'identificateur **content-integrity-algorithm-identifier** dans la séquence ASN.1 sur laquelle la signature est calculée;
3) la règle de codage ASN.1 (CER ou DER) à appliquer à la séquence ASN.1 avant hachage;
4) la fonction de hachage;
5) si la valeur de hachage doit être codée dans la chaîne binaire ASN.1 avant le chiffrement;
6) l'algorithme utilisé pour protéger la valeur de hachage (par exemple un algorithme de chiffrement asymétrique);
7) tous les paramètres de l'algorithme tels que les clés nécessaires, les valeurs initiales et les instructions de bourrage.

L'algorithme d'intégrité de contenu est un algorithme de chiffrement symétrique ou asymétrique.

Si on utilise un algorithme de chiffrement symétrique (*symmetric-encryption-algorithm*), la clé d'intégrité de contenu **content-integrity-key,** utilisée pour calculer l'argument de vérification d'intégrité de contenu **content-integrity-check** et utilisable par le destinataire pour valider ce même argument, peut être obtenue à partir du jeton de message **message-token** envoyé avec le message. La clé d'intégrité de contenu **content-integrity-key** peut également être distribuée par d'autres moyens.

NOTE 5 – L'utilisation d'un algorithme de chiffrement symétrique peut permettre une compression et un chiffrement simultanés du contenu du message pour créer la vérification **content-integrity-check**.

Si on utilise un algorithme de chiffrement asymétrique (*asymmetric-encryption-algorithm*), l'expéditeur du message peut utiliser sa propre clé secrète de chiffrement asymétrique (*secret-asymmetric-encryption-key*) pour calculer l'argument de la vérification d'intégrité de contenu **content-integrity-check**. Pour valider la valeur de vérification d'intégrité de contenu **content-integrity-check**, le destinataire peut utiliser la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) de l'expéditeur (clé publique sujet **subject-public-key**) établie à partir du certificat d'expéditeur **originator-certificate** ou des certificats d'expéditeur multiples **multiple-originator-certificates**.

NOTE 6 – Lorsque plusieurs certificats sont nécessaires, le certificat approprié peut être identifié à partir des arguments **certificate-selectors** et **certificate-selectors-override** par l'utilisation de l'extension d'usage de clé **key usage** ou de l'extension **certificate policies** définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8, ou par une combinaison des deux. Par exemple, le certificat nécessaire pour valider une signature numérique par destinataire (la valeur d'un argument de vérification d'intégrité de contenu **content-integrity-check** par destinataire) peut être identifié par l'argument **certificate-selectors-override** remis au destinataire. Si plusieurs certificats sont remis à l'utilisateur, le certificat approprié peut encore être déterminé par les extensions d'usage de clé **key usage** et par les politiques de certificat **certificate policies** (c'est-à-dire que l'extension **key usage** sera la signature numérique **digitalSignature**, l'identificateur d'objet contenu dans l'extension de politiques de certificat **certificate policies** peut indiquer la politique par laquelle la signature a été produite et doit être utilisée. Cette politique peut à son tour définir dans quels domaines la signature est valide).

8.2.1.1.1.29 Contrôle d'authentification d'origine de message message-origin-authentication-check

Cet argument fournit aux destinataires du message et à tout agent MTA participant au transfert du message un moyen d'authentifier l'origine du message (pour assurer l'élément de service d'authentification d'origine de message, tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur.

Le contrôle d'authentification d'origine de message **message-origin-authentication-check** fournit une preuve d'origine du message qui garantit que le contenu du message n'a pas été modifié (élément de service d'intégrité de contenu tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1) ainsi qu'une preuve d'association entre l'étiquette de sécurité **message-security-label** et le message lui-même.

Le contrôle d'authentification d'origine **message-origin-authentication-check** est calculé au moyen de l'algorithme (algorithme de chiffrement asymétrique et fonction de dispersion) identifié par l'identificateur d'algorithme d'authentification d'origine de message **message-origin-authentication-algorithm-identifier** (un identificateur d'algorithme **algorithm-identifier**).

Le contrôle d'authentification d'origine **message-origin-authentication-check** contient l'identificateur d'algorithme **message-origin-authentication-algorithm-identifier** ainsi qu'une version dispersée à chiffrement asymétrique de cet identificateur d'algorithme, du contenu du message **message-content**, de l'identificateur de contenu **content-identifier** et de l'étiquette de sécurité **message-security-label**. Les composantes facultatives sont incluses dans le contrôle d'authentification d'origine **message-origin-authentication-check** lorsqu'elles sont présentes dans le message.

Si la confidentialité du contenu (voir § 8.2.1.1.1.27) est également demandée, le contrôle d'authentification d'origine **message-origin-authentication-check** est établi au moyen de la version chiffrée du contenu du message (ce qui permet à une entité autre que le destinataire prévu, un agent MTA par exemple, de valider le contrôle d'authentification d'origine **message-origin-authentication-check** sans compromettre pour autant la confidentialité du contenu du message). Si on utilise une version en clair (c'est-à-dire non chiffrée) du contenu du message pour établir le contrôle d'authentification d'origine **message-origin-authentication-check**, cet argument assurera à la fois l'authentification d'origine du message et la non-répudiation d'origine du contenu du message (signature) telles qu'elles sont définies dans la Rec. UIT-T X.400 | ISO/CEI 10021-1. Si toutefois on utilise une version chiffrée du contenu du message, le contrôle d'authentification d'origine **message-origin-authentication-check** assurera l'authentification d'origine du message mais pas la non-répudiation d'origine de son contenu.

Le contrôle d'authentification d'origine **message-origin-authentication-check** peut être calculé par l'expéditeur du message à l'aide de sa clé secrète de chiffrement asymétrique secret-asymmetric-encryption-key. Les destinataires du message et tout agent MTA par lequel le message transite peuvent valider le contrôle d'authentification d'origine **message-origin-authentication-check** en utilisant la clé publique de chiffrement asymétrique public-asymmetric-encryption-key (clé publique sujet **subject-public-key**) de l'expéditeur du message, établie à partir du certificat d'expéditeur **originator-certificate**.

Des addenda ou de futures versions de la présente Recommandation | Norme internationale pourront définir d'autres formes de contrôle d'authentification d'origine **message-origin-authentication-check** (par exemple à base de techniques de chiffrement symétrique) que les agents MTA par lesquels le message est transféré pourront utiliser pour authentifier l'origine du message.

8.2.1.1.1.30 Etiquette de sécurité message-security-label

Cet argument associe une étiquette de sécurité **security-label** au message (ou à l'envoi-test). Il peut être produit par l'expéditeur du message (ou de l'envoi-test), conformément à la politique de sécurité en vigueur.

L'étiquette de sécurité **message-security-label** d'un rapport est la même que l'étiquette de sécurité **message-security-label** du message sujet (ou de l'envoi-test sujet).

Si des étiquettes de sécurité **security-labels** sont assignées aux utilisateurs MTS, aux agents MTA et à d'autres objets du système de messagerie MHS, le traitement par ces objets des messages, envois-tests et rapports assortis d'étiquettes de sécurité de message **message-security-labels** peut être déterminé par la politique de sécurité en vigueur. Si de telles étiquettes de sécurité **security-labels** ne sont pas assignées aux utilisateurs MTS, aux agents MTA et à d'autres objets du système MHS, le traitement par ces objets des messages, envois-tests et rapports assortis d'étiquettes de sécurité de message **message-security-labels** peut être librement déterminé.

Si des contextes de sécurité **security-contexts** sont établis entre l'expéditeur et un agent MTA (l'agent MTA d'origine) du système MTS (voir § 8.1.1.1.1.3 et § 8.2.1.4.1.5), l'étiquette de sécurité de message **message-security-label** que l'expéditeur peut assigner à un message (ou à un envoi-test) peut être déterminée par le contexte de sécurité **security-context** (contexte de sécurité de dépôt submission-security-context), conformément à la politique de sécurité en vigueur. Si aucun contexte de sécurité **security-context** n'a été établi entre l'expéditeur et l'agent MTA d'origine, l'assignation d'une étiquette de sécurité **message-security-label** à un message (ou à un envoi-test) peut se faire à la discrétion de l'expéditeur.

Si des contextes de sécurité **security-contexts** sont établis entre deux agents MTA (voir § 12.1.1.1.1.3), le transfert de messages, envois-tests et rapports entre les agents MTA peut être déterminé par les étiquettes de sécurité **message-security-labels** des messages, envois-tests ou rapports et par le contexte de sécurité **security-context** conformément à la politique de sécurité en vigueur. Si aucun contexte de sécurité **security-context** n'a été établi entre les agents MTA, le transfert des messages, envois-tests et rapports peut se faire à la discrétion de l'expéditeur.

Si des contextes de sécurité **security-contexts** sont établis entre un utilisateur MTS et un agent MTA (l'agent MTA de remise) du système MTS (voir § 8.1.1.1.1.3 et 8.3.1.3.1.7), la remise des messages et rapports peut être déterminée par les étiquettes de sécurité **message-security-labels** des messages et rapports et par le contexte de sécurité **security-context** (contexte de sécurité de remise), conformément à la politique de sécurité en vigueur. Si l'étiquette de sécurité **message-security-label** d'un message ou d'un rapport est admise par les étiquettes de sécurité utilisateur **user-security-labels** du destinataire telles qu'elles sont consignées mais non par le contexte de sécurité **security-context** courant du destinataire (contexte de sécurité de remise), l'agent MTA de remise peut retenir le message en instance. Si aucun contexte de sécurité **security-contexts** n'a été établi entre l'utilisateur MTS et l'agent MTA de remise, la remise des messages et rapports peut se faire à la discrétion de l'agent MTA de remise.

8.2.1.1.1.31 Demande de preuve de dépôt proof-of-submission-request

Cet argument indique si l'expéditeur demande ou non une preuve de dépôt **proof-of-submission** du message auprès du système MTS (pour assurer l'élément de service de preuve de dépôt tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur.

Cet argument peut prendre l'une des valeurs suivantes: **proof-of-submission-requested** (preuve de dépôt demandée) ou **proof-of-submission-not-requested** (preuve de dépôt non demandée).

En l'absence de cet argument, la valeur **proof-of-submission-not-requested** (preuve de dépôt non demandée) est adoptée par défaut.

8.2.1.1.1.32 Demande de preuve de remise proof-of-delivery-request

Cet argument indique si l'expéditeur demande ou non une preuve de remise **proof-of-delivery** du message au destinataire (pour assurer l'élément de service de preuve de remise, tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes: **proof-of-delivery-requested** (preuve de remise demandée) ou **proof-of-delivery-not-requested** (preuve de remise non demandée).

En l'absence de cet argument, la valeur **proof-of-delivery-not-requested** (preuve de remise non demandée) est adoptée par défaut.

8.2.1.1.1.33 Types d'origine d'informations codées original-encoded-information-types

Cet argument identifie les types d'informations codées **encoded-information-types** d'origine du contenu du message. Il peut être produit par l'expéditeur du message.

L'absence de cet argument indique que le type d'origine d'informations codées **original-encoded-information-types** du contenu du message est **unspecified** (non spécifié).

8.2.1.1.1.34 Type de contenu content-type

Cet argument identifie le type de contenu du message. Il identifie la syntaxe abstraite et les règles de codage adoptées. Il est produit par l'expéditeur du message. Le type de contenu **content-type** sera de type intégré ou étendu.

Un type de contenu **content-type** intégré peut prendre l'une des valeurs suivantes:

unidentified (non identifié): signale un type de contenu **content-type** non identifié et non contraint; l'utilisation du type de contenu **unidentified** (non identifié) se fait par accord bilatéral entre utilisateurs MTS;

external (externe): signale un type de contenu réservé aux situations d'interfonctionnement entre systèmes 1988 et systèmes 1984. Il ne sera utilisé qu'avec le protocole de transfert **mts-transfer-protocol-1984** (voir la Rec. UIT-T X.419 | ISO/CEI 10021-6);

NOTE 1 – Les règles d'interfonctionnement garantissent que le type de contenu **external content-type** n'est jamais utilisé conjointement avec la fonction de transfert **mts-transfer** ou le protocole **mts-transfer-protocol**. Bien que le type de contenu **external** soit conçu pour permettre l'interfonctionnement entre systèmes 1988 via des systèmes 1984 intermédiaires, un système 1984 peut remettre (ou déposer) un contenu de type **external** sous réserve que l'utilisateur MTS (ou l'agent MTA lui-même) exécute les règles de mise à jour (en surclassement ou en déclassement) indiquées dans la Rec. UIT-T X.419 | ISO/CEI 10021-6.

interpersonal-messaging-1984: identifie le type de contenu messagerie de personne à personne version 1984 défini dans la Rec. UIT-T X.420 | ISO/CEI 10021-7;

interpersonal-messaging-1988: identifie le type de contenu messagerie de personne à personne version1988 défini dans la Rec. UIT-T X.420 | ISO/CEI 10021-7;

edi-messaging: identifie le type de contenu **edim content-type** (messagerie EDI) défini dans la Rec. UIT-T X.435 | ISO/CEI 10021-9;

voice-messaging: identifie le type de contenu **vm content-type** (messagerie vocale) défini dans la Rec. UIT-T X.440.

Un type de contenu **content-type** étendu est spécifié au moyen d'un identificateur d'objet.

La présente Définition de service a défini la valeur particulière suivante de type de contenu étendu:

– **inner-envelope** (enveloppe interne): type de contenu **content-type** étendu qui est lui-même un message (enveloppe et contenu). Une fois le message remis au destinataire nommé sur l'enveloppe extérieure, celle-ci est retirée et le contenu est, si nécessaire, décrypté, de sorte que l'on obtient une enveloppe interne et son contenu. Les informations contenues dans l'enveloppe interne servent à transférer le contenu de cette enveloppe aux destinataires dont le nom figure dessus. Le type de contenu OCTET STRING (chaîne d'octets) est une unité **MTS-APDU** (voir la Figure 6 de la Rec. UIT-T X.419 | ISO/CEI 10021-6) codée en appliquant les règles de codage de base de l'ASN.1. (L'enveloppe intérieure et son contenu peuvent être protégés en sécurisant le contenu de l'enveloppe extérieure au moyen des arguments de sécurité (voir § 8.2.1.1.1.25 à § 8.2.1.1.1.32).)

D'autres types de contenu étendus normalisés pourront être définis dans d'autres spécifications de systèmes de messagerie ou dans d'autres Recommandations | Normes internationales. D'autres valeurs de cet argument peuvent être utilisées par accord bilatéral entre utilisateurs MTS.

NOTE 2 – En cas d'utilisation du service de confidentialité du contenu, la syntaxe et le codage identifiés par le type de contenu **content-type** sont ceux du contenu avant chiffrement.

8.2.1.1.1.35 Identificateur de contenu content-identifier

Cet argument contient un identificateur du contenu **content** du message. Il peut être produit par l'expéditeur.

L'identificateur de contenu **content-identifier** peut être remis aux destinataires du message et renvoyé à l'expéditeur avec tout rapport. Cet argument n'est pas modifié par le système MTS.

8.2.1.1.1.36 Corrélateur de contenu content-correlator

Cet argument contient des informations qui permettent à l'expéditeur du message de corréler du contenu **content** de ce message. Il peut être produit par l'expéditeur.

Le corrélateur de contenu **content-correlator** n'est pas remis aux destinataires, il est renvoyé à l'expéditeur avec tout rapport. Cet argument n'est pas modifié par le système MTS.

8.2.1.1.1.37 Contenu content

Cet argument contient les informations que le message est censé transmettre aux destinataires. Il doit être produit par l'expéditeur.

Sauf en cas de conversion, le contenu **content** du message n'est pas modifié par le système MTS, mais y transite en transparence.

La confidentialité du contenu **content** peut être assurée par chiffrement (voir § 8.2.1.1.1.27).

NOTE – La valeur de la chaîne d'octets contenant le contenu chiffré **encoded** n'est pas modifiée lors de son transit par le système MTS.

8.2.1.1.1.38 Type notification notification-type

Cet argument indique que le contenu est une notification et qu'il relève de l'un des trois types de notification (notification de type 1, de type 2 ou de type 3); l'utilisation de ces valeurs est définie dans la spécification de contenu **content** correspondante. Il peut être produit par l'expéditeur, mais seulement si le contenu **content** est effectivement une notification conformément à la spécification pertinente de contenu **content**.

L'indication **notification-type** n'est ni remise aux destinataires de message ni renvoyée à l'expéditeur en marge d'un rapport quelconque. Suivant la stratégie choisie, cet argument peut être vérifié lors du dépôt par le système MTS.

8.2.1.1.1.39 Message de service service-message

Cet argument indique que le message est émis à des fins de service. Il peut être produit par l'expéditeur, mais n'est utilisé que sur la base d'accords bilatéraux.

L'indication **service-message** n'est ni remise aux destinataires du message, ni renvoyée à l'expéditeur en marge d'un rapport quelconque. Suivant la stratégie choisie, cet argument peut être vérifié par le système MTS.

8.2.1.1.1.40 Destinataires exemptés de liste DL DL-exempted-recipients

Cet argument contient les noms **OR-names** de destinataires potentiels ne devant pas être ajoutés à l'ensemble des destinataires prévus suite au développement de liste DL. Il peut être produit par l'expéditeur du message.

Cet argument demeure inchangé durant le traitement MTA et est inclus dans les opérations ultérieures de transfert que le développement DL ait déjà eu lieu ou non.

L'argument destinataires exemptés de liste DL **DL-exempted-recipients** est remis au ou aux destinataires mais il n'est renvoyé au destinataire dans aucun rapport.

8.2.1.1.1.41 Certificats d'expéditeur multiples multiple-originator-certificates

Cet argument contient un certificat **certificate** de l'expéditeur du message, ou le nom d'annuaire **directory-name** d'une entrée dans l'annuaire qui contient un certificat de l'expéditeur, ou plusieurs certificats (ou noms d'annuaire) qui contiennent des trajets de certification différents, sont émis par des autorités de certification différentes ou ont des objets différents. Chaque certificat **certificate** doit être produit par une source fiable (c'est-à-dire par une autorité de certification), et peut être fourni par l'expéditeur du message.

L'argument certificats d'expéditeur multiples **multiple-originator-certificates** peut être utilisé pour véhiculer des copies certifiées d'informations publiques de l'expéditeur nécessaires à la vérification des signatures numériques ou devant être utilisées pour des accords de clé. Il peut véhiculer la clé publique de chiffrement asymétrique public-asymmetric-encryption-key (clé publique sujet **subject-public-key**) de l'expéditeur du message, ou d'autres informations publiques nécessaires au traitement d'accord de clé.

Plusieurs certificats **certificate**s ou noms d'annuaire **directory-name**s peuvent intervenir lorsque plus d'un seul type d'informations certifiées de l'expéditeur du message doit être véhiculé.

NOTE 1 – Si des certificats dédiés sont nécessaires pour chaque destinataire, alors ces certificats dédiés sont identifiés dans l'argument **certificate-selectors-override**.

NOTE 2 – Il peut être nécessaire, pour implémenter un accord de clé, d'avoir des certificats dans les deux arguments **multiple-originator-certificates** et **recipient-certificate**.

Lorsque, dans un argument certificats d'expéditeur multiples **multiple-originator-certificates** un certificat est utilisé à une fin particulière, des certificats en version 3 (voir Rec. UIT-T X.509 | ISO/CEI 9594-8) devront être utilisés pour indiquer l'objet de l'information contenue dans le certificat. Les extensions d'usage de clé **key usage** et politiques de certificat **certificate policies** des certificats en version 3 peuvent être utilisées de façon individuelle, ou de façon combinée, pour indiquer l'objet du certificat véhiculé dans l'argument certificat d'expéditeur multiple **multiple-originator-certificates.** Les extensions usage de clé **key usage** et politiques de certificat **certificate policies** peuvent indiquer si la clé publique asymétrique de chiffrement de l'expéditeur est requise pour valider une signature numérique dans n'importe lequel des arguments suivants, contrôle d'authentification d'origine de message **message-origin-authentication-check**, vérification d'intégrité de contenu **content-integrity-check** ou jeton de message **message-token**. Si plus d'une valeur de signature numérique est véhiculée au moyen des différents arguments vérification d'intégrité de contenu **content-integrity-check**, le certificat approprié peut être également indiqué par la combinaison des extensions de certificat usage de clé **key usage** et politiques de certificat **certificate policies**. Les extensions usage de clé **key usage** et politiques de certificat **certificate policies** peuvent indiquer si l'information publique de l'expéditeur est requise pour l'accord de clé dans le traitement de l'argument jeton de message **message-token**.

Plusieurs signatures numériques véhiculées dans les arguments contrôle d'authentification d'origine de message **message-origin-authentication-check**, vérification d'intégrité de contenu **content-integrity-check** et/ou jeton de message **message-token,** peuvent être produites par l'expéditeur d'un message. Si le même algorithme et la même clé publique asymétrique de l'expéditeur sont nécessaires pour valider toutes les signatures numériques, cela peut être indiqué par la combinaison des extensions de certificat d'usage de clé **key usage** et de politiques de certificat **certificate policies**.

NOTE 3 – Si des algorithmes et des clés publiques asymétriques d'expéditeur dédiés sont nécessaires à la vérification des signatures numériques pour chaque destinataire, alors des certificats dédiés sont également nécessaires pour chaque destinataire. Dans ce cas, le certificat dédié est identifié dans l'argument **certificate-selectors-override**.

8.2.1.1.1.42 Certificats par destinataire recipient-certificates

Cet argument contient un certificat **certificate** de destinataire du message et facultativement son trajet de certification. Ce certificat **certificate** doit être produit par une source fiable (c'est-à-dire une autorité de certification) et peut être fourni par l'expéditeur du message. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

L'argument **recipient-certificate** peut être utilisé pour transporter une copie certifiée d'informations publiques devant être utilisées pour des accords de clé. Il identifie la clé de chiffrement publique asymétrique public-asymmetric-encryption-key (clé publique sujet **subject-public-key**) du destinataire. Cette identification peut aussi être acheminée dans l'argument **certificate-selectors-override**. Une telle identification n'est nécessaire que si le destinataire a plusieurs certificats pour l'algorithme identifié.

Le certificat véhiculé dans l'argument **recipient-certificate** peut être utilisé pour des accords de clé, tels que la production des clés nécessaires au traitement des données chiffrées **encrypted-data** dans le jeton de message **message-token**.

Si le message est développé par une ou plusieurs listes DL sur le trajet du message, l'argument certificats par destinataire **recipient-certificate** peut être produit par la liste DL.

8.2.1.1.1.43 Sélecteurs de certificats certificate-selectors

Cet argument contient des informations suffisantes pour identifier un certificat **certificate** lorsqu'un utilisateur a plusieurs certificats avec le même identificateur d'algorithme **algorithm-identifier**. Cela permet d'identifier un certificat de l'expéditeur pour valider une signature numérique spécifique dans les arguments **message-origin-authentification-check**, **content-integrity-check**, ou **message-token**, ou d'utiliser ce certificat pour les accords de clé de chiffrement. Il permet également d'identifier un certificat de chaque destinataire pour les accords de clé ou le chiffrement asymétrique. Il peut être produit par l'expéditeur du message.

Chaque composante des sélecteurs de certificat **certificate-selectors** permet de spécifier des critères de sélection de certificat pour la concordance de certificat spécifiée au § 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8 qui est applicable à un certificat d'utilisateur. Avant de choisir un certificat, le destinataire ajoute l'identificateur d'algorithme approprié (dans le champ **subjectPublicKeyAlgID**) et l'heure de la soumission du message (ou de la création du jeton) à laquelle le certificat et la clé privée étaient valides (dans les champs **certificateValid** et **privateKeyValid**) conformément aux critères de sélection spécifiés par l'expéditeur. Les critères spécifiés, lorsqu'ils sont associés à ces valeurs, doivent suffire à sélectionner un seul certificat. Cela permet par exemple d'identifier de manière univoque un seul certificat par son émetteur **issuer** et son numéro de série **serial-number**, ou de manière générique une classe de certificats par objet de la clé (**key-purpose**) ou politique en matière de certificat (**certificate-policy**) (ce qui, après combinaison avec l'identificateur d'algorithme et la date de validité appropriés, fournira un seul certificat pour chaque utilisateur). La valeur de chaque composante s'applique à tous les destinataires sauf s'il y a une valeur dans la composante concernée de **certificate-selectors-override** pour le destinataire concerné. Les certificats identifiés peuvent (mais ce n'est pas nécessaire) être présents dans les arguments **originator-certificate** ou **multiple-originator-certificates**.

L'argument **certificate-selectors** contient les composantes suivantes:

encryption-recipient
encryption-originator
content-integrity-check
token-signature
message-origin-authentication

La composante *encryption-recipient* identifie un des certificats de destinataire; chacune des autres composantes identifie un des certificats de destinataire. Les deux premières composantes s'appliquent au chiffrement token-encryption si l'algorithme content-confidentially-algorithm est symétrique, et au chiffrement content-encryption si cet algorithme est asymétrique.

8.2.1.1.1.44 Violation des sélecteurs de certificats certificate-selectors-override

Cet argument contient des informations qui suffisent à identifier un certificat **certificate** lorsqu'un utilisateur a plusieurs certificats avec le même identificateur d'algorithme (**algorithm-identifier**). Il permet d'identifier un certificat de l'expéditeur afin de valider des signatures numériques spécifiques dans les arguments **content-integrity-check** ou **message-token**, ou d'utiliser ce certificat pour un accord de clé pour le chiffrement. Il permet aussi d'identifier un certificat pour chaque destinataire pour un accord de clé ou pour un chiffrement asymétrique. Il peut être produit par l'expéditeur du message. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

Cet argument est identique à l'argument **certificate-selectors**, à ceci près qu'il ne contient pas de composante *message-origin-authentication*.

Si cet argument est présent, alors la valeur contenue dans chaque composante présente remplace la valeur contenue dans la composante correspondante de l'argument **certificate-selectors** pour le destinataire concerné.

8.2.1.1.2 Résultats

Le Tableau 5 fournit la liste des résultats de l'opération abstraite de dépôt de message Message-submission, qualifie la présence de chaque résultat et spécifie le paragraphe dans lequel il est défini.

Tableau 5 – Résultats du dépôt de message Message-submission

Résultat	Présence	Paragraphe
Identificateur de dépôt de message *message-submission-identifier*	M	8.2.1.1.2.1
Heure de dépôt de message *message-submission-time*	M	8.2.1.1.2.2
Certificat d'agent MTA expéditeur *originating-MTA-certificate*	O	8.2.1.1.2.3
Preuve de dépôt *proof-of-submission*	C	8.2.1.1.2.4
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35

8.2.1.1.2.1 Identificateur de dépôt de message message-submission-identifier

Ce résultat contient un identificateur **MTS-identifier** qui identifie le dépôt de message de façon unique et sans ambiguïté; il est produit par le système MTS.

Le système MTS fournit l'identificateur de dépôt **message-submission-identifier** lorsque, par l'intermédiaire de l'opération abstraite de remise de rapport Report-delivery, il signale à l'utilisateur MTS la remise ou la non-remise du message.

L'utilisateur MTS fournit l'identificateur de dépôt **message-submission-identifier** lorsque, par l'intermédiaire de l'opération abstraite d'annulation de remise différée Cancel-deferred-delivery, il annule un message dont il a différé la remise.

8.2.1.1.2.2 Heure de dépôt de message message-submission-time

Ce résultat indique la date et l'heure **Time** auxquelles le système MTS accepte la responsabilité du message. Il est produit par le système MTS.

8.2.1.1.2.3 Certificat de l'agent MTA d'origine originating-MTA-certificate

Ce résultat contient le certificat de l'agent MTA auprès duquel le message a été déposé (agent MTA d'origine). Ce résultat est produit par une source de confiance (par exemple une autorité de certification) et peut être fourni par l'agent MTA d'origine si l'expéditeur du message a demandé une preuve de dépôt **proof-of-submission** (voir § 8.2.1.1.1.31) et si un algorithme de chiffrement asymétrique est utilisé pour établir la preuve de dépôt **proof-of-submission**.

Le certificat d'agent MTA d'origine **originating-MTA-certificate** peut servir à communiquer à l'expéditeur du message une copie certifiée de la clé publique de chiffrement asymétrique public-asymmetric-encryption-key (clé publique sujet **subject-public-key**) de l'agent MTA d'origine.

L'expéditeur du message peut utiliser la clé publique de chiffrement asymétrique public-asymmetric-encryption-key de l'agent MTA d'origine pour valider la preuve de dépôt **proof-of-submission**.

8.2.1.1.2.4 Preuve de dépôt proof-of-submission

Ce résultat fournit à l'expéditeur la preuve de dépôt du message auprès du système MTS (assurant ainsi l'élément de service de preuve de dépôt, tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Selon l'algorithme de chiffrement utilisé et la politique de sécurité en vigueur, cet argument peut également assurer l'élément de service de non-répudiation de dépôt (tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il est produit par l'agent MTA d'origine du système MTS, si l'expéditeur du message a demandé la preuve de dépôt **proof-of-submission** (voir § 8.2.1.1.1.31).

La preuve de dépôt **proof-of-submission** est établie au moyen de l'algorithme identifié par l'identificateur d'algorithme de preuve de dépôt **proof-of-submission-algorithm-identifier** (un identificateur d'algorithme **algorithm-identifier**).

La preuve de dépôt **proof-of-submission** contient l'identificateur d'algorithme de preuve de dépôt **proof-of-submission-algorithm-identifier** ainsi qu'une fonction chiffrée (version comprimée ou dispersée par exemple) de ce même identificateur, plus les arguments de dépôt du message (voir § 8.2.1.1.1) du message sujet, l'identificateur de dépôt **message-submission-identifier** et l'heure de dépôt **message-submission-time**.

La réception de ces résultats fournit à l'expéditeur une preuve de dépôt de message. La non-réception de ces résultats ne constitue ni une preuve de dépôt ni une preuve de non-dépôt (à moins d'utiliser une liaison sécurisée et une fonctionnalité fiable).

Si on utilise un algorithme de chiffrement asymétrique asymmetric-encryption-algorithm, la preuve de dépôt **proof-of-submission** peut être établie par l'agent MTA d'origine au moyen de la clé secrète de chiffrement asymétrique secret-asymmetric-encryption-key de l'agent MTA d'origine. L'expéditeur peut valider la preuve de dépôt **proof-of-submission** en utilisant la clé publique de chiffrement asymétrique public-asymmetric-encryption-key de l'agent MTA d'origine (une clé publique sujet **subject-public-key**) obtenue à partir du certificat de l'agent MTA d'origine **originating-MTA-certificate**. Une preuve de dépôt **proof-of-submission** asymétrique peut également assurer la fonction de non-répudiation de dépôt, sous réserve de la disponibilité d'une infrastructure appropriée de clés publiques.

Si on utilise un algorithme de chiffrement symétrique symmetric-encryption-algorithm, la clé de chiffrement symétrique utilisée par l'agent MTA d'origine pour établir la preuve de dépôt **proof-of-submission**, et que l'expéditeur peut également utiliser pour valider cette preuve de dépôt, peut être établie à partir des jetons de rattachement **bind-tokens** (voir § 8.1.1.1.1.3 et § 8.1.1.1.2.2) qui ont été échangés au moment de la constitution de l'association. La clé de chiffrement symétrique utilisée pour la preuve de dépôt **proof-of-submission** peut également être échangée par d'autres moyens. Si on utilise un algorithme de chiffrement symétrique symmetric-encryption-algorithm, la preuve de dépôt **proof-of-submission** ne peut assurer la fonction de non-répudiation de dépôt que si la politique de sécurité en vigueur prévoit l'intervention d'une tierce partie agissant en qualité de notaire.

8.2.1.1.3 Erreurs abstraites abstract-errors

Le Tableau 6 fournit la liste des erreurs abstraites qui peuvent perturber l'opération abstraite de dépôt de message Message-submission, indiquant pour chacune d'elles le paragraphe dans lequel elle est définie.

Tableau 6 – Erreurs abstraites de dépôt de message Message-submission

Erreur abstraite abstract-error	Paragraphe
Commande de dépôt non respectée *submission-control-violated*	8.2.2.1
Non-abonnement à l'élément de service *element-of-service-not-subscribed*	8.2.2.2
Expéditeur non valide *originator-invalid*	8.2.2.4
Destinataire mal spécifié *recipient-improperly-specified*	8.2.2.5
Demande incohérente *inconsistent-request*	8.2.2.7
Erreur de sécurité *security-error*	8.2.2.8
Fonction critique non prise en charge *unsupported-critical-function*	8.2.2.9
Erreur de rattachement distant *remote-bind-error*	8.2.2.10

8.2.1.2 Dépôt d'envoi-test probe-submission

L'opération abstraite de dépôt d'envoi-test probe-submission permet à un utilisateur MTS de déposer un envoi-test afin de savoir si un éventuel message (le message sujet subject-message) pourra être transféré et remis à un ou plusieurs utilisateurs MTS.

Le succès d'un envoi-test ne garantit pas qu'un message ultérieurement déposé pourra être effectivement remis, mais signifie plutôt que le nom du destinataire est correct et qu'aucun obstacle majeur n'entravera la remise du message.

Pour tout nom de destinataire **recipient-name** correspondant à une liste DL, l'opération abstraite de dépôt d'envoi-test probe-submission détermine si un développement de la liste DL spécifiée (mais pas d'une liste DL imbriquée quelconque) aura lieu.

Pour tout nom de destinataire **recipient-name** pour lequel un renvoi aurait lieu, l'opération abstraite de dépôt d'envoi-test détermine si l'éventuel message pourra être transféré et remis au destinataire suppléant.

L'utilisateur MTS fournit la plupart des arguments utilisés pour un dépôt de message ainsi que la longueur du contenu du message sujet subject-message. L'opération abstraite de dépôt d'envoi-test n'aboutit pas à la remise d'un message sujet aux destinataires, mais elle établit la vraisemblance d'un tel aboutissement à l'issue d'une opération abstraite de dépôt de message.

Le succès de l'opération abstraite signifie que le système MTS a accepté de prendre en charge l'envoi-test (mais non qu'il l'a déjà exécuté).

L'interruption de l'opération abstraite par une erreur abstraite indique que le système MTS ne peut prendre en charge l'envoi-test.

8.2.1.2.1 Arguments

Le Tableau 7 énumère les arguments de l'opération abstraite de dépôt d'envoi-test, en qualifie la présence et spécifie les paragraphes dans lesquels ils sont définis.

Tableau 7 – Arguments de dépôt d'envoi-test Probe-submission

Argument	Présence	Paragraphe
Argument d'expéditeur		
Nom d'expéditeur *originator-name*	M	8.2.1.1.1.1
Arguments de destinataire		
Nom de destinataire *recipient-name*	M	8.2.1.1.1.2
Autorisation de destinataire suppléant *alternate-recipient-allowed*	O	8.2.1.1.1.3
Interdiction de réassignation de destinataire *recipient-reassignment-prohibited*	O	8.2.1.1.1.4
Destinataire suppléant désigné par l'expéditeur *originator-requested-alternate-recipient*	O	8.2.1.1.1.5
Interdiction de développement de liste DL *DL-expansion-prohibited*	O	8.2.1.1.1.6
Arguments de conversion		
Interdiction de conversion implicite *implicit-conversion-prohibited*	O	8.2.1.1.1.9
Interdiction de conversion avec perte *conversion-with-loss-prohibited*	O	8.2.1.1.1.10
Conversion explicite *explicit-conversion*	O	8.2.1.1.1.11
Argument de méthode de remise		
Méthode de remise demandée *requested-delivery-method*	O	8.2.1.1.1.14
Argument de remise physique		
Attributs de restitution physique *physical-rendition-attributes*	O	8.2.1.1.1.20
Argument de demande de rapport		
Demande de rapport par l'expéditeur *originator-report-request*	M	8.2.1.1.1.22
Arguments de sécurité		
Certificat d'expéditeur *originator-certificate*	O	8.2.1.1.1.25
Contrôle d'authentification d'origine d'envoi-test *probe-origin-authentication-check*	O	8.2.1.2.1.1
Etiquette de sécurité de message *message-security-label*	O	8.2.1.1.1.30
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	O	8.2.1.1.1.33
Type de contenu *content-type*	M	8.2.1.1.1.34
Identificateur de contenu *content-identifier*	O	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	O	8.2.1.1.1.36
Longueur de contenu *content-length*	O	8.2.1.2.1.2
Type de notification *notification-type*	O	8.2.1.1.1.38
Message de service *service-message*	O	8.2.1.1.1.39

8.2.1.2.1.1 Contrôle d'authentification d'origine d'envoi-test probe-origin-authentication-check

Cet argument fournit à n'importe quel agent MTA, par lequel l'envoi-test transite, un moyen d'en authentifier l'origine (pour assurer l'élément de service d'authentification d'origine d'envoi-test tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'expéditeur de l'envoi-test.

Le contrôle d'authentification d'origine de l'envoi-test **probe-origin-authentication-check** fournit une preuve de l'origine de l'envoi-test (authentification d'origine d'envoi-test) ainsi qu'une preuve d'association entre l'étiquette de sécurité de message **message-security-label** et l'identificateur de contenu **content-identifier** du message sujet subject-message.

Le contrôle d'authentification d'origine de l'envoi-test **probe-origin-authentication-check** est calculé au moyen de l'algorithme identifié par l'identificateur d'algorithme d'authentification d'origine d'envoi-test **probe-origin-authentication-algorithm-identifier** (un identificateur d'algorithme **algorithm-identifier**).

Le contrôle d'authentification d'origine de l'envoi-test **probe-origin-authentication-check** contient l'identificateur d'algorithme d'authentification d'origine d'envoi-test **probe-origin-authentication-algorithm-identifier**, accompagné d'une transformée à chiffrement asymétrique dispersée de ce même identificateur, ainsi que l'identificateur de contenu

content-identifier et l'étiquette de sécurité **message-security-label** du message sujet. Lorsqu'elles sont présentes dans l'envoi-test, les composantes facultatives sont incluses dans le contrôle d'authentification d'origine de l'envoi-test **probe-origin-authentication-check**.

Le contrôle d'authentification d'origine de l'envoi-test **probe-origin-authentication-check** peut être calculé par l'expéditeur au moyen de la clé secrète de chiffrement asymétrique de l'expéditeur. Cet argument d'authentification peut être validé par n'importe quel agent MTA par lequel l'envoi-test transite, au moyen de la clé publique de chiffrement asymétrique de l'expéditeur (clé publique sujet **subject-public-key**), établie à partir du certificat d'expéditeur **originator-certificate**.

Des addenda ou de futures versions de la présente Recommandation | Norme internationale pourront définir d'autres formes de contrôle d'authentification d'origine d'envoi-test **probe-origin-authentication-check** (fondées par exemple sur des techniques de chiffrement symétrique) qui pourront être utilisées par les agents MTA par lesquels l'envoi-test transite pour authentifier l'origine de l'envoi-test.

8.2.1.2.1.2 Longueur de contenu content-length

Cet argument spécifie la longueur en octets du contenu **content** du message sujet. Il peut être produit par l'expéditeur de l'envoi-test.

8.2.1.2.2 Résultats

Le Tableau 8 énumère les résultats de l'opération abstraite de dépôt d'envoi-test Probe-submission, qualifie leur présence et spécifie les paragraphes dans lesquels ils sont définis.

Tableau 8 – Résultats du dépôt d'envoi-test Probe-submission

Résultat	Présence	Paragraphe
Identificateur de dépôt d'envoi-test *probe-submission-identifier*	M	8.2.1.2.2.1
Heure de dépôt d'envoi-test *probe-submission-time*	M	8.2.1.2.2.2
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35

8.2.1.2.2.1 Identificateur de dépôt d'envoi-test probe-submission-identifier

Ce résultat contient un identificateur **MTS-identifier** qui identifie le dépôt d'envoi-test d'une manière univoque. Il est produit par le système MTS.

Le système MTS fournit l'identificateur de dépôt d'envoi-test **probe-submission-identifier** lorsqu'il notifie à un utilisateur MTS, par l'intermédiaire de l'opération abstraite de remise de rapport Report-delivery, sa capacité ou son incapacité à remettre le message sujet subject-message.

8.2.1.2.2.2 Heure de dépôt d'envoi-test probe-submission-time

Ce résultat indique la date et l'heure **Time** auxquelles le système MTS a accepté de prendre en charge l'envoi-test. Il est produit par le système MTS.

8.2.1.2.3 Erreurs abstraites abstract-errors

Le Tableau 9 fournit la liste des erreurs abstraites abstract-errors qui peuvent perturber l'opération abstraite abstract-operation de dépôt d'envoi-test Probe-submission, et spécifie, pour chaque erreur abstraite abstract-error, le paragraphe dans lequel elle est définie.

Tableau 9 – Erreurs abstraites de dépôt d'envoi-test Probe-submission

Erreur abstraite abstract-error	Paragraphe
Commande de dépôt enfreinte *submission-control-violated*	8.2.2.1
Non-abonnement à l'élément de service *element-of-service-not-subscribed*	8.2.2.2
Expéditeur non valide *originator-invalid*	8.2.2.4
Destinataire incorrectement spécifié *recipient-improperly-specified*	8.2.2.5
Demande incohérente *inconsistent-request*	8.2.2.7
Erreur de sécurité *security-error*	8.2.2.8
Fonction critique non prise en charge *unsupported-critical-function*	8.2.2.9
Erreur de rattachement distant *remote-bind-error*	8.2.2.10

8.2.1.3 Annulation de remise différée Cancel-deferred-delivery

L'opération abstraite d'annulation de remise différée Cancel-deferred-delivery permet à un utilisateur MTS d'interrompre la remise différée d'un message qu'il a lui-même déposé par une opération abstraite de dépôt de message Message-submission.

L'utilisateur MTS identifie le message dont la remise doit être annulée au moyen de l'identificateur de dépôt de message **message-submission-identifier** renvoyé par le système MTS en réponse à un appel antérieur de l'opération abstraite de dépôt de message Message-submission.

L'achèvement avec succès de l'opération abstraite signifie que le système MTS a annulé la remise différée du message.

L'interruption de l'opération abstraite par une erreur abstraite indique que la remise différée ne peut être annulée. La remise différée d'un message ne peut pas être annulée lorsque le message a déjà été communiqué pour remise ou transfert dans le système MTS. Celui-ci peut refuser d'annuler la remise différée d'un message lorsqu'il a déjà fourni à l'expéditeur une preuve de dépôt **proof-of-submission**.

8.2.1.3.1 Arguments

Le Tableau 10 énumère les arguments de l'opération abstraite d'annulation de remise différée Cancel-deferred-delivery, en qualifie la présence et spécifie les paragraphes dans lesquels ils sont définis.

Tableau 10 – Arguments d'annulation de remise différée Cancel-deferred-delivery

Argument	Présence	Paragraphe
Argument de dépôt		
Identificateur de dépôt de message *message-submission-identifier*	M	8.2.1.3.1.1

8.2.1.3.1.1 Identificateur de dépôt de message message-submission-identifier

Cet argument contient l'identificateur de dépôt **message-submission-identifier** du message dont la remise différée doit être annulée. Il est fourni par l'utilisateur MTS.

L'identificateur de dépôt **message-submission-identifier** (un identificateur **MTS-identifier**) est celui qu'aura renvoyé le système MTS en réponse à un appel antérieur d'une opération abstraite de dépôt de message (voir § 8.2.1.1.2.1) avec demande de remise différée.

8.2.1.3.2 Résultats

L'opération abstraite d'annulation de remise différée Cancel-deferred-delivery renvoie un résultat vide comme indication de succès.

8.2.1.3.3 Erreurs abstraites abstract-errors

Le Tableau 11 énumère les erreurs abstraites qui peuvent interrompre une opération abstraite d'annulation de remise différée Cancel-deferred-delivery, et indique pour chacune d'entre elles le paragraphe dans lequel elle est définie.

Tableau 11 – Erreurs abstraites de l'annulation de remise différée Cancel-deferred-delivery

Erreur abstraite abstract-error	Paragraphe
Annulation de remise différée rejetée *deferred-delivery-cancellation-rejected*	8.2.2.3
Identificateur de dépôt de message non valide *message-submission-identifier-invalid*	8.2.2.6
Erreur de rattachement distant *remote-bind-error*	8.2.2.10

8.2.1.4 Commande de dépôt Submission-control

L'opération abstraite de commande de dépôt Submission-control permet au système MTS de limiter temporairement les opérations abstraites de point d'accès dépôt que l'utilisateur MTS peut appeler, ainsi que les messages que l'utilisateur MTS peut soumettre au système MTS par l'opération abstraite de dépôt de message Message-submission.

L'utilisateur MTS devrait suspendre les opérations abstraites et les messages interdits au moment considéré, plutôt que de les annuler.

L'achèvement avec succès de l'opération abstraite signifie que les commandes spécifiées sont maintenant en vigueur. Ces commandes remplacent n'importe quelle commande antérieure et demeurent en vigueur jusqu'à ce que l'association soit libérée ou que le système MTS invoque de nouveau l'opération abstraite de commande de dépôt Submission-control.

L'opération abstraite signale en retour toute opération abstraite que l'utilisateur MTS aurait pu invoquer et tout type de message qu'il aurait pu déposer en l'absence des commandes en vigueur.

8.2.1.4.1 Arguments

Le Tableau 12 énumère les arguments de l'opération abstraite abstract-operation de commande de dépôt Submission-control, en qualifie la présence et spécifie les paragraphes dans lesquels ils sont définis.

Tableau 12 – Arguments de commande de dépôt Submission-control

Argument	Présence	Paragraphe
Arguments de commande de dépôt		
Restriction *restrict*	O	8.2.1.4.1.1
Opérations permises *permissible-operations*	O	8.2.1.4.1.2
Priorité minimale permise *permissible-lowest-priority*	O	8.2.1.4.1.3
Longueur maximale permise de contenu *permissible-maximum-content-length*	O	8.2.1.4.1.4
Contexte de sécurité permis *permissible-security-context*	O	8.2.1.4.1.5

8.2.1.4.1.1 Restriction restrict

Cet argument indique si les commandes des opérations abstraites de point d'accès dépôt submission-port doivent être mises à jour ou supprimées. Il peut être produit par le système MTS.

Cet argument peut prendre l'une des valeurs suivantes:

update (mise à jour): les autres arguments mettent à jour les commandes en vigueur;

remove (suppression): toutes les commandes sont supprimées; les autres arguments sont ignorés.

En l'absence de cet argument, la valeur **update** (mise à jour) est adoptée par défaut.

8.2.1.4.1.2 Opérations permises permissible-operations

Cet argument indique les opérations abstraites qu'un utilisateur MTS peut appeler dans le système MTS. Il peut être produit par le système MTS.

Cet argument peut prendre la valeur **allowed** (permise) ou **prohibited** (interdite) pour chacune des fonctions suivantes:

message-submission (dépôt de message): l'utilisateur MTS peut ou ne peut pas appeler l'opération abstraite de dépôt de message Message-submission;

probe-submission (dépôt d'envoi-test): l'utilisateur MTS peut ou ne peut pas appeler l'opération abstraite de dépôt d'envoi-test Probe-submission.

Les autres opérations abstraites de point d'accès dépôt ne sont pas commandables et peuvent être invoquées à tout moment.

En l'absence de cet argument, les opérations abstraites que l'utilisateur MTS peut demander au système MTS ne sont pas modifiées. Si aucune commande antérieure n'est en vigueur, l'utilisateur MTS peut invoquer aussi bien l'opération abstraite de dépôt de message Message-submission que celle de dépôt d'envoi-test Probe-submission.

8.2.1.4.1.3 Priorité minimale permise permissible-lowest-priority

Cet argument contient la priorité **priority** plus faible de message que l'utilisateur MTS peut déposer auprès du système MTS par l'opération abstraite de dépôt de message Message-submission. Il peut être produit par le système MTS.

Il peut prendre les mêmes valeurs que l'argument de priorité priority de l'opération abstraite de dépôt de message Message-submission: priorité normale, non urgente ou urgente.

En l'absence de cet argument, cette priorité **priority** minimale reste inchangée. Si aucune commande antérieure n'est en vigueur, l'utilisateur MTS peut déposer des messages de priorité quelconque.

8.2.1.4.1.4 Longueur maximale permise de contenu permissible-maximum-content-length

Cet argument contient la longueur de contenu **content-length**, exprimée en octets, du plus long message que l'utilisateur MTS pourra déposer auprès du système MTS par l'opération abstraite de dépôt de message Message-submission. Il peut être produit par le système MTS.

En l'absence de cet argument, la longueur maximale permise de contenu **permissible-maximum-content-length** d'un message que l'utilisateur MTS peut déposer auprès du système MTS reste inchangée. En l'absence de commande antérieure, la longueur de contenu n'est pas explicitement limitée.

8.2.1.4.1.5 Contexte de sécurité permis permissible-security-context

Cet argument limite temporairement la sensibilité des opérations abstraites de point d'accès dépôt submission-port (contexte de sécurité de dépôt submission-security-context) que l'utilisateur MTS peut demander au système MTS. Il s'agit d'une restriction temporaire du contexte de sécurité **security-context** établi lors de la constitution de l'association (voir § 8.1.1.1.1.3). Il peut être produit par le système MTS.

Le contexte de sécurité permis **permissible-security-context** comprend une ou plusieurs étiquettes du jeu d'étiquettes de sécurité **security-labels** défini en tant que contexte de sécurité **security-context** lors de l'établissement de l'association.

En l'absence de cet argument, le contexte de sécurité **security-context** des opérations abstraites du point d'accès dépôt reste inchangé.

8.2.1.4.2 Résultats

Le Tableau 13 énumère les résultats de l'opération abstraite abstract-operation de commande de dépôt Submission-control, en qualifie la présence et spécifie les paragraphes dans lesquels ils sont définis.

Tableau 13 – Résultats de l'opération abstraite de commande de dépôt Submission-control

Résultat	Présence	Paragraphe
Résultats "en attente"		
Opérations en attente *waiting-operations*	O	8.2.1.4.2.1
Messages en attente *waiting-messages*	O	8.2.1.4.2.2
Types d'information codée en attente *waiting-encoded-information-types*	O	8.2.1.4.2.3
Types de contenu en attente *waiting-content-types*	O	8.2.1.4.2.4

8.2.1.4.2.1 Opérations en attente waiting-operations

Ce résultat indique les opérations abstraites mises en attente par l'utilisateur MTS, qui les demanderait au système MTS en l'absence des commandes en vigueur. Il peut être produit par l'utilisateur MTS.

Ce résultat peut prendre la valeur **holding** (en attente) ou **not-holding** (non en attente) dans chacun des cas suivants:

message-submission (dépôt de message): l'utilisateur MTS détient ou ne détient pas des messages en instance, et demanderait au système MTS l'opération abstraite de dépôt de message Message-submission, en l'absence des commandes en vigueur;

probe-submission (dépôt d'envoi-test): l'utilisateur MTS détient ou ne détient pas d'envois-tests en attente, et demanderait au système MTS l'opération abstraite de dépôt d'envoi-test Probe-submission, en l'absence des commandes en vigueur.

En l'absence de ce résultat, on peut supposer que l'utilisateur MTS, par suite des commandes en vigueur, ne retient pas de message ou d'envoi-test en attente de dépôt auprès du système MTS.

8.2.1.4.2.2 Messages en attente waiting-messages

Ce résultat indique le type de message que l'utilisateur MTS retient en attente de dépôt auprès du système MTS et qu'il déposerait par l'opération abstraite de dépôt de message Message-submission, n'était-ce les commandes en vigueur. Il peut être produit par l'utilisateur MTS.

Ce résultat peut prendre une ou plusieurs valeurs:

long-content (contenu trop long): l'utilisateur MTS retient des messages destinés au système MTS d'une longueur excédant la commande en vigueur de longueur maximale permise de contenu **permissible-maximum-content-length**;

low-priority (priorité trop faible): l'utilisateur MTS retient des messages destinés au système MTS d'une priorité inférieure à la valeur de la commande de priorité minimale permise **permissible-lowest-priority** en vigueur;

other-security-labels (étiquettes de sécurité non conformes): l'utilisateur MTS détient des messages destinés au système MTS dont les étiquettes de sécurité **message-security-labels** diffèrent des étiquettes autorisées par le contexte de sécurité en vigueur.

En l'absence de ces résultats, on peut supposer que l'utilisateur MTS ne retient aucun message ou envoi-test destiné au système MTS à cause de commandes en vigueur de longueur maximale permise de contenu **permissible-maximum-content-length**, de priorité minimale permise **permissible-lowest-priority** ou de contexte de sécurité permis **permissible-security-context**.

8.2.1.4.2.3 Types d'information codée en attente waiting-encoded-information-types

Ce résultat indique les types d'information codée **encoded-information-types** du contenu **content** des messages destinés au système MTS et retenus par l'utilisateur MTS à cause des commandes en vigueur. Il peut être produit par l'utilisateur MTS.

En l'absence de ce résultat, les types d'information codée **encoded-information-types** des messages retenus par l'utilisateur MTS en attente de dépôt auprès du système MTS sont **unspecified** (non spécifiés).

8.2.1.4.2.4 Types de contenu en attente waiting-content-types

Ce résultat indique les types de contenu **content-types** des messages retenus par l'utilisateur MTS en attente de dépôt auprès du système MTS à cause des commandes en vigueur. Il peut être produit par l'utilisateur MTS.

En l'absence de ce résultat, les types de contenu **content-types** des messages retenus par l'utilisateur MTS en attente de dépôt auprès du système MTS sont **unspecified** (non spécifiés).

8.2.1.4.3 Erreurs abstraites abstract-errors

Le Tableau 14 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite de commande de dépôt Submission-control, et indique le paragraphe où chacune d'elles est définie.

Tableau 14 – Erreurs abstraites de commande de dépôt Submission-control

Erreur abstraite abstract-error	Paragraphe
Erreur de sécurité *security-error*	8.2.2.8
Erreur de rattachement distant *remote-bind-error*	8.2.2.10

8.2.2 Erreurs abstraites abstract-errors

Le présent paragraphe contient la définition des erreurs abstraites d'accès de dépôt submission-port:

a) commande de dépôt enfreinte submission-control-violated;
b) élément de service non souscrit element-of-service-not-subscribed;
c) annulation de remise différée rejetée deferred-delivery-cancellation-rejected;
d) expéditeur non valide originator-invalid;
e) destinataire incorrectement spécifié recipient-improperly-specified;
f) identificateur de dépôt de message non valide message-submission-identifier-invalid;
g) demande incohérente inconsistent-request;
h) erreur de sécurité security-error;
i) fonction critique non prise en charge unsupported-critical-function;
j) erreur de rattachement distant remote-bind-error.

8.2.2.1 Commande de dépôt enfreinte submission-control-violated

L'erreur abstraite de commande de dépôt enfreinte submission-control-violated signale la transgression, par l'utilisateur MTS, d'une commande relative aux services d'accès de dépôt submission-port, commande précédemment imposée par le système MTS au moyen du service commande de dépôt Submission-control.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.2 Elément de service non souscrit element-of-service-not-subscribed

Cette erreur abstraite signale que l'opération abstraite demandée ne peut être assurée par le système MTS parce que l'utilisateur MTS n'est pas abonné à l'un des éléments de service figurant dans la requête.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.3 Annulation de remise différée rejetée deferred-delivery-cancellation-rejected

Cette erreur abstraite signale que le système MTS ne peut annuler la remise différée d'un message, soit parce que ce message a déjà été acheminé pour un transfert ou une remise, soit parce que le système MTS a fourni à l'expéditeur une preuve de dépôt **proof-of-submission**.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.4 Expéditeur non valide originator-invalid

Cette erreur abstraite signale que le message ou l'envoi-test ne peut être soumis, l'expéditeur n'étant pas correctement identifié.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.5 Destinataire incorrectement spécifié recipient-improperly-specified

Cette erreur abstraite signale que le dépôt de message ou de l'envoi-test ne peut avoir lieu car un ou plusieurs destinataires ne sont pas correctement spécifiés.

Cette erreur abstraite a les paramètres suivants, produits par le système MTS:

> **improperly-specified-recipients** (destinataires incorrectement spécifiés): suivi du ou des noms de destinataires incorrectement spécifiés.

8.2.2.6 Identificateur de dépôt de message non valide message-submission-identifier-invalid

Cette erreur abstraite signale que la remise différée d'un message ne peut être annulée parce que l'identificateur de dépôt du message **message-submission-identifier** n'est pas valide ou qu'il identifie un message soumis par un autre utilisateur MTS.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.7 Demande incohérente inconsistent-request

Cette erreur abstraite signale que l'opération abstraite demandée ne peut être assurée par le système MTS, l'utilisateur MTS ayant présenté une demande incohérente.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.8 Erreur de sécurité security-error

Cette erreur abstraite signale que l'opération abstraite demandée ne peut être assurée par le système MTS ou par l'utilisateur MTS parce qu'elle enfreindrait la politique de sécurité en vigueur.

Cette erreur abstraite contient les paramètres suivants:

> **security-problem** (problème de sécurité): suivi d'un identificateur de l'infraction de la politique de sécurité.

L'utilisation des codes d'erreur de sécurité security-error suivants dépend de la politique de sécurité et de l'implémentation des fonctions de sécurité. Ces codes d'erreur de sécurité peuvent, en particulier, être utilisés par une fonction commune de contrôle de sécurité contrôlant le fonctionnement de routine d'un agent UA, d'une mémoire MS ou d'un agent MTA et assurant que la politique de sécurité n'est pas enfreinte par le fonctionnement normal du composant du système MHS.

Le paramètre **security-problem** (problème de sécurité) peut prendre une des valeurs suivantes pour les opérations abstraites message-submission (dépôt de message) ou probe-submission (dépôt d'envoi test):

a) Les valeurs suivantes indiquent que la sécurité a été enfreinte par l'utilisateur:

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de service de sécurité): les services de sécurité demandés ne peuvent pas être fournis;

unauthorised-dl-name (nom de liste dl non autorisé)**:** le nom OR-name de l'utilisateur MTS destinataire identifie une liste DL dont l'utilisation est interdite pour des raisons de sécurité;

NOTE – Si l'agent MTA est incapable de déterminer le fait que le nom OR-name identifie une liste DL, la valeur **unauthorised-recipient-name** (nom de destinataire non autorisé) peut être utilisée à la place.

unauthorised-originator-name (nom d'expéditeur non autorisé): le nom OR-name de l'utilisateur MTS expéditeur n'est pas autorisé pour des raisons de sécurité;

unauthorised-recipient-name (nom de destinataire non autorisé): le nom OR-name de l'utilisateur MTS destinataire n'est pas autorisé pour des raisons de sécurité;

unknown-security-label (étiquette de sécurité inconnue): l'identificateur de politique de sécurité de l'étiquette de sécurité de message n'est pas reconnu par l'agent MTA. Une telle politique n'est pas mise en œuvre par l'agent MTA.

b) Les valeurs suivantes indiquent une erreur au sein du système de sécurité:

invalid-security-label (étiquette de sécurité invalide): l'identificateur de politique de sécurité de l'étiquette de sécurité de message identifie une politique connue par l'agent MTA, mais qui n'est pas acceptable pour ce système;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité obligatoire pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de dépôt a échoué pour des raisons de sécurité;

security-context-failure (échec de contexte de sécurité): l'étiquette de sécurité de message est incompatible avec le contexte de sécurité en vigueur.

Le paramètre security-problem (problème de sécurité) peut prendre une des valeurs suivantes pour l'opération abstraite de commande de dépôt Submission-control:

a) Les valeurs suivantes indiquent que la sécurité a été enfreinte par l'utilisateur:

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de services de sécurité): les services de sécurité demandés ne peuvent pas être fournis.

b) Les valeurs suivantes indiquent une erreur dans le système de sécurité:

incompatible-change-with-original-security-context (modification incompatible avec le contexte de sécurité initial): le contexte de sécurité permis permissible-security-context proposé n'est pas un sous-ensemble du contexte de sécurité initial;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité obligatoire pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de commande de dépôt Submission-control a échoué pour des raisons de sécurité.

8.2.2.9 Fonction critique non prise en charge unsupported-critical-function

Cette erreur abstraite signale qu'un argument de l'opération abstraite porte l'indication **critical-for-submission** (critique pour le dépôt) (voir § 9.2) mais qu'il n'est pas pris en charge par le système MTS.

Cette erreur abstraite n'a pas de paramètre.

8.2.2.10 Erreur de rattachement distant remote-bind-error

Cette erreur abstraite signale que l'opération abstraite demandée ne peut être effectuée par la mémoire de messages MS car celle-ci n'est pas en mesure de se rattacher au système MTS, ou parce qu'il n'existe aucune association entre la mémoire MS et l'agent UA. Cette erreur abstraite se produit en cas de dépôt indirect au système MTS via une mémoire MS, ou en cas d'appel par le système MTS d'une opération abstraite de commande de dépôt submission-control via une mémoire MS.

Cette erreur abstraite n'a pas de paramètre.

8.3 Point d'accès de remise delivery-port

Ce paragraphe contient la définition des opérations abstraites et des erreurs abstraites qui surviennent à un point d'accès de remise delivery-port.

8.3.1 Opérations abstraites abstract-operations

Ce paragraphe contient la définition des opérations abstraites suivantes du point d'accès de remise delivery-port:

a) remise de message Message-delivery;

b) remise de rapport Report-delivery;

c) commande de remise Delivery-control.

8.3.1.1 Remise de message message-delivery

Cette opération abstraite permet au système MTS de remettre un message à un utilisateur MTS.

L'utilisateur MTS ne refusera la remise d'un message que si cette remise enfreint les restrictions imposées par la commande de remise Delivery-control en vigueur.

8.3.1.1.1 Arguments

Le Tableau 15 énumère les arguments de l'opération abstraite de remise de message Message-delivery, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

Tableau 15 – Arguments de remise de message Message-delivery

Argument	Présence	Paragraphe
Arguments de remise		
Identificateur de remise de message *message-delivery-identifier*	M	8.3.1.1.1.1
Heure de remise de message *message-delivery-time*	M	8.3.1.1.1.2
Heure de dépôt de message *message-submission-time*	M	8.2.1.1.2.2
Informations de trace *trace-information*	O	12.2.1.1.1.3
Informations de trace interne *internal-trace-information*	O	12.2.1.1.1.4
Argument d'expéditeur		
Nom d'expéditeur *originator-name*	M	8.2.1.1.1.1
Arguments de destinataire		
Nom du destinataire présent *this-recipient-name*	M	8.3.1.1.1.3
Nom de destinataire initialement prévu *originally-intended-recipient-name*	C	8.3.1.1.1.4
Chronologie de réacheminement *redirection-history*	C	8.3.1.1.1.5
Noms d'autres destinataires *other-recipient-names*	C	8.3.1.1.1.6
Chronologie de développement de liste DL *DL-expansion-history*	C	8.3.1.1.1.7
Destinataires exemptés de la liste DL *DL-exempted-recipients*	O	8.2.1.1.1.40
Argument de priorité		
Priorité *priority*	C	8.2.1.1.1.8
Arguments de conversion		
Interdiction de conversion implicite *implicit-conversion-prohibited*	C	8.2.1.1.1.9
Interdiction de conversion avec perte *conversion-with-loss-prohibited*	C	8.2.1.1.1.10
Types convertis d'informations codées *converted-encoded-information-types*	C	8.3.1.1.1.8
Argument de méthode de remise		
Méthode de remise demandée *requested-delivery-method*	C	8.2.1.1.1.14

Tableau 15 – Arguments de remise de message Message-delivery

Argument	Présence	Paragraphe
Arguments de remise physique		
Interdiction de retransmission physique *physical-forwarding-prohibited*	C*	8.2.1.1.1.15
Demande d'adresse de retransmission physique *physical-forwarding-address-request*	C*	8.2.1.1.1.16
Modes de remise physique *physical-delivery-modes*	C*	8.2.1.1.1.17
Type de courrier recommandé *registered-mail-type*	C*	8.2.1.1.1.18
Numéro de destinataire pour avis *recipient-number-for-advice*	C*	8.2.1.1.1.19
Attributs de restitution physique *physical-rendition-attributes*	C*	8.2.1.1.1.20
Adresse de retour à l'expéditeur *originator-return-address*	C*	8.2.1.1.1.21
Demande de rapport de remise physique *physical-delivery-report-request*	C*	8.2.1.1.1.24
Arguments relatifs à la sécurité		
Certificat d'expéditeur *originator-certificate*	C	8.2.1.1.1.25
Jeton de message *message-token*	C	8.2.1.1.1.26
Identificateur d'algorithme de confidentialité de contenu *content-confidentiality-algorithm-identifier*	C	8.2.1.1.1.27
Contrôle d'intégrité de contenu *content-integrity-check*	C	8.2.1.1.1.28
Contrôle d'authentification d'origine de message *message-origin-authentication-check*	C	8.2.1.1.1.29
Etiquette de sécurité *message-security-label*	C	8.2.1.1.1.30
Demande de preuve de remise *proof-of-delivery-request*	C	8.2.1.1.1.32
Certificats d'expéditeurs multiples *multiple-originator-certificates*	O	8.2.1.1.1.41
Certificats de destinataires *recipient-certificate*	O	8.2.1.1.1.42
Sélecteurs de certificats *certificate-selectors*	O	8.2.1.1.1.43
Violation des sélecteurs de certificats *certificate-selectors-override*	O	8.2.1.1.1.44
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	C	8.2.1.1.1.33
Type de contenu *content-type*	M	8.2.1.1.1.34
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35
Contenu *content*	M	8.2.1.1.1.37

NOTE – C* Indique que ces arguments sont normalement absents pour les destinataires pour lesquels la remise physique n'est pas spécifiée, mais peuvent apparaître dans des situations particulières (par exemple en cas de réacheminement).

8.3.1.1.1.1Identificateur de remise de message message-delivery-identifier

Cet argument contient un identificateur **MTS-identifier** qui distingue le message de tous les autres au niveau du point d'accès de remise delivery-port. Il est produit par le système MTS et a la même valeur que l'identificateur de dépôt de message **message-submission-identifier** fourni à l'expéditeur du message lors du dépôt de ce dernier.

8.3.1.1.1.2 Heure de remise de message message-delivery-time

Cet argument contient la date et l'heure auxquelles a lieu la remise et auxquelles le système MTS se décharge de la responsabilité du message. Il est produit par le système MTS.

En cas de remise physique, cet argument indique la date et l'heure **Time** auxquelles l'unité d'accès de remise physique PDAU a pris la responsabilité d'imprimer puis de remettre le message.

Cet argument a la même valeur que l'argument d'heure de remise de message **message-delivery-time** notifié à l'expéditeur (voir § 8.3.1.2.1.9) dans un rapport de remise delivery-report.

8.3.1.1.1.3 Nom du destinataire présent this-recipient-name

Cet argument contient le nom **OR-name** du destinataire auquel est remis le message. Il est produit par le système MTS.

Cet argument a la même valeur que l'argument correspondant de nom du destinataire **recipient-name** (à savoir l'argument qui a entraîné la remise du message à ce destinataire) qui était présent dans le message immédiatement avant la remise.

Le nom de destinataire présent **this-recipient-name** contient le nom **OR-name** d'un destinataire individuel et non celui d'une liste DL.

Le nom **OR-name** du destinataire prévu (s'il est différent, le message ayant été réacheminé ou obtenu par expansion de liste DL) est contenu dans l'argument de nom de destinataire initialement prévu **originally-intended-recipient-name**.

8.3.1.1.1.4 Nom de destinataire initialement prévu originally-intended-recipient-name

Cet argument contient le nom **OR-name** du destinataire spécifié par l'expéditeur au moment du dépôt, tel qu'il a été modifié par la procédure de dépôt de message (voir § 14.6.1). Il est produit par le système MTS (lors de la remise de message ou de la production de rapport par l'agent MTA) si le nom **OR-name** du destinataire prévu a été remplacé suite à un développement de liste DL ou à un réacheminement.

8.3.1.1.1.5 Chronologie de réacheminement redirection-history

Cet argument consigne les événements de réacheminement qui ont eu lieu lors du transfert du message à travers le système MTS. Il est produit par le système MTS en cas de réacheminement. Pour chaque événement de réacheminement, il contient le nom **OR-name** du destinataire prévu avant réacheminement, l'heure **time** à laquelle le réacheminement a eu lieu et le motif du réacheminement.

Le motif de réacheminement **redirection-reason** prend l'une des valeurs suivantes:

recipient-assigned-alternate-recipient (destinataire suppléant désigné par le destinataire): le destinataire prévu a demandé le réacheminement du message à un destinataire suppléant désigné par lui; l'expéditeur du message n'a pas interdit la réassignation de destinataire (voir § 8.2.1.1.1.4); le système MTS a réacheminé le message vers le destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient**;

originator-requested-alternate-recipient (destinataire suppléant désigné par l'expéditeur): le message n'a pu être remis au destinataire prévu **intended-recipient** ou, le cas échéant, au destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient**; l'argument de destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient** a identifié un destinataire suppléant; le système MTS a réacheminé le message vers le destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient**;

recipient-MD-assigned-alternate-recipient (destinataire suppléant assigné par le domaine de gestion du destinataire): l'argument de nom de destinataire **recipient-name** n'a pas identifié un utilisateur MTS destinataire; l'argument d'autorisation de destinataire suppléant **alternate-recipient-allowed** produit par l'expéditeur a permis la remise à un destinataire suppléant; le système MTS a réacheminé le message vers un destinataire suppléant assigné par le MD (domaine de gestion) destinataire pour recevoir de tels messages;

directory-look-up (consultation de l'annuaire): l'adresse **OR-address** du destinataire prévu n'a pas identifié d'utilisateur MTS destinataire; le nom **OR-name** de ce destinataire contenait un nom d'annuaire **directory-name** qui a été utilisé pour obtenir une adresse **OR-address** différente pour ce même destinataire prévu; le système MTS a réacheminé le message vers cette adresse **OR-address** de remplacement du destinataire prévu;

alias: l'argument nom de destinataire **recipient-name** ne contenait pas d'adresse préférée pour l'utilisateur MTS spécifié; le système MTS a réacheminé le message vers une adresse préférée de cet utilisateur MTS.

NOTE 1 – La distinction entre adresse préférée et non préférée est établie par configuration locale.

Certains systèmes correspondant à des versions antérieures de la présente Spécification peuvent ne pas prendre en charge les valeurs **alias** ou **directory-look-up**. Ces valeurs ne leur seront alors pas transmises, sauf accord bilatéral.

NOTE 2 – A cette fin, il est recommandé que les réalisations d'agents MTA prévues pour fonctionner aux frontières entre anciens et nouveaux systèmes (aux frontières de domaines par exemple) soient dotées d'une fonction configurable leur permettant de modifier la chronologie de réacheminement. Une telle fonction remplacerait selon le cas la valeur **alias** par **recipient-assigned-alternate-recipient** (destinataire suppléant désigné par le destinataire) et **directory-look-up** par **originator-assigned-alternate-recipient** (destinataire suppléant désigné par l'expéditeur) lors du transfert du message vers l'agent MTA adjacent.

8.3.1.1.1.6 Noms d'autres destinataires other-recipient-names

Si l'expéditeur du message a demandé la divulgation des autres destinataires, cet argument contient les noms **OR-names** de tous les destinataires initialement spécifiés autres que celui qui est identifié par l'argument de nom de destinataire initial **originally-intended-recipient-name** s'il existe, sinon par l'argument de nom du destinataire présent **this-recipient-name**. Il est produit par le système MTS si et seulement si l'argument de divulgation des autres destinataires **disclosure-of-other-recipients** de l'opération abstraite de dépôt message-submission a pour valeur **disclosure-of-other-recipients-requested** (divulgation des autres destinataires demandée) et s'il existe au moins un tel autre destinataire.

Chaque nom d'autre destinataire **other-recipient-name** contient le nom **OR-name** d'un destinataire individuel ou d'une liste DL.

NOTE – Si une liste DL a été développée, les noms **OR-names** des membres de cette liste ne seront pas divulgués. Le nom **OR-name** d'une liste DL est divulgué si et seulement s'il s'agit d'un destinataire initialement prévu.

8.3.1.1.1.7 Chronologie de développement de liste DL DL-expansion-history

Cet argument contient la séquence de noms **OR-names** de toute liste DL développée pour trouver les destinataires de la copie du message, ainsi que la date et l'heure de chaque développement. Il est produit par le système MTS chaque fois qu'une liste est développée.

8.3.1.1.1.8 Types convertis d'informations codées converted-encoded-information-types

Cet argument identifie les types d'informations codées **encoded-information-types** du contenu du message après une éventuelle conversion. Il peut être produit par le système MTS.

8.3.1.1.2 Résultats

Le Tableau 16 énumère les résultats de l'opération abstraite de remise de message Message-delivery et, pour chacun d'eux, en qualifie la présence et identifie le paragraphe dans lequel il est défini.

Tableau 16 – Résultats de remise de message Message-delivery

Résultat	Présence	Paragraphe
Résultats de preuve de remise		
Certificat de destinataire *recipient-certificate*	O	8.3.1.1.2.1
Preuve de remise *proof-of-delivery*	C	8.3.1.1.2.2

8.3.1.1.2.1 Certificat de destinataire recipient-certificate

Cet argument contient le certificat du destinataire du message. Il est produit par une source de confiance (par exemple, une autorité de certification) et peut être fourni par le destinataire si l'expéditeur a demandé une preuve de remise **proof-of-delivery** (voir § 8.2.1.1.1.32) et qu'un algorithme de chiffrement asymétrique asymmetric-encryption-algorithm a servi à calculer la preuve de remise **proof-of-delivery**.

Le certificat de destinataire **recipient-certificate** peut servir à acheminer une copie conforme de la clé publique de chiffrement asymétrique public-asymmetric-encryption-key (clé sujet publique **subject-public-key**) du destinataire du message.

L'expéditeur peut utiliser la clé publique de chiffrement asymétrique public-asymmetric-encryption-key pour valider la preuve de remise **proof-of-delivery**.

8.3.1.1.2.2 Preuve de remise proof-of-delivery

Cet argument fournit à l'expéditeur la preuve que le message a été remis au destinataire (pour fournir l'élément de service de preuve de remise tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Selon l'algorithme de chiffrement utilisé et la politique de sécurité en vigueur, cet argument peut également fournir l'élément de service de non-répudiation de remise (tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il est produit par le destinataire du message si l'expéditeur a demandé une preuve de remise **proof-of-delivery** (voir 8.2.1.1.1.32).

La preuve de remise **proof-of-delivery** est calculée à l'aide de l'algorithme identifié par l'identificateur d'algorithme de preuve de remise **proof-of-delivery-algorithm-identifier**.

La preuve de remise **proof-of-delivery** contient l'identificateur d'algorithme de preuve de remise **proof-of-delivery-algorithm-identifier** et une fonction chiffrée (une version comprimée ou dispersée par exemple) de l'identificateur d'algorithme de preuve de remise **proof-of-delivery-algorithm-identifier**, l'heure de remise **delivery-time**, ainsi que le nom du destinataire présent **this-recipient-name**, le nom de destinataire initial **originally-intended-recipient-name**, le contenu du message **content**, l'identificateur de contenu **content-identifier** et l'étiquette de sécurité **message-security-label** du message remis. Les composantes facultatives sont incluses dans la preuve de remise **proof-of-delivery** si elles sont présentes dans le message remis. La preuve de remise **proof-of-delivery** est calculée au moyen du contenu du message tel qu'il est remis, qu'il soit chiffré ou en clair.

La réception de cet argument fournit à l'expéditeur la preuve de remise du message au destinataire. Mais sa non-réception ne constitue ni une preuve de remise, ni une preuve de non-remise (à moins d'utiliser un trajet sécurisé et une fonctionnalité fiable).

Si on utilise un algorithme de chiffrement asymétrique asymmetric-encryption-algorithm, la preuve de remise **proof-of-delivery** peut être calculée par le destinataire à l'aide de sa clé secrète de chiffrement asymétrique secret-asymmetric-encryption-key. L'expéditeur du message peut valider la preuve de remise **proof-of-delivery** à l'aide de la clé publique de chiffrement asymétrique public-asymmetric-encryption-key du destinataire (clé publique sujet **subject-public-key**) obtenue du certificat de destinataire **recipient-certificate**. Une preuve de remise **proof-of-delivery** asymétrique peut aussi assurer la non-répudiation de remise, sous réserve de la disponibilité d'une infrastructure appropriée de clés publiques.

Si on utilise un algorithme symétrique, le destinataire utilise une clé de chiffrement symétrique symmetric-encryption-key pour calculer la preuve de remise **proof-of-delivery**; l'expéditeur fait de même pour valider la preuve de remise **proof-of-delivery**. En cas d'utilisation de l'algorithme de chiffrement symétrique symmetric-encryption-algorithm, la preuve de remise **proof-of-delivery** ne peut assurer la non-répudiation de remise que si la politique de sécurité en vigueur prévoit la participation d'un tiers agissant comme notaire. Les moyens par lesquels la clé de chiffrement symétrique symmetric-encryption-key est distribuée ne sont pas encore définis par la présente Définition de service.

8.3.1.1.3 Erreurs abstraites abstract-errors

Le Tableau 17 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite de remise de message Message-delivery; et indique pour chacune d'elles le paragraphe où elles sont définies.

Tableau 17 – Erreurs abstraites de remise de message Message-delivery

Erreur abstraite abstract-error	Paragraphe
Commande de remise enfreinte *delivery-control-violated*	8.3.2.1
Erreur de sécurité *security-error*	8.3.2.3
Fonction critique non prise en charge *unsupported-critical-function*	8.3.2.4

8.3.1.2 Remise de rapport Report-delivery

L'opération abstraite de remise de rapport **Report-delivery** permet au système MTS d'accuser réception à l'utilisateur MTS d'un ou plusieurs résultats d'une opération abstraite précédemment appelée de dépôt de message Message-submission ou de dépôt d'envoi-test Probe-submission.

Dans le cas d'une opération abstraite de dépôt de message Message-submission, l'opération abstraite de remise de rapport Report-delivery indique la remise ou la non-remise du message déposé à un ou plusieurs destinataires.

Dans le cas d'une opération abstraite de dépôt d'envoi-test Probe-submission, l'opération abstraite de remise de rapport Report-delivery indique si le message aurait pu ou non être remis ou si le développement d'une liste DL aurait pu avoir lieu si le message avait été déposé.

Une seule invocation à l'opération abstraite de dépôt de message Message-submission ou de dépôt d'envoi-test Probe-submission peut donner lieu à plusieurs opérations abstraites de remise de rapport Report-delivery, chacune concernant un ou plusieurs destinataires prévus. Une seule opération abstraite de remise de rapport Report-delivery peut notifier la remise ou la non-remise à différents destinataires.

L'invocation de l'opération abstraite de dépôt de message Message-submission ou de dépôt d'envoi-test Probe-submission par un utilisateur MTS peut donner lieu à des opérations abstraites de remise de rapport Report-delivery à un autre utilisateur MTS, en l'occurrence de rapports remis au détenteur d'une liste DL.

L'utilisateur MTS ne refusera pas la remise d'un rapport à moins que cette remise n'enfreigne les restrictions de commande de remise Delivery-control en vigueur.

8.3.1.2.1 Arguments

Le Tableau 18 énumère les arguments de l'opération abstraite de remise de rapport Report-delivery, en qualifie la présence et précise les paragraphes dans lesquels ils sont définis.

Tableau 18 – Arguments de remise de rapport Report-delivery

Argument	Présence	Paragraphe
Argument de dépôt de sujet		
Identificateur de dépôt de sujet *subject-submission-identifier*	M	8.3.1.2.1.1
Arguments du destinataire		
Nom de destinataire effectif *actual-recipient-name*	M	8.3.1.2.1.2
Nom de destinataire initialement prévu *originally-intended-recipient-name*	C	8.3.1.1.1.4
Chronologie de réacheminement *redirection-history*	C	8.3.1.1.1.5
Expéditeur et chronologie de développement de liste DL *originator-and-DL-expansion-history*	C	8.3.1.2.1.3
Nom de liste DL au rapport *reporting-DL-name*	C	8.3.1.2.1.4
Arguments d'enveloppe de rapport		
Chronologie de réacheminement *redirection-history*	C	8.3.1.2.1.5
Informations de trace *trace-information*	O	12.2.1.1.1.3
Informations de trace interne *internal-trace-information*	O	12.2.1.1.1.4
Nom de l'agent MTA au rapport *reporting-MTA-name*	C	8.3.1.2.1.17
Argument de conversion		
Types convertis d'informations codées *converted-encoded-information-types*	C	8.3.1.2.1.6
Arguments d'informations supplémentaires		
Informations supplémentaires *supplementary-information*	C	8.3.1.2.1.7
Adresse de retransmission physique *physical-forwarding-address*	C	8.3.1.2.1.8
Arguments de remise		
Heure de remise de message *message-delivery-time*	C	8.3.1.2.1.9
Type d'utilisateur *type-of-MTS-user*	C	8.3.1.2.1.10
Arguments de non-remise		
Code de motif de non-remise *non-delivery-reason-code*	C	8.3.1.2.1.11
Code de diagnostic de non-remise *non-delivery-diagnostic-code*	C	8.3.1.2.1.12
Arguments de sécurité		
Certificat de destinataire *recipient-certificate*	C	8.3.1.1.2.1
Preuve de remise *proof-of-delivery*	C	8.3.1.1.2.2
Certificat de l'agent MTA au rapport *reporting-MTA-certificate*	C	8.3.1.2.1.13
Contrôle d'authentification d'origine de rapport *report-origin-authentication-check*	C	8.3.1.2.1.14
Etiquette de sécurité de message *message-security-label*	C	8.2.1.1.1.30
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	C	8.2.1.1.1.33
Type de contenu *content-type*	C	8.3.1.2.1.15
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	C	8.2.1.1.1.36
Contenu réacheminé *returned-content*	C	8.3.1.2.1.16

8.3.1.2.1.1 Identificateur de dépôt de sujet subject-submission-identifier

Cet argument contient l'identificateur de dépôt de message **message-submission-identifier** ou l'identificateur de dépôt d'envoi-test **probe-submission-identifier** du sujet du rapport. Il est fourni par le système MTS.

8.3.1.2.1.2 Nom de destinataire effectif actual-recipient-name

Cet argument contient le nom **OR-name** d'un destinataire. Il est produit soit par l'expéditeur du message, soit par le système MTS si le message a été réacheminé ou s'il y a eu développement de liste DL. Une valeur différente de cet argument est spécifiée pour chaque destinataire du sujet concerné par ce rapport.

Dans le cas d'un rapport de remise, le nom de destinataire effectif **actual-recipient-name** est le nom du destinataire effectif du message, et il a la même valeur que l'argument nom du destinataire présent **this-recipient-name** du message remis. Dans le cas d'un rapport de non-remise, le nom de destinataire effectif **actual-recipient-name** est le nom **OR-name** du destinataire vers lequel a été réacheminé le message lorsque la cause de non-remise est survenue.

Le nom de destinataire effectif **actual-recipient-name** peut être soit un nom de destinataire initialement spécifié, soit le nom **OR-name** d'un destinataire suppléant vers lequel le message a été réacheminé, ou le nom **OR-name** d'un membre de liste DL s'il y a eu développement de liste DL. Si le message a été réacheminé ou s'il y a eu développement de liste DL, le nom **OR-name** du destinataire initialement spécifié est contenu dans l'argument de nom de destinataire initialement prévu **originally-intended-recipient-name**.

Le nom du destinataire effectif **actual-recipient-name** contient le nom **OR-name** d'un destinataire individuel ou d'une liste DL.

8.3.1.2.1.3 Expéditeur et chronologie de développement de liste DL originator-and-DL-expansion-history

Cet argument contient une séquence de noms **OR-names** avec les dates et heures associées représentant la chronologie de l'origine du message sujet. Le premier nom **OR-name** de la séquence est celui de l'expéditeur du sujet, et la suite est la séquence de noms **OR-names** des listes DL développées lors de l'acheminement du sujet vers le destinataire (cette dernière étant la même que dans la chronologie de développement de liste DL **DL-expansion-history**). Il est produit par l'agent MTA d'origine du rapport lorsqu'un développement de liste DL a lieu.

L'argument d'expéditeur et chronologie de développement de liste DL **originator-and-DL-expansion-history** contient le nom **OR-name** de l'expéditeur du sujet et de chaque liste DL ainsi que la date et l'heure auxquelles l'événement associé s'est produit.

8.3.1.2.1.4 Nom de liste DL au rapport reporting-DL-name

Cet argument contient le nom **OR-name** de la liste DL qui fait rapport à son détenteur. Il est produit par un point de développement de liste DL-expansion-point (un agent MTA) lors de la transmission d'un rapport au détenteur de la DL, conformément à la politique de compte rendu de celle-ci.

Le nom de liste DL au rapport **reporting-DL-name** contient le nom **OR-name** de la liste DL qui fait rapport.

8.3.1.2.1.5 Chronologie de réacheminement redictory-history

Cet argument consigne les événements de réacheminement survenus pendant le transfert du rapport à travers le système MTS. Il est produit par le système MTS en cas de réacheminement. Pour chaque événement de réacheminement survenu, il contient le nom de destination de rapport **report-destination-name** avant réacheminement, l'heure **time** à laquelle le réacheminement a eu lieu et le motif du réacheminement. Les valeurs de motif de réacheminement **redirection-reason** sont définies au § 8.3.1.1.1.5, sauf que le destinataire suppléant demandé par l'expéditeur **originator-requested-alternate-recipient** ne s'applique pas à ces rapports.

NOTE – Dans le Tableau 18, l'argument de destinataire Redirection-history contient la chronologie de réacheminement de l'objet du rapport, tandis que l'argument Redirection-history de l'enveloppe du rapport contient la chronologie de réacheminement du rapport lui-même.

8.3.1.2.1.6 Types convertis d'information codée converted-encoded-information-types

Cet argument identifie en cas de conversion les types d'information codée **encoded-information-types** du contenu du message sujet subject-message après conversion. Dans le cas d'un rapport relatif à un message, cet argument indique les types d'information codée **encoded-information-types** effectifs du contenu du message converti. Dans le cas d'un rapport concernant un envoi-test, cet argument indique les types d'information codée qui auraient figuré dans le contenu du message sujet après conversion si ce message avait été déposé. Il peut être produit par le système MTS. Une valeur différente de ce paramètre peut être spécifiée pour chaque destinataire du sujet faisant l'objet du rapport.

8.3.1.2.1.7 Informations supplémentaires supplementary-information

Cet argument peut contenir des informations fournies par l'expéditeur du rapport sous forme de chaîne imprimable. Il peut être produit par l'agent MTA expéditeur du rapport ou par une unité d'accès associée. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du sujet faisant l'objet du rapport.

Les informations supplémentaires **supplementary-information** peuvent être utilisées par une unité d'accès télétex ou par une installation de conversion télétex/télex. Elles peuvent comporter un indicatif de réception, une durée de transmission télex ou une note et un message reçu enregistré sous forme de chaîne imprimable.

Les informations supplémentaires **supplementary-information** peuvent aussi être utilisées par d'autres unités d'accès ou par l'agent MTA expéditeur du rapport lui-même pour acheminer les informations imprimables vers l'expéditeur du message.

8.3.1.2.1.8 Adresse de retransmission physique physical-forwarding-address

Cet argument contient la nouvelle adresse postale **postal-OR-address** du destinataire physique du message. Il peut être produit par l'unité d'accès de remise physique PDAU associée à l'agent MTA expéditeur du rapport si l'expéditeur du message a demandé l'adresse de retransmission physique physical-forwarding-address du destinataire (voir § 8.2.1.1.1.16). Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du message sujet faisant l'objet du rapport.

8.3.1.2.1.9 Heure de remise de message message-delivery-time

Cet argument contient la date et l'heure **Time** auxquelles le message sujet a été (ou aurait été) remis à l'utilisateur MTS destinataire. Il est produit par le système MTS au moment où le message a été (ou aurait été) remis. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du sujet faisant l'objet du rapport.

En cas de remise physique, cet argument indique la date et l'heure **Time** auxquelles l'unité PDAU a assumé la responsabilité de l'impression puis de la remise du message.

Si le message sujet a été remis, la valeur de cet argument est la même que celle de l'argument d'heure de remise **message-delivery-time** du message remis (voir § 8.3.1.1.1.2).

8.3.1.2.1.10 Type d'utilisateur MTS type-of-MTS-user

Cet argument indique le type d'utilisateur MTS destinataire auquel le message a été (ou aurait été) remis. Il est produit par le système MTS au moment où le message a été (ou aurait été) remis avec succès. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du sujet faisant l'objet du rapport.

Cet argument peut prendre l'une des valeurs suivantes:

public: un agent UA détenu par une Administration;

private (privé): un agent UA détenu par une entité autre qu'une Administration;

ms: une mémoire de messages;

DL: une liste de distribution;

PDAU: une unité d'accès de remise physique (PDAU);

physical-recipient: le destinataire physique d'un système de remise physique;

other (autre): une unité d'accès d'un autre type.

8.3.1.2.1.11 Code de motif de non-remise non-delivery-reason-code

Cet argument contient un code indiquant le motif pour lequel la remise du message sujet a échoué (ou, dans le cas d'un envoi-test, aurait échoué). Il est produit par le système MTS si la remise du message s'était (ou se serait) terminée par un échec. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du sujet faisant l'objet du rapport.

Cet argument peut prendre l'une des valeurs suivantes:

transfer-failure (échec de transfert): indique que, pendant que le système MTS tentait de remettre ou faisait un essai de remise d'un message sujet, une défaillance de communication l'en a empêché;

unable-to-transfer (impossiblité de transfert): indique qu'en raison d'un problème au niveau du sujet lui-même, le système MTS n'a pu remettre le message sujet ou en faire l'essai de remise;

conversion-not-performed (conversion non effectuée): indique qu'une conversion nécessaire à la remise du message sujet a (ou aurait) été impossible;

physical-rendition-not-performed (restitution physique non effectuée): indique que l'unité d'accès PDAU a été dans l'incapacité de restituer physiquement le message sujet;

physical-delivery-not-performed (remise physique non effectuée): indique que le système de remise physique PDS a été dans l'incapacité de remettre physiquement le message sujet;

restricted-delivery (remise restreinte): indique que le destinataire est abonné à l'élément de service de remise restreinte restricted-delivery (tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1) qui a (ou aurait) empêché la remise du message sujet;

directory-operation-unsuccessful (échec d'une opération d'annuaire): indique l'échec d'une opération d'annuaire nécessaire;

deferred-delivery-not-performed (remise différée non exécutée): indique qu'il n'a pas été possible d'accéder à une demande de remise différée du message sujet;

transfer-failure-for-security-reason (échec de transfert pour des raisons de sécurité): indique qu'un échec lié à la sécurité a empêché le système MTS de remettre ou de remettre un envoi test du message sujet lors de sa tentative.

D'autres codes de motifs de non-remise **non-delivery-reason-codes** pourront être spécifiés dans des addenda ou dans des versions futures de la présente Recommandation | Norme internationale.

D'autres informations relatives à la nature du problème empêchant la remise sont données dans l'argument de code de diagnostic de non-remise **non-delivery-diagnostic-code**.

8.3.1.2.1.12 Code de diagnostic de non-remise non-delivery-diagnostic-code

Cet argument contient un code indiquant la nature du problème à l'origine de l'échec de remise ou d'essai de remise du message sujet. Il peut être produit par le système MTS s'il y a eu (ou s'il y aurait eu) échec de remise du message. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire prévu du sujet faisant l'objet du rapport.

Cet argument peut prendre une des valeurs suivantes:

unrecognised-OR-name (nom d'OR inconnu): l'argument de nom de destinataire **recipient-name** du sujet ne contient pas de nom **OR-name** connu du système MTS;

ambiguous-OR-name (nom d'OR ambigu): l'argument nom de destinataire **recipient-name** du sujet identifie plusieurs destinataires possibles (il y a donc ambiguïté);

MTS-congestion (encombrement du système MTS): le sujet n'a pu être acheminé en raison de l'encombrement du système MTS;

loop-detected (bouclage): circulation du sujet en boucle à l'intérieur du système MTS;

recipient-unavailable (destinataire occupé): l'utilisateur MTS destinataire était (ou aurait été) indisponible pour prendre livraison du message sujet;

maximum-time-expired (expiration du délai maximal): expiration du délai maximal pour la remise ou l'essai de remise du message sujet;

encoded-information-types-unsupported (types d'informations codées non pris en charge): les types d'informations codées du message sujet ne sont pas pris en charge par l'utilisateur MTS destinataire;

content-too-long (contenu trop long): la longueur de contenu **content-length** du message sujet est trop grande pour que l'utilisateur MTS destinataire puisse en prendre livraison (elle excède la longueur maximale de contenu de message remis);

conversion-impractical (conversion impossible): la conversion nécessaire à la remise du message sujet n'est pas possible;

implicit-conversion-prohibited (conversion implicite interdite): une conversion nécessaire à la remise du message sujet a été interdite par l'expéditeur du sujet (voir § 8.2.1.1.1.9);

implicit-conversion-not-subscribed (conversion implicite non souscrite): une conversion nécessaire à la remise du message sujet ne fait pas partie de l'abonnement du destinataire;

invalid-arguments (arguments invalides): un ou plusieurs arguments du sujet ont été reconnus non valides;

content-syntax-error (erreur de syntaxe de contenu): une erreur de syntaxe a été détectée dans le contenu du message sujet (ne s'applique pas aux envois-tests);

size-constraint-violation (contrainte de taille enfreinte): indique que la valeur d'un ou de plusieurs paramètres du sujet enfreint les contraintes de taille définies dans la présente Définition de service, et que le système MTS n'est pas préparé à traiter la ou les valeurs spécifiées;

protocol-violation (protocole enfreint): indique qu'un ou plusieurs arguments obligatoires manquent dans le sujet;

content-type-not-supported (type de contenu non pris en charge): indique que le traitement d'un type de contenu **content-type** non pris en charge par le système MTS était (ou aurait été) nécessaire pour remettre le message sujet;

too-many-recipients (destinataires trop nombreux): indique que le système MTS était (ou aurait été) dans l'impossibilité de remettre le message sujet en raison du nombre des destinataires spécifiés (voir § 8.2.1.1.1.2);

no-bilateral-agreement (absence d'accord bilatéral): indique que la remise du message sujet nécessite (ou nécessiterait) un accord bilatéral qui n'existe pas;

unsupported-critical-function (fonction critique non prise en charge): indique qu'une fonction critique nécessaire au transfert ou à la remise du message sujet n'est pas assurée par l'agent MTA expéditeur du rapport;

conversion-with-loss-prohibited (conversion avec perte interdite): une conversion nécessaire à la remise du message sujet aurait entraîné une perte d'information alors que la conversion avec perte est interdite par l'expéditeur (voir § 8.2.1.1.1.10);

line-too-long (ligne trop longue): une conversion nécessaire à la remise du message sujet subject-message aurait entraîné une perte d'information, la ligne initiale étant trop longue;

page-split (coupure de page): une conversion nécessaire à la remise du message sujet aurait entraîné une perte d'information due au partage d'une page initiale;

pictorial-symbol-loss (perte de symbole graphique): une conversion nécessaire à la remise du message sujet aurait entraîné une perte d'information résultant de la perte d'un ou de plusieurs symboles graphiques;

punctuation-symbol-loss (perte de signe de ponctuation): une conversion nécessaire à la remise du message sujet aurait entraîné une perte d'information résultant de la perte d'un ou de plusieurs signes de ponctuation;

alphabetic-character-loss (perte de caractère alphabétique): une conversion nécessaire à la remise du message sujet aurait entraîné une perte d'information résultant de la perte d'un ou de plusieurs caractères alphabétiques;

multiple-information-loss (perte d'informations multiples): une conversion nécessaire à la remise du message sujet aurait entraîné de multiples pertes d'informations;

recipient-reassignment-prohibited (réassignation de destinataire interdite): indique que le système MTS était (ou aurait été) dans l'incapacité de remettre le message sujet, l'expéditeur ayant interdit le réacheminement vers un destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient** (voir § 8.2.1.1.1.4);

redirection-loop-detected (boucle de réacheminement détectée): le message sujet n'a pu être réacheminé vers un destinataire suppléant, ce dernier ayant déjà réacheminé le même message (boucle de réacheminement);

DL-expansion-prohibited (développement de liste DL interdit): indique que le système MTS était (ou aurait été) dans l'incapacité de remettre le message sujet, l'expéditeur ayant interdit le développement des listes DL (voir § 8.2.1.1.1.6);

no-DL-submit-permission (absence de permission de dépôt de liste DL): l'expéditeur du sujet (ou la liste DL dont cette liste DL est membre dans le cas de listes DL imbriquées) n'a pas la permission de soumettre des messages à cette liste DL;

DL-expansion-failure (échec de développement de liste DL): indique que le système MTS n'a pu mener à bien le développement d'une liste DL;

physical-rendition-attributes-not-supported (attributs de restitution physique non pris en charge): l'unité d'accès de remise physique PDAU ne prend pas en charge les attributs de restitution physique nécessaires (voir § 8.2.1.1.1.20);

undeliverable-mail-physical-delivery-address-incorrect (courrier non remis: adresse de remise physique incorrecte): le message sujet n'a pu être remis, l'adresse **postal-OR-address** spécifiée pour le destinataire étant incorrecte;

undeliverable-mail-physical-delivery-office-incorrect-or-invalid (courrier non remis: bureau de remise physique incorrect ou invalide): le message sujet n'a pu être remis, le bureau de remise physique identifié par l'adresse **postal-OR-address** spécifiée pour le destinataire étant incorrect ou non valide (n'existant pas);

undeliverable-mail-physical-delivery-address-incomplete (courrier non remis: adresse de remise physique incomplète): le message sujet n'a pu être remis, l'adresse **postal-OR-address** spécifiée pour le destinataire étant incomplète;

undeliverable-mail-recipient-unknown (courrier non remis: inconnu à l'adresse): le message sujet n'a pu être remis, le destinataire spécifié par l'adresse **postal-OR-address** étant inconnu à cette adresse;

undeliverable-mail-recipient-deceased (courrier non remis: destinataire décédé): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** étant décédé;

undeliverable-mail-organization-expired (courrier non remis: organisation supprimée): le message sujet n'a pu être remis, l'organisation destinataire spécifiée dans l'adresse **postal-OR-address** n'existant plus;

undeliverable-mail-recipient-refused-to-accept (courrier non remis: le destinataire refuse de le recevoir): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** ayant refusé de le recevoir;

undeliverable-mail-recipient-did-not-claim (courrier non remis: non réclamé par le destinataire): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** n'ayant pas ramassé le courrier;

undeliverable-mail-recipient-changed-address-permanently (courrier non remis: changement définitif d'adresse de destinataire): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** ayant définitivement changé d'adresse ("déménagé") et la retransmission ne s'appliquant pas;

undeliverable-mail-recipient-changed-address-temporarily (courrier non remis: changement temporaire d'adresse de destinataire): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** ayant momentanément changé d'adresse ("en voyage") et la retransmission ne s'appliquant pas;

undeliverable-mail-recipient-changed-temporary-address (courrier non remis: changement d'adresse temporaire de destinataire): le message sujet n'a pu être remis, le destinataire spécifié dans l'adresse **postal-OR-address** ayant modifié son adresse temporaire ("est parti") et la retransmission ne s'appliquant pas;

undeliverable-mail-new-address-unknown (courrier non remis: nouvelle adresse inconnue): le message sujet n'a pu être remis, le destinataire ayant déménagé sans laisser de nouvelle adresse;

undeliverable-mail-recipient-did-not-want-forwarding (courrier non remis: refus de retransmission par le destinataire): le message sujet n'a pu être remis, car cela aurait nécessité une retransmission physique que le destinataire refuse;

undeliverable-mail-originator-prohibited-forwarding (courrier non remis: interdiction de retransmission par l'expéditeur): la retransmission physique nécessaire à la remise du message sujet a été interdite par l'expéditeur du message sujet (voir § 8.2.1.1.1.15);

secure-messaging-error (erreur de sécurité de messagerie): le sujet n'a pu être acheminé car l'étiquette de sécurité du message enfreindrait la politique de sécurité en vigueur, ce qui va à l'encontre du contexte de sécurité;

unable-to-downgrade (impossibilité d'adapter vers le bas): le sujet n'a pu être transféré car il n'a pu être adapté vers le bas (voir Annexe B de la Rec. UIT-T X.419 | ISO/CEI 10021-6);

unable-to-complete-transfer (impossibilité de transférer): le système destinataire indique qu'il est dans l'impossibilité permanente de mener à bien le transfert du sujet; c'est le cas par exemple si le sujet à transférer est d'une taille telle qu'il ne pourra jamais être accepté;

transfer-attempts-limit-reached (limite de tentatives de transfert atteinte): le nombre maximal ou la durée maximale de répétition des tentatives de transfert du sujet a été atteint;

incorrect-notification-type (type de notification incorrecte): le message sujet contient un argument **notification-type** (type de notification) qui ne correspond pas à son contenu **content**.

Pour des erreurs de sécurité, cet argument peut prendre une des valeurs suivantes:

a) Les valeurs suivantes indiquent que la sécurité a été enfreinte par l'utilisateur:

DL-expansion-prohibited-by-security-policy (développement de liste DL interdit par la politique de sécurité): le message sujet était adressé à une liste DL mais la politique de sécurité interdisait le développement de cette liste DL;

forbidden-alternate-recipient (destinataire suppléant interdit): le message sujet aurait été réacheminé mais le nouveau destinataire est inacceptable pour des raisons de sécurité;

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de service de sécurité): les services de sécurité demandés ne peuvent pas être fournis;

unauthorised-DL-member (membre de liste DL non autorisé): le développement de la liste DL n'a pas été effectué car l'agent MTA a découvert que l'un des membres de la liste DL n'était pas autorisé, par la politique de sécurité, à recevoir ce message;

unauthorised-DL-name (nom de liste DL non autorisé): l'agent MTA a détecté que le nom OR-name du destinataire identifie une liste DL mais que la politique de sécurité locale ne permet pas le transfert en aval vers le point de développement de la liste DL;

unauthorised-originally-intended-recipient-name (nom de destinataire initialement prévu non autorisé): le nom OR-name du destinataire initialement prévu du message réacheminé ou développé par liste DL n'est pas autorisé pour des raisons de sécurité;

unauthorised-originator-name (nom d'expéditeur non autorisé): le nom OR-name de l'utilisateur MTS expéditeur n'est pas autorisé pour des raisons de sécurité;

unauthorised-recipient-name (nom de destinataire non autorisé): le nom OR-name de l'utilisateur MTS destinataire n'est pas autorisé pour des raisons de sécurité;

unreliable-system (système non fiable): la remise du message sujet exigerait que le message sujet soit transféré à un système non sécurisé, ce qui est incompatible avec l'étiquette de sécurité de message.

b) Les valeurs suivantes indiquent une erreur au sein du système de sécurité:

authentication-failure-on-subject-message (échec d'authentification du message sujet): la validation de l'argument contrôle d'authentification d'origine de message message-origin-authentication-check, ou de l'argument jeton de message message-token (par exemple signature, ou toute autre données de jeton) a échoué et le contenu du message sujet ne pouvait donc pas être authentifié ou validé;

decryption-failed (échec du déchiffrement): le contenu du message sujet n'a pas pu être déchiffré;

decryption-key-unobtainable (clé de déchiffrement impossible à obtenir): la clé nécessaire n'a pu être obtenue pour déchiffrer les données chiffrées du jeton de message message-token encrypted-data ou pour la confidentialité du contenu;

double-envelope-creation-failure (échec de la création de double enveloppe): la politique de sécurité nécessitait la création d'une enveloppe externe pour protéger le message sujet. Cependant, l'agent MTA a été incapable de créer une enveloppe externe;

double-enveloping-message-restoring-failure (échec de la restitution du message doublement enveloppé): le message sujet contenait une enveloppe intérieure, mais un échec des services de sécurité sur l'enveloppe extérieure n'a pas permis à l'agent MTA d'extraire le message intérieur pour un traitement ultérieur;

failure-of-proof-of-message (échec de preuve de message): une erreur a été détectée dans les arguments de preuve de sécurité dans le message sujet;

integrity-failure-on-subject-message (échec d'intégrité sur le message sujet): la validation de l'argument de vérification d'intégrité de contenu a échoué, et le contenu du message sujet n'a donc pas pu être validé;

invalid-security-label (étiquette de sécurité non valide): l'identificateur de la politique de sécurité dans l'étiquette de sécurité du message identifie une politique connue par l'agent UA ou MTA destinataire mais qui n'est pas acceptable pour ce système;

key-failure (échec de clé): les clés nécessaires ne peuvent pas être obtenues;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité requis pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de transfert ou de remise a échoué pour des raisons de sécurité;

repudiation-failure-of-message (échec de répudiation du message): la politique de sécurité nécessitait l'utilisation d'une signature avec des propriétés de non-répudiation, mais le message sujet n'était pas signé avec une signature d'expédition non répudiable;

security-context-failure-message (échec du contexte de sécurité du message): l'étiquette de sécurité de message n'est pas compatible avec le contexte de sécurité en vigueur;

token-decryption-failed (échec du déchiffrement du jeton): le jeton du message n'a pas pu être déchiffré;

token-error (erreur de jeton): une erreur a été détectée au niveau de l'argument du jeton du message sujet;

unknown-security-label (étiquette de sécurité inconnue): l'identificateur de la politique de sécurité contenu dans l'étiquette de sécurité de message n'est pas reconnu par l'agent UA ou MTA destinataire. Une telle politique n'est pas offerte par ce système;

unsupported-algorithm-identifier (identificateur d'algorithme non offert): le destinataire ne met pas en œuvre les identificateurs d'algorithmes utilisés dans l'argument de sécurité du message sujet;

unsupported-security-policy (politique de sécurité non offerte): le destinataire n'offre pas la politique de sécurité demandée, comme cela est identifié dans l'argument d'étiquette de sécurité du message sujet (message-security-label).

D'autres codes de diagnostic de non-remise **non-delivery-diagnostic-codes** pourront être spécifiés dans des addenda ou de futures versions de la présente Recommandation | Norme internationale.

8.3.1.2.1.13 Certificat d'agent MTA au rapport reporting-MTA-certificate

Cet argument contient le **certificate** certificat de l'agent MTA qui a produit le rapport. Il est produit par une source de confiance (par exemple une autorité de certification) et peut être fourni par l'agent MTA faisant rapport en cas de fourniture d'un contrôle d'authentification d'origine de rapport **report-origin-authentication-check**.

Le certificat de l'agent MTA au rapport **reporting-MTA-certificate** peut être utilisé pour acheminer une copie certifiée de la clé publique de chiffrement asymétrique (clé publique sujet **subject-public-key**) de l'agent MTA au rapport.

La clé publique de chiffrement asymétrique de l'agent MTA au rapport peut être utilisée par l'expéditeur et par n'importe quel agent MTA par lequel le rapport transite pour valider le contrôle d'authentification d'origine de rapport **report-origin-authentication-check**.

8.3.1.2.1.14 Contrôle d'authentification d'origine de rapport report-origin-authentication-check

Cet argument fournit à l'expéditeur du message sujet (ou de l'envoi-test sujet), ainsi qu'à tout autre agent MTA par lequel le rapport transite, un moyen d'authentifier l'origine du rapport (afin d'assurer l'élément de service d'authentification d'origine du rapport tel qu'il est défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1). Il peut être produit par l'agent MTA au rapport si un contrôle d'authentification d'origine de message (ou d'envoi-test) **message-** (ou **probe-**) **origin-authentication-check** figure dans le sujet.

Le contrôle d'authentification d'origine **report-origin-authentication-check** fournit une preuve de l'origine du rapport (authentification d'origine du rapport) et la preuve d'une association entre l'étiquette de sécurité de message **message-security-label** et le rapport.

Le contrôle d'authentification d'origine de rapport **report-origin-authentication-check** est calculé au moyen d'un algorithme identifié par l'identificateur d'algorithme d'authentification d'origine de rapport **report-origin-authentication-algorithm-identifier**.

Le contrôle d'authentification d'origine de rapport **report-origin-authentication-check** contient l'identificateur d'algorithme d'authentification d'origine de rapport **report-origin-authentication-algorithm-identifier** et une version dispersée à chiffrement asymétrique:

de l'identificateur d'algorithme d'authentification d'origine de rapport **report-origin-authentication-algorithm-identifier**;

de l'identificateur de contenu **content-identifier** du sujet;

de l'étiquette de sécurité **message-security-label** du sujet;

et de toutes les valeurs des arguments suivants (par destinataire):

nom du destinataire effectif **actual-recipient-name**;

nom de destinataire initialement prévu **originally-intended-recipient-name**; et:

pour un rapport de remise delivery-report:

l'heure de remise **message-delivery-time**;

le type d'utilisateur **type-of-MTS-user**;

le certificat de destinataire **recipient-certificate** s'il a été demandé par l'expéditeur pour les destinataires que ce rapport concerne;

la preuve de remise **proof-of-delivery** si elle a été demandée par l'expéditeur pour les destinataires que ce rapport concerne et si le rapport concerne un message; ou

pour un rapport de non-remise non-delivery-report:

le code de motif de non-remise **non-delivery-reason-code**; et

le code de diagnostic de non-remise **non-delivery-diagnostic-code**.

Des composantes facultatives sont incluses dans le contrôle d'authentification d'origine **report-origin-authentication-check** si elles figurent dans le rapport.

Le contrôle d'authentification d'origine de rapport **report-origin-authentication-check** peut être calculé par l'agent MTA au rapport au moyen de la clé secrète de chiffrement asymétrique de l'agent MTA au rapport. Ce contrôle d'authentification peut être validé par l'expéditeur du sujet et par n'importe quel agent MTA par lequel ce rapport transite, à l'aide de la clé publique de chiffrement asymétrique de l'agent MTA au rapport (clé publique sujet **subject-public-key**) obtenue à partir du certificat de l'agent MTA au rapport **reporting-MTA-certificate**.

Des addenda ou de futures versions de la présente Recommandation | Norme internationale pourront définir d'autres formes de contrôle d'authentification d'origine de rapport **report-origin-authentication-check** (fondées, par exemple, sur des techniques de chiffrement symétrique) qui pourront être utilisées par les agents MTA par lesquels le rapport transite pour authentifier l'origine du rapport.

8.3.1.2.1.15 Type de contenu content-type

Cet argument identifie le type du contenu **content** du message (voir § 8.2.1.1.1.34). Il doit être produit par l'agent MTA rapporteur. Cet argument ne peut être absent à la réception que si le rapport est produit ou relayé par un système de version 1984.

8.3.1.2.1.16 Contenu renvoyé returned-content

Cet argument contient le contenu **content** du message sujet si son expéditeur a indiqué que le contenu **content** devait être renvoyé (voir § 8.2.1.1.1.23). Il doit être produit par l'expéditeur et peut être renvoyé par le système MTS (si l'agent MTA au rapport ou l'agent MTA expéditeur assure l'élément de service de renvoi du contenu).

Cet argument ne peut être présent que si l'opération de remise de rapport Report-delivery comporte au moins un rapport de non-remise et si le destinataire du rapport est l'expéditeur du message sujet (et non, par exemple, le détenteur d'une liste DL (voir § 8.3.1.2.1.4)).

Cet argument sera absent si une quelconque conversion de type d'information codée **encoded-information-type** a été effectuée sur le contenu **content** du message sujet.

8.3.1.2.1.17 Nom de l'agent MTA au rapport Reporting-MTA-name

Cet argument identifie l'agent MTA qui a créé le rapport. Il comprend un nom MTA-name, un identificateur global de domaine et, en option, un nom d'annuaire d'un agent de transfert de message MHS **MHS Message Transfer Agent** (voir § A.1.3 de la Rec. UIT-T X.402 | ISO/CEI 10021-2). Il peut être produit par l'agent MTA au rapport, mais seulement si cela est exigé par la politique de sécurité en vigueur.

NOTE 1 – Indépendamment de toute utilisation à des fins de sécurité, cet argument peut être utilisé à des fins de diagnostic pour indiquer l'agent MTA qui a produit le rapport.

NOTE 2 – L'information de trace interne contient également le nom de l'agent MTA au rapport. Dans les environnements où l'information de trace interne n'est détruite en aucun point entre l'expéditeur et le destinataire, l'information de trace interne peut être utilisée à la place de cet élément.

NOTE 3 – Lorsqu'elle est utilisée avec des services tels que l'authentification d'origine ou la preuve de remise, une politique de sécurité typique exige que ce paramètre soit produit chaque fois que ces services sont invoqués.

8.3.1.2.2 Résultats

L'opération abstraite de remise de rapport Report-delivery renvoie un résultat vide comme indication de succès.

8.3.1.2.3 Erreurs abstraites abstract-errors

Le Tableau 19 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite de remise de rapport Report-delivery et identifie le paragraphe dans lequel chacune est définie.

Tableau 19 – Erreurs abstraites de remise de rapport Report-delivery

Erreur abstraite abstract-error	Paragraphe
Commande de remise enfreinte *delivery-control-violated*	8.3.2.1
Erreur de sécurité *security-error*	8.3.2.3
Fonction critique non prise en charge *unsupported-critical-function*	8.3.2.4

8.3.1.3 Commande de remise Delivery-control

L'opération abstraite de commande de remise Delivery-control permet à l'utilisateur MTS de limiter temporairement les opérations abstraites que le système MTS peut invoquer au point d'accès de remise delivery-port, ainsi que les messages que le système MTS peut remettre à l'utilisateur MTS par une opération abstraite de remise de message Message-delivery.

Le système MTS suspend, plutôt que de les abandonner, les opérations abstraites et les messages actuellement interdits.

La réussite de l'opération abstraite signifie que les commandes spécifiées sont maintenant en vigueur. Ces commandes annulent et remplacent toutes les autres commandes précédemment en vigueur et restent en cours jusqu'à ce que l'association soit libérée, que l'utilisateur MTS rappelle l'opération abstraite de commande de remise Delivery-control

ou qu'il invoque l'opération abstraite d'enregistrement de l'accès administration-port pour imposer des contraintes plus sévères que les commandes précédemment spécifiées.

L'opération abstraite renvoie une indication signalant toute opération abstraite que le système MTS aurait pu invoquer, et tout type de message que le système MTS aurait pu remettre ou signaler, en l'absence des commandes en vigueur.

8.3.1.3.1 Arguments

Le Tableau 20 énumère les arguments de l'opération abstraite de commande de remise Delivery-control, en qualifie la présence et identifie les paragraphes où ils sont définis.

Tableau 20 – Arguments de la commande de remise Delivery-control

Argument	Présence	Paragraphe
Arguments de commande de remise		
Restriction *restrict*	O	8.3.1.3.1.1
Opérations permises *permissible-operations*	O	8.3.1.3.1.2
Plus faible priorité permise *permissible-lowest-priority*	O	8.3.1.3.1.3
Types permis d'information codée *permissible-encoded-information-types*	O	8.3.1.3.1.4
Types permis de contenu *permissible-content-types*	O	8.3.1.3.1.5
Longueur maximale permise de contenu *permissible-maximum-content-length*	O	8.3.1.3.1.6
Contexte de sécurité permis *permissible-security-context*	O	8.3.1.3.1.7

8.3.1.3.1.1 Restriction restrict

Cet argument indique si les commandes relevant des opérations abstraites du point d'accès de remise delivery-port doivent être mises à jour ou supprimées. Il peut être généré par l'utilisateur MTS.

Cet argument peut prendre l'une des valeurs suivantes:

update (mise à jour): les autres arguments mettent à jour les commandes en vigueur;

remove (suppression): toutes les commandes temporaires sont supprimées (les commandes par défaut enregistrées dans le système MTS par l'opération abstraite d'enregistrement de l'accès administration-port s'appliquent); les autres arguments seront ignorés.

En l'absence de cet argument, c'est la valeur **update** (mise à jour) qui prévaut par défaut.

8.3.1.3.1.2 Opérations permises permissible-operations

Cet argument indique les opérations abstraites que le système MTS peut invoquer à l'utilisateur MTS. Il peut être généré par l'utilisateur MTS.

Cet argument peut prendre la valeur **allowed** (permis) ou **prohibited** (interdit) pour chacun des éléments qui suivent:

message-delivery (remise de message): le système MTS peut ou non invoquer l'opération abstraite de remise de message Message-delivery;

report-delivery (remise de rapport): le système MTS peut ou non invoquer l'opération abstraite de remise de rapport Report-delivery.

Les autres opérations abstraites du point d'accès de remise delivery-port ne dépendent pas des commandes et peuvent être invoquées à tout moment.

En l'absence de cet argument, les opérations abstraites que le système MTS peut invoquer à l'utilisateur MTS restent inchangées. Si aucune invocation de l'opération abstraite de commande de remise Delivery-control n'a eu encore lieu sur l'association, c'est la commande par défaut enregistrée dans le système MTS par l'opération abstraite d'enregistrement de l'accès administration-port qui s'applique.

8.3.1.3.1.3 Plus faible priorité permise permissible-lowest-priority

Cet argument contient la plus faible priorité **priority** de message que le système MTS puisse remettre à l'utilisateur MTS par l'opération abstraite de remise Message-delivery. Il peut être produit par l'utilisateur MTS.

Cet argument peut prendre une des valeurs suivantes de l'argument priorité **priority** de l'opération abstraite de dépôt de message: normal non urgent ou urgent.

En l'absence de cet argument, la priorité **priority** du message le moins prioritaire que le système MTS puisse remettre à l'utilisateur MTS reste inchangée. S'il n'y a pas eu d'appel antérieur de l'opération abstraite de commande de remise Delivery-control sur cette association, c'est la commande par défaut enregistrée dans le système MTS au moyen de l'opération abstraite d'enregistrement de l'accès d'administration qui s'applique.

8.3.1.3.1.4 Types permis d'informations codées permissible-encoded-information-types

Cet argument indique les types d'informations codées **encoded-information-types** qui apparaissent dans les messages que le système MTS fournit à l'utilisateur MTS par l'opération abstraite de remise Message-delivery. Il peut être produit par l'utilisateur MTS.

L'argument inclut les sous-arguments **acceptable-encoded-information-types** (types acceptables), **unacceptable-encoded-information-types** (types inacceptables) et **exclusively-acceptable-encoded-information-types** (types exclusivement acceptables), chacun de ces sous-arguments identifiant une liste de types d'informations codées (voir § 8.4.1.1.1.3.1).

En l'absence de cet argument, les types permis d'informations codées **permissible-encoded-information-types** que le système MTS peut remettre à l'utilisateur MTS restent inchangés. Si aucun appel de l'opération abstraite de commande de remise Delivery-control n'a antérieurement eu lieu sur l'association, la commande par défaut enregistrée dans le système MTS par l'opération abstraite d'enregistrement Registre de l'accès d'administration s'applique.

8.3.1.3.1.5 Types permis de contenu permissible-content-types

Cet argument indique les seuls types de contenu qui figureront dans les messages que le système MTS remet à l'utilisateur MTS par l'opération abstraite de remise de message Message-delivery. Il peut être produit par l'utilisateur MTS.

Les types permis de contenu **permissible-content-types** spécifiés feront partie de ceux qui auront été autorisés à long terme par une invocation antérieure de l'opération abstraite d'enregistrement de l'accès d'administration (types de contenu pouvant être remis **deliverable-content-types**).

En l'absence de cet argument, les types permis de contenu **permissible-content-types** que le système MTS peut remettre à l'utilisateur MTS restent inchangés. Si aucun appel de l'opération abstraite de commande de remise Delivery-control n'a antérieurement eu lieu sur l'association, la commande par défaut enregistrée dans le système MTS par l'opération abstraite d'enregistrement Registre de l'accès d'administration s'applique.

8.3.1.3.1.6 Longueur maximale permise de contenu permissible-maximum-content-length

Cet argument contient la longueur de contenu **content-length**, exprimée en octets, du contenu le plus long que le système MTS puisse remettre à l'utilisateur MTS par l'opération abstraite de remise de message Message-delivery. Il peut être produit par l'utilisateur MTS.

La longueur maximale permise de contenu **permissible-maximum-content-length** n'excédera pas celle qui aura été autorisée à long terme par un appel antérieur de l'opération abstraite d'enregistrement Registre d'accès d'administration (longueur maximale de contenu pouvant être remise **deliverable-maximum-content-length**).

En l'absence de cet argument, la longueur maximale permise de contenu **permissible-maximum-content-length** d'un message que le système MTS peut remettre à l'utilisateur MTS reste inchangée. Si aucune invocation de l'opération abstraite de commande de remise Delivery-control n'a antérieurement eu lieu sur l'association, la commande par défaut enregistrée dans le système MTS par l'opération abstraite d'enregistrement Registre d'accès d'administration s'applique.

8.3.1.3.1.7 Contexte de sécurité permis permissible-security-context

Cet argument limite temporairement le caractère de sensibilité des opérations abstraites du point d'accès de remise delivery-port (contexte de sécurité de remise delivery-security-context) que le système MTS peut invoquer à l'utilisateur MTS. Il s'agit d'une restriction temporaire du contexte de sécurité **security-context** établi au moment de la mise en place de l'association (voir § 8.1.1.1.1.4). Il peut être produit par l'utilisateur MTS.

Le contexte de sécurité permis **permissible-security-context** comprend une ou plusieurs des étiquettes du jeu d'étiquettes de sécurité **security-labels** établi comme contexte de sécurité au moment de la mise en place de l'association.

En l'absence de cet argument, le contexte de sécurité des opérations abstraites de point d'accès de remise reste inchangé.

8.3.1.3.2 Résultats

Le Tableau 21 énumère les résultats de l'opération abstraite de commande de remise Delivery-control, en qualifie la présence et identifie les paragraphes où ils sont définis.

Tableau 21 – Résultats de commande de remise Delivery-control

Résultat	Présence	Paragraphe
Résultats "*en attente*"		
Opérations en attente *waiting-operations*	O	8.3.1.3.2.1
Messages en attente *waiting-messages*	O	8.3.1.3.2.2
Types d'informations codées en attente *waiting-encoded-information-types*	O	8.3.1.3.2.3
Types de contenu en attente *waiting-content-types*	O	8.3.1.3.2.4

8.3.1.3.2.1 Opérations en attente waiting-operations

Ce résultat indique les opérations abstraites mises en attente par le système MTS et que celui-ci aurait invoqué à l'utilisateur MTS si ce n'était les commandes en vigueur. Il peut être produit par le système MTS.

Ce résultat peut prendre la valeur **holding** (rétention) ou **not-holding** (non-rétention) pour chacun des éléments suivants:

message-delivery (remise de message): le système MTS ne retient pas de messages ou en retient et invoquerait l'opération abstraite de remise de message Message-delivery à l'utilisateur MTS si ce n'était les commandes en vigueur;

report-delivery (remise de rapport): le système MTS ne retient pas de rapports ou en retient et demanderait l'opération abstraite de remise de rapport Report-delivery à l'utilisateur MTS si ce n'était les commandes en vigueur.

En l'absence de ce résultat, on peut supposer que le système MTS n'a mis aucun message ou rapport en attente en raison des commandes en vigueur.

8.3.1.3.2.2 Messages en attente waiting-messages

Ce résultat indique le type de message que le système MTS a mis en attente de remise à l'utilisateur MTS et qu'il remettrait par l'opération abstraite de remise de message, si ce n'était les commandes en vigueur. Il peut être généré par le système MTS.

Ce résultat peut prendre une ou plusieurs des valeurs suivantes:

long-content (contenu long): le système MTS retient des messages destinés à l'utilisateur MTS, car leur longueur excède la longueur maximale permise de contenu **permissible-maximum-content-length** en vigueur;

low-priority (priorité trop faible): le système MTS retient des messages destinés à l'utilisateur MTS, car leur priorité est inférieure à la commande de plus faible priorité permise **permissible-lowest-priority** en vigueur;

other-security-labels (étiquettes de sécurité non conformes): le système MTS retient des messages destinés à l'utilisateur MTS, car leurs étiquettes de sécurité **message-security-labels** diffèrent de celles qui sont permises par le contexte de sécurité en vigueur.

En l'absence de ce résultat, on peut supposer que le système MTS ne retient aucun message en attente de remise à l'utilisateur MTS en raison des commandes en vigueur de longueur maximale permise de contenu **permissible-maximum-content-length**, de plus faible priorité permise **permissible-lowest-priority** ou de contexte de sécurité permis **permissible-security-context**.

8.3.1.3.2.3 Types d'informations codées en attente waiting-encoded-information-types

Ce résultat indique les types d'informations codées **encoded-information-types** contenues dans tout message mis par le système MTS en attente de remise à l'utilisateur MTS, en raison des commandes en vigueur. Il peut être produit par le système MTS.

En l'absence de ce résultat, le type d'informations codées **encoded-information-type** de tout message retenu par le système MTS en vue de sa remise à l'utilisateur MTS est **unspecified** (non spécifié).

8.3.1.3.2.4 Types de contenu en attente waiting-content-types

Ce résultat indique le type de contenu **content-types** de tout message mis par le système MTS en attente de remise à l'utilisateur MTS, en raison des commandes en vigueur. Il peut être produit par le système MTS.

En l'absence de ce résultat, le type de contenu **content-types** de tout message mis par le système MTS en attente de remise à l'utilisateur MTS est **unspecified** (non spécifié).

8.3.1.3.3 Erreurs abstraites abstract-errors

Le Tableau 22 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite de commande de remise Delivery-control et indique pour chacune d'elles le paragraphe dans lequel elle est définie.

Tableau 22 – Erreurs abstraites de commande de remise Delivery-control

Erreur abstraite abstract-error	Paragraphe
Paramètres d'enregistrement enfreints par la commande *control-violates-registration*	8.3.2.2
Erreur de sécurité *security-error*	8.3.2.3
Opération refusée *operation-refused*	8.3.2.5

8.3.2 Erreurs abstraites abstract-errors

Ce paragraphe définit les erreurs abstraites suivantes de point d'accès de remise delivery-port:

a) commande de remise enfreinte *delivery-control-violated*;

b) paramètres d'enregistrement enfreints par la commande *control-violates-registration*;

c) erreur de sécurité *security-error*;

d) fonction critique non prise en charge *unsupported-critical-function*;

e) opération refusée *operation-refused*.

8.3.2.1 Commande de remise enfreinte delivery-control-violated

Cette erreur abstraite signale la transgression par le système MTS d'une commande d'opération abstraite du point d'accès de remise delivery-port imposée par l'utilisateur MTS au moyen de l'opération abstraite de commande de remise Delivery-control.

L'erreur abstraite de commande de remise enfreinte delivery-control-violated n'a pas de paramètre.

8.3.2.2 Paramètres d'enregistrement enfreints par la commande control-violates-registration

Cette erreur abstraite signale que le système MTS ne peut accepter les commandes que l'utilisateur MTS tente d'imposer aux opérations abstraites de point d'accès de remise delivery-port car elles enfreignent les paramètres d'enregistrement existants.

Cette erreur abstraite n'a pas de paramètre.

8.3.2.3 Erreur de sécurité security-error

Cette erreur abstraite signale que l'utilisateur MTS ne peut accéder à la demande d'opération abstraite car celle-ci transgresserait la politique de sécurité en vigueur.

Cette erreur abstraite prend les paramètres suivants, produits par l'utilisateur MTS:

security-problem (problème de sécurité): suivi d'un identificateur du motif d'infraction à la politique de sécurité.

Le paramètre problème de sécurité **security-problem** peut prendre une des valeurs suivantes pour les opérations abstraites de remise de message Message-delivery ou de remise de rapport Report-delivery:

a) Les valeurs suivantes indiquent que la sécurité a été enfreinte par l'utilisateur:

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de services de sécurité): les services de sécurité demandés ne peuvent pas être offerts;

unauthorised-originally-intended-recipient-name (nom de destinataire initialement prévu non autorisé): le nom OR-name du destinataire initialement prévu du message réacheminé ou du message étendu par liste DL n'est pas autorisé pour des raisons de sécurité;

unauthorised-originator-name (nom d'expéditeur non autorisé): le nom O-R name de l'utilisateur MTS expéditeur n'est pas autorisé pour des raisons de sécurité;

unauthorised-recipient-name (nom de destinataire non autorisé): le nom O-R name de l'utilisateur MTS destinataire n'est pas autorisé pour des raisons de sécurité.

b) Les valeurs suivantes indiquent une erreur au sein du système de sécurité:

authentication-failure-on-subject-message (échec d'authentification du message sujet): la validation de l'argument contrôle d'authentification d'origine de message message-origin-authentication-check, ou de l'argument jeton de message message-token (par exemple signature, ou toute autre donnée de jeton) a échoué et le contenu du message sujet n'a donc pas pu être authentifié ou validé;

decryption-failed (échec du déchiffrement): le contenu du message sujet n'a pas pu être déchiffré;

decryption-key-unobtainable (clé de déchiffrement impossible à obtenir): la clé nécessaire pour déchiffrer les données chiffrées du jeton de message message-token encrypted-data ou pour la confidentialité du contenu n'a pas pu être obtenue;

failure-of-proof-of-message (échec de preuve de message): une erreur a été détectée dans les arguments de preuve de sécurité dans le message sujet;

integrity-failure-on-subject-message (échec d'intégrité sur le message sujet): la validation de l'argument de vérification d'intégrité de contenu a échoué, et le contenu du message sujet n'a donc pas pu être validé;

invalid-security-label (étiquette de sécurité non valide): l'identificateur de la politique de sécurité dans l'étiquette de sécurité du message identifie une politique connue par l'agent UA mais qui n'est pas acceptable par cet agent UA;

key-failure (échec de clé): les clés nécessaires n'ont pas pu être obtenues;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité exigé pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de remise a échoué pour des raisons de sécurité;

repudiation-failure-of-message (échec de répudiation du message): la politique de sécurité nécessitait l'utilisation d'une signature ayant des propriétés de non-répudiation, mais le message n'était pas signé avec une signature d'expédition non répudiable;

security-context-failure (échec du contexte de sécurité): l'étiquette de sécurité de message n'est pas compatible avec le contexte de sécurité en vigueur;

token-decryption-failed (échec du déchiffrement du jeton): le jeton du message n'a pas pu être déchiffré;

token-error (erreur de jeton): une erreur a été détectée au niveau de l'argument du jeton du message;

unknown-security-label (étiquette de sécurité inconnue): l'identificateur de la politique de sécurité dans l'étiquette de sécurité de message n'est pas reconnue par l'agent UA. Une telle politique n'est pas offerte par l'agent UA.

unsupported-algorithm-identifier (identificateur d'algorithme non offert): le destinataire ne met pas en œuvre les identificateurs d'algorithme utilisés dans l'argument de sécurité du message;

unsupported-security-policy (politique de sécurité non offerte): le destinataire n'offre pas la politique de sécurité demandée, comme cela est identifié dans l'argument de l'étiquette de sécurité du message.

Le paramètre problème de sécurité peut prendre une des valeurs suivantes pour l'opération abstraite de contrôle de remise Delivery-control:

a) Les valeurs suivantes indiquent que la sécurité est enfreinte par l'utilisateur:

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de services de sécurité): les services de sécurité demandés ne peuvent pas être fournis.

b) Les valeurs suivantes indiquent une erreur au sein du système de sécurité:

incompatible-change-with-original-security-context (modification incompatible avec le contexte de sécurité initial): le contexte de sécurité permis proposé n'est pas un sous-ensemble du contexte de sécurité initial;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité obligatoire pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de commande de remise **Delivery-control** a échoué pour des raisons de sécurité.

8.3.2.4 Fonction critique non prise en charge unsupported-critical-function

Cette erreur abstraite signale qu'un argument de l'opération abstraite porte la mention **critical-for-delivery** (critique pour la remise) (voir § 9.2) mais qu'il n'est pas pris en charge par l'utilisateur MTS.

Cette erreur abstraite n'a pas de paramètre.

8.3.2.5 Opération refusée operation-refused

Cette erreur abstraite indique que le système MTS a refusé d'effectuer une opération en raison de règles locales. Cette erreur a deux paramètres produits par le système MTS, l'argument refusé **refused-argument** et le motif du refus **refusal-reason**.

Le paramètre **refused-argument** indique quel argument de l'opération a provoqué le refus. Pour l'opération de contrôle de remise il indique l'un des arguments énumérés au Tableau 20 ou, pour la classe pouvant être remise, l'une de ses composantes, ou encore un argument d'extension. Pour l'opération d'enregistrement il indique l'un des arguments énumérés au Tableau 23 ou un argument d'extension.

Le paramètre motif de refus **refusal-reason** prend l'une des valeurs suivantes:

facility-unavailable (fonctionnalité indisponible): l'utilisateur a tenté d'utiliser une fonctionnalité que le système MTS ne propose pas à ses utilisateurs;

facility-not-subscribed (non-abonnement à la fonctionnalité): l'utilisateur a tenté d'utiliser une fonctionnalité qui nécessite un abonnement sans y être abonné;

parameter-unacceptable (paramètre inacceptable): l'utilisateur a spécifié une valeur de paramètre que l'agent MTA ne peut accepter.

8.4 Accès d'administration

Le présent paragraphe définit les opérations abstraites et les erreurs abstraites qui surviennent à un accès d'administration.

8.4.1 Opérations abstraites abstract-operations

Le présent paragraphe définit les opérations abstraites suivantes d'accès d'administration:

a) enregistrement Register;

b) modification des pouvoirs Change-credentials.

8.4.1.1 Enregistrement Register

L'opération abstraite d'enregistrement Register permet à l'utilisateur MTS d'apporter des modifications à long terme aux divers paramètres d'utilisateur MTS consignés par le système MTS chargé de la remise de messages à l'utilisateur MTS.

De telles modifications restent en vigueur jusqu'à ce qu'elles soient supplantées par un nouvel appel de l'opération abstraite d'enregistrement Register. Toutefois, certains paramètres peuvent être momentanément annulés et remplacés par appel de l'opération abstraite de commande de remise Delivery-control.

NOTE 1 – Cette opération abstraite doit être appelée avant de pouvoir utiliser toute autre opération abstraite de point d'accès de dépôt (submission-port), de remise (delivery-port) ou d'administration (administration-port), et avant qu'un enregistrement équivalent par des moyens locaux ait eu lieu.

NOTE 2 – Cette opération abstraite n'englobe pas les paramètres de base auxquels fait appel l'élément de service d'assignation de destinataire suppléant Alternate Recipient Assignment défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1. La manière dont ces paramètres sont fournis et modifiés est du ressort local.

NOTE 3 – Des mécanismes autres que l'enregistrement peuvent être utilisés pour affecter une valeur à l'un quelconque des paramètres d'enregistrement.

NOTE 4 – La définition de l'opération abstraite d'enregistrement utilisable dans un contexte d'application de la Norme de 1988 est donnée dans l'Annexe C.

8.4.1.1.1 Arguments

Le Tableau 23 énumère les arguments de l'opération abstraite d'enregistrement Register, en qualifie la présence et identifie les paragraphes où ils sont définis.

Tableau 23 – Arguments d'enregistrement Register

Argument	Présence	Paragraphe
Arguments d'enregistrement		
Nom d'utilisateur *user-name*	O	8.4.1.1.1.1
Adresse d'utilisateur *user-address*	O	8.4.1.1.1.2
Classes pouvant être remises *deliverable-classes*	O	8.4.1.1.1.3
Réacheminement assigné par le destinataire *recipient-assigned-redirections*	O	8.4.1.1.1.4
Remise restreinte *restricted-delivery*	O	8.4.1.1.1.5
Extraction-enregistrement *retrieve-registrations*	O	8.4.1.1.1.6
Arguments de commande de remise par défaut		8.4.1.1.1.7
Opérations permises *permissible-operations*	O	8.3.1.3.1.2
Plus faible priorité permise *permissible-lowest-priority*	O	8.3.1.3.1.3
Types permis d'informations codées *permissible-encoded-information-types*	O	8.3.1.3.1.4
Types permis de contenu *permissible-content-types*	O	8.3.1.3.1.5
Longueur maximale permise de contenu *permissible-maximum-content-length*	O	8.3.1.3.1.6

8.4.1.1.1.1 Nom d'utilisateur user-name

Cet argument contient, s'il doit être modifié, le nom **OR-name** de l'utilisateur MTS. Il peut être produit par l'utilisateur MTS.

Un domaine de gestion MD n'est pas nécessaire pour accorder aux utilisateurs MTS la capacité de modifier leurs propres noms **OR-names**. Si toutefois il intervient, le domaine MD peut limiter cette capacité. Il peut interdire à certains utilisateurs MTS de modifier leurs noms **OR-names** ou en limiter le choix à un sous-ensemble localement défini des composantes de leurs noms **OR-names**. Un nouveau nom **OR-name** proposé sera rejeté si son adresse OR est déjà attribuée à un autre utilisateur MTS ou à une liste DL.

En l'absence de cet argument, le nom d'utilisateur **user-name** de l'utilisateur MTS reste inchangé.

8.4.1.1.1.2 Adresse d'utilisateur user-address

Cet argument contient l'adresse d'utilisateur **user-address** de l'utilisateur MTS si elle est demandée par le système MTS ou si elle doit être modifiée. Il peut être produit par l'utilisateur MTS.

L'adresse d'utilisateur **user-address** peut contenir une des formes d'adresse suivantes de l'utilisateur MTS:

X.121 address et/ou le **TSAP-ID** (identificateur de point d'accès du service transport);

PSAP address (adresse de point d'accès du service présentation).

D'autres formes d'adresse d'utilisateur pourront être définies dans des addenda ou de futures versions de la présente Recommandation | Norme internationale.

En l'absence de cet argument, l'adresse **user-address** de l'utilisateur MTS (s'il y en a) reste inchangée.

8.4.1.1.1.3 Classes livrables deliverable-classes

Cet argument contient tous les ensembles de critères qui déterminent quels messages doivent être remis à l'utilisateur MTS et si l'un quelconque de ces critères doit être modifié. S'il est présent, cet argument remplace les classes livrables **deliverable-classes** précédemment enregistrées. Il peut être produit par l'utilisateur MTS.

Chaque ensemble de critères forme une classe livrable **deliverable-class**. La classe livrable contient, à titre facultatif, les contraintes relatives aux types d'informations codées **encoded-information-types-constraints**, les types de contenu livrables **deliverable-content-types**, la longueur de contenu maximale livrable **deliverable-maximum-content-length** et les étiquettes de sécurité livrables **deliverable-security-labels**. L'absence de valeurs pour une composante particulière indique qu'aucune restriction n'est imposée aux valeurs de cette composante dans cette classe livrable **deliverable-class**.

Le système MTS ne remet un message à l'utilisateur MTS que si le message répond à tous les critères au moins dans une classe livrable **deliverable-class** de l'ensemble enregistré.

En l'absence de cet argument, les classes livrables **deliverable-classes** restent inchangées.

8.4.1.1.1.3.1 Contraintes de types d'informations codées encoded-information-types-constraints

Cette composante indique les types d'informations codées **encoded-information-types** que le système MTS doit permettre de faire figurer dans les messages remis à l'utilisateur MTS, s'il y a lieu de soumettre ces éléments à des contraintes dans le cadre d'une classe livrable **deliverable-class**.

Cette composante comprend les types d'informations codées acceptables **acceptable-encoded-information-types**, inacceptables **unacceptable-encoded-information-types**, et exclusivement acceptables **exclusively-acceptable-encoded-information-types**, identifiant chacun une liste de types d'informations codées.

Un message qui ne comporte pas de liste de types d'informations codées **encoded-information-types** satisfera à toutes les contraintes relatives aux types d'informations codées **encoded-information-types-constraints**.

Si les types d'informations codées **encoded-information-types** du message à remettre sont incompatibles avec la contrainte **encoded-information-types-constraints**, le message ne satisfera pas aux contraintes de la classe livrable **deliverable-class**, et il n'est pas nécessaire d'examiner les autres critères de cette classe.

Le système MTS détermine si un message satisfait à la contrainte **encoded-information-types-constraints** de la classe **deliverable-class** en appliquant la procédure définie au § 14.3.4.4, point 7 (c).

Les types d'informations codées **encoded-information-types** contenus du message à remettre sont ceux qui figureraient dans le message une fois toutes les conversions éventuelles effectuées.

Selon les prescriptions locales ou les capacités offertes par l'environnement informatique de l'utilisateur, celui-ci peut choisir l'une des formules d'enregistrement suivantes:

a) permettre la remise de tous les messages quels que soient les types d'informations codées **encoded-information-types** qu'ils contiennent. Dans ce cas, on n'enregistrera aucune contrainte **encoded-information-types-constraints**;

b) permettre la remise de tous les messages sauf ceux qui contiennent au moins un des types figurant dans l'ensemble enregistré des types d'informations codées inacceptables. Dans ce cas, on n'enregistrera pas de types acceptables ou exclusivement acceptables;

NOTE 1 – Ce type d'enregistrement peut s'avérer utile par exemple pour un utilisateur de mémoire MS qui ne prend pas en charge les composantes vocales, afin d'éviter que des messages comportant des parties vocales importantes ne viennent consommer l'espace mémoire disponible affecté aux messages remis;

c) permettre la remise du message s'il contient au moins un des types acceptables. Dans ce cas, on n'enregistrera pas de types inacceptables ou exclusivement acceptables;

NOTE 2 – Un utilisateur du système de messagerie de personne à personne (IPMS) pourra demander par exemple que lui soient remis tous les messages contenant une partie de texte en caractères IA5, de manière à pouvoir évaluer l'importance des informations figurant dans les autres parties du message et décider ainsi de l'opportunité de rechercher d'autres moyens pour en traiter le reste.

d) imposer à tous les types d'informations codées du message d'avoir été enregistrés comme exclusivement acceptables; sinon, rejeter le message. Dans ce cas, on n'enregistrera pas de types acceptables ou inacceptables;

NOTE 3 – Ce type d'enregistrement peut s'avérer utile si l'agent utilisateur ne prend en charge par exemple qu'un petit nombre de types d'informations codées. Une telle situation est identique au service assuré par l'opération abstraite d'enregistrement Register-88.

e) permettre la remise du message si celui-ci ne contient pas de type d'information inacceptable, et contient au moins un type acceptable, ou ne contient que des types exclusivement acceptables. Dans ce cas, on pourra enregistrer des types acceptables, inacceptables et exclusivement acceptables.

NOTE 4 – Ce cas regroupe les situations b), c) et d). Un utilisateur du système de messagerie IPMS pourra utiliser par exemple cette combinaison pour s'assurer de ne jamais recevoir des textes à partie vocale, de toujours se faire remettre les textes en transfert de fichier (si tant est qu'ils ne contiennent pas de partie vocale) et, en l'absence de ces deux types d'éléments de texte, de ne se faire remettre que les messages contenant un ensemble donné de types d'informations codées.

Le système MTS renverra un message d'erreur si l'utilisateur MTS tente d'enregistrer un type d'information codée à la fois comme inacceptable et comme soit acceptable ou exclusivement acceptable.

Les types d'informations codées acceptables et exclusivement acceptables indiquent également les types d'informations codées éventuels dans lesquels la conversion peut éventuellement être effectuée.

En l'absence de cette composante, aucune contrainte n'est imposée aux types d'informations codées.

8.4.1.1.1.3.2 Types de contenu livrables deliverable-content-types

Cette composante indique les types de contenu que le système MTS permet de faire figurer dans les messages remis à l'utilisateur MTS, s'il y a lieu de soumettre ces éléments à des contraintes dans le cadre d'une classe livrable **deliverable-class**.

Si la longueur **content-length** du message à remettre excède la longueur maximale livrable **deliverable-maximum-content-length**, le message ne satisfait pas aux contraintes de la classe livrable et il n'est pas nécessaire d'examiner les autres critères de remise. Lors de son enregistrement, l'utilisateur MTS peut indiquer qu'il accepte le type de contenu non identifié **unidentified**.

En l'absence de cette composante, aucune contrainte n'est imposée aux types de contenu livrables.

8.4.1.1.1.3.3 Longueur maximale de contenu livrable deliverable-maximum-content-length

Cette composante indique la longueur maximale en octets du contenu que le système MTS permet de faire figurer dans les messages remis à l'utilisateur MTS, s'il y a lieu de soumettre cet élément à des contraintes dans le cadre d'une classe livrable **deliverable-class**.

Si la longueur **content-length** du message à remettre excède la longueur maximale de contenu livrable **deliverable-maximum-content-length**, le message ne satisfait pas aux contraintes de la classe livrable et il n'est pas nécessaire d'examiner les autres critères de remise.

En l'absence de cette composante, la longueur maximale de contenu livrable des messages ne doit faire l'objet d'aucune restriction.

8.4.1.1.1.3.4 Etiquettes de sécurité livrables deliverable-security-labels

Cette composante indique les étiquettes de sécurité de l'utilisateur MTS, s'il y a lieu de soumettre ces éléments à des contraintes dans le cadre d'une classe livrable **deliverable-class**.

Si les étiquettes de sécurité du message à remettre ne correspondent pas à celles qui sont indiquées par l'attribut **deliverable-security-labels**, le message ne satisfait pas aux contraintes de la classe livrable et il n'est pas nécessaire d'examiner les autres critères de remise.

Certaines politiques de sécurité peuvent n'autoriser la modification de l'attribut **deliverable-security-labels** que par un échange de la sorte sur une liaison sécurisée. Il est aussi possible de recourir à des moyens locaux sûrs pour modifier cet attribut.

En l'absence de cette composante, aucune contrainte n'est imposée aux messages en matière d'étiquettes de sécurité livrables.

8.4.1.1.1.4 Réacheminements assignés par le destinataire recipient-assigned-redirection

Si l'assignation des destinataires suppléants doit être modifiée, cet argument contient une liste ordonnée des noms OR des destinataires suppléants et, éventuellement, une ou plusieurs classes de réacheminement associées à chaque destinataire suppléant. Si cet argument est présent, sa valeur remplace complètement toute assignation précédente de destinataires suppléants. Il peut être produit par l'utilisateur MTS.

Si un ou plusieurs destinataires suppléants sont spécifiés, chaque message ou rapport destiné à l'utilisateur MTS doit être réacheminé vers le premier destinataire suppléant pour lequel le message répond aux critères dans l'une des classes de réacheminement associées à ce destinataire suppléant. Les messages ou rapports ne répondant aux critères d'aucune des classes de réacheminement d'un destinataire suppléant quelconque désigné par le destinataire doivent continuer à être remis à l'utilisateur MTS. L'ordre des destinataires suppléants est spécifié par l'utilisateur MTS. L'absence de toute classe de réacheminement indique un destinataire suppléant vers lequel tous les messages ou rapports doivent être réacheminés, à l'exception de ceux qui répondent aux critères de classes de réacheminement plus spécifiques associées à des destinataires suppléants le précédant dans la liste des suppléants. L'absence de destinataire suppléant assigné par le destinataire indique la remise à l'utilisateur MTS.

NOTE – Si la liste de réacheminements assignés par le destinataire comporte un nom sans classe de réacheminement, celui-ci doit figurer en dernier car un élément venant à la suite ne sera jamais utilisé.

La classe de réacheminement peut, à titre facultatif, contenir une longueur de contenu maximale et des ensembles de valeurs pour chacun des arguments suivants: types d'informations codées, type de contenu, restrictions relatives aux étiquettes de sécurité pouvant être remises et priorité. L'absence de valeurs pour un type particulier indique qu'aucune restriction n'est imposée aux valeurs de ce type dans cette classe de réacheminement. La classe de réacheminement indique également les types d'objet d'information MHS auxquels la classe de réacheminement s'applique, à savoir messages seulement, rapports seulement ou messages et rapports.

L'argument **recipient-assigned-alternate-recipient** (destinataire suppléant assigné par le destinataire) contient le nom **OR-name** du destinataire suppléant.

Si l'argument **recipient-assigned-redirections** (réacheminements assignés par le destinataire) contient un seul élément sans les sous-arguments Destinataire suppléant assigné par le destinataire et Classe de réacheminement, aucun destinataire suppléant assigné par le destinataire n'est enregistré.

Lorsque les arguments Réacheminements assignés par le destinataire et Classes pouvant être remises sont enregistrés ensemble, le réacheminement a priorité sur les restrictions de remise.

En l'absence de cet argument, les réacheminements éventuellement assignés par le destinataire restent inchangés.

8.4.1.1.1.5 Remise restreinte restricted-delivery

Cet argument indique, si la remise restreinte doit être modifiée, les noms OR d'autres utilisateurs MTS dont l'utilisateur MTS accepte (ou n'accepte pas) de recevoir les messages; il comprend une liste ordonnée de restrictions. Si l'argument Remise restreinte est présent, sa valeur remplace complètement toute valeur précédente. Il peut être produit par l'utilisateur MTS.

Le système MTS doit rejeter comme ne pouvant être remis tout message provenant d'un utilisateur MTS (ou ayant fait l'objet d'un réacheminement ou d'une extension de liste DL par cet utilisateur) et dont l'utilisateur MTS destinataire n'accepte pas la remise. Chaque restriction peut spécifier une source qui est autorisée ou non sous la forme d'un nom OR complet ou d'un nom OR schématique.

Si une ou plusieurs restrictions sont enregistrées, on compare les sources (expéditeur, chronologie de réacheminement, chronologie d'extension de liste DL) de chaque message à la liste ordonnée de restrictions jusqu'à l'apparition d'une correspondance. La comparaison s'arrête immédiatement dès qu'une correspondance avec une restriction apparaît et le message est remis ou non selon qu'il est autorisé ou non. S'il n'y a aucune restriction correspondante, le message est remis.

Les procédures permettant de déterminer les correspondances exactes et schématiques des noms OR sont spécifiées dans la Rec. UIT-T X.402 | ISO/CEI 10021-2.

L'utilisateur MTS peut se faire enregistrer pour recevoir tous les messages, ce qui correspond à l'état précédant tout enregistrement de remise restreinte, en spécifiant une seule restriction dans laquelle tous les types de source sont permis et le nom de source est omis.

Lorsque les arguments Remise restreinte et Réacheminements assignés par le destinataire sont enregistrés ensemble, le réacheminement a la priorité sur la remise restreinte.

En l'absence de cet argument, la remise restreinte reste inchangée.

8.4.1.1.1.6 Extraction d'enregistrements retrieve-registrations

Cet argument indique que les divers enregistrements demandés par l'utilisateur MTS seront renvoyés dans le résultat de l'opération abstraite d'enregistrement.

Le résultat renvoyé reflète l'état des informations enregistrées après le traitement de tous les autres arguments du Registre.

L'argument contient plusieurs éléments dont chacun, s'il est positionné, demande la valeur enregistrée de la classe d'informations correspondante.

En l'absence de cet argument, aucune information d'enregistrement n'est demandée.

8.4.1.1.1.7 Arguments de commande de remise par défaut default-delivery-control-arguments

Les arguments de commande de remise par défaut sont les mêmes que les arguments de l'opération abstraite de commande de remise; ils sont définis au § 8.3.1.3.1. A l'exception de l'argument Contexte de sécurité admissible, ils peuvent être produits par l'utilisateur MTS.

Les commandes par défaut sont enregistrées comme arguments de l'opération abstraite d'enregistrement. Elles sont effectives au début de l'établissement d'une association et le restent jusqu'à ce qu'elles soient supplantées par un appel de l'opération abstraite de commande de remise.

Les arguments de commande par défaut ne doivent pas autoriser de messages dont la remise est interdite par les valeurs enregistrées en vigueur de l'argument Types d'informations codées livrables, de l'argument Types de contenu livrables ou de l'argument Longueur de contenu maximale livrable.

8.4.1.1.2 Résultats

L'opération abstraite d'enregistrement renvoie un résultat vide sauf si un résultat d'extension est présent ou si l'argument Extraction d'enregistrements était présent dans la demande. Dans ce dernier cas, les enregistrements identifiés dans l'argument Extraction d'enregistrements sont renvoyés.

Les résultats sont identiques aux arguments de l'opération abstraite d'enregistrement énumérés dans le Tableau 23 (sauf que l'argument Extraction d'enregistrements est absent).

8.4.1.1.3 Erreurs abstraites abstract-errors

Le Tableau 24 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite d'enregistrement Register et identifie les articles dans lesquels elles sont définies.

Tableau 24 – Erreurs abstraites d'enregistrement *Register*

Erreur abstraite abstract-error	Paragraphe
Rejet d'enregistrement *register-rejected*	8.4.2.1
Erreur de rattachement distant *remote-bind-error*	8.2.2.10
Opération refusée *operation-refused*	8.3.2.5
Erreur de sécurité *security-error*	8.4.2.4

8.4.1.2 Modification des pouvoirs Change-credentials

Cette opération abstraite permet à l'utilisateur MTS de modifier les pouvoirs d'authentification simple **credentials** de l'utilisateur MTS consignés par le système MTS, ou à celui-ci de modifier ses pouvoirs consignés par l'utilisateur MTS.

Les pouvoirs d'authentification simple sont échangés au cours de l'établissement d'une association en vue de l'authentification mutuelle des identités du système MTS et de l'utilisateur MTS.

L'achèvement avec succès de l'opération abstraite signifie que les pouvoirs d'authentification simple ont été modifiés.

L'interruption de l'opération abstraite par une erreur abstraite indique que les pouvoirs n'ont pas été modifiés, soit parce que les anciens pouvoirs d'authentification simple étaient incorrectement spécifiés, soit parce que les nouveaux sont inacceptables.

8.4.1.2.1 Arguments

Le Tableau 25 énumère les arguments de l'opération abstraite de modification des pouvoirs Change-credentials, en qualifie la présence et identifie les articles où ils sont définis.

Tableau 25 – Arguments de l'opération abstraite de modification des pouvoirs Change-credentials

Argument	Présence	Paragraphe
Arguments de pouvoirs		
Anciens pouvoirs *old-credentials*	M	8.4.1.2.1.1
Nouveaux pouvoirs *new-credentials*	M	8.4.1.2.1.2

8.4.1.2.1.1 Anciens pouvoirs old-credentials

Cet argument contient les (anciens) pouvoirs en vigueur de l'appelant de l'opération abstraite tels qu'ils sont consignés par l'exécutant de l'opération abstraite. Il doit être produit par l'appelant de l'opération abstraite.

En cas d'utilisation d'une authentification simple, les pouvoirs comprennent un simple mot de passe **password** associé au nom d'utilisateur **user-name**, ou nom **MTA-name**, de l'appelant.

8.4.1.2.1.2 Nouveaux pouvoirs new-credentials

Cet argument contient les nouveaux pouvoirs proposés de l'appelant de l'opération abstraite, à consigner par l'exécutant de cette opération abstraite. Il doit être produit par l'appelant.

La politique de sécurité en vigueur peut imposer des restrictions sur le type des nouveaux pouvoirs **new-credentials**.

8.4.1.2.2 Résultats

L'opération abstraite de modification des pouvoirs **change-credentials** renvoie un résultat vide comme indication de succès.

8.4.1.2.3 Erreurs abstraites abstract-errors

Le Tableau 26 énumère les erreurs abstraites qui peuvent interrompre une opération abstraite de modification des pouvoirs Change-credentials et identifie pour chacune d'elles l'article où elle est décrite.

Tableau 26 – Erreurs abstraites de l'opération abstraite de modification des pouvoirs

Erreur abstraite abstract-error	Paragraphe
Nouveaux pouvoirs inacceptables *new-credentials-unacceptable*	8.4.2.2
Anciens pouvoirs incorrectement spécifiés *old-credentials-incorrectly-specified*	8.4.2.3
Erreur de rattachement distant *remote-bind-error*	8.2.2.10
Erreur de sécurité *security-error*	8.4.2.4

8.4.2 Erreurs abstraites abstract-errors

Le présent paragraphe contient la définition des erreurs abstraites d'accès d'administration administration-port suivantes:

a) rejet d'enregistrement *register-rejected*;

b) nouveaux pouvoirs inacceptables *new-credentials-unacceptable*;

c) anciens pouvoirs incorrectement spécifiés *old-credentials-incorrectly-specified*;

d) erreur de sécurité *security-error*.

8.4.2.1 Rejet d'enregistrement register-rejected

L'erreur abstraite de rejet d'enregistrement **register-rejected** signale que les paramètres demandés ne peuvent être enregistrés car l'un d'eux au moins est incorrectement spécifié.

L'erreur abstraite de rejet d'enregistrement n'a pas de paramètre.

8.4.2.2 Nouveaux pouvoirs inacceptables new-credentials-unacceptable

Cette erreur abstraite signale que les pouvoirs ne peuvent être modifiés, les nouveaux pouvoirs **new-credentials** étant inacceptables.

L'erreur abstraite de nouveaux pouvoirs inacceptables n'a pas de paramètre.

8.4.2.3 Anciens pouvoirs incorrectement spécifiés old-credentials-incorrectly-specified

Cette erreur abstraite signale que les pouvoirs ne peuvent être modifiés, les (anciens) pouvoirs en vigueur ayant été incorrectement spécifiés.

L'erreur abstraite d'anciens pouvoirs incorrectement spécifiés n'a pas de paramètre.

8.4.2.4 Erreur de sécurité security-error

L'erreur abstraite Erreur de sécurité Security-error signale que l'opération abstraite demandée n'a pas pu être fournie par le système MTS ou par l'utilisateur MTS car il enfreindrait la politique de sécurité en vigueur.

L'erreur abstraite Erreur de sécurité security-error a les paramètres suivants:

security-problem (problème de sécurité): un identificateur de la raison de l'infraction à la politique de sécurité.

Le paramètre problème de sécurité peut prendre une des valeurs suivantes pour l'opération abstraite d'enregistrement Register:

forbidden-user-security-label-register (enregistrement d'étiquette de sécurité interdit à l'utilisateur): l'utilisateur n'est pas autorisé à utiliser l'opération d'enregistrement pour modifier les étiquettes de sécurité;

invalid-security-label-update (mise à jour d'étiquette de sécurité non valide): la valeur proposée pour l'étiquette de sécurité pouvant être remise n'est pas acceptable par la politique de sécurité;

mandatory-parameter-absence (absence de paramètre obligatoire): un élément de sécurité obligatoire pour la conformité à la politique de sécurité en vigueur est absent;

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération d'enregistrement Register a échoué pour des raisons de sécurité;

redirection-prohibited (réacheminement interdit): la politique de sécurité interdit l'enregistrement des réacheminements assignés par le destinataire **recipient-assigned-redirections**;

refused-alternate-recipient-name (nom de destinataire suppléant refusé): le destinataire suppléant demandé n'est pas acceptable pour des raisons de sécurité;

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de services de sécurité): les services de sécurité demandés ne peuvent pas être offerts;

unauthorised-security-label-update (mise à jour d'étiquette de sécurité non autorisée): l'utilisateur n'est pas autorisé, par la politique de sécurité, à mettre à jour l'étiquette de sécurité pouvant être remise Deliverable-security-label;

unauthorised-user-name (nom d'utilisateur non autorisé): la nouvelle valeur proposée pour le nom **user-name** est inacceptable pour des raisons de sécurité.

Le paramètre problème de sécurité peut prendre une des valeurs suivantes pour l'opération de modification des pouvoirs Change-credentials:

operation-security-failure (échec de l'opération pour des raisons de sécurité): l'opération de modification des pouvoirs Change-credentials a échoué pour des raisons de sécurité;

security-policy-violation (politique de sécurité enfreinte): la politique de sécurité est enfreinte;

security-services-refusal (refus de services de sécurité): les services de sécurité demandés ne peuvent pas être fournis.

8.5 Types de paramètre commun

Le présent paragraphe définit un certain nombre de types de paramètre commun du service abstrait MTS.

8.5.1 Identificateur MTS-identifier

Des identificateurs **MTS-identifiers** sont affectés par le système MTS pour distinguer les messages et les envois-tests au niveau du service abstrait MTS et pour distinguer les messages, les envois-tests et les rapports à l'intérieur du système MTS.

L'identificateur **MTS-identifier** attribué à un message au point d'accès de dépôt (identificateur de dépôt de message **message-submission-identifier**) est identique à l'identificateur de message **message-identifier** correspondant au niveau d'un accès de transfert et à l'identificateur de remise de message **message-delivery-identifier** correspondant au niveau d'un point d'accès de remise. De manière analogue, l'identificateur **MTS-identifier** affecté à un envoi-test au niveau d'un accès de dépôt (identificateur de dépôt d'envoi-test **probe-submission-identifier**) est identique à l'identificateur d'envoi-test **probe-identifier** correspondant au niveau d'un accès de transfert. Des identificateurs **MTS-identifiers** sont également affectés aux rapports aux points d'accès de transfert (identificateur de rapport **report-identifier**).

Un identificateur **MTS-identifier** comprend:

un identificateur local **local-identifier** affecté par l'agent MTA, qui identifie sans ambiguïté l'événement auquel il se rapporte à l'intérieur du domaine de gestion MD;

l'identificateur global de domaine **global-domain-identifier** du domaine MD, qui assure que l'identificateur du système MTS est dépourvu d'ambiguïté dans tout le système MTS.

8.5.2 Identificateur global de domaine global-domain-identifier

Un identificateur global de domaine **global-domain-identifier** identifie sans ambiguïté un domaine de gestion MD à l'intérieur du système MHS.

Il sert à garantir la non-ambiguïté d'un identificateur **MTS-identifier** dans l'ensemble du système MTS et à identifier l'origine d'un élément d'information de trace **trace-information-element**.

Dans le cas d'un domaine de gestion d'administration ADMD, l'identificateur **global-domain-identifier** est formé du nom de pays **country-name** et du nom de domaine d'administration **administration-domain-name**.

Dans le cas d'un domaine de gestion privé PRMD, il est formé du nom de pays **country-name** et, facultativement, du nom de domaine d'administration **administration-domain-name** de l'ADMD associé, plus un identificateur de domaine privé **private-domain-identifier**. Cet identificateur **private-domain-identifier** est une identification unique du PRMD et peut être identique au nom de domaine privé **private-domain-name** du PRMD. Que cette identification se fasse relativement au pays désigné par le nom de pays **country-name** ou à l'ADMD associé relève de la compétence nationale. Dans le deuxième cas, le nom de ce domaine d'administration **administration-domain-name** doit être mentionné. Si le nom de domaine d'administration **administration-domain-name** est facultatif dans le service abstrait mais obligatoire dans la syntaxe abstraite et qu'aucune valeur n'est spécifiée, il doit être codé comme un espacement simple (voir § 18.3.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2).

NOTE – La distinction entre identificateur de domaine privé **private-domain-identifier** et nom de domaine privé **private-domain-name** a été retenue afin d'assurer la compatibilité amont avec la Rec. CCITT X.411 (version 1984). Ils seront souvent identiques.

8.5.3 Nom MTA-name

Un nom **MTA-name** est un identificateur d'agent MTA qui en assure l'identification univoque au sein du domaine MD auquel il appartient.

8.5.4 Heure (time)

Un paramètre d'heure **Time** est spécifié en temps universel coordonné (UTC, *coordinated universal time*) et peut comporter facultativement une indication de décalage horaire pour exprimer l'heure locale. La précision de l'heure est la seconde, ou la minute; elle est déterminée par le générateur du paramètre.

8.5.5 Nom OR-name

Un nom **OR-name** identifie l'expéditeur ou le destinataire d'un message selon les principes de dénomination et d'adressage décrits dans la Rec. UIT-T X.402 | ISO/CEI 10021-2.

A un point d'accès de dépôt, un nom **OR-name** comprend une adresse **OR-address** ou un nom d'annuaire **directory-name**, ou les deux (adresse ou nom d'annuaire **OR-address-and-or-directory-name**). A tous les autres types d'accès, un nom **OR-name** comprend une adresse **OR-address** et, facultativement, un nom d'annuaire **directory-name** (adresse OR nom d'annuaire facultatif **OR-address-and-optional-directory-name**). Un nom d'annuaire **directory-name** et une adresse **OR-address** peuvent désigner chacun un expéditeur ou un destinataire individuel, ou une liste DL.

Un nom d'annuaire **directory-name** sera conforme à la définition de la Rec. UIT-T X.501 | ISO/CEI 9594-2. Le système MTS n'utilise le nom d'annuaire **directory-name** que si l'adresse **OR-address** est absente ou non valide.

Une adresse **OR-address** comprend un certain nombre d'attributs normalisés **standard-attributes** choisis parmi ceux qui sont définis dans la Rec. UIT-T X.402 | ISO/CEI 10021-2, et, facultativement, un certain nombre d'attributs définis par le domaine MD auquel est abonné l'expéditeur ou le destinataire (attributs définis par le domaine **domain-defined-attributes**).

Dans la définition de syntaxe abstraite de l'article 9, les attributs normalisés sont représentés par les attributs normalisés intégrés **built-in-standard-attributes** et par les attributs normalisés étendus **extension-standard-attributes**, tandis que les attributs définis par le domaine sont représentés par les attributs intégrés définis par le domaine **built-in-domain-defined-attributes** et par les attributs étendus définis par le domaine **extension-domain-defined-attributes**.

Le § 18.5 de la Rec. UIT-T X.402 | ISO/CEI 10021-2 spécifie différentes formes d'adresses **OR-address**. On y indique également les attributs normalisés et les attributs définis par le domaine qui peuvent être conjointement utilisés pour constituer une adresse **OR-address** valide.

Le § 18.3 de la Rec. UIT-T X.402 | ISO/CEI 10021-2 spécifie les règles relatives aux jeux de caractères – numériques, imprimables télétex, et universels – qui peuvent servir à former la valeur d'un attribut normalisé particulier. Il définit donc les combinaisons valides des différentes variantes de cet attribut normalisé en syntaxe abstraite.

8.5.6 Types d'informations codées encoded-information-types

Les types d'informations codées **encoded-information-types** d'un message sont le ou les types d'information qui apparaissent dans son contenu. Il est possible de spécifier des types d'informations codées tant de base qu'à définition externe; en l'absence de spécification, les informations codées d'un message sont du type **unspecified** (non spécifié).

Les types d'informations codées de base sont ceux qui ont été initialement définis dans la Rec. CCITT X.411 (version 1984). Le type **unknown** (inconnu) est utilisé pour désigner un type d'informations codées qui, dans cette instance, n'est pas indiqué par un type d'informations codées à définition externe et n'appartient pas à un des types suivants: type **ia5-text** (téléimprimante) défini dans la Rec. CCITT T.50; type **g3-facsimile** (télécopie G3) défini dans les Recommandations T.4 et T.30 du CCITT; type **g4-class-1** (télécopie G4 classe 1) défini dans les Recommandations T.5, T.6, T.400 et T.503 du CCITT; type **teletex** défini dans les Recommandations F.200, T.61 et T.60 du CCITT; type **videotex** défini dans les Recommandations T.100 et T.101 du CCITT; type **simple-formattable-document (sfd)** (document formatable simple) et type **telex** définis dans la Rec. CCITT X.420 (version 1984); (les parties de corps SFD et TLX ne sont plus définies dans les Recommandations du CCITT); type **mixed-mode** (mode mixte) défini dans les Recommandations T.400 et T.501 du CCITT.

NOTE 1 – Le type d'informations codées inconnues **unknown** est prévu pour représenter les types d'informations codées à définition externe lors d'un repli sur un système de 1984 (il reste présent après une remise à niveau) et aussi pour représenter des types d'information particuliers lorsque aucun type d'informations codées à définition externe n'a été défini.

Les types d'informations codées à définition externe sont ceux qui ne correspondent pas à des types d'informations codées de base.

Dans la définition en syntaxe abstraite de l'article 9, les types d'informations codées **encoded-information-type** sont la réunion logique des types d'informations codées intégrés **built-in-encoded-information-types** et étendus **extended-encoded-information-type**. Ces derniers sont ceux auxquels des identificateurs d'objets ont été affectés par une autorité compétente. Ils comprennent à la fois les types d'informations codées normalisés et à définition privée.

Un type d'informations codées de base peut être représenté de manière équivalente soit par un bit dans le champ des types intégrés d'informations codées **built-in-encoded-information-types**, ou par un type étendu d'informations codées **extended-encoded-information-type**. L'Annexe A joue le rôle d'autorité d'enregistrement pour les identificateurs d'objets à utiliser pour l'enregistrement des types étendus d'informations codées **extended-encoded-information-type** faisant partie des types d'informations codées de base.

Un type d'informations codées à définition externe est toujours représenté par un type étendu d'informations codées **extended-encoded-information-type**. D'autres normes définissent des identificateurs d'objets qui peuvent être utilisés comme type étendu d'informations codées **extended-encoded-information-types**.

Des paramètres autres que de base **non-basic-parameters** sont définis pour les types d'informations codées de base **g3-facsimile** (télécopie G3) et **teletex** à seule fin de préserver la compatibilité amont avec la version 1984 de la Rec. CCITT X.411. Il est recommandé de définir et d'utiliser un type d'informations codées à définition externe chaque fois qu'il sera nécessaire de combiner un type d'informations codées de base et un jeu spécifique de paramètres autres que de base **non-basic-parameters**.

NOTE 2 – Les paramètres autres que de base **non-basic-parameters** seront vraisemblablement supprimés dans une version future de la présente Recommandation | Norme internationale.

Les paramètres autres que de base **non-basic-parameters** pour la télécopie G3 correspondent au champ d'informations de télécopie (FIF, *facsimile information field*) à trois ou quatre octets acheminé par le signal de commande numérique (DCS, *digital command signal*) défini dans la Rec. CCITT T.30. Ces paramètres sont: **two-dimensional** (bidimensionnel), **fine-resolution** (haute résolution), **unlimited-length** (longueur illimitée), **b4-length** (longueur B4), **a3-width** (largeur A3), **b4-width** (largeur B4) et **uncompressed** (sans compression).

Les paramètres autres que de base **non-basic-parameters** pour le **teletex** correspondent aux capacités autres que de base du terminal acheminées par la commande de début de document (CDS, *command document start*) définie dans la Rec. CCITT T.62. Les paramètres sont: **graphic-character-sets** (jeux de caractères graphiques): facultatif, **control-character-sets** (jeux de caractères de commande): facultatif, **page-formats** (formats de page): facultatif, **miscellaneous-terminal-capabilities** (capacités diverses de terminal): facultatif, et **private-use** (usage privé).

Les éventuels paramètres autres que de base **non-basic-parameters** représentent la réunion logique des paramètres non de base de chaque instance de type d'informations codées existant dans un contenu de message. Aussi, ce paramètre sert uniquement à indiquer s'il y a compatibilité de type d'informations codées ou si une conversion s'impose. Dans ce dernier cas, le contenu du message est examiné afin de déterminer lequel des paramètres autres que de base **non-basic-parameters** s'applique à chacune des instances de type d'informations codées.

8.5.7 Certificat (certificate)

Un certificat **certificate** peut servir à acheminer une copie vérifiée de la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) du sujet du certificat **certificate**.

Un certificat **certificate** contient un ou plusieurs éléments d'information de certification. Chaque instance d'informations de certification contient les paramètres suivants:

signature-algorithm-identifier: identificateur de l'algorithme **algorithm-identifier** que l'autorité de certification émettrice du certificat **certificate** a utilisé pour calculer la **signature**;

issuer: nom d'annuaire **directory-name** de l'autorité de certification qui a émis le certificat **certificate**;

validity: date et heure avant lesquelles il ne convient pas d'utiliser le certificat **certificate**, et date et heure après lesquelles on ne devrait pas se fier à ce certificat **certificate**;

subject: nom d'annuaire **directory-name** du sujet du certificat **certificate**;

subject-public-key: clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) du sujet;

algorithm: identificateurs d'algorithmes **algorithm-identifiers**, associés à une clé publique de sujet **subject-public-key**;

signature: version dispersée à chiffrement asymétrique des paramètres ci-dessus, calculée par l'autorité de certification qui a émis le certificat **certificate** en utilisant l'algorithme identifié par l'identificateur d'algorithme de signature **signature-algorithm-identifier** ainsi que la clé secrète de chiffrement asymétrique (*secret-asymmetric-encryption-key*) de l'autorité de certification.

Les certificats de version 3 seront utilisés lorsque l'expéditeur ou les destinataires ont plus d'un ensemble d'informations à certifier.

Les certificats de version 3 comportent une capacité d'extension des informations à signer dans le cadre du certificat. Les extensions de certificat normalisées sont définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Les différentes extensions normalisées peuvent être utilisées pour indiquer l'objet des informations contenues dans le certificat. Les extensions normalisées sont résumées ci-après:

- **Key and policy information**: Ces extensions de certificat et de liste CRL véhiculent des informations additionnelles sur les clés concernées, incluant des identificateurs de clés pour les clés de sujet et d'émetteur, des indicateurs sur l'usage prévu ou restreint de la clé, et des indicateurs de politique de certificat;
- **Subject and issuer attributes**: ces extensions de certificat et de liste CRL prennent en charge d'autres noms, de différents types, pour un sujet de certificat, un émetteur de certificat, ou un émetteur de liste CRL. Afin d'aider l'utilisateur du certificat à s'assurer que le sujet de certificat est une personne ou une entité particulière, ces extensions peuvent également véhiculer des informations additionnelles d'attribut concernant le sujet de certificat;
- **Certification path constraints**: Ces extensions de certificat permettent d'inclure des spécifications de contraintes dans des certificats d'autorité CA, c'est-à-dire des certificats pour des autorités CA émis par d'autres autorités CA, afin de faciliter le traitement automatique des trajets de certification lorsque plusieurs politiques de certificat sont concernées. Plusieurs politiques de certificat interviennent lorsque les politiques varient en fonction de différentes applications d'un environnement ou lorsque l'interfonctionnement avec des environnements externes intervient. Les contraintes peuvent restreindre les types de certificats pouvant être utilisés par l'autorité CA sujet ou pouvant intervenir ultérieurement dans le trajet de certification;
- **Basic CRL extensions**: Ces extensions de liste CRL permettent à une liste CRL d'inclure des indications sur la raison de la révocation, d'offrir la suspension provisoire d'un certificat, et d'inclure des numéros d'ordre de séquences d'émission de liste CRL afin de permettre aux utilisateurs de certificat de détecter des listes CRL manquantes dans une séquence d'un émetteur de listes CRL;
- **CRL distribution points** et **delta-CRL**: Ces extensions de certificat et de liste CRL permettent de séparer l'ensemble complet des informations de révocation d'une autorité CA dans des listes CRL distinctes et permettent de combiner les informations de révocation de plusieurs autorités CA dans une liste CRL. Ces extensions prennent également en charge l'utilisation de listes CRL partielles en indiquant seulement les modifications survenues depuis une émission précédente de liste CRL.

Les extensions des informations de clé et de politique **key and policy information** peuvent être utilisées pour indiquer quel certificat est associé à une signature numérique accompagnant le message, y compris le contrôle d'authentification d'origine de message **message origin-authentication-check**, et/ou les arguments de vérification d'intégrité de contenu **content-integrity-check** et de jeton de message **message-token** des destinataires individuels.

Si l'expéditeur et un destinataire de certificat **certificate** sont desservis par la même autorité d'authentification, le destinataire peut utiliser la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) de l'autorité de certification pour valider le certificat **certificate** et en tirer la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) (clé publique de sujet **subject-public-key**).

Si l'expéditeur et un destinataire de certificat **certificate** sont desservis par des autorités de certification différentes, le destinataire peut avoir besoin d'un trajet de certification de retour (*return-certification-path*) pour authentifier le certificat **certificate** de l'expéditeur. Pour cette raison, le certificat **certificate** peut comporter un trajet de certification **certification-path** associé.

Le trajet de certification **certification-path** peut comprendre un trajet de certification vers l'avant **forward-certification-path**, qui comporte le certificat de l'autorité de certification émettrice du certificat **certificate**, ainsi que les certificats de toutes les autorités de certification supérieures. Le trajet de certification vers l'avant **forward-certification-path** peut aussi comporter des certificats d'autres autorités de certification, avec certification croisée soit par l'autorité de certification qui a émis le certificat **certificate**, soit par des autorités de certification supérieures.

Un destinataire du certificat **certificate** peut compléter le trajet de certification (*certification-path*) de retour nécessaire entre le destinataire et l'expéditeur du certificat **certificate** en adjoignant son propre trajet de certification vers l'arrière (*reverse-certification-path*) au trajet de certification vers l'avant **forward-certification-path** fourni par l'expéditeur, en un point de confiance mutuelle. Le trajet de certification vers l'arrière (*reverse-certification-path*) comporte le certificat vers l'arrière de l'autorité de certification du destinataire du certificat **certificate**, ainsi que les certificats vers l'arrière de toutes les autorités de certification supérieures. Le trajet de certification vers l'arrière (*reverse-certification-path*) peut aussi comporter les certificats vers l'arrière d'autres autorités de certification, avec certification croisée par l'autorité de certification du destinataire du certificat **certificate** ou par l'une quelconque de ses autorités de certification supérieures.

Le trajet de certification de retour (*return-certification-path*) ainsi formé permet au destinataire du certificat **certificate** de valider chaque certificat, tour à tour, dans le trajet de certification de retour (*return-certification-path*), pour en tirer la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) de l'autorité de certification émettrice du certificat **certificate**. Le destinataire peut ensuite utiliser cette clé publique pour valider le certificat **certificate** et en tirer la clé publique de chiffrement asymétrique (*public-asymmetric-encryption-key*) de l'expéditeur (clé publique de sujet **subject-public-key**).

L'extension de certificat relative aux contraintes de trajet de certification **certification path constraints** permet d'inclure des spécifications de contraintes dans les certificats d'autorité CA et peut donc être utilisée pour indiquer toutes les restrictions ou tous les contrôles relatifs à l'utilisation du trajet de certification **certification-path**.

La forme d'un certificat **certificate** est définie dans la Rec. UIT-T X.509 | ISO/CEI 9594-8 comme certificat **certificates** de type données.

NOTE – L'utilisation du terme certificat **certificate** dans la présente spécification est différent de l'utilisation du même terme dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Le premier type peut, en option, contenir un trajet de certification alors que le dernier ne le peut pas. Dans la Rec. UIT-T X.509 | ISO/CEI 9594-8 le terme équivalent au terme certificat **certificate** de la présente spécification est certificats **certificates** avec la lettre "s".

Lorsqu'un certificat **certificate** doit être utilisé à une fin particulière, des certificats en version 3 (voir Rec. UIT-T X.509 | ISO/CEI 9594-8) doivent être utilisés pour indiquer l'objet des informations contenues dans le certificat.

Lorsqu'un certificat **certificate** est requis pour valider une signature numérique spécifique dans l'argument de vérification d'intégrité de contenu **content-integrity-check check** ou dans l'argument de jeton de message **message-token**, des certificats en version 3 doivent toujours être utilisés. L'extension de certificat appelée *champ de politiques de certification* **certification policies field** du certificat de l'expéditeur devra indiquer que le certificat (et le trajet de certification) doit être utilisé par le destinataire du message pour valider la signature numérique spécifique contenue dans l'argument de vérification d'intégrité de contenu **content-integrity-check,** ou dans l'argument de jeton de message **message-token** (voir § 8.2.1.1.1.28). Si toutes les signatures emploient le même algorithme et la même clé publique, il sera simplement nécessaire d'identifier une politique de sécurité dans l'argument de champ de politiques de certification, sinon des identificateurs d'objet distincts seront nécessaires pour chaque type de signature.

8.5.8 Jeton

Un jeton (**token**) peut servir à acheminer vers le destinataire du jeton des informations protégées relevant de la sécurité. Le jeton garantit tant l'authenticité de l'information publique relevant de la sécurité que la confidentialité et l'authenticité des informations secrètes relevant de la sécurité.

Le type du jeton est identifié par un identificateur de type **token-type-identifier**. Un seul type de jeton est actuellement défini dans la présente Définition de service: le jeton asymétrique **asymmetric-token**. D'autres types de jeton pourront être définis dans des addenda ou dans des versions futures de la présente Recommandation | Norme internationale; par exemple, des jetons fondés sur les techniques de chiffrement symétrique.

Un jeton asymétrique **asymmetric-token** contient les paramètres suivants:

signature-algorithm-identifier: identificateur **algorithm-identifier** pour l'algorithme utilisé par l'expéditeur de jeton afin de calculer la signature;

recipient-name: soit **l'adresse** ou le **nom d'annuaire OR-address-and-or-directory-name** du destinataire prévu du jeton **token** soit, en cas d'authentification renforcée du rattachement MTA-bind, le nom **MTA-name** et, facultativement, l'identificateur **global-domain-identifier** de l'agent MTA homologue (c'est-à-dire le demandé du jeton de rattachement); ou, en cas d'authentification forte dans un rattachement MTS, le nom **MTA name** et, facultativement, l'identificateur **global-domain-identifier** de l'agent MTA, où le jeton est produit par l'utilisateur du MTS, ou l'adresse **OR-address-and-optional-directory-name** de l'utilisateur du système MTS lorsque le jeton est produit par le système MTS; ou, en cas d'authentification renforcée dans un rattachement MS, l'adresse **OR-address-and-optional-directory-name** de l'utilisateur de la mémoire MS (lorsque le jeton est produit par la mémoire MS ou par l'utilisateur de celle-ci);

time: date et heure auxquelles le jeton a été produit;

signed-data: information publique touchant à la sécurité;

encryption-algorithm-identifier: identificateur **algorithm-identifier** pour l'algorithme utilisé par l'expéditeur du jeton pour calculer les données chiffrées **encrypted-data**;

encrypted-data: informations secrètes touchant à la sécurité chiffrée par l'expéditeur du jeton au moyen de l'algorithme identifié par l'identificateur d'algorithme de chiffrement et la clé publique de chiffrement asymétrique du destinataire prévu du jeton;

signature: une version dispersée à chiffrement de manière asymétrique, des paramètres ci-dessus, calculée par l'expéditeur du jeton au moyen de l'algorithme identifié par l'identificateur d'algorithme de signature **signature-algorithm-identifier** et la clé secrète de chiffrement asymétrique de l'expéditeur.

La forme d'un jeton est définie en détail dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Il est possible d'utiliser des algorithmes symétriques dans le cadre des jetons asymétriques sous réserve que:

l'algorithme (pour l'identificateur d'algorithme de signature **signature-algorithm-identifier** ou de chiffrement **encryption-algorithm-identifier**) soit utilisé pour identifier un algorithme de chiffrement symétrique enregistré;

la gestion des clés symétriques (les clés de distribution par exemple) soit effectuée extérieurement au système MTS.

NOTE 1 – Lorsque des algorithmes symétriques sont utilisés pour des données signées **signed-data**, l'authentification de l'origine du message, telle qu'elle est définie dans la Rec. UIT-T X.402 | ISO/CEI 10021-2, n'est pas assurée par le jeton. Celui-ci fournit seulement la preuve que le message a été signé par un détenteur de la clé symétrique (c'est-à-dire par un membre d'un groupe fermé d'utilisateurs).

NOTE 2 – Les identificateurs d'algorithmes de signature **signature-algorithm-identifier** et de chiffrement **encryption-algorithm-identifier** peuvent être définis indépendamment; il est donc possible d'utiliser simultanément des algorithmes symétriques et asymétriques dans un même jeton.

8.5.9 Etiquette de sécurité security-label

Les étiquettes de sécurité **security-labels** peuvent être utilisées pour associer les informations touchant à la sécurité à des objets situés à l'intérieur du système MTS.

Les étiquettes de sécurité peuvent être affectées à un objet conformément à la politique de sécurité en vigueur pour cet objet. Cette politique de sécurité peut également définir la manière d'utiliser les étiquettes de sécurité pour mettre en œuvre cette politique.

Dans le cadre de la présente Définition de service, les étiquettes de sécurité **security-labels** peuvent être associées à des messages, à des envois-tests et à des rapports (voir § 8.2.1.1.1.30), à des utilisateurs MTS (voir § 8.4.1.1.1.3.4), à des domaines de gestion MD, à des agents MTA et à des associations entre un utilisateur MTS et un domaine MD (ou un agent MTA) (voir § 8.1.1.1.1.4), ou entre plusieurs domaines MD (ou agents MTA) (voir § 12.1.1.1.1.3). Hors du cadre de la présente Définition de service, la politique de sécurité peut, par choix local ou par accord bilatéral, affecter des étiquettes de sécurité supplémentaires à d'autres objets à l'intérieur du système MTS (des trajets sécurisés par exemple).

Une étiquette de sécurité **security-label** comprend une série d'attributs de sécurité **security-attributes**. Ceux-ci peuvent inclure un identificateur de politique de sécurité **security-policy-identifier**, une classification de sécurité **security-classification**, une marque de secret **privacy-mark** et un ensemble de catégories de sécurité **security-categories**.

Un identificateur de politique de sécurité **security-policy-identifier** peut servir à identifier la politique de sécurité en vigueur à laquelle obéit l'étiquette de sécurité **security-label**.

S'il est présent, un attribut de classification de sécurité **security-classification** peut prendre l'une des valeurs d'une liste hiérarchique. La hiérarchie de base de classification de sécurité **security-classification** est définie dans la présente Définition de service, mais l'utilisation de ces valeurs est définie par la politique de sécurité en vigueur. Des valeurs additionnelles de classification de sécurité **security-classification** peuvent également être définies avec leur ordre hiérarchique par une politique de sécurité sur la base d'un choix local ou d'un accord bilatéral. La hiérarchie de base de la classification de sécurité **security-classification** est, par ordre ascendant: **unmarked** (non marqué), **unclassified** (non classifié), **restricted** (diffusion restreinte), **confidential** (confidentiel), **secret**, **top-secret**.

Une indication de marque de caractère privé **privacy-mark**, si elle est présente, est une chaîne imprimable. Son contenu peut être défini par une politique de sécurité qui peut définir la liste des valeurs à utiliser ou permettre à l'expéditeur de l'étiquette de sécurité d'en déterminer la valeur. Des exemples d'indication du caractère privé sont: '**IN CONFIDENCE**' et '**IN STRICTEST CONFIDENCE**'.

S'il est présent, l'ensemble de catégories de sécurité **security-categories** impose des limitations supplémentaires dans le contexte de la classification de sécurité **security-classification** ou de la marque de caractère privé **privacy-mark**, généralement sur la base de 'l'information nécessaire'. Les catégories de sécurité **security-categories** et leurs valeurs peuvent être définies par une politique de sécurité par choix local ou par accord bilatéral. Comme exemple de catégorie de sécurité **security-category** possible, on peut citer notamment des affixes à la classification de sécurité ou au caractère privé (par exemple, '**PERSONAL-**', '**STAFF-**', '**COMMERCIAL-**', etc.), les groupes fermés d'utilisateurs, les mots de code, etc.

8.5.10 Identificateur d'algorithme algorithm-identifier

Un identificateur d'algorithme **algorithm-identifier** identifie un algorithme et tous les paramètres **algorithm-parameters** qui lui sont nécessaires. Il définit également les règles de codage ASN.1 utilisées.

L'identificateur d'algorithme peut être pris dans un registre international d'algorithmes ou être défini par accord bilatéral.

8.5.11 Mot de passe password

Un mot de passe est composé d'une chaîne de caractères de l'alphabet international IA5 ou d'une chaîne d'octets.

Lorsqu'une chaîne d'octets est le résultat du codage dans un environnement 8 bits d'une chaîne de caractères de l'IA5, le choix entre les deux représentations, chaîne de caractères ou chaîne d'octets, sera considéré comme non significatif.

NOTE 1 – Cette règle d'équivalence n'empêche pas un mot de passe d'être une chaîne d'octets ne résultant pas du codage d'une quelconque chaîne de caractères IA5.

NOTE 2 – "Le codage dans un environnement 8 bits" signifie que le bit de poids le plus élevé dans chaque octet est un zéro et non un bit de parité; il s'agit du codage des chaînes de caractères IA5 mis en œuvre par les règles de codage de base de l'ASN.1. Un mot de passe en chaîne de caractères IA5 doit avoir le bit supérieur de chaque octet à zéro avant de l'inscrire comme valeur d'attribut de mot de passe d'utilisateur, attribut défini par la Rec. UIT-T X.520 | ISO/CEI 9594-6 (l'annuaire) comme étant une chaîne d'octets. La règle équivalente a été établie pour faciliter l'utilisation de cet attribut d'annuaire.

NOTE 3 – Lorsque les règles de codage de base de l'ASN.1 sont appliquées, il est possible de comparer deux mots de passe de la manière suivante: les octets de chaque mot de passe sont extraits de leurs codages BER (règles de codage de base de l'ASN.1), ces mots de passe étant d'origine ou résultant d'une première transformation. Les techniques d'extraction sont les mêmes qu'il s'agisse de chaînes de caractères IA5 ou de chaînes d'octets. Si les valeurs extraites sont identiques octet à octet, les deux mots de passe correspondent.

9 Définition de syntaxe abstraite du système de transfert de messages MTS

La syntaxe abstraite du service abstrait MTS est définie à la Figure 2. Les aspects du service abstrait MTS version 1988 qui diffèrent de la version de 1994 sont indiqués dans l'Annexe C.

La syntaxe abstraite du service abstrait MTS est définie à l'aide de la notation de syntaxe abstraite (ASN.1) 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, et à l'aide des conventions adoptées pour la définition du service abstrait décrites dans la Rec. UIT-T X.402 | ISO/CEI 10021-2, qui utilise la notation d'opérations distantes définie dans la Rec. UIT-T X.880 | ISO/CEI 13712-1.

La définition de la syntaxe abstraite du service abstrait MTS comporte les parties principales suivantes:

prologue: déclarations des exports provenant du module de service abstrait MTS et des imports à destination de ce module (voir la Figure 2, parties 1 et 2);

objets et points d'accès: définitions des objets du système MTS et de l'utilisateur MTS ainsi que de leurs points d'accès de dépôt (submission-ports), de remise (delivery-ports) et d'administration (administration-ports) (voir la Figure 2, parties 2 et 3);

rattachement MTS-bind et détachement MTS-unbind: définitions du rattachement MTS-bind et du détachement MTS-unbind utilisés pour établir et libérer des associations entre un utilisateur MTS et le système MTS (voir la Figure 2, parties 3 et 4);

point d'accès de dépôt: définitions des opérations abstraites de l'accès de dépôt submission-port: dépôt de message Message-submission, dépôt d'envoi-test Probe-submission, annulation de remise différée Cancel-deffered-delivery, et commande de dépôt Submission-control, ainsi que de leurs erreurs abstraites (voir la Figure 2, parties 4 à 7);

point d'accès de remise: définitions des opérations abstraites de l'accès de remise delivery-port: remise de message Message-delivery, remise de rapport Report-delivery et commande de remise Delivery-control, ainsi que de leurs erreurs abstraites (voir la Figure 2, parties 7 à 9);

accès d'administration: définition des opérations abstraites de l'accès d'administration administration-port: enregistrement Register et modification des pouvoirs Change-credentials ainsi que leurs erreurs abstraites (voir la Figure 2, parties 9 à 11);

enveloppe de dépôt de message: définition de l'enveloppe de dépôt de message message-submission-envelope (voir la Figure 2, partie 11);

enveloppe de dépôt d'envoi-test: définition de l'enveloppe de dépôt d'envoi-test probe-submission-envelope (voir la Figure 2, partie 12);

enveloppe de remise de message: définition de l'enveloppe de remise de message message-delivery-envelope (voir la Figure 2, parties 12 et 13);

enveloppe de remise de rapport: définition de l'enveloppe de remise de rapport report-delivery-envelope (voir la Figure 2, parties 13 et 14);

champs d'enveloppe: définition des champs d'enveloppe (voir la Figure 2, parties 14 à 16);

champs d'extension: définitions des champs d'extension (voir la Figure 2, parties 17 à 22);

types de paramètres communs: définitions des types de paramètres communs (voir la Figure 2, parties 23 à 29).

NOTE – Le module sous-entend un certain nombre de modifications au protocole P3 défini dans la Rec. CCITT X.411 (version 1984). Ces modifications sont mises en évidence par soulignement. En ce qui concerne les opérations de commande de remise et d'enregistrement, ces modifications ne sont indiquées qu'en Annexe C.

[NOTE – Le module applique des contraintes de taille aux types de données de longueur variable en utilisant l'extension de sous-typage SIZE de l'ASN.1. La violation d'une contrainte de taille constitue une violation du protocole.]

9.1 Mécanisme d'extension

Un mécanisme, indiqué à la Figure 2 (partie 17), permet de définir les extensions. En présence d'extensions, un ensemble paramétré d'objets informationnels indique les extensions définies dans la présente Définition de service qui peuvent être présentes, mais peut également inclure d'autres extensions définies par ailleurs (des extensions privées par exemple, ou des extensions définies dans des addenda ou de futures versions de la présente Recommandation | Norme internationale).

NOTE 1 – Seules les extensions définies dans la présente Recommandation | Norme internationale et dans des addenda ou de futures versions de celle-ci peuvent être identifiées par un type d'extension normalisée *standard-extension*. Toute autre extension définie par ailleurs est identifiée par un type d'extension privée *private-extension*.

Chaque type d'extension doit apparaître une fois au plus dans un ensemble de champs d'extension de type "ensemble de" (SET OF ExtensionField). Le même type d'extension peut apparaître en divers endroits du protocole. Cela s'applique à la fois aux extensions normalisées et aux extensions privées.

NOTE 2 – Les extensions par message et par destinataire sont regroupées au moment de la remise. Cela doit être pris en considération lorsqu'une extension privée est définie.

9.2 Mécanisme de criticité

Chaque champ d'extension **extension-field** défini dans la Figure 2 (parties 13 à 18) porte une indication de sa criticité pour les opérations de dépôt, de transfert et de remise. Les valeurs de criticité **criticality** peuvent être indiquées lors de la production du champ d'extension **extension-field**.

Le mécanisme de criticité est conçu pour prendre en charge la transparence contrôlée des fonctions étendues. Une fonction non critique peut être ignorée mais ne doit être supprimée que lors de la remise ou du déclassement d'un message (voir l'Annexe B de la Rec. UIT-T X.419 | ISO/CEI 10021-6), alors qu'une fonction critique doit être connue et correctement effectuée pour que la procédure normale puisse se poursuivre.

NOTE – Les messages comportant des fonctions critiques ou non critiques peuvent être rejetés lors de leur dépôt avec comme indication d'erreur de dépôt Element-of-service-not-subscribed (élément de service non souscrit) lorsque la fonction correspond à un élément de service auquel l'utilisateur ne s'est pas abonné, ou qui n'est pas disponible pour l'abonnement.

En général, ou bien l'entité chargée de l'opération abstraite traitera correctement l'argument d'une opération abstraite signalé comme critique pour le type d'accès, ou alors il y aura signalisation d'erreur de la manière appropriée. Le demandeur d'une opération abstraite traitera également correctement toute fonction indiquée comme critique pour le type d'accès.

Si l'opération abstraite est d'un type qui signale un éventuel résultat négatif, l'impossibilité de mener à bien une fonction critique sera signalée par l'envoi en retour de l'erreur abstraite de fonction critique non prise en charge unsupported-critical-function. Si l'opération abstraite n'est pas d'un type qui signale un éventuel résultat négatif, il faudra faire appel à une opération abstraite (un rapport par exemple) pour acheminer le résultat négatif de l'opération précédente (en utilisant par exemple dans le rapport le code de diagnostic de non-remise de fonction critique non prise en charge **unsupported-critical-function non-delivery-diagnostic-code**).

Une extension apparaissant dans le résultat d'une opération abstraite ne doit pas être marquée comme étant critique pour le type d'accès.

Si, dans une opération abstraite de dépôt de message (Message-submission) ou d'envoi-test (Probe-submision), une fonction porte la mention **critical-for-submission** (critique pour le dépôt) le système MTS mènera à bien les procédures définies pour une telle fonction, ou alors renverra une erreur abstraite de fonction critique non prise en charge unsupported-critical-function.

Si, dans le transfert d'un message ou d'un envoi-test, une fonction porte la mention **critical-for-transfer** (critique pour le transfert), l'agent MTA destinataire mènera à bien les procédures définies pour une telle fonction ou alors renverra un rapport de non-remise non-delivery-report portant le code de diagnostic de non-remise de fonction critique non prise en charge **unsupported-critical-function**. Si un agent MTA ne peut prendre en charge une fonction portant la mention **critical-for-transfer** (critique pour le transfert) dans un rapport, il ignorera ce rapport (une politique ou un accord local peuvent imposer le contrôle de cette action). Une extension portant l'indication **critical-for-transfer** (critique pour le transfert) et apparaissant en argument d'une opération de dépôt de message Message-submission ou d'envoi-test Probe-submission apparaîtra inchangée dans l'opération de transfert de message Message-transfer ou d'envoi-test Probe-transfer résultante au niveau d'un accès de transfert transfer-port.

Si une fonction porte la mention **critical-for-delivery** (critique pour la remise), l'agent MTA de remise mènera à bien les procédures définies pour une telle fonction ou alors ne remettra pas le message ou l'envoi-test et renverra un rapport de non-remise portant le code de diagnostic de non-remise de fonction critique non prise en charge **unsupported-critical-function**. Un utilisateur MTS destinataire effectuera correctement les procédures définies pour une fonction portant la mention **critical-for-delivery** (critique pour la remise) ou renverra une erreur abstraite de fonction critique non prise en charge **unsupported-critical-function**. Une extension portant la mention **critical-for-delivery** (critique pour la remise) et apparaissant en argument d'une opération de dépôt de message Message-submission ou d'envoi-test Probe-submission apparaîtra inchangée dans une opération transfert de message Message-transfer ou d'envoi-test Probe-transfer résultante au niveau d'un accès de transfert transfer-port. Une extension portant la mention **critical-for-delivery** (critique pour la remise) et apparaissant en argument d'une opération transfert de message Message-transfer ou d'envoi-test Probe-transfer apparaîtra inchangée dans toute opération de transfert de message Message-transfer ou d'envoi-test Probe-transfer au niveau d'un accès de transfert transfer-port.

Un agent MTA qui produit un rapport ne copiera pas de fonctions critiques non prises en charge à partir du sujet dans le rapport. Lorsqu'il produira un rapport, un agent MTA indiquera la criticité **criticality** (pour le transfert ou la remise) de toute fonction prise en charge copiée du sujet dans le rapport; la criticité d'une fonction dans un rapport peut être différente de sa criticité dans le sujet.

Si l'agent MTA ou l'utilisateur MTS ne peut exécuter correctement les procédures définies pour une fonction portant la mention **critical-for-delivery** (critique pour la remise) dans un rapport, celui-ci est supprimé.

Les procédures liées aux champs d'extension **extension-fields** et à leurs indications de criticité sont définies plus en détail à l'article 14.

La présente Définition de service définit, au moyen de la notation par classes d'objets informationnels de l'ASN.1, les valeurs recommandées des indications de criticité des champs d'extension **extension-fields** devant être fournies par l'expéditeur d'un message. L'expéditeur d'un message ou d'un envoi-test peut choisir, message par message, ou conformément à une politique locale (la politique de sécurité par exemple) de fixer l'indication de criticité d'un champ d'extension à une valeur plus forte ou plus faible par rapport à celle que définit la présente Définition de service.

Le Tableau 27 identifie toutes les possibilités offertes à un agent MTA pour toutes les combinaisons de criticité.

Tableau 27 – Actions de l'agent MTA selon la criticité

CRITICITÉ			DÉPÔT*	FACE AVANT*	REMISE*	REPLI +
Dépôt	**Transfert**	**Remise**	**§ 14.6**	**§ 14.3.2**	**§ 14.7**	
			A, R, E	A, R	A, R, D	A, D
		x	A, R, E	A, R	A, N	A, N
	x		A, R, E	A, N	A, R, D	A, N
	x	x	A, R, E	A, N	A, N	A, N
x			A, E	A, R	A, R, D	A, D
X		x	A, E	A, R	A, N	A, N
X	x		A, E	A, N	A, R, D	A, N
X	x	x	A, E	A, N	A, N	A, N

* Voir les Figures 6 et 7 pour ces étiquettes

\+ Voir l'Annexe B de la Rec. UIT-T X.419 | ISO/CEI 10021-6

x Bit de criticité activé

A Agit sur la sémantique

D Ignore l'extension et remet le message ou fonctionne en repli selon le cas

E Erreur de dépôt (pas d'abonnement à élément de service)

N Non-remise des messages ou des envois-tests, suppression des rapports (fonction critique non prise en charge)

R Remet ou relaye en transfert, selon le cas, en maintenant l'extension intacte, mais n'agit pas sur la sémantique

Figure 2 – Définition de syntaxe abstraite du service abstrait MTS (Début)

```
--      Figure 2 – Partie 1 de 29

MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
                     version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

--      Prologue

--      Exporte tout

IMPORTS

        -- Opérations distantes

        CONNECTION-PACKAGE, CONTRACT, ERROR, OPERATION, OPERATION-PACKAGE, ROS-OBJECT-CLASS
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
        remote-operations(4)
                        informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions { joint-iso-itu-t remote-operations(4)
                        useful-definitions(7) version1(0) }

        -- Service abstrait MTA

        internal-trace-information, trace-information
                ----
                FROM MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mta-abstract-service(2) version-1999(1) }

        -- Extension du service abstrait de mémoire MS

        forwarding-request
                ----
                FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
                        abstract-service(1) version-1999(1) }

        -- IPM Information Objects

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                        information-objects(2) version-1999(1) }

        -- Identificateurs d'objets

        id-att-physicalRendition-basic, id-cp-mts-connect, id-ct-mts-access,
        id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user, id-pt-administration,
        id-pt-delivery, id-pt-submission, id-tok-asymmetricToken
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }
```

```
--      Figure 2 - Partie 1 de 29

        -- Codes d'erreur et codes d'opérations

        err-control-violates-registration, err-deferred-delivery-cancellation-rejected,
        err-delivery-control-violated, err-element-of-service-not-subscribed,
        err-inconsistent-request, err-message-submission-identifier-invalid,
        err-new-credentials-unacceptable, err-old-credentials-incorrectly-specified,
        err-operation-refused, err-originator-invalid, err-recipient-improperly-specified,
        err-register-rejected, err-remote-bind-error, err-security-error,
        err-submission-control-violated, err-unsupported-critical-function,
        op-cancel-deferred-delivery, op-change-credentials, op-delivery-control,
        op-message-delivery, op-message-submission, op-probe-submission, op-register,
        op-report-delivery, op-submission-control
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                        mts-access-protocol(1) version-1999(1) }
```

```
--      Figure 2 – Partie 2 de 29
```

-- Définitions d'annuaire

```
        Name
                ----
                FROM InformationFramework { joint-iso-itu-t ds(5) module(1)
                        informationFramework(1) 3 }

        PresentationAddress
                ----
                FROM SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
                        selectedAttributeTypes(5) 3 }

        ALGORITHM, AlgorithmIdentifier, Certificates, ENCRYPTED { }, SIGNATURE { }, SIGNED { }
                ----
                FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
                        authenticationFramework(7) 3 }
```

-- Extensions de certificat

```
        CertificateAssertion
                ----
                FROM CertificateExtensions {joint-iso-itu-t ds(5) module(1)
                        certificateExtensions(26) 0 }
```

-- Limites supérieures

```
        ub-bit-options, ub-built-in-content-type, ub-built-in-encoded-information-types,
        ub-certificates, ub-common-name-length, ub-content-id-length, ub-content-length,
        ub-content-types, ub-country-name-alpha-length, ub-country-name-numeric-length,
        ub-deliverable-class, ub-diagnostic-codes, ub-dl-expansions,
        ub-domain-defined-attributes, ub-domain-defined-attribute-type-length,
        ub-domain-defined-attribute-value-length, ub-domain-name-length,
        ub-encoded-information-types, ub-extension-attributes, ub-extension-types,
        ub-e163-4-number-length, ub-e163-4-sub-address-length, ub-generation-qualifier-length,
        ub-given-name-length, ub-initials-length, ub-integer-options, ub-local-id-length,
        ub-mta-name-length, ub-mts-user-types, ub-numeric-user-id-length,
        ub-organization-name-length, ub-organizational-units,
        ub-organizational-unit-name-length, ub-orig-and-dl-expansions, ub-password-length,
        ub-pds-name-length, ub-pds-parameter-length, ub-pds-physical-address-lines,
        ub-postal-code-length, ub-privacy-mark-length, ub-queue-size, ub-reason-codes,
        ub-recipients, ub-recipient-number-for-advice-length, ub-redirections,
        ub-redirection-classes, ub-restrictions, ub-security-categories, ub-security-labels,
        ub-security-problems, ub-supplementary-info-length, ub-surname-length,
        ub-terminal-id-length, ub-tsap-id-length, ub-unformatted-address-length,
        ub-universal-generation-qualifier-length, ub-universal-given-name-length,
        ub-universal-initials-length, ub-universal-surname-length, ub-x121-address-length
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        upper-bounds(3) version-1999(1) };

        operationObject1 OPERATION ::= {LINKED  {operationObject2}}
        operationObject2 OPERATION ::= {LINKED  {operationObject3}}
        operationObject3 OPERATION ::= {LINKED  {operationObject4}}
        operationObject4 OPERATION ::= {LINKED  {...}}
```

-- Objets

```
MHS-OBJECT ::= ROS-OBJECT-CLASS

mts MHS-OBJECT ::= {
        INITIATES   { mts-forced-access-contract }
        RESPONDS    { mts-access-contract }
        ID          id-ot-mts }

mts-user MHS-OBJECT ::= {
        INITIATES   { mts-access-contract }
        RESPONDS    { mts-forced-access-contract }
        ID          id-ot-mts-user }
```

-- Contrats

```
mts-access-contract CONTRACT ::= {
        CONNECTION              mts-connect
        INITIATOR CONSUMER OF   { submission | delivery | administration }
        ID                      id-ct-mts-access }
```

```
--      Figure 2 - Partie 2 de 29

mts-forced-access-contract CONTRACT ::= {
       CONNECTION              mts-connect
       RESPONDER CONSUMER OF   { submission | delivery | administration }
       ID                      id-ct-mts-forced-access }
```

```
--      Figure 2 – Partie 3 de 29
```

-- Bloc de connexion

```
mts-connect CONNECTION-PACKAGE ::= {
       BIND        mts-bind
       UNBIND      mts-unbind
       ID          id-cp-mts-connect }
```

-- Accès

```
PORT ::= OPERATION-PACKAGE

submission PORT ::= {
       OPERATIONS      {operationObject1,...}  /* Cet ensemble d'objets informationnels doit
être extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle
que définie dans la Rec. UIT-T X.880) */
       CONSUMER INVOKES  {message-submission | probe-submission | cancel-deferred-
delivery,...} /* Cet ensemble d'objets informationnels doit être extensible parce qu'il est
utilisé par l'opération de réacheminement Forward {} (telle que définie dans la Rec. UIT-T
X.880) */
       SUPPLIER INVOKES  {submission-control,...} /* Cet ensemble d'objets informationnels
doit être extensible parce qu'il est utilisé par l'opération de réacheminement Forward {}
(telle que définie dans la Rec. UIT-T X.880) */
       ID                id-pt-submission}

delivery PORT ::= {
       OPERATIONS {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       CONSUMER INVOKES {delivery-control,...} /* Cet ensemble d'objets informationnels doit
être extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle
que définie dans la Rec. UIT-T X.880) */
       SUPPLIER INVOKES {message-delivery | report-delivery,...} /* Cet ensemble d'objets
informationnels doit être extensible parce qu'il est utilisé par l'opération de réacheminement
Forward {} (telle que définie dans la Rec. UIT-T X.880) */
       ID id-pt-delivery }

administration PORT ::= {
       OPERATIONS {change-credentials,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       CONSUMER INVOKES {register,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       SUPPLIER INVOKES {operationObject1,...} /* Cet ensemble d'objets informationnels doit
être extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle
que définie dans la Rec. UIT-T X.880) */
       ID id-pt-administration
```

-- Rattachement (MTS-bind) et détachement (MTS-unbind)

```
ABSTRACT-OPERATION ::= OPERATION

ABSTRACT-ERROR ::= ERROR

mts-bind ABSTRACT-OPERATION ::= {
       ARGUMENT    MTSBindArgument
       RESULT      MTSBindResult
       ERRORS      { mts-bind-error } }

MTSBindArgument ::=  SET {
       initiator-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       initiator-credentials [2] InitiatorCredentials,
       security-context      [3] SecurityContext OPTIONAL,
       ... ,
       extensions            [5] SET OF ExtensionField {{ MTSBindExtensions }} DEFAULT { } }

MTSBindExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées
```

```
--      Figure 2 - Partie 3 de 29

MTSBindResult ::= SET {
       responder-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       responder-credentials [2] ResponderCredentials,
       ... ,
       extensions            [3] SET OF ExtensionField {{ MTSBindResultExtensions }}
                                                                    DEFAULT { } }

MTSBindResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

mts-bind-error ABSTRACT-ERROR ::= {
       PARAMETER  INTEGER {
              busy                                  (0),
              authentication-error                  (2),
              unacceptable-dialogue-mode            (3),
              unacceptable-security-context         (4),
              inadequate-association-confidentiality (5) } (0..ub-integer-options) }

mts-unbind ABSTRACT-OPERATION ::= emptyUnbind
```

```
--      Figure 2 – Partie 4 de 29

--      Paramètres de commande d'association

ObjectName ::= CHOICE {
       user-agent ORAddressAndOptionalDirectoryName,
       mTA [0] MTAName,
       message-store [4] ORAddressAndOptionalDirectoryName}

MessagesWaiting ::= SET {
       urgent [0] DeliveryQueue,
       normal [1] DeliveryQueue,
       non-urgent [2] DeliveryQueue }

DeliveryQueue ::= SET {
       messages [0] INTEGER (0..ub-queue-size),
       octets [1] INTEGER (0..ub-content-length) OPTIONAL }

InitiatorCredentials ::= Credentials

ResponderCredentials ::= Credentials

Credentials ::= CHOICE {
       simple Password,
       strong [0] StrongCredentials,
       ... ,
       protected [1] ProtectedPassword }

Password ::= CHOICE {
       ia5-string IA5String (SIZE (0..ub-password-length)),
       octet-string OCTET STRING (SIZE (0..ub-password-length)) }

StrongCredentials ::= SET {
       bind-token [0] Token OPTIONAL,
       certificate [1] Certificates OPTIONAL,
       ... ,
       certificate-selector [2] CertificateAssertion OPTIONAL }

ProtectedPassword ::= SET {
       signature SIGNATURE { SET {
              password Password,
              time1 [0] UTCTime OPTIONAL,
              time2 [1] UTCTime OPTIONAL,
              random1 [2] BIT STRING OPTIONAL,
              random2 [3] BIT STRING OPTIONAL } },
       time1 [0] UTCTime OPTIONAL,
       time2 [1] UTCTime OPTIONAL,
       random1 [2] BIT STRING OPTIONAL,
       random2 [3] BIT STRING OPTIONAL }

SecurityContext ::= SET SIZE (1..ub-security-labels) OF SecurityLabel

--      Accès de dépôt

message-submission ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageSubmissionArgument
       RESULT            MessageSubmissionResult
       ERRORS            { submission-control-violated |
                           element-of-service-not-subscribed |
                           originator-invalid |
                           recipient-improperly-specified |
                           inconsistent-request |
                           security-error |
                           unsupported-critical-function |
                           remote-bind-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-submission }
```

```
--      Figure 2 - Partie 5 de 29

MessageSubmissionArgument ::= SEQUENCE {
       envelope MessageSubmissionEnvelope,
       content Content }

MessageSubmissionResult ::= SET {
       message-submission-identifier MessageSubmissionIdentifier,
       message-submission-time [0] MessageSubmissionTime,
       content-identifier ContentIdentifier OPTIONAL,
       extensions [1] SET OF ExtensionField {{ MessageSubmissionResultExtensions }}
                                                                    DEFAULT { } }

MessageSubmissionResultExtensions EXTENSION ::= {
       -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:
       originating-MTA-certificate |
       proof-of-submission |
       PrivateExtensions, ... }

probe-submission ABSTRACT-OPERATION ::= {
       ARGUMENT          ProbeSubmissionArgument
       RESULT            ProbeSubmissionResult
       ERRORS            { submission-control-violated |
                           element-of-service-not-subscribed |
                           originator-invalid |
                           recipient-improperly-specified |
                           inconsistent-request |
                           security-error |
                           unsupported-critical-function |
                           remote-bind-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-probe-submission }

ProbeSubmissionArgument ::= ProbeSubmissionEnvelope

ProbeSubmissionResult ::= SET {
       probe-submission-identifier ProbeSubmissionIdentifier,
       probe-submission-time [0] ProbeSubmissionTime,
       content-identifier ContentIdentifier OPTIONAL,
       extensions [1] SET OF ExtensionField {{ ProbeResultExtensions }} DEFAULT { } }

ProbeResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:

cancel-deferred-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          CancelDeferredDeliveryArgument
       RESULT            CancelDeferredDeliveryResult
       ERRORS            { deferred-delivery-cancellation-rejected |
                           message-submission-identifier-invalid |
                           remote-bind-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-cancel-deferred-delivery }

CancelDeferredDeliveryArgument ::= MessageSubmissionIdentifier

CancelDeferredDeliveryResult ::= NULL

submission-control ABSTRACT-OPERATION ::= {
       ARGUMENT          SubmissionControlArgument
       RESULT            SubmissionControlResult
       ERRORS            { security-error | remote-bind-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-submission-control }
```

```
--      Figure 2 - Partie 5 de 29

SubmissionControlArgument ::= SubmissionControls

SubmissionControlResult ::= Waiting
```

```
--      Figure 2 - Partie 6 de 29

submission-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-submission-control-violated }

element-of-service-not-subscribed ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-element-of-service-not-subscribed }

deferred-delivery-cancellation-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-deferred-delivery-cancellation-rejected }

originator-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-originator-invalid }

recipient-improperly-specified ABSTRACT-ERROR ::= {
       PARAMETER   ImproperlySpecifiedRecipients
       CODE        err-recipient-improperly-specified }

ImproperlySpecifiedRecipients ::= SEQUENCE SIZE (1..ub-recipients) OF RecipientName

message-submission-identifier-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-message-submission-identifier-invalid }

inconsistent-request ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-inconsistent-request }

security-error ABSTRACT-ERROR ::= {
       PARAMETER   SecurityProblem
       CODE        err-security-error }

SecurityProblem ::= INTEGER {
       assemby-instructions-conflict-with-security-services (0),
       authentication-problem (1),
       authentication-failure-on-subject-message (2),
       confidentiality-association-problem (3),
       decryption-failed (4),
       decryption-key-unobtainable (5),
       failure-of-proof-of-message (6),
       forbidden-user-security-label-register (7),
       incompatible-change-with-original-security-context (8),
       integrity-failure-on-subject-message (9),
       invalid-security-label (10),
       invalid-security-label-update (11),
       key-failure (12),
       mandatory-parameter-absence (13),
       operation-security-failure (14),
       redirection-prohibited (15),
       refused-alternate-recipient-name (16),
       repudiation-failure-of-message (17),
       responder-credentials-checking-problem (18),
       security-context-failure (19),
       security-context-problem (20),
       security-policy-violation (21),
       security-services-refusal (22),
       token-decryption-failed (23),
       token-error (24),
       unable-to-aggregate-security-labels (25),
       unauthorised-dl-name (26),
       unauthorised-entry-class (27),
       unauthorised-originally-intended-recipient-name (28),
       unauthorised-originator-name (29),
       unauthorised-recipient-name (30),
       unauthorised-security-label-update (31),
       unauthorised-user-name (32),
       unknown-security-label (33),
       unsupported-algorithm-identifier (34),
       unsupported-security-policy (35) } (0..ub-security-problems)

unsupported-critical-function ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-unsupported-critical-function }
```

```
--      Figure 2 - Partie 6 de 29

remote-bind-error ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-remote-bind-error }

--      Paramètres d'accès de dépôt

MessageSubmissionIdentifier ::= MTSIdentifier

MessageSubmissionTime ::= Time

ProbeSubmissionIdentifier ::= MTSIdentifier

ProbeSubmissionTime ::= Time

SubmissionControls ::= Controls (WITH COMPONENTS {
       ...,
       permissible-content-types ABSENT,
       permissible-encoded-information-types ABSENT })

Waiting ::= SET {
       waiting-operations [0] Operations DEFAULT { },
       waiting-messages [1] WaitingMessages DEFAULT { },
       waiting-content-types [2] SET SIZE (0..ub-content-types) OF ContentType DEFAULT { },
       waiting-encoded-information-types EncodedInformationTypes OPTIONAL }
```

```
--      Figure 2 - Partie 7 de 29

Operations ::= BIT STRING {
       probe-submission-or-report-delivery (0),
       message-submission-or-message-delivery (1) } (SIZE (0..ub-bit-options))
       -- en attente 'un', sinon 'zéro'

WaitingMessages ::= BIT STRING {
       long-content (0),
       low-priority (1),
       other-security-labels (2) } (SIZE (0..ub-bit-options))

--      Accès de remise

message-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageDeliveryArgument
       RESULT            MessageDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-delivery }

MessageDeliveryArgument ::= SEQUENCE {
       COMPONENTS OF MessageDeliveryEnvelope,
       content Content }

MessageDeliveryResult ::=  SET {
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] IMPLICIT ProofOfDelivery OPTIONAL,
       ... ,
       extensions [2] SET OF ExtensionField {{ MessageDeliveryResultExtensions }} DEFAULT { }}

MessageDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

report-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          ReportDeliveryArgument
       RESULT            ReportDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-report-delivery }

ReportDeliveryArgument ::= SET {
       COMPONENTS OF ReportDeliveryEnvelope,
       returned-content [0] Content OPTIONAL }

ReportDeliveryResult ::= CHOICE {
       empty-result NULL,
       ... ,
       extensions SET SIZE (1..MAX) OF ExtensionField {{ ReportDeliveryResultExtensions }} }

ReportDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

delivery-control ABSTRACT-OPERATION ::= {
       ARGUMENT          DeliveryControlArgument
       RESULT            DeliveryControlResult
       ERRORS            { control-violates-registration | security-error | operation-refused}
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-delivery-control }

DeliveryControlArgument ::= SET {
       COMPONENTS OF DeliveryControls,
       extensions [6] SET OF ExtensionField {{ DeliveryControlExtensions }} DEFAULT { } }
```

```
--      Figure 2 - Partie 7 de 29

DeliveryControlExtensions EXTENSION ::= { PrivateExtensions, ... }
        -- Peut contenir des extensions privées et de futures extensions normalisées
```

```
--      Figure 2 - Partie 8 de 29


DeliveryControlResult ::= SET {
       COMPONENTS OF Waiting,
       extensions [6] SET OF ExtensionField {{ DeliveryControlResultExtensions }} DEFAULT { }}

DeliveryControlResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

delivery-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-delivery-control-violated }

control-violates-registration ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-control-violates-registration }

operation-refused ABSTRACT-ERROR ::= {
       PARAMETER   RefusedOperation
       CODE        err-operation-refused }

RefusedOperation ::= SET {
       refused-argument CHOICE {
              built-in-argument [1] RefusedArgument,
              refused-extension EXTENSION.&id },
       refusal-reason [2] RefusalReason }

RefusedArgument ::= INTEGER {
       user-name (0),
       user-address (1),
       deliverable-content-types (2),
       deliverable-maximum-content-length (3),
       deliverable-encoded-information-types-constraints (4),
       deliverable-security-labels (5),
       recipient-assigned-redirections (6),
       restricted-delivery (7),
       retrieve-registrations (8), -- la valeur 9 est réservée à d'éventuelles extensions des arguments
                                   -- d'enregistrement (Register)

       restrict (10),
       permissible-operations (11),
       permissible-lowest-priority (12),
       permissible-encoded-information-types (13),
       permissible-content-types (14),
       permissible-maximum-content-length (15),
       permissible-security-context (16) } (0..ub-integer-options)

RefusalReason ::= INTEGER {
       facility-unavailable (0),
       facility-not-subscribed (1),
       parameter-unacceptable (2) } (0..ub-integer-options)

--      Accès de remise

RecipientCertificate ::= Certificates

ProofOfDelivery ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfDeliveryAlgorithmIdentifier,
       delivery-time MessageDeliveryTime,
       this-recipient-name ThisRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProofOfDeliveryAlgorithmIdentifier ::= AlgorithmIdentifier

DeliveryControls ::= Controls
```

```
--      Figure 2 – Partie 9 de 29


Controls ::= SET {
       restrict [0] BOOLEAN DEFAULT TRUE,
       -- mise à jour 'Vrai', suppression 'Faux'
       permissible-operations [1] Operations OPTIONAL,
       permissible-maximum-content-length [2] ContentLength OPTIONAL,
       permissible-lowest-priority Priority OPTIONAL,
       permissible-content-types [4] ContentTypes OPTIONAL,
       permissible-encoded-information-types PermissibleEncodedInformationTypes OPTIONAL,
       permissible-security-context [5] SecurityContext OPTIONAL }

--      Note – Les étiquettes [0], [1] et [2] ne sont modifiées que pour l'opération Register

PermissibleEncodedInformationTypes ::= EncodedInformationTypesConstraints

--      Accès d'administration

register ABSTRACT-OPERATION ::= {
       ARGUMENT          RegisterArgument
       RESULT            RegisterResult
       ERRORS            { register-rejected | remote-bind-error | operation-refused |
                           security-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }

RegisterArgument ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-class SET SIZE (1..ub-deliverable-class) OF DeliverableClass OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       redirections [3] Redirections OPTIONAL,
       restricted-delivery [4] RestrictedDelivery OPTIONAL,
       retrieve-registrations [5] RegistrationTypes OPTIONAL,
       extensions [6] SET OF ExtensionField {{ RegisterExtensions }} DEFAULT { } }

RegisterExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

RegisterResult ::= CHOICE {
       empty-result NULL,
       non-empty-result SET {
              registered-information [0] RegisterArgument (WITH COMPONENTS {
                     ... ,
                     retrieve-registrations ABSENT} ) OPTIONAL,
              extensions [1] SET OF ExtensionField {{ RegisterResultExtensions }} DEFAULT {}}}

RegisterResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

change-credentials ABSTRACT-OPERATION ::= {
       ARGUMENT          ChangeCredentialsArgument
       RESULT            NULL
       ERRORS            { new-credentials-unacceptable |
old-credentials-incorrectly-specified |
                           remote-bind-error | security-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward {} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-change-credentials }

ChangeCredentialsArgument ::= SET {
       old-credentials [0] Credentials (WITH COMPONENTS { simple }),
       new-credentials [1] Credentials (WITH COMPONENTS { simple }) }

register-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-register-rejected }
```

```
--      Figure 2 - Partie 9 de 29

new-credentials-unacceptable ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-new-credentials-unacceptable }
```

```
--      Figure 2 – Partie 10 de 29

old-credentials-incorrectly-specified ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-old-credentials-incorrectly-specified }

--      Paramètres d'accès d'administration

UserName ::= ORAddressAndOptionalDirectoryName

UserAddress ::= CHOICE {
       x121 [0] SEQUENCE {
              x121-address NumericString (SIZE (1..ub-x121-address-length)) OPTIONAL,
              tsap-id PrintableString (SIZE (1..ub-tsap-id-length)) OPTIONAL },
       presentation [1] PSAPAddress }

PSAPAddress ::= PresentationAddress

DeliverableClass ::= MessageClass (WITH COMPONENTS  {
       ... ,
       priority ABSENT,
       objects ABSENT,
       applies-only-to ABSENT })

DefaultDeliveryControls ::= Controls (WITH COMPONENTS {
       ... ,
       restrict ABSENT,
       permissible-security-context ABSENT })

Redirections ::= SEQUENCE SIZE (1..ub-redirections) OF RecipientRedirection

RecipientRedirection ::= SET {
       redirection-classes [0] SET SIZE (1..ub-redirection-classes) OF RedirectionClass
                                                                              OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                              OPTIONAL }

RedirectionClass ::=  MessageClass

MessageClass ::= SET {
       content-types [0] ContentTypes OPTIONAL,
       maximum-content-length [1] ContentLength OPTIONAL,
       encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,
       security-labels [3] SecurityContext OPTIONAL,
       priority [4] SET OF Priority OPTIONAL,
       objects [5] ENUMERATED { messages (0), reports (1), both (2), ... } DEFAULT both,
       applies-only-to [6] SEQUENCE OF Restriction OPTIONAL, -- Non pris en considération
                                                              -- dans le cas de rapports --
       extensions [7] SET OF ExtensionField {{ MessageClassExtensions }} DEFAULT { } }

EncodedInformationTypesConstraints ::= SEQUENCE {
       unacceptable-eits           [0] ExtendedEncodedInformationTypes OPTIONAL,
       acceptable-eits             [1] ExtendedEncodedInformationTypes OPTIONAL,
       exclusively-acceptable-eits [2] ExtendedEncodedInformationTypes OPTIONAL }

MessageClassExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- Peut contenir des extensions privées et de futures extensions normalisées

RecipientAssignedAlternateRecipient ::= ORAddressAndOrDirectoryName

RestrictedDelivery ::=  SEQUENCE SIZE (1..ub-restrictions) OF Restriction

Restriction ::= SET {
       permitted BOOLEAN DEFAULT TRUE,
       source-type BIT STRING {
              originated-by (0),
              redirected-by (1),
              dl-expanded-by (2) } DEFAULT { originated-by, redirected-by, dl-expanded-by },
       source-name ExactOrPattern OPTIONAL }

ExactOrPattern ::= CHOICE {
       exact-match [0] ORName,
       pattern-match [1] ORName }
```

-- Figure 2 – Partie 11 de 29

```
RegistrationTypes ::=  SEQUENCE {
       standard-parameters [0] BIT STRING {
              user-name (0),
              user-address (1),
              deliverable-class (2),
              default-delivery-controls (3),
              redirections (4),
              restricted-delivery (5) } OPTIONAL,
       extensions [1] SET OF EXTENSION.&id ({ RegisterExtensions }) OPTIONAL }

-- Enveloppe de dépôt de message

MessageSubmissionEnvelope ::= SET {
       COMPONENTS OF PerMessageSubmissionFields,
       per-recipient-fields [1] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientMessageSubmissionFields }

PerMessageSubmissionFields ::= SET {
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       priority Priority DEFAULT normal,
       per-message-indicators PerMessageIndicators DEFAULT { },
       deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerMessageSubmissionExtensions }} DEFAULT { } }

PerMessageSubmissionExtensions EXTENSION ::= {
       -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       latest-delivery-time |
       originator-return-address |
       originator-certificate |
       content-confidentiality-algorithm-identifier |
       message-origin-authentication-check |
       message-security-label |
       proof-of-submission-request |
       content-correlator |
       dl-exempted-recipients |
       certificate-selectors |
       multiple-originator-certificates |
       forwarding-request -- pour le service abstrait MS uniquement -- |
       PrivateExtensions, ... }

PerRecipientMessageSubmissionFields ::= SET {
       recipient-name RecipientName,
       originator-report-request [0] OriginatorReportRequest,
       explicit-conversion [1] ExplicitConversion OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerRecipientMessageSubmissionExtensions }}
              DEFAULT { } }

PerRecipientMessageSubmissionExtensions EXTENSION ::= {
       -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:
       originator-requested-alternate-recipient |
       requested-delivery-method |
       physical-forwarding-prohibited |
       physical-forwarding-address-request |
       physical-delivery-modes |
       registered-mail-type |
       recipient-number-for-advice |
       physical-rendition-attributes |
       physical-delivery-report-request |
       message-token |
       content-integrity-check |
       proof-of-delivery-request |
       certificate-selectors-override |
       recipient-certificate |
       IPMPerRecipientEnvelopeExtensions |
       PrivateExtensions, ... }
```

```
--      Figure 2 – Partie 12 de 29

--      Enveloppe de dépôt de message d'essai

ProbeSubmissionEnvelope ::= SET {
       COMPONENTS OF PerProbeSubmissionFields,
       per-recipient-fields [3] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientProbeSubmissionFields }

PerProbeSubmissionFields ::= SET {
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       content-length [0] ContentLength OPTIONAL,
       per-message-indicators PerMessageIndicators DEFAULT { },
       extensions [2] SET OF ExtensionField {{ PerProbeSubmissionExtensions }} DEFAULT { } }

PerProbeSubmissionExtensions EXTENSION ::= {
       -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       originator-certificate |
       message-security-label |
       content-correlator |
       probe-origin-authentication-check |
       PrivateExtensions, ... }

PerRecipientProbeSubmissionFields ::= SET {
       recipient-name RecipientName,
       originator-report-request [0] OriginatorReportRequest,
       explicit-conversion [1] ExplicitConversion OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerRecipientProbeSubmissionExtensions }}
                                                                              DEFAULT { } }

PerRecipientProbeSubmissionExtensions EXTENSION ::= {
       -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
       -- une seule instance au plus de chaque type d'extension:
       originator-requested-alternate-recipient |
       requested-delivery-method |
       physical-rendition-attributes |
       PrivateExtensions, ... }

--      Enveloppe de remise de message

MessageDeliveryEnvelope ::= SEQUENCE {
       message-delivery-identifier MessageDeliveryIdentifier,
       message-delivery-time MessageDeliveryTime,
       other-fields OtherMessageDeliveryFields }

OtherMessageDeliveryFields ::= SET {
       content-type DeliveredContentType,
       originator-name DeliveredOriginatorName,
       original-encoded-information-types [1] OriginalEncodedInformationTypes OPTIONAL,
       priority Priority DEFAULT normal,
       delivery-flags [2] DeliveryFlags OPTIONAL,
       other-recipient-names [3] OtherRecipientNames OPTIONAL,
       this-recipient-name [4] ThisRecipientName,
       originally-intended-recipient-name [5] OriginallyIntendedRecipientName OPTIONAL,
       converted-encoded-information-types [6] ConvertedEncodedInformationTypes OPTIONAL,
       message-submission-time [7] MessageSubmissionTime,
       content-identifier [8] ContentIdentifier OPTIONAL,
       extensions [9] SET OF ExtensionField {{ MessageDeliveryExtensions }} DEFAULT { } }
```

```
--      Figure 2 - Partie 13 de 29

MessageDeliveryExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        conversion-with-loss-prohibited |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        originator-return-address |
        physical-delivery-report-request |
        originator-certificate |
        message-token |
        content-confidentiality-algorithm-identifier |
        content-integrity-check |
        message-origin-authentication-check |
        message-security-label |
        proof-of-delivery-request |
        dl-exempted-recipients |
        certificate-selectors |
        certificate-selectors-override |
        multiple-originator-certificates |
        recipient-certificate |
        IPMPerRecipientEnvelopeExtensions |
        redirection-history |
        dl-expansion-history |
        trace-information |
        internal-trace-information |
        PrivateExtensions, ... }

--      Enveloppe de remise de rapport

ReportDeliveryEnvelope ::= SET {
        COMPONENTS OF PerReportDeliveryFields,
        per-recipient-fields SEQUENCE SIZE (1..ub-recipients) OF
                                                PerRecipientReportDeliveryFields }

PerReportDeliveryFields ::= SET {
        subject-submission-identifier SubjectSubmissionIdentifier,
        content-identifier ContentIdentifier OPTIONAL,
        content-type ContentType OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        extensions [1] SET OF ExtensionField {{ ReportDeliveryExtensions }} DEFAULT { } }

ReportDeliveryExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        message-security-label |
        content-correlator |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        trace-information |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

PerRecipientReportDeliveryFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        report-type [1] ReportType,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        originally-intended-recipient-name [2] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [3] SupplementaryInformation OPTIONAL,
        extensions [4] SET OF ExtensionField {{ PerRecipientReportDeliveryExtensions }}
                                                                        DEFAULT { } }

PerRecipientReportDeliveryExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }
```

```
--      Figure 2 – Partie 14 de 29

ReportType ::= CHOICE {
       delivery [0] DeliveryReport,
       non-delivery [1] NonDeliveryReport }

DeliveryReport ::= SET {
       message-delivery-time [0] MessageDeliveryTime,
       type-of-MTS-user [1] TypeOfMTSUser DEFAULT public }

NonDeliveryReport ::= SET {
       non-delivery-reason-code [0] NonDeliveryReasonCode,
       non-delivery-diagnostic-code [1] NonDeliveryDiagnosticCode OPTIONAL }

--      Champs d'enveloppe

OriginatorName ::= ORAddressAndOrDirectoryName

DeliveredOriginatorName ::= ORAddressAndOptionalDirectoryName

OriginalEncodedInformationTypes ::= EncodedInformationTypes

ContentTypes ::= SET SIZE (1..ub-content-types) OF ContentType

ContentType ::= CHOICE {
       built-in BuiltInContentType,
       extended ExtendedContentType }

BuiltInContentType ::= [APPLICATION 6] INTEGER {
       unidentified (0),
       external (1),                -- identifié par l'identificateur d'objet de contenu EXTERNAL
       interpersonal-messaging-1984 (2),
       interpersonal-messaging-1988 (22),
       edi-messaging (35),
       voice-messaging (40) } (0..ub-built-in-content-type)

ExtendedContentType ::= OBJECT IDENTIFIER

DeliveredContentType ::= CHOICE {
       built-in [0] BuiltInContentType,
       extended ExtendedContentType }

ContentIdentifier ::= [APPLICATION 10] PrintableString (SIZE (1..ub-content-id-length))

PerMessageIndicators ::= [APPLICATION 8] BIT STRING {
       disclosure-of-other-recipients (0), -- divulgation d'autres destinataires demandée 'un',
                                           -- divulgation d'autres destinataires interdite 'zéro';
                                           -- ignoré pour le dépôt de message d'essai
       implicit-conversion-prohibited (1), -- conversion implicite interdite 'un',
                                           -- conversion implicite autorisée 'zéro'
       alternate-recipient-allowed (2),            -- destinataire suppléant autorisé 'un',
                                           -- destinataire suppléant interdit 'zéro'
       content-return-request (3),         -- renvoi du contenu demandé 'un',
                                           -- renvoi du contenu non demandé 'zéro';
                                           -- ignoré pour le dépôt de message d'essai
       reserved (4),                       -- bit réservé par MOTIS 1986
       bit-5 (5),
       bit-6 (6),                          -- notification de type 1 : bit 5 'zéro' et bit 6 'un'
                                           -- notification de type 2 : bit 5 'un' et bit 6 'zéro'
                                           -- notification de type 3 : bit 5 'un' et bit 6 'un'
                                           -- le mappage entre les types de notification 1, 2, 3
                                           -- et les types de notification propres au contenu est défini
                                           -- dans les spécifications de contenu appropriées
       service-message (7)                 -- le contenu du message est relatif au service;
                                           -- il peut s'agir d'une notification relative à un message de
                                           -- service; il n'est utilisé que sur accord mutuel -- }
       (SIZE (0..ub-bit-options))

RecipientName ::= ORAddressAndOrDirectoryName
```

-- Figure 2 – Partie 15 de 29

```
OriginatorReportRequest ::= BIT STRING {
       report (3),
       non-delivery-report (4)
       -- un bit au plus sera égal à 'un':
       -- un bit de rapport à 'un' requiert un 'rapport';
       -- un bit de rapport de non-remise à 'un' requiert un 'rapport de non-remise';
       -- les deux bits à 'zéro' requièrent 'pas de rapport' -- } (SIZE (0..ub-bit-options))

ExplicitConversion ::= INTEGER {
       ia5-text-to-teletex (0),
       -- les valeurs de 1 à 7 ne sont plus définies
       ia5-text-to-g3-facsimile (8),
       ia5-text-to-g4-class-1 (9),
       ia5-text-to-videotex (10),
       teletex-to-ia5-text (11),
       teletex-to-g3-facsimile (12),
       teletex-to-g4-class-1 (13),
       teletex-to-videotex (14),
       -- la valeur 15 n'est  plus définie
       videotex-to-ia5-text (16),
       videotex-to-teletex (17) } (0..ub-integer-options)

DeferredDeliveryTime ::= Time

Priority ::= [APPLICATION 7] ENUMERATED {
       normal (0),
       non-urgent  (1),
       urgent (2) }

ContentLength ::= INTEGER (0..ub-content-length)

MessageDeliveryIdentifier ::= MTSIdentifier

MessageDeliveryTime ::= Time

DeliveryFlags ::= BIT STRING {
       implicit-conversion-prohibited (1)  -- conversion implicite interdite 'un',
                                           -- conversion implicite autorisée 'zéro' --  }
       (SIZE (0..ub-bit-options))

OtherRecipientNames ::= SEQUENCE SIZE (1..ub-recipients) OF OtherRecipientName

OtherRecipientName ::= ORAddressAndOptionalDirectoryName

ThisRecipientName ::= ORAddressAndOptionalDirectoryName

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName

ConvertedEncodedInformationTypes ::= EncodedInformationTypes

SubjectSubmissionIdentifier ::= MTSIdentifier

ActualRecipientName ::= ORAddressAndOrDirectoryName

TypeOfMTSUser ::= INTEGER {
       public (0),
       private (1),
       ms (2),
       dl (3),
       pdau (4),
       physical-recipient (5),
       other (6) } (0..ub-mts-user-types)
```

```
--      Figure 2 – Partie 16 de 29

NonDeliveryReasonCode ::= INTEGER {
        transfer-failure (0),
        unable-to-transfer (1),
        conversion-not-performed (2),
        physical-rendition-not-performed (3),
        physical-delivery-not-performed (4),
        restricted-delivery (5),
        directory-operation-unsuccessful (6),
        deferred-delivery-not-performed (7),
        transfer-failure-for-security-reason (8) } (0..ub-reason-codes)

NonDeliveryDiagnosticCode ::= INTEGER {
        unrecognised-OR-name (0),
        ambiguous-OR-name (1),
        mts-congestion (2),
        loop-detected (3),
        recipient-unavailable (4),
        maximum-time-expired (5),
        encoded-information-types-unsupported (6),
        content-too-long (7),
        conversion-impractical (8),
        implicit-conversion-prohibited (9),
        implicit-conversion-not-subscribed (10),
        invalid-arguments (11),
        content-syntax-error (12),
        size-constraint-violation (13),
        protocol-violation (14),
        content-type-not-supported (15),
        too-many-recipients (16),
        no-bilateral-agreement (17),
        unsupported-critical-function (18),
        conversion-with-loss-prohibited (19),
        line-too-long (20),
        page-split (21),
        pictorial-symbol-loss (22),
        punctuation-symbol-loss (23),
        alphabetic-character-loss (24),
        multiple-information-loss (25),
        recipient-reassignment-prohibited (26),
        redirection-loop-detected (27),
        dl-expansion-prohibited (28),
        no-dl-submit-permission (29),
        dl-expansion-failure (30),
        physical-rendition-attributes-not-supported (31),
        undeliverable-mail-physical-delivery-address-incorrect (32),
        undeliverable-mail-physical-delivery-office-incorrect-or-invalid (33),
        undeliverable-mail-physical-delivery-address-incomplete (34),
        undeliverable-mail-recipient-unknown (35),
        undeliverable-mail-recipient-deceased (36),
        undeliverable-mail-organization-expired (37),
        undeliverable-mail-recipient-refused-to-accept (38),
        undeliverable-mail-recipient-did-not-claim (39),
        undeliverable-mail-recipient-changed-address-permanently (40),
        undeliverable-mail-recipient-changed-address-temporarily (41),
        undeliverable-mail-recipient-changed-temporary-address (42),
        undeliverable-mail-new-address-unknown (43),
        undeliverable-mail-recipient-did-not-want-forwarding (44),
        undeliverable-mail-originator-prohibited-forwarding (45),
        secure-messaging-error (46),
        unable-to-downgrade (47),
        unable-to-complete-transfer (48),
        transfer-attempts-limit-reached (49),
        incorrect-notification-type (50),
        dl-expansion-prohibited-by-security-policy (51),
        forbidden-alternate-recipient (52),
        security-policy-violation (53),
        security-services-refusal (54),
        unauthorised-dl-member (55),
        unauthorised-dl-name (56),
        unauthorised-originally-intended-recipient-name (57),
        unauthorised-originator-name (58),
        unauthorised-recipient-name (59),
        unreliable-system (60),
        authentication-failure-on-subject-message (61),
```

-- **Figure 2 – Partie 16 de 29**

```
        decryption-failed (62),
        decryption-key-unobtainable (63),
        double-envelope-creation-failure (64),
        double-enveloping-message-restoring-failure (65),
        failure-of-proof-of-message (66),
        integrity-failure-on-subject-message (67),
        invalid-security-label (68),
        key-failure (69),
        mandatory-parameter-absence (70),
        operation-security-failure (71),
        repudiation-failure-of-message (72),
        security-context-failure (73),
        token-decryption-failed (74),
        token-error (75),
        unknown-security-label (76),
        unsupported-algorithm-identifier (77),
        unsupported-security-policy (78) } (0..ub-diagnostic-codes)

SupplementaryInformation ::= PrintableString (SIZE (1..ub-supplementary-info-length))
```

```
--      Figure 2 - Partie 17 de 29

--      Champs d'extension

EXTENSION ::= CLASS {
       &id ExtensionType UNIQUE,
       &Type OPTIONAL,
       &absent &Type OPTIONAL,
       &recommended Criticality DEFAULT { } }
WITH SYNTAX {
       [&Type [IF ABSENT &absent],]
       [RECOMMENDED CRITICALITY &recommended,]
       IDENTIFIED BY &id }

ExtensionType ::= CHOICE {
       standard-extension [0] INTEGER (0..ub-extension-types),
       private-extension [3] OBJECT IDENTIFIER }

Criticality ::= BIT STRING {
       for-submission (0),
       for-transfer (1),
       for-delivery (2) } (SIZE (0..ub-bit-options))     -- critique 'un', non critique 'zéro'

ExtensionField {EXTENSION:ChosenFrom} ::= SEQUENCE {
       type EXTENSION.&id({ChosenFrom}),
       criticality [1] Criticality DEFAULT { },
       value [2] EXTENSION.&Type({ChosenFrom} {@type}) DEFAULT NULL:NULL }

PrivateExtensions EXTENSION ::= {
       -- Toute valeur sera relayée et remise si elle n'est pas critique (voir Tableau 27)
       -- sauf les valeurs à la sémantique desquelles l'agent MTA obéit, et
       -- qui sont définies comme devant être supprimées si elles sont exécutées.
       -- Doit être IDENTIFIE par le type extension privée ExtensionType.private-extension -- ... }

recipient-reassignment-prohibited EXTENSION ::= {
       RecipientReassignmentProhibited IF ABSENT recipient-reassignment-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:1 }

RecipientReassignmentProhibited ::= ENUMERATED {
       recipient-reassignment-allowed (0),
       recipient-reassignment-prohibited (1) }

originator-requested-alternate-recipient EXTENSION ::= {
       OriginatorRequestedAlternateRecipient,
       RECOMMENDED CRITICALITY {for-submission},
       IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOrDirectoryName
-- Le destinataire suppléant désigné par l'expéditeur tel qu'il est ici défini diffère
-- du champ du même nom défini à la Figure 4 car, lors du dépôt, la présence de
-- l'adresse OR-address n'est pas indispensable alors qu'elle l'est lors du transfert.

dl-expansion-prohibited EXTENSION ::= {
       DLExpansionProhibited IF ABSENT dl-expansion-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:3 }

DLExpansionProhibited ::= ENUMERATED {
       dl-expansion-allowed (0),
       dl-expansion-prohibited (1) }

conversion-with-loss-prohibited EXTENSION ::= {
       ConversionWithLossProhibited IF ABSENT conversion-with-loss-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:4 }
```

```
--      Figure 2 - Partie 18 de 29

ConversionWithLossProhibited ::= ENUMERATED {
       conversion-with-loss-allowed (0),
       conversion-with-loss-prohibited (1) }

latest-delivery-time EXTENSION ::= {
       LatestDeliveryTime,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:5 }

LatestDeliveryTime ::= Time

requested-delivery-method EXTENSION ::= {
       RequestedDeliveryMethod IF ABSENT { any-delivery-method },
       IDENTIFIED BY standard-extension:6 }

RequestedDeliveryMethod ::= SEQUENCE OF INTEGER { -- tous différents, par ordre de
                                                  -- préférence décroissant
       any-delivery-method (0),
       mhs-delivery (1),
       physical-delivery (2),
       telex-delivery (3),
       teletex-delivery (4),
       g3-facsimile-delivery (5),
       g4-facsimile-delivery (6),
       ia5-terminal-delivery (7),
       videotex-delivery (8),
       telephone-delivery (9) } (0..ub-integer-options)

physical-forwarding-prohibited EXTENSION ::= {
       PhysicalForwardingProhibited IF ABSENT physical-forwarding-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:7 }

PhysicalForwardingProhibited ::= ENUMERATED {
       physical-forwarding-allowed (0),
       physical-forwarding-prohibited (1) }

physical-forwarding-address-request EXTENSION ::= {
       PhysicalForwardingAddressRequest IF ABSENT physical-forwarding-address-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:8 }

PhysicalForwardingAddressRequest ::= ENUMERATED {
       physical-forwarding-address-not-requested (0),
       physical-forwarding-address-requested (1) }

physical-delivery-modes EXTENSION ::= {
       PhysicalDeliveryModes IF ABSENT ordinary-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:9 }

PhysicalDeliveryModes ::= BIT STRING {
       ordinary-mail (0),
       special-delivery (1),
       express-mail (2),
       counter-collection (3),
       counter-collection-with-telephone-advice (4),
       counter-collection-with-telex-advice (5),
       counter-collection-with-teletex-advice (6),
       bureau-fax-delivery (7)
       -- les bits 0 à 6 s'excluent mutuellement
       -- le bit 7 est choisi indépendamment des autres -- } (SIZE (0..ub-bit-options))
```

```
--      Figure 2 - Partie 19 de 29

registered-mail-type EXTENSION ::= {
       RegisteredMailType IF ABSENT non-registered-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:10 }

RegisteredMailType ::= INTEGER {
       non-registered-mail (0),
       registered-mail (1),
       registered-mail-to-addressee-in-person (2) } (0..ub-integer-options)

recipient-number-for-advice EXTENSION ::= {
       RecipientNumberForAdvice,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:11 }

RecipientNumberForAdvice ::= TeletexString (SIZE (1..ub-recipient-number-for-advice-length))

physical-rendition-attributes EXTENSION ::= {
       PhysicalRenditionAttributes IF ABSENT id-att-physicalRendition-basic,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:12 }

PhysicalRenditionAttributes ::= OBJECT IDENTIFIER

originator-return-address EXTENSION ::= {
       OriginatorReturnAddress,
       IDENTIFIED BY standard-extension:13 }

OriginatorReturnAddress ::= ORAddress

physical-delivery-report-request EXTENSION ::= {
       PhysicalDeliveryReportRequest IF ABSENT return-of-undeliverable-mail-by-PDS,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:14 }

PhysicalDeliveryReportRequest ::= INTEGER {
       return-of-undeliverable-mail-by-PDS (0),
       return-of-notification-by-PDS (1),
       return-of-notification-by-MHS (2),
       return-of-notification-by-MHS-and-PDS (3) } (0..ub-integer-options)

originator-certificate EXTENSION ::= {
       OriginatorCertificate,
       IDENTIFIED BY standard-extension:15 }

OriginatorCertificate ::= Certificates

message-token EXTENSION ::= {
       MessageToken,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:16 }

MessageToken ::= Token

content-confidentiality-algorithm-identifier EXTENSION ::= {
       ContentConfidentialityAlgorithmIdentifier,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:17 }

ContentConfidentialityAlgorithmIdentifier ::= AlgorithmIdentifier
```

```
--      Figure 2 - Partie 20 de 29

content-integrity-check EXTENSION ::= {
       ContentIntegrityCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:18 }

ContentIntegrityCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ContentIntegrityAlgorithmIdentifier OPTIONAL,
       content Content } }

ContentIntegrityAlgorithmIdentifier ::= AlgorithmIdentifier

message-origin-authentication-check EXTENSION ::= {
       MessageOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:19 }

MessageOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier MessageOriginAuthenticationAlgorithmIdentifier,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

MessageOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

message-security-label EXTENSION ::= {
       MessageSecurityLabel,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:20 }

MessageSecurityLabel ::= SecurityLabel

proof-of-submission-request EXTENSION ::= {
       ProofOfSubmissionRequest IF ABSENT proof-of-submission-not-requested,
       RECOMMENDED CRITICALITY {for-submission},
       IDENTIFIED BY standard-extension:21 }

ProofOfSubmissionRequest ::= ENUMERATED {
       proof-of-submission-not-requested (0),
       proof-of-submission-requested (1) }

proof-of-delivery-request EXTENSION ::= {
       ProofOfDeliveryRequest IF ABSENT proof-of-delivery-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:22 }

ProofOfDeliveryRequest ::= ENUMERATED {
       proof-of-delivery-not-requested (0),
       proof-of-delivery-requested (1) }

content-correlator EXTENSION ::= {
       ContentCorrelator,
       IDENTIFIED BY standard-extension:23 }

ContentCorrelator ::= CHOICE {
       ia5text IA5String,
       octets  OCTET STRING }

probe-origin-authentication-check EXTENSION ::= {
       ProbeOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:24 }
```

```
--      Figure 2 – Partie 21 de 29

ProbeOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProbeOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProbeOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

redirection-history EXTENSION ::= {
       RedirectionHistory,
       IDENTIFIED BY standard-extension:25 }

RedirectionHistory ::= SEQUENCE SIZE (1..ub-redirections) OF Redirection

Redirection ::= SEQUENCE {
       intended-recipient-name IntendedRecipientName,
       redirection-reason RedirectionReason }

IntendedRecipientName ::= SEQUENCE {
       intended-recipient ORAddressAndOptionalDirectoryName,
       redirection-time Time }

RedirectionReason ::= ENUMERATED {
       recipient-assigned-alternate-recipient (0),
       originator-requested-alternate-recipient (1),
       recipient-MD-assigned-alternate-recipient (2),
       -- Il se peut que les valeurs suivantes ne soient pas prises en charge par les implémentations
       -- de versions antérieures à la présente Définition de service
       directory-look-up (3),
       alias (4),
       ... }

dl-expansion-history EXTENSION ::= {
       DLExpansionHistory,
       IDENTIFIED BY standard-extension:26 }

DLExpansionHistory ::= SEQUENCE SIZE (1..ub-dl-expansions) OF DLExpansion

DLExpansion ::= SEQUENCE {
       dl ORAddressAndOptionalDirectoryName,
       dl-expansion-time Time }

physical-forwarding-address EXTENSION ::= {
       PhysicalForwardingAddress,
       IDENTIFIED BY standard-extension:27 }

PhysicalForwardingAddress ::= ORAddressAndOptionalDirectoryName

recipient-certificate EXTENSION ::= {
       RecipientCertificate,
       IDENTIFIED BY standard-extension:28 }

proof-of-delivery EXTENSION ::= {
       ProofOfDelivery,
       IDENTIFIED BY standard-extension:29 }

originator-and-DL-expansion-history EXTENSION ::= {
       OriginatorAndDLExpansionHistory,
       IDENTIFIED BY standard-extension:30 }

OriginatorAndDLExpansionHistory ::= SEQUENCE SIZE (2..ub-orig-and-dl-expansions) OF
              OriginatorAndDLExpansion

OriginatorAndDLExpansion ::= SEQUENCE {
       originator-or-dl-name ORAddressAndOptionalDirectoryName,
       origination-or-expansion-time Time }
```

```
--      Figure 2 - Partie 22 de 29

reporting-DL-name EXTENSION ::= {
       ReportingDLName,
       IDENTIFIED BY standard-extension:31 }

ReportingDLName ::= ORAddressAndOptionalDirectoryName

reporting-MTA-certificate EXTENSION ::= {
       ReportingMTACertificate,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:32 }

ReportingMTACertificate ::= Certificates

report-origin-authentication-check EXTENSION ::= {
       ReportOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:33 }

ReportOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ReportOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL,
       per-recipient SEQUENCE SIZE (1..ub-recipients) OF PerRecipientReportFields } }

ReportOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

PerRecipientReportFields ::= SEQUENCE {
       actual-recipient-name ActualRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       report-type CHOICE {
              delivery [0] PerRecipientDeliveryReportFields,
              non-delivery [1] PerRecipientNonDeliveryReportFields } }

PerRecipientDeliveryReportFields ::= SEQUENCE {
       message-delivery-time MessageDeliveryTime,
       type-of-MTS-user TypeOfMTSUser,
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] ProofOfDelivery OPTIONAL }

PerRecipientNonDeliveryReportFields ::= SEQUENCE {
       non-delivery-reason-code NonDeliveryReasonCode,
       non-delivery-diagnostic-code NonDeliveryDiagnosticCode OPTIONAL }

originating-MTA-certificate EXTENSION ::= {
       OriginatingMTACertificate,
       IDENTIFIED BY standard-extension:34 }

OriginatingMTACertificate ::= Certificates

proof-of-submission EXTENSION ::= {
       ProofOfSubmission,
       IDENTIFIED BY standard-extension:35 }

ProofOfSubmission ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfSubmissionAlgorithmIdentifier,
       message-submission-envelope MessageSubmissionEnvelope,
       content Content,
       message-submission-identifier MessageSubmissionIdentifier,
       message-submission-time MessageSubmissionTime } }

ProofOfSubmissionAlgorithmIdentifier ::= AlgorithmIdentifier

reporting-MTA-name EXTENSION ::= {
       ReportingMTAName,
       IDENTIFIED BY standard-extension:39 }

ReportingMTAName ::= SEQUENCE {
       domain GlobalDomainIdentifier,
       mta-name MTAName,
       mta-directory-name [0] Name OPTIONAL }
```

```
--      Figure 2 – Partie 22 de 29

multiple-originator-certificates EXTENSION ::= {
       ExtendedCertificates,
       IDENTIFIED BY standard-extension:40 }

ExtendedCertificates ::= SET SIZE (1..ub-certificates) OF ExtendedCertificate

ExtendedCertificate ::= CHOICE {
       directory-entry [0] Name,  -- -- Nom d'une entrée de l'annuaire où le certificat peut être trouvé
       certificate [1] Certificates}

dl-exempted-recipients EXTENSION ::= {
       DLExemptedRecipients,
       IDENTIFIED BY standard-extension:42 }

DLExemptedRecipients ::= SET OF ORAddressAndOrDirectoryName

certificate-selectors EXTENSION ::= {
       CertificateSelectors,
       IDENTIFIED BY standard-extension:45 }

CertificateSelectors ::= SET {
       encryption-recipient           [0] CertificateAssertion OPTIONAL,
       encryption-originator          [1] CertificateAssertion OPTIONAL,
       content-integrity-check        [2] CertificateAssertion OPTIONAL,
       token-signature                [3] CertificateAssertion OPTIONAL,
       message-origin-authentication  [4] CertificateAssertion OPTIONAL}

certificate-selectors-override EXTENSION ::= {
       CertificateSelectors (WITH COMPONENTS{...,
              message-origin-authentication ABSENT}),
       IDENTIFIED BY standard-extension:46 }

-- Certaines extensions normalisées sont définies ailleurs:
--       36 (demandes de réacheminement) dans la Rec. UIT-T X.413 | ISO/CEI 10021-5;
--       37 (informations de suivi) et 38 (informations de suivi interne) dans la Figure 4;
--       41 (destinataires de copie muette), 43 (jetons de chiffrement de partie de corps), et
--       44 (jetons de contenu réacheminé) dans la Rec. UIT-T X.420 | ISO/CEI 10021-7
```

```
--      Figure 2 - Partie 23 de 29

--      Types communs de paramètres

Content ::= OCTET STRING            -- lorsque le type de contenu prend la valeur entière external (externe),
                                    -- la chaîne d'octets content prend la valeur du codage ASN.1
                                    -- du contenu externe; un contenu externe est un type
                                    -- de données externe EXTERNAL

MTSIdentifier ::= [APPLICATION 4] SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       local-identifier LocalIdentifier }

LocalIdentifier ::= IA5String (SIZE (1..ub-local-id-length))

GlobalDomainIdentifier ::= [APPLICATION 3] SEQUENCE {
       country-name CountryName,
       administration-domain-name AdministrationDomainName,
       private-domain-identifier PrivateDomainIdentifier OPTIONAL }

PrivateDomainIdentifier ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

MTAName ::= IA5String (SIZE (1..ub-mta-name-length))

Time ::= UTCTime

--      Noms OR

ORAddressAndOrDirectoryName ::= ORName

ORAddressAndOptionalDirectoryName ::= ORName

ORName ::= [APPLICATION 0] SEQUENCE {
       -- adresse -- COMPONENTS OF ORAddress,
       directory-name [0] Name OPTIONAL }

ORAddress ::= SEQUENCE {
       built-in-standard-attributes BuiltInStandardAttributes,
       built-in-domain-defined-attributes BuiltInDomainDefinedAttributes OPTIONAL,
       -- voir également les attributs définis du domaine télétex
       extension-attributes ExtensionAttributes OPTIONAL }

--      L'adresse OR est sémantiquement absente du nom OR si la séquence d'attributs normalisés intégrés est vide
--      et si les attributs intégrés définis par le domaine et les attributs d'extension sont tous deux omis.

--      Attributs normalisés intégrés

BuiltInStandardAttributes ::= SEQUENCE {
       country-name CountryName OPTIONAL,
       administration-domain-name AdministrationDomainName OPTIONAL,
       network-address [0] NetworkAddress OPTIONAL,
       -- voir également l'adresse réseau étendue
       terminal-identifier [1] TerminalIdentifier OPTIONAL,
       private-domain-name [2] PrivateDomainName OPTIONAL,
       organization-name [3] OrganizationName OPTIONAL,
       -- voir également le nom télétex d'organisation
       numeric-user-identifier [4] NumericUserIdentifier OPTIONAL,
       personal-name [5] PersonalName OPTIONAL,
       -- voir également le nom télétex personnel
       organizational-unit-names [6] OrganizationalUnitNames OPTIONAL
       -- voir également les noms télétex d'unités organisationnelles -- }
```

-- Figure 2 – Partie 24 de 29

```
CountryName ::= [APPLICATION 1] CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
       numeric NumericString (SIZE (0..ub-domain-name-length)),
       printable PrintableString (SIZE (0..ub-domain-name-length)) }

NetworkAddress ::= X121Address
-- voir également l'adresse réseau étendue

X121Address ::= NumericString (SIZE (1..ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE (1..ub-terminal-id-length))

PrivateDomainName ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

OrganizationName ::= PrintableString (SIZE (1..ub-organization-name-length))
-- voir également le nom télétex d'organisation

NumericUserIdentifier ::= NumericString (SIZE (1..ub-numeric-user-id-length))

PersonalName ::= SET {
       surname [0] PrintableString (SIZE (1..ub-surname-length)),
       given-name [1] PrintableString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] PrintableString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] PrintableString (SIZE (1..ub-generation-qualifier-length))
                                                                          OPTIONAL}
-- voir également le nom télétex personnel

OrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
                                                          OrganizationalUnitName
-- voir également les noms télétex d'unités organisationnelles

OrganizationalUnitName ::= PrintableString (SIZE (1..ub-organizational-unit-name-length))

-- Attributs intégrés définis par le domaine

BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
                                   BuiltInDomainDefinedAttribute

BuiltInDomainDefinedAttribute ::= SEQUENCE {
       type PrintableString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value PrintableString (SIZE (1..ub-domain-defined-attribute-value-length)) }

--      Attributs d'extension

ExtensionAttributes ::= SET SIZE (1..ub-extension-attributes) OF ExtensionAttribute

ExtensionAttribute ::= SEQUENCE {
       extension-attribute-type [0] EXTENSION-ATTRIBUTE.&id ({ExtensionAttributeTable}),
       extension-attribute-value [1] EXTENSION-ATTRIBUTE.&Type ({ExtensionAttributeTable}
                                                          {@extension-attribute-type}) }

EXTENSION-ATTRIBUTE ::= CLASS {
       &id    INTEGER (0..ub-extension-attributes) UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```

```
--      Figure 2 - Partie 25 de 29

ExtensionAttributeTable EXTENSION-ATTRIBUTE ::= {
       common-name |
       teletex-common-name |
       universal-common-name |
       teletex-organization-name |
       universal-organization-name |
       teletex-personal-name |
       universal-personal-name |
       teletex-organizational-unit-names |
       universal-organizational-unit-names |
       teletex-domain-defined-attributes |
       universal-domain-defined-attributes |
       pds-name |
       physical-delivery-country-name |
       postal-code |
       physical-delivery-office-name |
       universal-physical-delivery-office-name |
       physical-delivery-office-number |
       universal-physical-delivery-office-number |
       extension-OR-address-components |
       universal-extension-OR-address-components |
       physical-delivery-personal-name |
       universal-physical-delivery-personal-name |
       physical-delivery-organization-name |
       universal-physical-delivery-organization-name |
       extension-physical-delivery-address-components |
       universal-extension-physical-delivery-address-components |
       unformatted-postal-address |
       universal-unformatted-postal-address |
       street-address |
       universal-street-address |
       post-office-box-address |
       universal-post-office-box-address |
       poste-restante-address |
       universal-poste-restante-address |
       unique-postal-name |
       universal-unique-postal-name |
       local-postal-attributes |
       universal-local-postal-attributes |
       extended-network-address |
       terminal-type }

--      Attributs d'extension normalisés

common-name EXTENSION-ATTRIBUTE ::= {CommonName IDENTIFIED BY 1}

CommonName ::= PrintableString (SIZE (1..ub-common-name-length))

teletex-common-name EXTENSION-ATTRIBUTE ::= {TeletexCommonName IDENTIFIED BY 2}

TeletexCommonName ::= TeletexString (SIZE (1..ub-common-name-length))

universal-common-name EXTENSION-ATTRIBUTE ::= {UniversalCommonName IDENTIFIED BY 24}

UniversalCommonName ::= UniversalOrBMPString {ub-common-name-length}

teletex-organization-name EXTENSION-ATTRIBUTE ::= {TeletexOrganizationName IDENTIFIED BY 3}

TeletexOrganizationName ::= TeletexString (SIZE (1..ub-organization-name-length))

universal-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationName IDENTIFIED BY 25}

UniversalOrganizationName ::= UniversalOrBMPString {ub-organization-name-length}

teletex-personal-name EXTENSION-ATTRIBUTE ::= {TeletexPersonalName IDENTIFIED BY 4}

TeletexPersonalName ::= SET {
       surname [0] TeletexString (SIZE (1..ub-surname-length)),
       given-name [1] TeletexString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] TeletexString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] TeletexString (SIZE (1..ub-generation-qualifier-length))
                                                                              OPTIONAL }
```

```
--      Figure 2 – Partie 25 de 29

universal-personal-name EXTENSION-ATTRIBUTE ::= {UniversalPersonalName IDENTIFIED BY 26}

UniversalPersonalName ::= SET {
       surname [0] UniversalOrBMPString {ub-universal-surname-length},
       --      Si un langage est spécifié au sein d'un nom de famille, alors ce langage s'applique à chacun
       --      des composants optionnels suivants à moins que le composant ne spécifie un autre langage.
       given-name [1] UniversalOrBMPString {ub-universal-given-name-length} OPTIONAL,
       initials [2] UniversalOrBMPString {ub-universal-initials-length} OPTIONAL,
       generation-qualifier [3]
              UniversalOrBMPString {ub-universal-generation-qualifier-length} OPTIONAL }

teletex-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {TeletexOrganizationalUnitNames IDENTIFIED BY 5}

TeletexOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       TeletexOrganizationalUnitName

TeletexOrganizationalUnitName ::= TeletexString (SIZE (1..ub-organizational-unit-name-length))

universal-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationalUnitNames IDENTIFIED BY 27}

UniversalOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       UniversalOrganizationalUnitName
       --      Si un nom d'unité spécifie un langage, alors ce langage s'applique aux noms d'unité
       --      subordonnés à moins que le subordonné ne spécifie un autre langage.

UniversalOrganizationalUnitName ::= UniversalOrBMPString {ub-organizational-unit-name-length}

UniversalOrBMPString{INTEGER:ub-string-length} ::= SET {
       character-encoding CHOICE {
              two-octets BMPString (SIZE(1..ub-string-length)),
              four-octets UniversalString (SIZE(1..ub-string-length)) },
       iso-639-language-code PrintableString (SIZE(2|5)) OPTIONAL }

pds-name EXTENSION-ATTRIBUTE ::= {PDSName IDENTIFIED BY 7}

PDSName ::= PrintableString (SIZE (1..ub-pds-name-length))

physical-delivery-country-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryCountryName IDENTIFIED BY 8}
```

```
--      Figure 2 - Partie 26 de 29

PhysicalDeliveryCountryName ::= CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

postal-code EXTENSION-ATTRIBUTE ::= {PostalCode IDENTIFIED BY 9}

PostalCode ::= CHOICE {
       numeric-code NumericString (SIZE (1..ub-postal-code-length)),
       printable-code PrintableString (SIZE (1..ub-postal-code-length)) }

physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeName IDENTIFIED BY 10}

PhysicalDeliveryOfficeName ::= PDSParameter

universal-physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeName IDENTIFIED BY 29}

UniversalPhysicalDeliveryOfficeName ::= UniversalPDSParameter

physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeNumber IDENTIFIED BY 11}

PhysicalDeliveryOfficeNumber ::= PDSParameter

universal-physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeNumber IDENTIFIED BY 30}

UniversalPhysicalDeliveryOfficeNumber ::= UniversalPDSParameter

extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionORAddressComponents IDENTIFIED BY 12}

ExtensionORAddressComponents ::= PDSParameter

universal-extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionORAddressComponents IDENTIFIED BY 31}

UniversalExtensionORAddressComponents ::= UniversalPDSParameter

physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryPersonalName IDENTIFIED BY 13}

PhysicalDeliveryPersonalName ::= PDSParameter

universal-physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryPersonalName IDENTIFIED BY 32}

UniversalPhysicalDeliveryPersonalName ::= UniversalPDSParameter

physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOrganizationName IDENTIFIED BY 14}

PhysicalDeliveryOrganizationName ::= PDSParameter

universal-physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOrganizationName IDENTIFIED BY 33}

UniversalPhysicalDeliveryOrganizationName ::= UniversalPDSParameter

extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 15}

ExtensionPhysicalDeliveryAddressComponents ::= PDSParameter

universal-extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 34}

UniversalExtensionPhysicalDeliveryAddressComponents ::= UniversalPDSParameter
```

```
--      Figure 2 - Partie 26 de 29

unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UnformattedPostalAddress IDENTIFIED BY 16}

UnformattedPostalAddress ::= SET {
       printable-address SEQUENCE SIZE (1..ub-pds-physical-address-lines) OF
              PrintableString (SIZE (1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE (1..ub-unformatted-address-length)) OPTIONAL }

universal-unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UniversalUnformattedPostalAddress IDENTIFIED BY 35}

UniversalUnformattedPostalAddress ::= UniversalOrBMPString {ub-unformatted-address-length}

street-address EXTENSION-ATTRIBUTE ::= {StreetAddress IDENTIFIED BY 17}

StreetAddress ::= PDSParameter

universal-street-address EXTENSION-ATTRIBUTE ::= {UniversalStreetAddress IDENTIFIED BY 36}

UniversalStreetAddress ::= UniversalPDSParameter

post-office-box-address EXTENSION-ATTRIBUTE ::= {PostOfficeBoxAddress IDENTIFIED BY 18}

PostOfficeBoxAddress ::= PDSParameter

universal-post-office-box-address EXTENSION-ATTRIBUTE ::=
       {UniversalPostOfficeBoxAddress IDENTIFIED BY 37}

UniversalPostOfficeBoxAddress ::= UniversalPDSParameter

poste-restante-address EXTENSION-ATTRIBUTE ::= {PosteRestanteAddress IDENTIFIED BY 19}

PosteRestanteAddress ::= PDSParameter

universal-poste-restante-address EXTENSION-ATTRIBUTE ::=
       {UniversalPosteRestanteAddress IDENTIFIED BY 38}

UniversalPosteRestanteAddress ::= UniversalPDSParameter

unique-postal-name EXTENSION-ATTRIBUTE ::= {UniquePostalName IDENTIFIED BY 20}

UniquePostalName ::= PDSParameter

universal-unique-postal-name EXTENSION-ATTRIBUTE ::=
       {UniversalUniquePostalName IDENTIFIED BY 39}

UniversalUniquePostalName ::= UniversalPDSParameter

local-postal-attributes EXTENSION-ATTRIBUTE ::= {LocalPostalAttributes IDENTIFIED BY 21}

LocalPostalAttributes ::= PDSParameter
```

```
--      Figure 2 - Partie 27 de 29

universal-local-postal-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalLocalPostalAttributes IDENTIFIED BY 40}

UniversalLocalPostalAttributes ::= UniversalPDSParameter

PDSParameter ::= SET {
       printable-string PrintableString (SIZE(1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE(1..ub-pds-parameter-length)) OPTIONAL }

UniversalPDSParameter ::= UniversalOrBMPString {ub-pds-parameter-length}

extended-network-address EXTENSION-ATTRIBUTE ::= {ExtendedNetworkAddress IDENTIFIED BY 22}

ExtendedNetworkAddress ::= CHOICE {
       e163-4-address SEQUENCE {
              number [0] NumericString (SIZE (1..ub-e163-4-number-length)),
              sub-address [1] NumericString (SIZE (1..ub-e163-4-sub-address-length))
                                                                              OPTIONAL },
       psap-address [0] PresentationAddress }

terminal-type EXTENSION-ATTRIBUTE ::= {TerminalType IDENTIFIED BY 23}

TerminalType ::= INTEGER {
       telex (3),
       teletex (4),
       g3-facsimile (5),
       g4-facsimile (6),
       ia5-terminal (7),
       videotex (8) } (0..ub-integer-options)

--      Attributs d'extension définis par le domaine

teletex-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {TeletexDomainDefinedAttributes IDENTIFIED BY 6}

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       TeletexDomainDefinedAttribute

TeletexDomainDefinedAttribute ::= SEQUENCE {
       type TeletexString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value TeletexString (SIZE (1..ub-domain-defined-attribute-value-length)) }

universal-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalDomainDefinedAttributes IDENTIFIED BY 28}

UniversalDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       UniversalDomainDefinedAttribute

UniversalDomainDefinedAttribute ::= SEQUENCE {
       type UniversalOrBMPString {ub-domain-defined-attribute-type-length},
       value UniversalOrBMPString {ub-domain-defined-attribute-value-length} }

--      Types d'informations codées

EncodedInformationTypes ::= [APPLICATION 5] SET {
       built-in-encoded-information-types [0] BuiltInEncodedInformationTypes,
       -- paramètres autres que de base -- COMPONENTS OF NonBasicParameters,
       extended-encoded-information-types [4] ExtendedEncodedInformationTypes OPTIONAL }

--      Types intégrés d'informations codées

BuiltInEncodedInformationTypes ::= BIT STRING {
       unknown (0),
       ia5-text (2),
       g3-facsimile (3),
       g4-class-1 (4),
       teletex (5),
       videotex (6),
       voice (7),
       sfd (8),
       mixed-mode (9) } (SIZE (0..ub-built-in-encoded-information-types))
```

```
--      Figure 2 - Partie 27 de 29
```

-- Types d'extension d'informations codées

```
ExtendedEncodedInformationTypes ::= SET SIZE (1..ub-encoded-information-types) OF
              ExtendedEncodedInformationType

ExtendedEncodedInformationType ::= OBJECT IDENTIFIER
```

-- Paramètres autres que de base

```
NonBasicParameters ::= SET {
       g3-facsimile [1] G3FacsimileNonBasicParameters DEFAULT { },
       teletex [2] TeletexNonBasicParameters DEFAULT { } }
```

```
--      Figure 2 - Partie 28 de 29

G3FacsimileNonBasicParameters ::= BIT STRING {
       two-dimensional (8),                -- Défini dans la Rec. UIT-T T.30
       fine-resolution (9),                --
       unlimited-length (20),              -- Ces valeurs de bit sont choisies de telle sorte que,
       b4-length (21),                     -- lorsqu'elles sont codées à l'aide des règles de codage de base
       a3-width (22),                      -- de l'ASN.1, les octets qui en résultent ont les mêmes valeurs
       b4-width (23),                      -- que pour le codage de la Rec. T.30
       t6-coding (25),                     --
       uncompressed (30),                  -- Les bits zéro de traîne ne sont pas significatifs.
       width-middle-864-of-1728 (37),      -- Il est recommandé que les versions d'implémentation
       width-middle-1216-of-1728 (38),     -- ne codent pas plus de 32 bits, sauf si les bits de numéro
       resolution-type (44),               -- supérieur ne sont pas égaux à zéro.
       resolution-400x400 (45),
       resolution-300x300 (46),
       resolution-8x15 (47),
       edi (49),
       dtm (50),
       bft (51),
       mixed-mode (58),
       character-mode (60),
       twelve-bits (65),
       preferred-huffmann (66),
       full-colour (67),
       jpeg (68),
       processable-mode-26 (71) }

TeletexNonBasicParameters ::= SET {
       graphic-character-sets [0] TeletexString OPTIONAL,
       control-character-sets [1] TeletexString OPTIONAL,
       page-formats [2] OCTET STRING OPTIONAL,
       miscellaneous-terminal-capabilities [3] TeletexString OPTIONAL,
       private-use [4] OCTET STRING OPTIONAL      -- longueur maximale en octets de ub-teletex-private-use-
                                                     length --  }

       -- tel que le définit la Rec. CCITT T.62

--      Jeton

Token ::= SEQUENCE {
       token-type-identifier [0] TOKEN.&id ({TokensTable}),
       token [1] TOKEN.&Type ({TokensTable} {@token-type-identifier}) }

TOKEN ::= TYPE-IDENTIFIER

TokensTable TOKEN ::= { asymmetric-token, ... }

asymmetric-token TOKEN ::= {AsymmetricToken IDENTIFIED BY id-tok-asymmetricToken}

AsymmetricToken ::= SIGNED { SEQUENCE {
       signature-algorithm-identifier AlgorithmIdentifier,
       name CHOICE {
              recipient-name RecipientName,
              mta [3] SEQUENCE {
                     global-domain-identifier GlobalDomainIdentifier OPTIONAL,
                     mta-name MTAName } },
       time Time,
       signed-data [0] TokenData OPTIONAL,
       encryption-algorithm-identifier [1] AlgorithmIdentifier OPTIONAL,
       encrypted-data [2] ENCRYPTED { TokenData } OPTIONAL } }

TokenData ::= SEQUENCE {
       type [0] TOKEN-DATA.&id ({TokenDataTable}),
       value [1] TOKEN-DATA.&Type ({TokenDataTable} {@type}) }

TOKEN-DATA ::= CLASS {
       &id INTEGER UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```

```
--      Figure 2 - Partie 29 de 29

TokenDataTable TOKEN-DATA ::= {
       bind-token-signed-data |
       message-token-signed-data |
       message-token-encrypted-data |
       bind-token-encrypted-data, ... }

bind-token-signed-data TOKEN-DATA ::= {BindTokenSignedData IDENTIFIED BY 1}

BindTokenSignedData ::= RandomNumber

RandomNumber ::= BIT STRING

message-token-signed-data TOKEN-DATA ::= {MessageTokenSignedData IDENTIFIED BY 2}

MessageTokenSignedData ::= SEQUENCE {
       content-confidentiality-algorithm-identifier [0]
              ContentConfidentialityAlgorithmIdentifier OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       proof-of-delivery-request [3] ProofOfDeliveryRequest OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

message-token-encrypted-data TOKEN-DATA ::= {MessageTokenEncryptedData IDENTIFIED BY 3}

MessageTokenEncryptedData ::= SEQUENCE {
       content-confidentiality-key [0] EncryptionKey OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       content-integrity-key [3] EncryptionKey OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

EncryptionKey ::= BIT STRING

bind-token-encrypted-data TOKEN-DATA ::= {BindTokenEncryptedData IDENTIFIED BY 4}

BindTokenEncryptedData ::= EXTERNAL

--      Etiquette de sécurité

SecurityLabel ::= SET {
       security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
       security-classification SecurityClassification OPTIONAL,
       privacy-mark PrivacyMark OPTIONAL,
       security-categories SecurityCategories OPTIONAL }

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
       unmarked (0),
       unclassified (1),
       restricted (2),
       confidential (3),
       secret (4),
       top-secret (5) } (0..ub-integer-options)

PrivacyMark ::= PrintableString (SIZE (1..ub-privacy-mark-length))

SecurityCategories ::= SET SIZE (1..ub-security-categories) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
       type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
       value [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type}) }

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= { ... }

END     -- Fin du service abstrait MTS MTSAbstractService
```

Figure 2 – Définition de syntaxe abstraite du service abstrait MTS (fin)

SECTION 3 – SERVICE ABSTRAIT D'AGENT DE TRANSFERT DE MESSAGES

10 Modèle affiné de système de transfert de messages (MTS)

L'article 6 décrit le système MTS comme un objet, sans référence à sa structure interne. Le présent article affine le modèle du système de messagerie MTS, décrit les objets qui le composent ainsi que les accès qu'ils partagent.

La Figure 3 présente un modèle de système MTS avec sa structure interne.

Le système MTS comporte un ensemble d'objets d'agent de transfert de message (MTA), qui coopèrent pour constituer le système MTS et offrir le service abstrait MTS à ses utilisateurs. Ce sont les agents MTA qui assurent les fonctions actives du système MTS, à savoir le transfert des messages, des envois-tests et des rapports, la production des rapports et la conversion de contenu.

Les objets MTA ont également des accès, dont certains sont précisément ceux qui sont également visibles à la limite de l'objet MTS, c'est-à-dire les accès de présentation, de remise et d'administration. Toutefois, les agents MTA possèdent également un autre type d'accès – l'accès de transfert – qui assure la distribution du service abstrait MTS entre les agents MTA et n'est pas visible en limite de l'objet MTS.

Un accès de transfert permet à un agent MTA de transférer des messages, des envois-tests et des rapports vers un autre agent MTA. En général, un message, un envoi-test ou un rapport devra être transféré plusieurs fois entre différents agents MTA avant d'atteindre la destination prévue.

Si un message est adressé à plusieurs destinataires desservis par plusieurs agents MTA distincts, ce message doit être transféré dans le système MTS par plusieurs trajets différents. Du point de vue d'un agent MTA de transit, il y aura par exemple deux trajets différents menant à deux groupes distincts de destinataires. Au niveau d'un tel agent MTA, deux copies du message seront créées et transmises chacune à l'agent MTA suivant, sur son trajet respectif. Le processus de reproduction et d'aiguillage du message est répété jusqu'à ce que chaque copie ait atteint un agent MTA de destination finale, où le message pourra être remis à un ou plusieurs utilisateurs MTS destinataires.

Chaque agent MTA le long d'un trajet emprunté par un message est responsable de la remise ou du transfert du message à un sous-ensemble particulier de destinataires initialement spécifiés. D'autres agents MTA se chargent de la remise ou du transfert aux autres destinataires, à l'aide des copies de messages créées en chemin.

Les rapports de remise ou de non-remise d'un message à un ou plusieurs utilisateurs MTS destinataires sont produits par les agents MTA conformément à la demande de l'expéditeur du message et de l'agent MTA expéditeur. Un agent MTA peut produire un rapport de remise après avoir remis avec succès une copie d'un message à un utilisateur MTS destinataire. Il peut produire un rapport de non-remise après avoir constaté l'impossibilité de remettre une copie de message à un ou plusieurs destinataires, c'est-à-dire l'impossibilité pour lui de remettre directement le message à ces utilisateurs MTS destinataires, ou de le transférer vers un agent MTA adjacent qui se chargerait de la remise ou du transfert du message.

Par souci d'efficacité, un agent MTA peut produire un unique rapport multiple concernant plusieurs copies d'un même message multidestinataires dont il est responsable. Les rapports de remise et de non-remise peuvent être regroupés en un seul. Toutefois, pour que des rapports soient ainsi regroupés, il faut que le message ait subi, le cas échéant, la même conversion de contenu pour tous les destinataires concernés.

Les rapports concernant des copies d'un même message multidestinataires mais produits par des agents MTA différents ne sont pas regroupés par un agent MTA intermédiaire quelconque, mais restent distincts.

Le cas échéant, un agent MTA peut effectuer une conversion de contenu. Lorsque ni l'utilisateur MTS expéditeur, ni l'utilisateur MTS destinataire ne demandent ou n'interdisent la conversion, un agent MTA pourra effectuer une conversion implicite des types d'informations codées d'un message pour l'adapter aux types d'informations codées que le destinataire peut recevoir. L'expéditeur peut également demander explicitement la conversion de types d'informations codées spécifiques pour un utilisateur MTS destinataire particulier.

Les accès de dépôt, de remise et d'administration d'un agent MTA qui sont également visibles à la limite du MTS sont définis dans la section 2 de la présente Définition de service. Les articles suivants de la présente section définissent l'accès de transfert d'un agent MTA et les procédures suivies par les agents MTA pour assurer le fonctionnement réparti correct du système MTS.

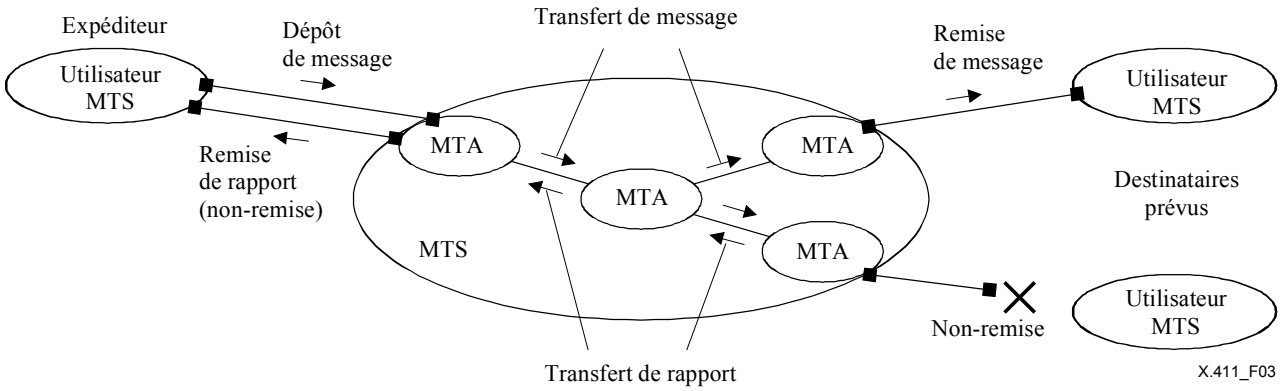


Figure 3 – Modèle affiné du système de transfert des messages

11 Aperçu général du service abstrait d'agent de transfert de messages MTA

La section 2 définit le service abstrait MTS fourni par les accès de dépôt, de remise et d'administration d'un agent MTA. Le présent article définit les opérations abstraites suivantes qui sont assurées par les accès de transfert des agents MTA:

Rattachement MTA-bind et détachement MTA-unbind

a) Rattachement;

b) Détachement.

Opérations abstraites de l'accès de transfert

c) Transfert de message;

d) Transfert d'envoi-test;

e) Transfert de rapport.

11.1 Rattachement MTA-bind et détachement MTA-unbind

Le rattachement **MTA-bind** permet à un agent MTA d'établir une association avec un autre agent MTA. Les opérations abstraites autres que le rattachement **MTA-bind** ne peuvent être invoquées que dans le contexte d'une association déjà établie.

Le détachement **MTA-unbind** permet au demandeur de l'association de libérer l'association qu'il a établie.

11.2 Opérations abstraites de l'accès de transfert

L'opération abstraite de transfert de message **Message-transfer** permet à un agent MTA de transférer un message vers un autre agent MTA.

L'opération abstraite de transfert d'envoi-test **Probe-transfer** permet à un agent MTA de transférer un envoi-test vers un autre agent MTA.

L'opération abstraite de transfert de rapport **Report-transfer** permet à un agent MTA de transférer un rapport vers un autre agent MTA.

12 Définition du service abstrait d'agent de transfert des messages MTA

Le service abstrait MTS est défini à l'article 8. Le présent article définit la sémantique des paramètres du service abstrait fourni par les accès de transfert **transfer-ports** des agents MTA.

Le § 12.1 définit le rattachement et le détachement. Le § 12.2 définit l'accès de transfert. Le § 12.3 définit certains types de paramètres communs.

La syntaxe abstraite du service abstrait MTA est définie à l'article 13.

12.1 Rattachement MTA-bind et détachement MTA-unbind

Le présent paragraphe définit les services abstraits utilisés pour établir et libérer les associations entre agents MTA.

12.1.1 Rattachement abstrait et détachement abstrait

Le présent paragraphe définit le rattachement abstrait et le détachement abstrait suivants:

a) rattachement;

b) détachement.

12.1.1.1 Rattachement MTA-bind

Le rattachement permet à un agent MTA d'établir une association avec un autre agent MTA.

Le rattachement établit les pouvoirs **credentials** des agents MTA qui interagiront, ainsi que le contexte d'application **application-context** et le contexte de sécurité **security-context** de l'association. Une association ne peut être libérée que par le demandeur de cette association (par appel à l'opération de détachement).

Les opérations abstraites autres que le rattachement ne peuvent être invoquées que dans le contexte d'une association établie.

L'achèvement avec succès du rattachement signifie l'établissement d'une association.

L'interruption du rattachement par une erreur de rattachement indique que l'association n'a pas été établie.

12.1.1.1.1 Arguments

Le Tableau 28 énumère les arguments du rattachement, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

Tableau 28 – Arguments du rattachement MTA-bind

Argument	Présence	Paragraphe
Arguments du rattachement		
Nom du demandeur *initiator-name*	O	12.1.1.1.1
Pouvoirs du demandeur *initiator-credentials*	O	12.1.1.1.2
Contexte de sécurité *security-context*	O	12.1.1.1.3

12.1.1.1.1.1 Nom du demandeur initiator-name

Cet argument contient le nom du demandeur de l'association. Il peut être produit par celui-ci.

Le nom est un nom **MTA-name**.

12.1.1.1.1.2 Pouvoirs du demandeur initiator-credentials

Cet argument contient les pouvoirs **credentials** du demandeur de l'association. Il peut être produit par le demandeur de l'association.

Les pouvoirs du demandeur **initiator-credentials** peuvent être utilisés par le demandé pour authentifier l'identité du demandeur (voir la Rec. UIT-T X.509 | ISO/CEI 9594-8).

Si seule l'authentification simple est proposée, les pouvoirs du demandeur **initiator-credentials** comportent un mot de passe **password** simple associé au nom de demandeur **initiator-name**.

S'il s'agit d'une authentification forte, les pouvoirs du demandeur **initiator-credentials** comportent un jeton de rattachement de demandeur **initiator-bind-token** et, à titre facultatif, un certificat de demandeur **initiator-certificate** ou sélecteur **certificate-selector**.

Le jeton **token** de rattachement de demandeur **initiator-bind-token** est produit par le demandeur de l'association. Si ce jeton est asymétrique **asymmetric-token**, les données signées **signed-data** comportent un nombre aléatoire **random-number**. Les données chiffrées **encrypted-data** d'un jeton asymétrique **asymmetric-token** peuvent être utilisées pour acheminer des renseignements relevant de la sécurité (par exemple, une ou plusieurs clés de chiffrement symétrique) qui servent à sécuriser l'association; elles peuvent également ne pas figurer dans le jeton de rattachement de demandeur **initiator-bind-token**.

Des algorithmes symétriques peuvent être utilisés dans le cadre des jetons asymétriques ci-dessus (voir § 8.5.8).

Le certificat du demandeur **initiator-certificate** est un certificat du demandeur de l'association, établi par une source sûre (une autorité de certification par exemple) et, facultativement, des certificats additionnels qui indiquent un trajet de certification pour le certificat du demandeur. Il peut être fourni par le demandeur de l'association, si le jeton de rattachement du demandeur **initiator-bind-token** est un jeton asymétrique **asymmetric-token**. Le certificat **initiator-certificate** doit contenir le nom **MTA-name** du demandeur dans un nom mta-name (voir § A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) de la composante *otherName* de son champ de variante nominative d'entité (voir § 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), à moins que la politique de sécurité n'indique une autre possibilité de rattachement du certificat à l'agent MTA demandeur. Le certificat du demandeur **initiator-certificate** peut être utilisé pour acheminer une copie certifiée de la clé publique de chiffrement asymétrique (clé publique sujet **subject-public-key**) du demandeur de l'association. La clé publique de chiffrement asymétrique du demandeur peut être utilisée par le demandé pour valider le jeton de rattachement du demandeur **initiator-bind-token** et pour calculer les données chiffrées **encrypted-data** contenues dans le jeton de rattachement du demandé **responder-bind-token**. Si le demandé est réputé disposer du certificat du demandeur ou y avoir accès (par l'annuaire par exemple), le certificat du demandeur pourra être omis et, lorsque le demandeur a plusieurs certificats, un sélecteur **certificate-selector** peut être fourni pour identifier le certificat au moyen de l'un des critères de sélection spécifiés pour la correspondance de certificat (voir § 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

12.1.1.1.1.3 Contexte de sécurité security-context

Cet argument indique le contexte de sécurité **security-context** dans lequel le demandeur de l'association propose de travailler. Il peut être établi par le demandeur de l'association.

Le contexte de sécurité **security-context** comporte une ou plusieurs étiquettes de sécurité **security-labels** qui définissent le caractère sensible des interactions qui peuvent se produire entre les agents MTA pendant la durée de l'association, conformément à la politique de sécurité en vigueur. Le contexte de sécurité **security-context** devra être autorisé par les étiquettes de sécurité **security-labels** associées aux domaines de gestion MD (agents MTA).

Si des contextes de sécurité ne sont pas déterminés entre les agents MTA, le niveau de sensibilité des interactions pouvant se produire entre les agents MTA pourra être laissé à la discrétion de l'appelant de l'opération abstraite.

12.1.1.1.2 Résultats

Le Tableau 29 énumère les résultats du rattachement, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

Tableau 29 – Résultats de rattachement MTA-bind

Résultat	Présence	Paragraphe
Résultats du rattachement		
Nom du demandé *responder-name*	O	12.1.1.1.2.1
Pouvoirs du demandé *responder-credentials*	O	12.1.1.1.2.2

12.1.1.1.2.1 Nom du demandé responder-name

Cet argument contient le nom du demandé de l'association. Il peut être produit par le demandé.

Le nom est un nom **MTA-name.**

12.1.1.1.2.2 Pouvoirs du demandé responder-credentials

Cet argument contient les pouvoirs du demandé de l'association. Il peut être produit par le demandé.

Les pouvoirs du demandé **responder-credentials** peuvent être utilisés par le demandeur pour authentifier l'identité du demandé (voir la Rec. UIT-T X.509 | ISO/CEI 9594-8).

S'il s'agit d'une authentification simple, les pouvoirs du demandé **responder-credentials** comportent un mot de passe **password** simple associé au nom du demandé **responder-name**.

S'il s'agit d'une authentification forte, les pouvoirs du demandé **responder-credentials** comportent un jeton de rattachement de demandé **responder-bind-token,** produit par le demandé de l'association et, facultativement, un certificat **responder-certificate** ou un sélecteur **certificate-selector**.

Ce jeton doit être du même type que le jeton de rattachement du demandeur **initiator-bind-token**. Si le jeton de rattachement de demandé **responder-bind-token** est asymétrique, les données signées **signed-data** comportent un nombre aléatoire **random-number** (qui peut être lié au nombre aléatoire fourni par le jeton de rattachement du demandeur). Les données chiffrées **encrypted-data** d'un jeton asymétrique peuvent être utilisées pour acheminer des renseignements relevant de la sécurité (une ou plusieurs clés de chiffrement symétrique par exemple) qui servent à sécuriser l'association; elles peuvent également ne pas figurer dans le jeton de rattachement de demandé.

Des algorithmes symétriques peuvent être utilisés dans le cadre du jeton asymétrique ci-dessus (voir § 8.5.8).

Le certificat **responder-certificate** est un **certificate** du demandeur de l'association produit par une source de confiance (par exemple l'autorité de certification) et, facultativement, des certificats additionnels indiquant un trajet de certification pour le certificat du demandeur. Il peut être fourni par le demandé de l'association si le jeton de rattachement du demandé **responder-bind-token** est un jeton **asymmetric-token**. Le certificat **responder-certificate** doit contenir le nom **MTA-name** du demandé dans un nom *mta-name* (voir § A.5.1 de la Rec. UIT-T X.402 | ISO/CEI 10021-2) de la composante *otherName* de son champ de variante nominative d'entité (voir § 12.3.2.1 de la Rec. UIT-T X.509 | ISO/CEI 9594-8), à moins que la politique de sécurité ne fournisse une autre possibilité de rattachement du certificat à l'agent MTA demandé. Le certificat **responder-certificate** peut être utilisé pour acheminer une copie vérifiée de la clé publique de chiffrement asymétrique (**subject-public-key**) du demandé de l'association. Cette clé peut être utilisée par le demandeur pour valider le jeton **responder-bind-token**. Si le demandeur est réputé avoir le **certificate** ou y avoir accès (via l'annuaire), le certificat **responder-certificate** peut être omis et, si le demandé a plusieurs certificats, un sélecteur **certificate-selector** peut être fourni pour identifier le certificat au moyen de l'un des critères de sélection spécifiés pour la correspondance de certificat (voir § 12.7.2 de la Rec. UIT-T X.509 | ISO/CEI 9594-8).

12.1.1.1.3 Erreurs de rattachement bind-errors

Les erreurs de rattachement qui peuvent interrompre le rattachement **MTA-bind** sont définies au § 12.1.2.

12.1.1.2 Détachement MTA-unbind

Le détachement permet au demandeur de l'association de libérer une association qu'il a établie.

12.1.1.2.1 Arguments

Le service de détachement n'a pas d'argument.

12.1.1.2.2 Résultats

Le service de détachement renvoie un résultat vide en guise d'indication de libération de l'association.

12.1.1.2.3 Erreurs de détachement unbind-errors

Aucune erreur de détachement **unbind-errors** ne peut interrompre le détachement.

12.1.2 Erreurs de rattachement bind-errors

Le présent paragraphe définit les erreurs de rattachement suivantes:

a) erreur d'authentification;
b) occupé;
c) mode de dialogue inacceptable;
d) contexte de sécurité inacceptable;
e) confidentialité d'association inadaptée.

12.1.2.1 Authentication-error (erreur d'authentification)

L'erreur de rattachement (erreur d'authentification) indique qu'une association ne peut pas être établie en raison d'une erreur d'authentification; les pouvoirs du demandeur **credentials** ne sont pas acceptables ou sont incorrectement spécifiés.

Cette erreur n'a pas de paramètre.

12.1.2.2 Busy (occupé)

L'erreur de rattachement (occupé) indique qu'une association ne peut être établie, le demandeur étant occupé.

Cette erreur n'a pas de paramètre.

12.1.2.3 Unacceptable-dialogue-mode (mode de dialogue inacceptable)

L'erreur de rattachement **unacceptable-dialogue-mode** (mode de dialogue inacceptable) indique que le mode de dialogue proposé par le demandeur de l'association est inacceptable pour le demandé (voir l'article 12 de la Rec. UIT-T X.419 | ISO/CEI 10021-6).

Cette erreur n'a pas de paramètre.

12.1.2.4 Contexte de sécurité inacceptable (unacceptable-security-context)

L'erreur de rattachement (contexte de sécurité inacceptable) indique que le contexte de sécurité **security-context** proposé par le demandeur de l'association est inacceptable pour le demandé.

Cette erreur n'a pas de paramètre.

12.1.2.5 Inadequate-association-confidentiality (confidentialité d'association inadaptée)

L'erreur de rattachement (confidentialité d'association inadaptée) indique qu'une association ne peut pas être établie car la connexion sous-jacente ne fournit pas la confidentialité nécessaire.

12.2 Accès de transfert

Le présent paragraphe définit les opérations abstraites et les erreurs abstraites qui se produisent à un accès de transfert.

12.2.1 Opérations abstraites abstract-operations

Le présent paragraphe définit les opérations abstraites suivantes de l'accès de transfert:

a) transfert de message;

b) transfert d'envoi-test;

c) transfert de rapport.

12.2.1.1 Transfert de message Message-transfer

L'opération abstraite de transfert de message permet à un agent MTA de transférer un message vers un autre agent MTA.

12.2.1.1.1 Arguments

Le Tableau 30 énumère les arguments de l'opération abstraite de transfert de message, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

12.2.1.1.1.1 Identificateur de message message-identifier

Cet argument contient un identificateur **MTS-identifier** qui permet de distinguer le message de tous les autres messages, envois-tests et rapports au sein du système MTS. Il doit être produit par l'agent MTA expéditeur du message et doit avoir la même valeur que l'identificateur de dépôt de message **message-submission-identifier** fourni à l'expéditeur lors du dépôt du message, et que l'identificateur de remise de message **message-delivery-identifier** fourni aux destinataires lors de la remise de celui-ci.

Lorsqu'un message est dupliqué pour être acheminé vers plusieurs destinataires par l'intermédiaire de différents agents MTA, chaque copie du message contient l'identificateur de message **message-identifier** de l'original.

12.2.1.1.1.2 Information bilatérale par domaine per-domain-bilateral-information

Cet argument contient des informations à l'intention des domaines de gestion MD que le message rencontrera lors de son transit à travers le système MTS. Il peut être établi par le domaine MD expéditeur.

Cet argument peut contenir zéro ou plusieurs éléments, chacun comprenant:

l'information bilatérale **bilateral-information** destinée à un domaine MD;

le nom de pays **country-name**, et, facultativement, le nom de domaine d'administration **administration-domain-name** et facultativement, l'identificateur de domaine privé **private-domain-identifier** du domaine MD auquel l'information bilatérale **bilateral-information** est destinée.

12.2.1.1.1.3 Informations de trace trace-information

Cet argument consigne les opérations effectuées sur le message (ou l'envoi-test, ou le rapport), par chaque domaine MD par lequel transite le message (ou l'envoi-test, ou le rapport) lors de son transfert à travers le système MTS (voir § 12.3.1). Il doit être produit par chaque domaine MD par lequel transite le message (ou l'envoi-test, ou le rapport).

Tableau 30 – Arguments de transfert de message Message-transfer

Argument	Présence	Paragraphe
Arguments de relais		
Identificateur de message *message-identifier*	M	12.2.1.1.1.1
Information bilatérale par domaine *per-domain-bilateral-information*	C	12.2.1.1.1.2
Informations de trace *trace-information*	M	12.2.1.1.1.3
Informations de trace interne *internal-trace-information*	C	12.2.1.1.1.4
Chronologie de développement *DL-expansion-history*	C	8.3.1.1.1.7
Argument d'expéditeur		
Nom d'expéditeur *originator-name*	M	8.2.1.1.1.1
Arguments de destinataire		
Nom de destinataire *recipient-name*	M	8.2.1.1.1.2
Numéro de destinataire initialement spécifié *originally-specified-recipient-number*	M	12.2.1.1.1.5
Responsabilité *responsibility*	M	12.2.1.1.1.6
Interdiction de développement *DL-expansion-prohibited*	C	8.2.1.1.1.6
Divulgation d'autres destinataires *disclosure-of-other-recipients*	C	8.2.1.1.1.7
Destinataires exemptés de la liste DL *DL-exempted-recipients*	O	8.2.1.1.1.40
Arguments de réacheminement		
Autorisation de destinataire suppléant *alternate-recipient-allowed*	C	8.2.1.1.1.3
Interdiction de réassignation de destinataire *recipient-reassignment-prohibited*	C	8.2.1.1.1.4
Destinataire suppléant désigné par l'expéditeur *originator-requested-alternate-recipient*	C	8.2.1.1.1.5
Chronologie de réacheminement *redirection-history*	C	8.3.1.1.1.5
Argument de priorité		
Priorité *priority*	C	8.2.1.1.1.8
Arguments de conversion		
Interdiction de conversion implicite *implicit-conversion-prohibited*	C	8.2.1.1.1.9
Interdiction de conversion avec perte *conversion-with-loss-prohibited*	C	8.2.1.1.1.10
Conversion explicite *explicit-conversion*	C	12.2.1.1.1.9
Arguments d'heure de remise		
Heure de remise différée *deferred-delivery-time*	C	12.2.1.1.1.7
Heure limite de remise *latest-delivery-time*	C	8.2.1.1.1.13
Argument de méthode de remise		
Méthode de remise demandée *requested-delivery-method*	C	8.2.1.1.1.14
Arguments de remise physique		
Interdiction de retransmission physique *physical-forwarding-prohibited*	C	8.2.1.1.1.15
Demande d'adresse de retransmission physique *physical-forwarding-address-request*	C	8.2.1.1.1.16
Modes de remise physique *physical-delivery-modes*	C	8.2.1.1.1.17
Type de courrier recommandé *registered-mail-type*	C	8.2.1.1.1.18
Numéro de destinataire pour avis *recipient-number-for-advice*	C	8.2.1.1.1.19
Attributs de restitution physique *physical-rendition-attributes*	C	8.2.1.1.1.20
Adresse de retour à l'expéditeur *originator-return-address*	C	8.2.1.1.1.21
Arguments de demande de rapport de remise		
Demande de rapport par l'expéditeur *originator-report-request*	M	8.2.1.1.1.22
Demande de rapport de l'agent MTA expéditeur *originating-MTA-report-request*	M	12.2.1.1.1.8
Demande de réacheminement de contenu *content-return-request*	C	8.2.1.1.1.23
Demande de rapport de remise physique *physical-delivery-report-request*	C	8.2.1.1.1.24

Tableau 30 – Arguments de transfert de message Message-transfer

Argument	Présence	Paragraphe
Arguments de sécurité		
Certificat d'expéditeur *originator-certificate*	C	8.2.1.1.1.25
Jeton de message *message-token*	C	8.2.1.1.1.26
Identificateur d'algorithme de confidentialité de contenu *content-confidentiality-algorithm-identifier*	C	8.2.1.1.1.27
Contrôle d'intégrité de contenu *content-integrity-check*	C	8.2.1.1.1.28
Contrôle d'authentification d'origine de message *message-origin-authentication-check*	C	8.2.1.1.1.29
Etiquette de sécurité *message-security-label*	C	8.2.1.1.1.30
Demande de preuve de remise *proof-of-delivery-request*	C	8.2.1.1.1.32
Certificats d'expéditeurs multiples *multiple-originator-certificates*	O	8.2.1.1.1.41
Certificats de destinataire *recipient-certificates*	O	8.2.1.1.1.42
Sélecteurs de certificats *certificate-selectors*	O	8.2.1.1.1.43
Violation des sélecteurs de certificats *certificate-selectors-override*	O	8.2.1.1.1.44
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	C	8.2.1.1.1.33
Type de contenu *content-type*	M	8.2.1.1.1.34
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	C	8.2.1.1.1.36
Contenu *content*	M	8.2.1.1.1.37
Type de notification *notification-type*	O	8.2.1.1.1.38
Message de service *service-message*	O	8.2.1.1.1.39

12.2.1.1.1.4 Informations de trace interne internal-trace-information

Cet argument consigne les opérations effectuées sur le message (ou l'envoi-test, ou le rapport) par chaque agent MTA par lequel transite le message (ou l'envoi-test, ou le rapport) pendant son transfert à l'intérieur d'un domaine MD (voir § 12.3.1). Il doit être produit par chaque agent MTA par lequel transite le message (ou l'envoi-test, ou le rapport) dans le domaine MD.

Selon la politique locale, un agent MTA peut (sans y être obligé) supprimer les informations de trace interne **internal-trace-information** qui ont trait aux autres domaines MD, lors de la remise, du transfert vers un autre domaine MD ou de la réception en provenance d'un autre domaine MD.

12.2.1.1.1.5 Numéro de destinataire initialement spécifié originally-specified-recipient-number

Cet argument doit être produit par l'agent MTA expéditeur. Une valeur différente de cet argument sera spécifiée pour chaque destinataire initialement spécifié.

Le numéro de destinataire initialement spécifié **originally-specified-recipient-number** est un nombre entier compris entre un et le nombre de destinataires initialement spécifiés.

Il existe une relation biunivoque liant chaque numéro de destinataire initialement spécifié au nom de destinataire **recipient-name** au moment du dépôt du message, mais il ne faut pas en déduire la validité de la relation au moment de la remise du message. En d'autres termes, la valeur d'un numéro de destinataire initialement spécifié peut être utilisée pour identifier un nom de destinataire initialement spécifié, mais non le réceptionnaire effectif du message.

12.2.1.1.1.6 Responsibility (responsabilité)

Cet argument indique si l'agent MTA destinataire doit être chargé soit de remettre le message à un destinataire, soit de le transmettre à un autre agent MTA pour être ultérieurement remis au destinataire. Il doit être produit par l'agent MTA expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du message.

Cet argument peut prendre l'une des valeurs suivantes: **responsible** (responsable) ou **not-responsible** (non responsable).

12.2.1.1.1.7 Heure de remise différée deferred-delivery-time

Cet argument est défini au § 8.2.1.1.1.12. Il peut apparaître dans un message à l'accès de transfert s'il existe un accord bilatéral stipulant qu'un agent MTA autre que l'agent MTA expéditeur peut différer la remise du message. Il disparaîtra dès que la demande d'ajournement aura été exécutée.

En l'absence d'accord bilatéral, un agent MTA pourra:

a) différer la remise du message;

b) traiter le message comme s'il n'y avait pas d'argument d'heure de remise différée **deferred-delivery-time**;

c) si l'heure de remise différée n'est pas encore passée, ne pas remettre le message avec pour code motif **deferred-delivery-not-performed** (remise différée non exécutée) et pour code diagnostic de non-remise **no-bilateral-agreement** (pas d'accord bilatéral), le choix entre ces mesures étant du ressort local.

12.2.1.1.1.8 Demande de rapport de l'agent MTA expéditeur originating-MTA-report-request

Cet argument indique le genre de rapport demandé par l'agent MTA expéditeur. Il doit être produit par l'agent MTA expéditeur. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire.

Cet argument peut prendre l'une des valeurs suivantes:

non-delivery-report: un rapport est renvoyé seulement en cas de non-remise et il contient seulement la dernière information de trace **last-trace-information**;

report: un rapport est renvoyé en cas de remise ou de non-remise et il contient seulement la dernière information de trace **last-trace-information**;

audited-report: un rapport est renvoyé en cas de remise ou de non-remise et il contient l'information de trace complète **trace-information**.

La valeur spécifiée par l'argument de demande de rapport de l'agent MTA expéditeur **originating-MTA-report-request** doit être supérieure ou égale à la valeur spécifiée dans l'argument de demande de rapport de l'expéditeur **originator-report-request**, le classement de ces valeurs étant par ordre croissant: **no-report** (pas de rapport), **non-delivery-report** (rapport de non-remise), **report** (rapport), **audited-report** (rapport vérifié).

12.2.1.1.1.9 Conversion explicite explicit-conversion

Cet argument est défini au § 8.2.1.1.1.11. Une fois réalisée la conversion explicite spécifiée, l'argument doit être supprimé.

12.2.1.1.2 Résultats

L'opération abstraite de transfert de message ne renvoie pas de résultat.

12.2.1.1.3 Erreurs abstraites abstract-errors

Aucune erreur abstraite ne peut interrompre l'opération abstraite de transfert de message.

12.2.1.2 Transfert d'envoi-test Probe-transfer

L'opération abstraite de transfert d'envoi-test permet à un agent MTA de transférer un envoi-test vers un autre agent MTA.

12.2.1.2.1 Arguments

Le Tableau 31 énumère les arguments de l'opération abstraite de transfert d'envoi-test, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

12.2.1.2.1.1 Identificateur de l'envoi-test probe-identifier

Cet argument contient un identificateur **MTS-identifier** qui permet de distinguer l'envoi-test de tous les autres messages, envois-tests et rapports à l'intérieur du MTS. Il doit être produit par l'agent MTA expéditeur de l'envoi-test et aura la même valeur que l'identificateur de dépôt d'envoi-test **probe-submission-identifier** fourni à l'expéditeur de l'envoi-test lors du dépôt de celui-ci.

12.2.1.2.2 Résultats

L'opération abstraite de transfert d'envoi-test ne renvoie pas de résultats.

12.2.1.2.3 Erreurs abstraites abstract-errors

Aucune erreur abstraite ne peut interrompre l'opération abstraite de transfert d'envoi-test.

12.2.1.3 Transfert de rapport Report-transfer

L'opération abstraite de transfert de rapport permet à un agent MTA de transférer un rapport vers un autre agent MTA.

Tableau 31 – Arguments de transfert d'envoi-test Probe-transfer

Argument	Présence	Paragraphe
Arguments de relais		
Identificateur de l'envoi-test *probe-identifier*	M	12.2.1.2.1.1
Information bilatérale par domaine *per-domain-bilateral-information*	C	12.2.1.1.1.2
Informations de trace *trace-information*	M	12.2.1.1.1.3
Informations de trace interne *internal-trace-information*	C	12.2.1.1.1.4
Argument d'expéditeur		
Nom d'expéditeur *originator-name*	M	8.2.1.1.1.1
Arguments de destinataire		
Nom de destinataire *recipient-name*	M	8.2.1.1.1.2
Numéro de destinataire initialement spécifié *originally-specified-recipient-number*	M	12.2.1.1.1.5
Responsabilité *responsibility*	M	12.2.1.1.1.6
Interdiction de développement *DL-expansion-prohibited*	C	8.2.1.1.1.6
Arguments de réacheminement		
Autorisation de destinataire suppléant *alternate-recipient-allowed*	C	8.2.1.1.1.3
Interdiction de réassignation de destinataire *recipient-reassignment-prohibited*	C	8.2.1.1.1.4
Destinataire suppléant désigné par l'expéditeur *originator-requested-alternate-recipient*	C	8.2.1.1.1.5
Chronologie de réacheminement *redirection-history*	C	8.3.1.1.1.5
Arguments de conversion		
Interdiction de conversion implicite *implicit-conversion-prohibited*	C	8.2.1.1.1.9
Interdiction de conversion avec perte *conversion-with-loss-prohibited*	C	8.2.1.1.1.10
Conversion explicite *explicit-conversion*	C	8.2.1.1.1.11
Argument de méthode de remise		
Méthode de remise demandée *requested-delivery-method*	C	8.2.1.1.1.14
Argument de remise physique		
Attributs de restitution physique *physical-rendition-attributes*	C	8.2.1.1.1.20
Arguments de demande de rapport		
Demande de rapport de l'expéditeur *originator-report-request*	M	8.2.1.1.1.22
Demande de rapport de l'agent MTA expéditeur *originating-MTA-report-request*	M	12.2.1.1.1.8
Arguments de sécurité		
Certificat d'expéditeur *originator-certificate*	C	8.2.1.1.1.25
Contrôle d'authentification d'origine d'envoi-test *probe-origin-authentication-check*	C	8.2.1.2.1.1
Etiquette de sécurité *message-security-label*	C	8.2.1.1.1.30
Arguments de contenu		
Types d'origine d'informations codées *original-encoded-information-types*	C	8.2.1.1.1.33
Type de contenu *content-type*	M	8.2.1.1.1.34
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	C	8.2.1.1.1.36
Longueur de contenu *content-length*	C	8.2.1.2.1.2
Type de notification *notification-type*	C	8.2.1.1.1.38
Message de service *service-message*	O	8.2.1.1.1.39

12.2.1.3.1 Arguments

Le Tableau 32 énumère les arguments de l'opération abstraite de transfert de rapport, en qualifie la présence et indique les paragraphes dans lesquels ils sont définis.

Tableau 32 – Arguments de transfert de rapport Report-transfer

Argument	Présence	Paragraphe
Arguments de relais		
Identificateur de rapport *report-identifier*	M	12.2.1.3.1.1
Informations de trace *trace-information*	M	12.2.1.1.1.3
Informations de trace interne *internal-trace-information*	C	12.2.1.1.1.4
Chronologie de réacheminement *redirection-history*	C	8.3.1.2.1.5
Argument d'origine de rapport		
Nom de l'agent MTA au rapport *reporting-MTA-name*	C	8.3.1.2.1.17
Argument de destination de rapport		
Nom de destination de rapport *report-destination-name*	M	12.2.1.3.1.2
Argument de demande de rapport		
Demande de rapport de l'expéditeur *originator-report-request*	M	8.2.1.1.1.22
Arguments de trace du sujet		
Identificateur de sujet *subject-identifier*	M	12.2.1.3.1.3
Numéro de destinataire initialement spécifié *originally-specified-recipient-number*	M	12.2.1.1.1.5
Information de trace intermédiaire de sujet *subject-intermediate-trace-information*	C	12.2.1.3.1.4
Heure d'arrivée *arrival-time*	M	12.2.1.3.1.5
Expéditeur et chronologie de développement de DL *originator-and-DL-expansion-history*	C	8.3.1.2.1.3
Nom de DL au rapport *reporting-DL-name*	C	8.3.1.2.1.4
Argument de conversion		
Types convertis d'informations codées *converted-encoded-information-types*	C	8.3.1.2.1.6
Arguments d'informations supplémentaires		
Informations supplémentaires *supplementary-information*	C	8.3.1.2.1.7
Adresse de retransmission physique *physical-forwarding-address*	C	8.3.1.2.1.8
Arguments de réacheminement du sujet		
Nom de destinataire effectif *actual-recipient-name*	M	8.3.1.2.1.2
Nom de destinataire initialement prévu *originally-intended-recipient-name*	C	8.3.1.1.1.4
Chronologie de réacheminement *redirection-history*	C	8.3.1.1.1.5
Arguments de contenu		
Types d'origine d'information codée *original-encoded-information-types*	C	8.2.1.1.1.33
Type de contenu *content-type*	C	8.3.1.2.1.15
Identificateur de contenu *content-identifier*	C	8.2.1.1.1.35
Corrélateur de contenu *content-correlator*	C	8.2.1.1.1.36
Contenu renvoyé *returned-content*	C	8.3.1.2.1.16
Arguments de remise		
Heure de remise de message *message-delivery-time*	C	8.3.1.2.1.9
Type d'utilisateur *type-of-MTS-user*	C	8.3.1.2.1.10
Arguments de non-remise		
Code de motif de non-remise *non-delivery-reason-code*	C	8.3.1.2.1.11
Code de diagnostic de non-remise *non-delivery-diagnostic-code*	C	8.3.1.2.1.12
Arguments de sécurité		
Certificat de destinataire *recipient-certificate*	C	8.3.1.1.2.1
Preuve de remise *proof-of-delivery*	C	8.3.1.1.2.2
Certificat de l'agent MTA au rapport *reporting-MTA-certificate*	C	8.3.1.2.1.13
Contrôle d'authentification d'origine de rapport *report-origin-authentication-check*	C	8.3.1.2.1.14

Etiquette de sécurité *message-security-label*	C	8.2.1.1.1.30
Argument d'informations supplémentaires		
Informations supplémentaires *additional-information*	C	12.2.1.3.1.6

12.2.1.3.1.1 Identificateur de rapport report-identifier

Cet argument contient un identificateur **MTS-identifier** qui permet de distinguer le rapport de tous les autres messages, envois-tests et rapports à l'intérieur du système MTS. Il doit être produit par l'agent MTA expéditeur du rapport.

12.2.1.3.1.2 Nom de destination de rapport report-destination-name

Cet argument contient le nom **OR-name** de la destination immédiate du rapport. Il doit être produit par l'agent MTA expéditeur du rapport, et modifié ensuite par les points de développement de liste DL si des listes DL quelconques ont été développées pour ajouter des destinataires au sujet.

L'agent MTA expéditeur du rapport doit attribuer à cet argument le nom d'expéditeur **originator-name** du sujet si celui-ci n'a pas de chronologie de développement **DL-expansion-history**, ou le dernier nom **OR-name** dans cette chronologie **DL-expansion-history** si elle figure dans le sujet.

Un point de développement de liste DL peut remplacer son propre nom **OR-name** dans cet argument par le nom **OR-name** qui précède immédiatement le sien dans l'argument d'expéditeur et de chronologie de développement de liste DL **originator-and-DL-expansion-history** du rapport, ou par tout autre nom **OR-name** conformément à la politique d'établissement de rapport de la liste DL.

12.2.1.3.1.3 Identificateur de sujet subject-identifier

Cet argument contient l'identificateur de message **message-identifier** (ou identificateur de l'envoi-test **probe-identifier**) du sujet (un identificateur **MTS-identifier**). Il doit être établi par l'agent MTA expéditeur du sujet.

12.2.1.3.1.4 Information de trace intermédiaire de sujet subject-intermediate-trace-information

Cet argument contient l'information de trace **trace-information** présente dans le sujet lors de son transfert à travers le domaine MD au rapport. Il sera présent si et seulement si un rapport vérifié et confirmé est demandé par l'agent MTA expéditeur du sujet. Il peut être produit par l'agent MTA au rapport.

NOTE – L'inclusion dans l'information de trace intermédiaire de sujet **subject-intermediate-trace-information** de l'information de trace interne **internal-trace-information** présente dans le sujet lors de son transfert vers l'agent MTA au rapport pourra faire l'objet d'une future normalisation.

12.2.1.3.1.5 Heure d'arrivée arrival-time

Cet argument contient la date et l'heure **time** auxquelles le sujet a pénétré dans le domaine MD au rapport. Il doit être produit par le domaine MD expéditeur du rapport. Une valeur différente de cet argument peut être spécifiée pour chaque destinataire du sujet auquel le rapport a trait.

12.2.1.3.1.6 Information supplémentaire additional-information

La spécification du contenu de cet argument se fait par accord bilatéral entre domaines MD.

12.2.1.3.2 Résultats

L'opération abstraite de transfert de rapport ne renvoie pas de résultats.

12.2.1.3.3 Erreurs abstraites abstract-errors

Aucune erreur abstraite ne peut interrompre l'opération abstraite de transfert de rapport.

12.2.2 Erreurs abstraites abstract-errors

L'accès de transfert n'a pas d'erreurs abstraites.

12.3 Types de paramètres communs

Le présent paragraphe définit un certain nombre de types de paramètres communs du service abstrait d'agent MTA.

12.3.1 Information de trace trace-information et information de trace interne internal-trace-information

L'information de trace **trace-information** consigne les actions entreprises par chaque domaine de gestion MD au passage d'un message, d'un envoi-test ou d'un rapport lors du transfert de celui-ci à travers le système MTS.

L'information de trace interne **internal-trace-information** consigne les actions entreprises par chaque agent MTA au passage d'un message, d'un envoi-test ou d'un rapport lors du transfert de celui-ci à travers un domaine MD. Cette information de trace interne pourra être supprimée du message, de l'envoi-test ou du rapport avant de quitter un domaine MD. Un domaine MD peut (sans pour autant y être obligé) supprimer l'information de trace interne relative à un autre domaine MD.

L'information de trace **trace-information** (ou de trace interne **internal-trace-information**) comporte une séquence d'éléments d'information de trace **trace-information-elements** (ou de trace interne **internal-trace-information-elements**). Le premier élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) est celui qui est fourni par le domaine MD expéditeur (ou par l'agent MTA expéditeur) du message, de l'envoi-test ou du rapport. Le deuxième élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) est celui que fournit le domaine MD (ou l'agent MTA) suivant par lequel passe le message, l'envoi-test ou le rapport, et ainsi de suite. Chaque domaine MD (ou agent MTA) ajoute son élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) à la fin de la séquence existante. Une information de trace **trace-information** est ajoutée au message, à l'envoi-test ou au rapport par le premier agent MTA rencontré par celui-ci dans chaque domaine MD traversé; cette information est si nécessaire modifiée par les agents MTA suivants du même domaine MD.

Chaque élément d'information de trace **trace-information-element** comporte l'identificateur global de domaine **global-domain-identifier** du domaine MD dont il émane.

Chaque élément d'information de trace interne **internal-trace-information-element** comporte le nom **MTA-name** de l'agent MTA dont il émane ainsi que l'identificateur global de domaine **global-domain-identifier** du domaine MD auquel appartient l'agent MTA.

Chaque élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) comporte l'heure d'arrivée **arrival-time** à laquelle le message, l'envoi-test ou le rapport pénètre dans le domaine MD (ou l'agent MTA). Dans le cas du domaine MD expéditeur (ou de l'agent MTA expéditeur) du message, de l'envoi-test ou du rapport, l'heure d'arrivée **arrival-time** correspond respectivement à l'heure de dépôt du message, de dépôt de l'envoi-test ou d'établissement du rapport.

Chaque élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) précise l'action d'acheminement **routing-action** que le domaine MD (ou l'agent MTA) dont il émane a effectuée sur le message, l'envoi-test ou le rapport. **Relayed** (relayé) est l'action d'acheminement normale permettant de transférer le message, l'envoi-test ou le rapport à un autre domaine MD (ou agent MTA). **Rerouted** (réacheminé) indique qu'une tentative a déjà été faite pour acheminer le message, l'envoi-test ou le rapport vers un domaine essayé **attempted-domain** (ou agent MTA essayé **attempted-MTA**); l'identificateur global **global-domain-identifier** du domaine essayé figure dans l'élément d'information de trace **trace-information-element**; si la tentative de réacheminement visait un autre agent MTA situé dans le même domaine MD, le nom **MTA-name** de l'agent MTA essayé figure alors dans l'élément d'information de trace interne **internal-trace-information-element**; si la tentative de réacheminement concerne un autre domaine MD, l'identificateur global **global-domain-identifier** du domaine essayé figure alors dans l'élément d'information de trace interne **internal-trace-information-element** à la place d'un nom **MTA-name**.

Chaque élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) précise également toute action supplémentaire que le domaine MD (ou l'agent MTA) dont il émane a entreprise concernant le message, l'envoi-test ou le rapport. Les indications relatives à de telles actions supplémentaires **additional-actions** figurant dans les éléments d'information de trace interne **internal-trace-information-elements** pendant la traversée d'un domaine MD figureront également dans le ou les éléments d'information de trace **trace-information-elements** correspondant au passage dans ce domaine MD.

Si une remise différée a obligé le domaine MD (ou l'agent MTA) dont émane l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) à retenir le message pendant un certain laps de temps, l'heure différée correspondant au début du traitement du message aux fins de remise ou de transfert figurera également dans l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**). Ce paramètre ne figure pas dans les éléments d'information de trace ou de trace interne des envois-tests et des rapports.

Si le domaine MD (ou l'agent MTA) dont émane l'élément d'information de trace **trace-information-element** ou de trace interne **internal-trace-information-element** soumet un message à une conversion, les types convertis d'information codée **converted-encoded-information-types** résultant de cette conversion figureront également dans l'élément d'information de trace ou de trace interne. Dans le cas d'un envoi-test, un domaine MD (ou un agent MTA) qui aurait converti le message sujet indiquera dans son élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) les types d'information codée **encoded-information-types** que le message sujet **subject-message** aurait contenus après conversion. Ce paramètre ne figure pas dans l'information de trace ou de trace interne des rapports.

Si le domaine MD (ou l'agent MTA) renvoie un message ou un envoi-test (pour certains mais pas nécessairement tous les destinataires du message ou de l'envoi-test), l'indication **redirected** (réacheminé) est portée dans l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**).

Si le domaine MD (ou l'agent MTA) développe une liste DL d'un message, l'indication **dl-operation** (développement) est portée dans l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**). Si le domaine MD (ou l'agent MTA) est un point de développement de liste **DL-expansion-point** et qu'il remplace son propre nom **OR-name** dans le nom de destination d'un rapport **report-destination-name** par un autre nom **OR-name** (voir § 12.2.1.3.1.2), l'indication **dl-operation** (développement) est portée dans l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) du rapport. Ce paramètre est absent de l'information de trace ou de trace interne des envois-tests.

La détection et la suppression de boucle sont réalisées par un domaine MD (ou un agent MTA) à la réception d'un message, d'un envoi-test ou d'un rapport d'un autre domaine MD (ou agent MTA). Les messages, envois-tests et rapports peuvent légitimement entrer à nouveau dans un domaine MD (ou un agent MTA) pour plusieurs raisons (réacheminement, etc.) et, par conséquent, un message, un envoi-test ou un rapport peut avoir plusieurs éléments d'information distincts de trace **trace-information-elements** (ou de trace interne **internal-trace-information-elements**) provenant d'un même domaine MD (ou agent MTA). Chaque fois qu'un message, un envoi-test ou un rapport est transmis par un domaine MD (ou un agent MTA), la production des éléments d'information de trace ou de trace interne est effectuée de la façon suivante:

i) un élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) est ajouté et porte l'indication **relayed** (relayé);

ii) en cas de tentative de réacheminement, l'élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) ajouté conformément au i) est modifié en **rerouted** (réacheminé) et le nombre d'éléments d'information de trace ou de trace interne ajoutés par le domaine MD (ou l'agent MTA) pour cette traversée du domaine MD (ou de l'agent MTA) reste égal à un;

iii) chaque nouvelle tentative de réacheminement est signalée par l'ajout d'un nouvel élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) portant l'indication **rerouted** (réacheminé).

Plusieurs tentatives de réacheminement peuvent avoir lieu vers le même domaine MD (ou agent MTA).

Chaque élément d'information de trace **trace-information-element** (ou de trace interne **internal-trace-information-element**) ajouté par un domaine MD (ou agent MTA) peut inclure des indications d'actions supplémentaires **additional-actions** appliquées par le domaine MD (ou l'agent MTA) au message ou à l'envoi-test [c'est-à-dire heure différée **deferred-time** (indication absente de l'information de trace ou de trace interne des envois-tests), types convertis d'information codée **converted-encoded-information-types,** et **redirected** (réacheminé) ou **dl-operation** (développement)]. Pour indiquer l'ordre dans lequel le réacheminement et le développement de liste DL ont eu lieu, les indications réacheminé et développement (**redirected and dl-operation**) doivent apparaître dans un seul élément d'information de trace (**trace-information-element**) ou de trace interne (**internal-trace-information-element**).

13 Définition de syntaxe abstraite de l'agent de transfert des messages MTA

La syntaxe abstraite du service abstrait d'agent MTA est définie à la Figure 4.

Cette définition a été faite au moyen de la notation de syntaxe abstraite (ASN.1) 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, et des conventions adoptées pour la définition des services abstraits et figurant dans la Rec. UIT-T X.402 | ISO/CEI 10021-2, qui utilise la notation pour les opérations distantes définie dans la Rec. UIT-T X.880 | ISO/CEI 13712-1.

La définition de syntaxe abstraite du service abstrait d'agent MTA comporte les principales parties suivantes:

prologue: déclarations des exports provenant du module du service abstrai d'agent MTA et des imports à destination de ce module (voir la Figure 4, partie 1);

objets et accès: définitions de l'objet MTA et de l'accès de transfert (voir la Figure 4, partie 2);

rattachement MTA-bind et détachement MTA-unbind: définitions du rattachement et du détachement utilisés pour établir des associations entre MTA et les libérer (voir la Figure 4, partie 2);

accès de transfert: définitions des opérations abstraites de l'accès de transfert: transfert de message, d'envoi-test et de rapport (voir la Figure 4, partie 3);

enveloppe de transfert de message: définition de l'enveloppe de transfert de message (voir la Figure 4, parties 3 à 4);

enveloppe de transfert d'envoi-test: définition de l'enveloppe de transfert d'envoi-test (voir la Figure 4, partie 4);

enveloppe et contenu de transfert de rapport: définitions de l'enveloppe de transfert de rapport et du contenu de transfert de rapport (voir la Figure 4, partie 5);

champs d'enveloppe et de contenu de rapport: définitions des champs de l'enveloppe et du contenu de rapport (voir la Figure 4, parties 5 à 7);

champs d'extension: définitions des champs d'extension extension-fields (voir la Figure 4, partie 7);

types de paramètres communs: définitions des types de paramètres communs (voir la Figure 4, parties 7 à 8).

NOTE – Le module suppose un certain nombre de modifications au protocole P1 défini dans la Rec. CCITT X.411 (version 1984). Ces modifications sont mises en évidence par soulignement.

Chaque champ d'extension **extension-field** défini à la Figure 4 (partie 6) contient une indication de criticité aux fins du dépôt, du transfert et de la remise. Le mécanisme de criticité est décrit au § 9.2 et les procédures relatives aux champs d'extension **extension-fields** ainsi qu'à leurs indications de criticité sont définies plus en détail à l'article 14.

```
MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mta-abstract-service(2)
              version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exporte tout

IMPORTS

        -- Opérations distantes

        CONNECTION-PACKAGE, CONTRACT
                ----
                FROM Remote-Operations-Information-Objects {joint-iso-itu-t remote-operations(4)
                        informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions {joint-iso-itu-t remote-operations(4)
                        useful-definitions(7) version1(0) }

-- Paramètres du service abstrait MTS

        ABSTRACT-ERROR, ABSTRACT-OPERATION, administration, AdministrationDomainName,
        certificate-selectors, certificate-selectors-override, Content, ContentIdentifier,
        ContentLength, ContentType, content-confidentiality-algorithm-identifier,
        content-correlator, content-integrity-check, conversion-with-loss-prohibited,
        ConvertedEncodedInformationTypes, CountryName, DeferredDeliveryTime, delivery,
        dl-exempted-recipients, dl-expansion-history, dl-expansion-prohibited,
        ExplicitConversion, EXTENSION, ExtensionField { }, GlobalDomainIdentifier,
        InitiatorCredentials, latest-delivery-time, message-origin-authentication-check,
        message-security-label, message-token, MHS-OBJECT, MTAName, MTSIdentifier,
        multiple-originator-certificates, ORAddressAndOptionalDirectoryName,
        OriginalEncodedInformationTypes, originator-and-DL-expansion-history,
        originator-certificate, originator-return-address, PerMessageIndicators,
        physical-delivery-modes, physical-delivery-report-request, physical-forwarding-address,
        physical-forwarding-address-request, physical-forwarding-prohibited,
        physical-rendition-attributes, PORT, Priority, PrivateDomainIdentifier,
        PrivateExtensions, probe-origin-authentication-check, proof-of-delivery,
        proof-of-delivery-request, recipient-certificate, recipient-number-for-advice,
        recipient-reassignment-prohibited, redirection-history, registered-mail-type,
        reporting-DL-name, reporting-MTA-certificate, reporting-MTA-name, ReportType,
        report-origin-authentication-check, requested-delivery-method, ResponderCredentials,
        SecurityContext, submission, SupplementaryInformation, Time
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- Objets informationnels de messagerie IPM

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                        information-objects(2) version-1999(1) }

        -- Identificateurs d'objets

        id-cp-mta-connect, id-ct-mta-transfer, id-ot-mta, id-pt-transfer
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 1 de 8)

```
        -- Limites supérieures

        ub-bit-options, ub-integer-options, ub-recipients, ub-transfers
        ----
        FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                version-1999(1) };

--      Objets

mta MHS-OBJECT ::= {
        BOTH  { mta-transfer }
        ID    id-ot-mta }

--      Contrats

mta-transfer CONTRACT ::= {
        CONNECTION     mta-connect
        OPERATIONS OF  { transfer }
        ID             id-ct-mta-transfer }

--      Paquetage de connexion

mta-connect CONNECTION-PACKAGE ::= {
        BIND        mta-bind
        UNBIND      mta-unbind
        ID          id-cp-mta-connect }

--      Accès

transfer PORT ::= {
        OPERATIONS  { message-transfer | probe-transfer | report-transfer }
        ID          id-pt-transfer }

--      Attachement (MTA-bind) et détachement (MTA-unbind)

mta-bind ABSTRACT-OPERATION ::= {
        ARGUMENT  MTABindArgument
        RESULT    MTABindResult
        ERRORS    { mta-bind-error } }

mta-unbind ABSTRACT-OPERATION ::= emptyUnbind

MTABindArgument ::= CHOICE {
        unauthenticated NULL,        -- si l'authentification n'est pas demandée
        authenticated [1] SET {      -- si l'authentification est demandée
                initiator-name [0] MTAName,
                initiator-credentials [1] InitiatorCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ),
                security-context [2] SecurityContext OPTIONAL } }

MTABindResult ::= CHOICE {
        unauthenticated NULL,        -- si l'authentification n'est pas demandée
        authenticated [1] SET {      -- si l'authentification est demandée
                responder-name [0] MTAName,
                responder-credentials [1] ResponderCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ) } }

mta-bind-error ABSTRACT-ERROR ::= {
        PARAMETER  INTEGER {
                busy (0),
                authentication-error (2),
                unacceptable-dialogue-mode (3),
                unacceptable-security-context (4),
                inadequate-association-confidentiality (5) } (0..ub-integer-options) }
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 2 de 8)

```
--      Accès de transfert

message-transfer ABSTRACT-OPERATION ::= {
        ARGUMENT Message }

probe-transfer ABSTRACT-OPERATION ::= {
        ARGUMENT Probe }

report-transfer ABSTRACT-OPERATION ::= {
        ARGUMENT Report }

Message ::= SEQUENCE {
                envelope MessageTransferEnvelope,
                content Content }

Probe ::= ProbeTransferEnvelope

Report ::= SEQUENCE {
                envelope ReportTransferEnvelope,
                content ReportTransferContent }

--      Enveloppe de transfert de message

MessageTransferEnvelope ::= SET {
        COMPONENTS OF PerMessageTransferFields,
        per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientMessageTransferFields }

PerMessageTransferFields ::= SET {
        message-identifier MessageIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        priority Priority DEFAULT normal,
        per-message-indicators PerMessageIndicators DEFAULT { },
        deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
        per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
                PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extensions [3] SET OF ExtensionField {{ MessageTransferExtensions }} DEFAULT { } }

MessageTransferExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        recipient-reassignment-prohibited |
        dl-expansion-prohibited |
        conversion-with-loss-prohibited |
        latest-delivery-time |
        originator-return-address |
        originator-certificate |
        content-confidentiality-algorithm-identifier |
        message-origin-authentication-check |
        message-security-label |
        content-correlator |
        dl-exempted-recipients |
        certificate-selectors |
        multiple-originator-certificates |
        dl-expansion-history |
        internal-trace-information |
        PrivateExtensions, ... }

PerRecipientMessageTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extensions [3] SET OF ExtensionField {{ PerRecipientMessageTransferExtensions }}
                                                                        DEFAULT { } }
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 3 de 8)

```
PerRecipientMessageTransferExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        physical-delivery-report-request |
        message-token |
        content-integrity-check |
        proof-of-delivery-request |
        certificate-selectors-override |
        recipient-certificate |
        redirection-history |
        IPMPerRecipientEnvelopeExtensions |
        PrivateExtensions, ... }

--      Enveloppe de transfert de message d'essai

ProbeTransferEnvelope ::= SET {
        COMPONENTS OF PerProbeTransferFields,
        per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
PerRecipientProbeTransferFields}

PerProbeTransferFields ::= SET {
        probe-identifier ProbeIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT { },
        per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
                PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extensions [3] SET OF ExtensionField {{ ProbeTransferExtensions }} DEFAULT { } }

ProbeTransferExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        recipient-reassignment-prohibited |
        dl-expansion-prohibited |
        conversion-with-loss-prohibited |
        originator-certificate |
        message-security-label |
        content-correlator |
        probe-origin-authentication-check |
        internal-trace-information |
        PrivateExtensions, ... }

PerRecipientProbeTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extensions [3] SET OF ExtensionField {{ PerRecipientProbeTransferExtensions }}
                                                                        DEFAULT { } }

PerRecipientProbeTransferExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-rendition-attributes |
        redirection-history |
        PrivateExtensions, ... }
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 4 de 8)

```
--      Enveloppe de transfert de rapport

ReportTransferEnvelope ::= SET {
        report-identifier ReportIdentifier,
        report-destination-name ReportDestinationName,
        trace-information TraceInformation,
        extensions [1] SET OF ExtensionField {{ ReportTransferEnvelopeExtensions }}
                                                                    DEFAULT { } }

ReportTransferEnvelopeExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        message-security-label |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

--      Contenu de transfert de rapport

ReportTransferContent ::= SET {
        COMPONENTS OF PerReportTransferFields,
        per-recipient-fields [0] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientReportTransferFields}

PerReportTransferFields ::= SET {
        subject-identifier SubjectIdentifier,
        subject-intermediate-trace-information SubjectIntermediateTraceInformation OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType OPTIONAL,
        content-identifier ContentIdentifier OPTIONAL,
        returned-content [1] Content OPTIONAL,
        additional-information [2] AdditionalInformation OPTIONAL,
        extensions [3] SET OF ExtensionField {{ ReportTransferContentExtensions }}
                                                                    DEFAULT { } }

ReportTransferContentExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        content-correlator |
        PrivateExtensions, ... }

PerRecipientReportTransferFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        originally-specified-recipient-number [1] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [2] PerRecipientIndicators,
        last-trace-information [3] LastTraceInformation,
        originally-intended-recipient-name [4] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [5] SupplementaryInformation OPTIONAL,
        extensions [6] SET OF ExtensionField {{ PerRecipientReportTransferExtensions }}
                                                                    DEFAULT { } }

PerRecipientReportTransferExtensions EXTENSION ::= {
        -- Peut contenir les extensions suivantes, des extensions privées ou de futures extensions normalisées,
        -- une seule instance au plus de chaque type d'extension:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }

--      Champs d'enveloppe et de contenu de rapport

MessageIdentifier ::= MTSIdentifier

OriginatorName ::= ORAddressAndOptionalDirectoryName
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 5 de 8)

```
PerDomainBilateralInformation ::= SEQUENCE {
       COMPONENTS OF BILATERAL.&id,
       bilateral-information BILATERAL.&Type }

BILATERAL ::= CLASS {
       &id BilateralDomain UNIQUE,
       &Type }
WITH SYNTAX { &Type, IDENTIFIED BY &id }

BilateralDomain ::= SEQUENCE {
       country-name CountryName,
       domain CHOICE {
              administration-domain-name AdministrationDomainName,
              private-domain SEQUENCE {
                     administration-domain-name [0] AdministrationDomainName,
                     private-domain-identifier [1] PrivateDomainIdentifier } } }

RecipientName ::= ORAddressAndOptionalDirectoryName

OriginallySpecifiedRecipientNumber ::= INTEGER (1..ub-recipients)

PerRecipientIndicators ::= BIT STRING {
       responsibility (0),
       -- responsable 'un', non responsable 'zéro'
       originating-MTA-report (1),
       originating-MTA-non-delivery-report (2),
       --  bit de rapport du MTA expéditeur ou bit de rapport de non-remise du MTA expéditeur
       --  ou les deux sont mis à 'un':
       --  bit de rapport de MTA expéditeur à 'un' = demande de 'rapport';
       --  bit de rapport de non-remise de MTA expéditeur à 'un'  demande de 'rapport de non-remise';
       --  les deux bits à 'un' =  demande de 'rapport vérifié';
       -- les bits 0 à 2 =  pas de contenu de transfert de rapport
       originator-report (3),
       originator-non-delivery-report (4),
       -- au plus un bit à 'un':
       -- bit de rapport d'expéditeur à 'un' = demande de 'rapport';
       -- bit de rapport de non-remise d'expéditeur à 'un' demande de 'rapport de non remise';
       -- les deux bits à 'zero' pas de rapport
       reserved-5 (5),
       reserved-6 (6),
       reserved-7 (7)
       -- les bits réservés 5 à 7 doivent être à 'zéro' -- } (SIZE (8..ub-bit-options))

ProbeIdentifier ::= MTSIdentifier

ReportIdentifier ::= MTSIdentifier

ReportDestinationName ::= ORAddressAndOptionalDirectoryName

SubjectIdentifier ::= MessageOrProbeIdentifier

MessageOrProbeIdentifier ::= MTSIdentifier

SubjectIntermediateTraceInformation ::= TraceInformation

--      Les informations supplémentaires ne sont conservées que pour assurer la compatibilité amont
--      et leur utilisation dans les systèmes nouveaux est vivement déconseillée

ADDITIONAL ::= CLASS { &Type }

AdditionalInformation ::= ADDITIONAL.&Type  -- longueur maximale en octets du champ ub-additional-info
tous codages compris

ActualRecipientName ::= ORAddressAndOptionalDirectoryName
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 6 de 8)

```
LastTraceInformation ::= SET {
       arrival-time [0] ArrivalTime,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       report-type [1] ReportType }

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName


--      Champs d'extension

originator-requested-alternate-recipient EXTENSION ::= {
       OriginatorRequestedAlternateRecipient,
       IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOptionalDirectoryName

trace-information EXTENSION ::= {
       TraceInformation,
       IDENTIFIED BY standard-extension:37 }

internal-trace-information EXTENSION ::= {
       InternalTraceInformation,
       IDENTIFIED BY standard-extension:38 }

InternalTraceInformation ::= SEQUENCE SIZE (1..ub-transfers) OF
InternalTraceInformationElement

InternalTraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       mta-name MTAName,
       mta-supplied-information MTASuppliedInformation }

MTASuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted CHOICE {
              mta MTAName,
              domain GlobalDomainIdentifier } OPTIONAL,
       -- opérations supplémentaires -- COMPONENTS OF InternalAdditionalActions }

InternalAdditionalActions ::= AdditionalActions


--      Types de paramètres communs

TraceInformation ::= [APPLICATION 9] SEQUENCE SIZE (1..ub-transfers) OF
TraceInformationElement

TraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       domain-supplied-information DomainSuppliedInformation }

DomainSuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted-domain GlobalDomainIdentifier OPTIONAL,
       -- opérations supplémentaires -- COMPONENTS OF AdditionalActions }

AdditionalActions ::= SET {
       deferred-time [1] DeferredTime OPTIONAL,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       other-actions [3] OtherActions DEFAULT { } }

RoutingAction ::= ENUMERATED {
       relayed (0),
       rerouted (1) }
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 7 de 8)

```
DeferredTime ::= Time

ArrivalTime ::= Time

OtherActions ::= BIT STRING {
       redirected (0),
       dl-operation (1) } (SIZE (0..ub-bit-options))

END     -- Fin du service abstrait d'agent MTA
```

Figure 4 – Définition de syntaxe abstraite du service abstrait MTA (partie 8 de 8)

SECTION 4 – PROCÉDURES DE FONCTIONNEMENT RÉPARTI DU SYSTÈME MTS

14 Procédures de fonctionnement réparti du système MTS

Les procédures décrites dans le présent article se rapportent au fonctionnement réparti du système MTS et sont exécutées par les agents MTA. Chaque agent MTA effectue de manière indépendante les procédures décrites ci-dessous; c'est l'action collective de tous les agents MTA qui constitue le service abstrait du système MTS offert aux utilisateurs de ce système.

Bien que ces procédures incluent la plupart des opérations importantes requises d'un agent MTA, de nombreux détails ont volontairement été omis par souci de clarté et afin d'éviter les redondances inutiles. Pour un traitement complet des opérations d'agent MTA, on se reportera aux définitions du service abstrait.

14.1 Aperçu général du modèle MTA

14.1.1 Organisation et technique de modélisation

La description des procédures afférentes à un agent MTA unique est fondée sur le modèle représenté dans les Figures 5 à 11 et décrit dans ce qui suit. A noter que ce modèle est donné ici à seule fin descriptive et qu'il n'est en aucune façon destiné à imposer quelque contrainte à la mise en œuvre d'un agent MTA.

Ni les procédures décrites ni l'ordre des étapes de traitement qui les composent n'impliquent l'imposition d'une quelconque caractéristique spécifique à un agent MTA effectif.

Le modèle fait une distinction entre *modules* et *procédures*. Les *modules*, au sens qui leur est attribué ici, sont des entités de traitement autonomes auxquelles peuvent faire appel d'autres modules ou des événements externes à l'agent MTA, et qui peuvent elles-mêmes faire appel à d'autres modules ou produire des événements externes. Les modules ne sont pas liés entre eux par une structure de commande explicitement décrite; une telle structure de commande entre modules découlerait plutôt du schéma de leurs appels croisés. Les modules correspondent à des *objets* au sens du langage orienté-objet.

Les *procédures* sont utilisées ici au sens conventionnel de la programmation. Elles sont orientées vers des tâches ou des fonctions. Elles peuvent appeler d'autres procédures, façon sous-programme, avec retour du contrôle à la procédure appelante après achèvement de la procédure appelée. La profondeur d'imbrication de ces appels est arbitraire, et une procédure peut s'appeler elle-même récursivement. Les procédures sont liées entre elles par des structures de commande explicitement définies, constituées par les appels de procédures et par les dispositions conventionnelles de programmation telles que les itérations et les exécutions conditionnelles.

Dans ce modèle, les procédures existent au sein de modules. Chaque module contient au moins une procédure et peut en contenir plusieurs. Dans le dernier cas, les procédures et la structure de commande sont explicitement décrites. Dans le premier cas, l'existence d'une procédure unique de module est habituellement considérée comme implicite.

A l'aide de telles techniques de modélisation, un processus d'application d'agent MTA peut être affiné comme suit: pour chaque opération abstraite (de consommation ou de fourniture) pouvant être réalisée entre un agent MTA et les utilisateurs MTS qu'il dessert, ou entre un agent MTA et les autres agents MTA avec lesquels il coopère, il existe un module unique appelé *module externe*. L'ensemble des modules externes est responsable de l'entrée et de la sortie des messages, des envois-tests, et des rapports vers et hors l'agent MTA, ainsi que de la prise en charge d'opérations telles que le rattachement MTS-bind, le détachement MTS-unbind, l'enregistrement (Register), la commande de dépôt Submission-control et la commande de remise Delivery-control. Les modules externes sont représentés à la Figure 5 et décrits, groupés par accès, aux § 14.5 à 14.10.

Pour effectuer les diverses opérations abstraites dont il a la charge, un agent MTA doit procéder à certaines opérations de traitement pour chaque message, envoi-test, ou rapport entrant ou sortant. Dans le modèle, ces opérations sont du ressort des *modules internes* représentés à la Figure 6 et décrits aux § 14.2 à 14.4.

Les relations entre modules externes et internes d'un même agent MTA s'opèrent de la façon suivante: un module externe ne communique qu'avec un module interne et non avec un autre module externe ou directement avec une procédure au sein d'un module interne. Par conséquent, les modules internes ne prennent pas seulement en charge le gros du traitement à l'intérieur de l'agent MTA, mais servent aussi de liaison entre les modules externes de ce dernier. Outre les modules internes, la Figure 6 montre les modules externes avec lesquels ils communiquent.

L'agent MTA est piloté par les événements en ce sens qu'il reste inactif jusqu'à ce qu'un événement soit détecté sur l'un de ses accès. De nombreux événements, tels que l'appel par un utilisateur MTS ou un autre agent MTA, d'une opération abstraite de rattachement MTS-bind, de commande de dépôt Submission-control, de commande de remise Delivery-control ou d'enregistrement (Register) sont directement et complètement pris en charge par le module affecté à cette opération abstraite. Cependant, d'autres événements déclenchent un traitement qui peut se répercuter dans l'ensemble de l'agent MTA, se prolonger dans le temps et déclencher finalement un ou plusieurs événements de sortie. Ce sont ces événements qui mettent en action les modules de traitement internes. Ces événements sont:

a) entrée via l'accès de dépôt d'un message ou d'un envoi-test expédié par un utilisateur MTS localement pris en charge;

b) entrée via l'accès de transfert d'un message, d'un envoi-test, ou d'un rapport relayé par un autre agent MTA.

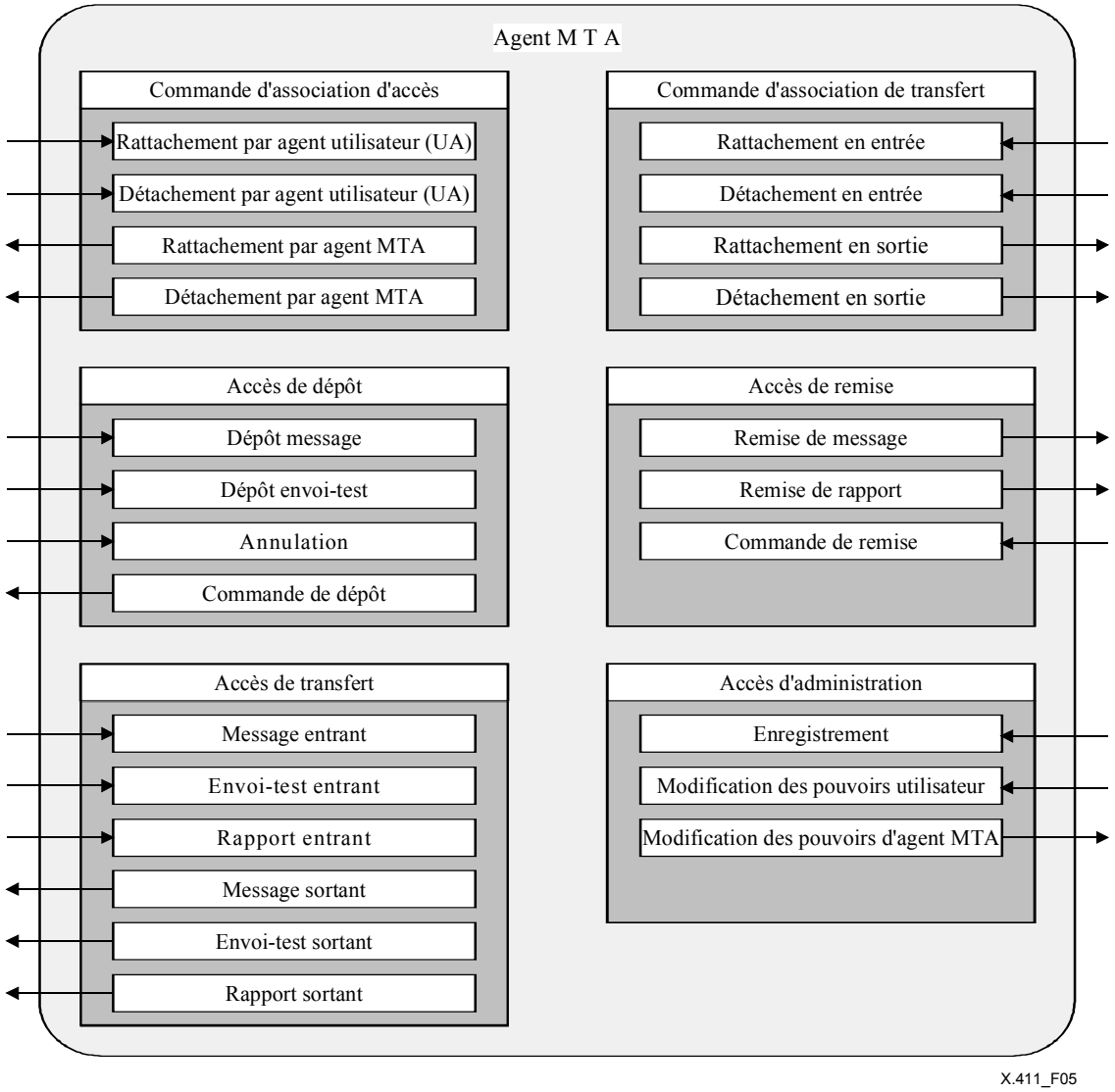


Figure 5 – Accès et modules d'un agent MTA

Comme le traitement au sein d'un agent MTA peut devenir assez complexe, surtout avec des messages multidestinataires, le modèle suppose, en guise de dispositif de consignation interne, que chaque message véhicule avec lui un ensemble d'instructions, l'une concernant le message dans son ensemble, plus une instruction relative à chaque destinataire. Ces instructions permettent de guider le message à travers les étapes de traitement et d'acheminer l'information entre les modules et les procédures internes aux agents MTA.

NOTE 1 – Les procédures décrites ici se rapportent essentiellement au traitement d'un message unique. Une telle démarche est suffisante à tous égards sauf un: la mise en file d'attente des messages et la priorité relative de l'appel aux procédures sont commandées explicitement par l'argument **priority** (priorité) dans le cas d'un message entrant par l'accès de dépôt submission-port ou de transfert transfer-port, ou implicitement (priorité urgente) dans le cas d'un rapport ou d'un envoi-test produit en interne ou entrant par l'accès de transfert transfer-port.

NOTE 2 – Un agent MTA peut spécifier plusieurs fenêtres temporelles de remise par défaut pour chacune des priorités de message [par exemple les valeurs définies dans les Recommandations de la série F.400]. Le système MTS, et donc chaque agent MTA impliqué dans le traitement, doivent tenir compte de ces valeurs au cours du traitement du message. Par exemple, l'agent MTA peut appliquer une heure limite de remise. Si cette période expire avant la remise, l'agent MTA produit un rapport de non-remise non-delivery-report et supprime le message. Les mesures requises dans ce cas sont les mêmes que pour le cas où l'heure limite de remise **latest-delivery-time** est écoulée.

NOTE 3 – En raison de sa complexité, l'information de trace trace-information n'est pas abordée exhaustivement. Certains détails importants sont explicités, mais le traitement complet et exhaustif de l'information de trace est donné au § 12.3.1.

NOTE 4 – La Rec. UIT-T X.412 | ISO/CEI 10021-10 spécifie un certain nombre d'ajouts et de modifications aux procédures décrites dans la présente Définition de service, qui s'appliquent aux agents MTA prétendant à conformité avec la Rec. UIT-T X.412 | ISO/CEI 10021-10.

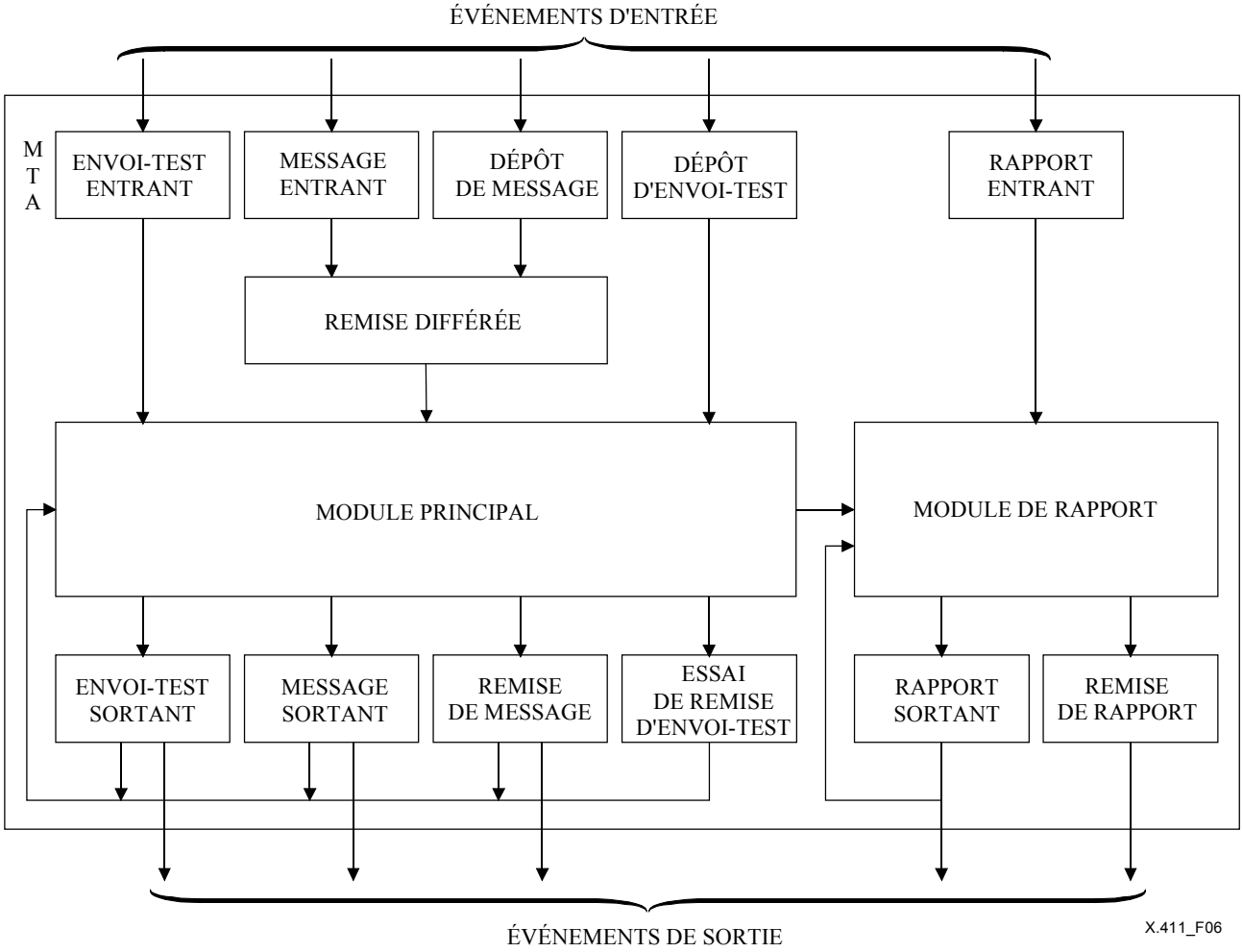


Figure 6 – Relations entre modules internes et externes

14.2 Module de remise différée

Ce module fournit l'élément de service de remise différée Deferred Delivery. Il est appelé par les modules de dépôt de message et de message entrant, qui lui transmettent un message pour vérifier s'il comporte une demande de remise différée et le retenir si nécessaire. Il appelle le module principal en transmettant le message lorsque sa procédure interne unique est achevée.

14.2.1 Procédure de remise différée Deferred-delivery

14.2.1.1 Arguments

Message à vérifier afin de déterminer s'il comporte une demande de remise différée et afin de le retenir si nécessaire.

14.2.1.2 Résultats

La procédure envoie en retour le message. En cas de remise différée, le message est accompagné d'une estampille d'heure d'arrivée.

14.2.1.3 Erreurs

Le message avec les instructions détaillant le problème rencontré.

14.2.1.4 Description de la procédure

1) Un champ d'heure de remise différée **deferred-delivery-time** est recherché dans le message. S'il n'y en a pas, le message est retourné et la procédure prend fin. S'il est présent, l'heure de remise différée **deferred-delivery-time** est comparée au temps courant. Si cette heure de remise différée est passée, la procédure envoie en retour le message après suppression du champ d'heure de remise différée, puis elle prend fin.
2) Cette étape ne s'applique qu'à un message provenant du module de message entrant. L'agent MTA vérifie s'il existe un accord bilatéral lui imposant d'assurer le service de remise différée pour ce message. Si un tel accord existe, la procédure se poursuit à l'étape 3. Sinon, une des deux opérations suivantes est exécutée:
   a) le message est envoyé en retour sans être différé et la procédure prend fin;
   b) la procédure envoie en retour le message avec une instruction de production de rapport portant le code de motif de non-remise **deferred-delivery-not-performed** (remise différée non exécutée) et le code diagnostic de non-remise **no-bilateral-agreement** (pas d'accord bilatéral), puis elle prend fin.
3) Selon la politique choisie, une des opérations suivantes est exécutée:
   a) s'il existe un accord bilatéral avec le ou les domaines ou l'agent ou les agents MTA vers lesquels le message doit être transféré, stipulant que ces domaines ou agents MTA vont prendre la responsabilité de la remise différée, alors la procédure envoie en retour le message sans le différer, puis elle prend fin;
   b) le temps courant est noté comme étant le temps d'arrivée du message et celui-ci est retenu jusqu'à l'heure de remise différée **deferred-delivery-time**; la procédure envoie en retour alors le message accompagné de l'estampille d'heure d'arrivée après avoir supprimé le champ d'heure de remise différée, puis elle prend fin.

NOTE – Il est nécessaire de supprimer le champ d'heure de remise différée une fois l'ajournement réalisé, de manière à éviter tout risque de non-remise (voir l'étape 2 b) lors du transfert du message à un autre domaine en cas de désynchronisation des horloges.

14.3 Module principal

Le module principal assure l'essentiel du traitement des messages et des envois-tests qui entrent dans l'agent MTA. La Figure 6 montre les relations existant entre le module principal et les modules qu'il peut appeler ou qui peuvent l'appeler. Le module principal peut être appelé par:

1) le module d'envoi-test entrant, qui transmet un envoi-test;
2) le module de remise différée, qui transmet un message;
3) le module de dépôt d'envoi-test, qui transmet un envoi-test.

Dans le cas d'une situation d'erreur ou si un rapport de remise avec succès est nécessaire, le module principal peut également être appelé par:

4) le module de message sortant, qui transmet un message avec une instruction par message indiquant le problème rencontré;
5) le module d'envoi-test sortant, qui transmet un envoi-test avec une instruction par message indiquant le problème rencontré;
6) le module de remise de message qui transmet un message avec des instructions par destinataire indiquant le ou les problèmes rencontrés ou le ou les succès obtenus;

7) le module d'essai de remise d'envoi-test, qui transmet un envoi-test avec des instructions par destinataire indiquant le ou les problèmes rencontrés ou le ou les succès obtenus;

8) le module de remise différée, qui transmet un message avec des instructions indiquant le problème rencontré.

Le module principal contient des procédures qui prennent en charge collectivement les fonctions suivantes:

traitement de trace;

détection de boucle;

acheminement et réacheminement;

renvoi au destinataire;

conversion de contenu;

développement de la liste de distribution;

duplication des messages;

authentification d'origine des messages et des envois-tests;

résolution de nom.

Les procédures qui assurent ces fonctions sont appelées par une procédure de commande unique qui guide le traitement de chaque message ou envoi-test reçu par le module principal. La Figure 7 montre l'organisation des procédures de commande et des procédures subsidiaires à l'intérieur du module principal; la Figure 8 montre le flux d'information à l'intérieur de ces procédures.

Pour chaque message ou envoi-test reçu, le module principal appelle la procédure de commande avec ce message ou envoi-test en argument. La procédure de commande retourne alors un ou plusieurs duplicata de ce message ou envoi-test assortis des instructions appropriées. Selon la nature de ces instructions, le module principal appelle alors:

1) le module de message sortant, auquel il transmet chaque message avec une instruction de transfert par message;

2) le module d'envoi-test sortant, auquel il transmet chaque envoi-test avec une instruction de transfert par message;

3) le module de remise de message, auquel il transmet chaque message avec une ou plusieurs instructions de remise par destinataire;

4) le module d'essai de remise d'envoi-test, auquel il transmet chaque envoi-test avec une ou plusieurs instructions de remise par destinataire;

5) le module de rapport, auquel il transmet chaque message ou envoi-test avec une instruction par message et/ou une ou plusieurs instructions par destinataire relatives à la production de rapport.

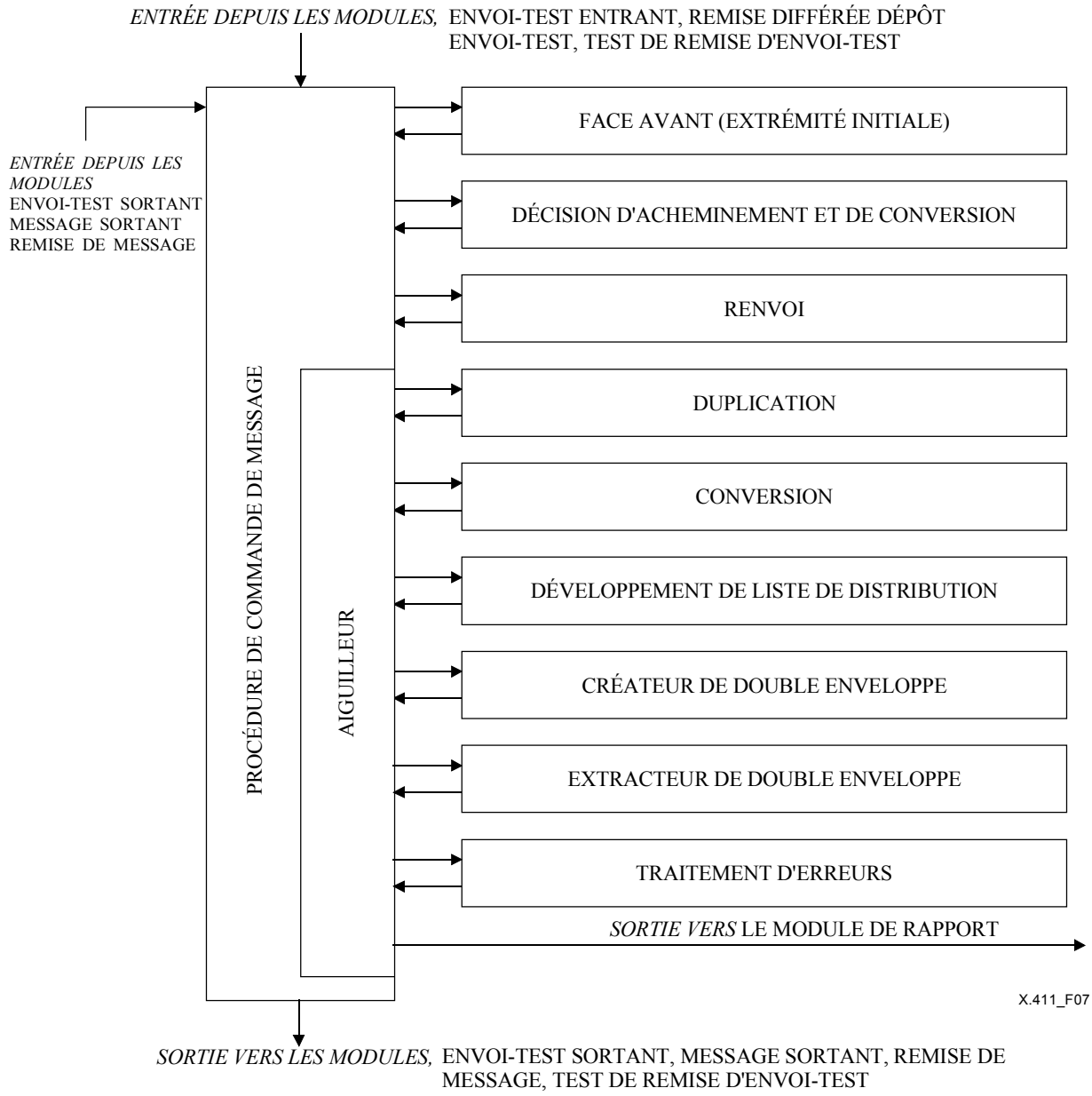
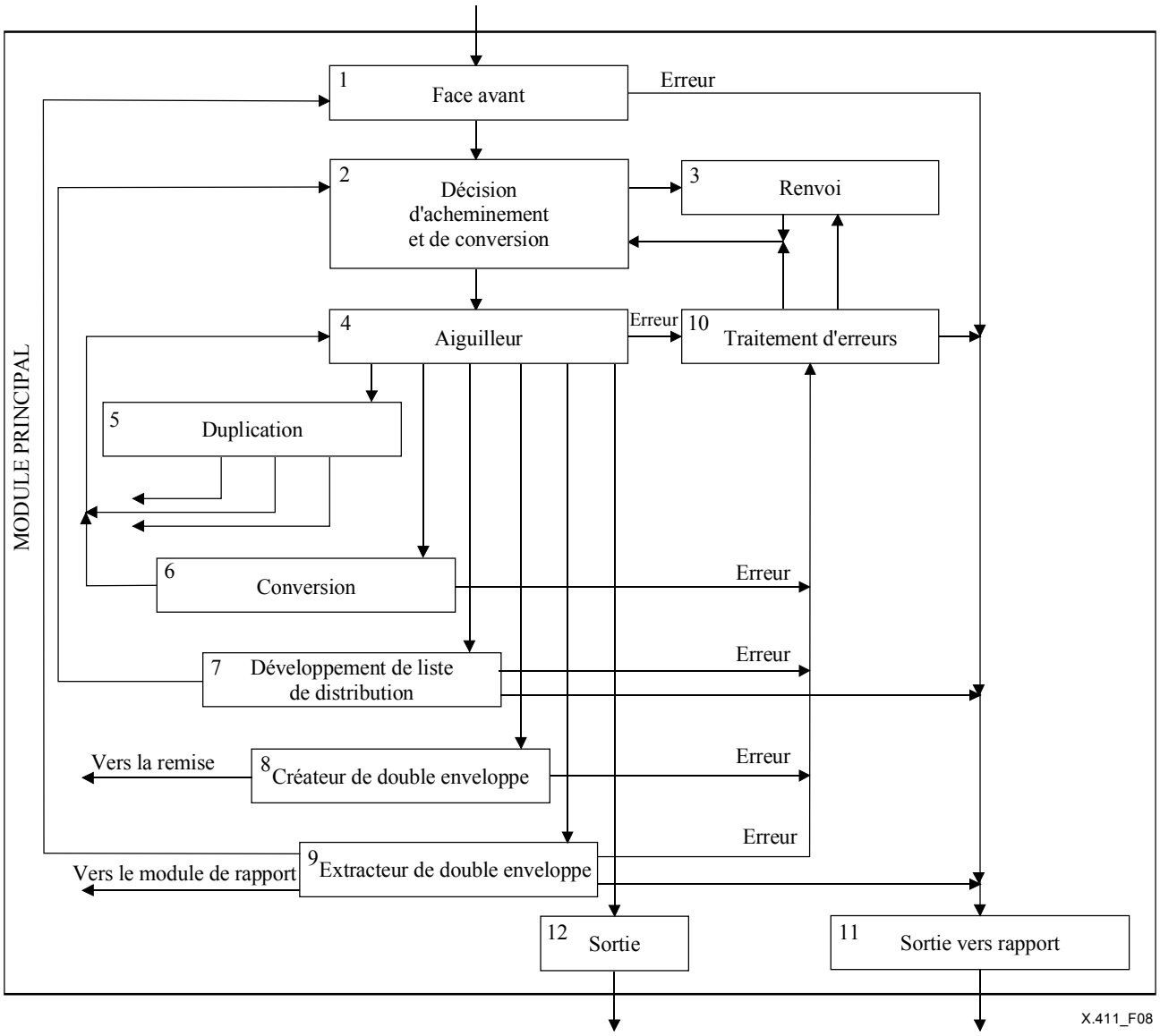


Figure 7 – Organisation des procédures à l'intérieur du module principal



NOTE – Les numéros indiqués dans cette figure se rapportent aux numéros d'étapes de la logique des procédures de commande (voir § 14.3.1.4).

Figure 8 – Flux d'information à l'intérieur du module principal

14.3.1 Procédure de commande (Control)

Cette procédure oriente tout message ou envoi-test entrant à travers les autres procédures du module principal. Le flux général d'informations est représenté à la Figure 8.

14.3.1.1 Arguments

L'un des arguments suivants (ces arguments correspondent aux messages et envois-tests qui peuvent être transmis au module principal sur appel):

1) un envoi-test sans instructions (issu du module d'envoi-test entrant ou de dépôt d'envoi-test);
2) un message sans instructions mais avec l'estampille facultative d'heure d'arrivée (issue du module de remise différée);
3) un message ou envoi-test avec une instruction par message décrivant un problème de transfert (issu d'un module de message sortant ou d'envoi-test sortant);
4) un message ou envoi-test avec instructions par destinataire décrivant les problèmes ou les succès de remise (en provenance d'un module de remise de message ou d'essai de remise d'envoi-test).

14.3.1.2 Résultats

1) un ou plusieurs duplicata de l'argument de message ou d'envoi-test, accompagnés chacun par une instruction par message indiquant le transfert;
2) un ou plusieurs duplicata de l'argument de message ou d'envoi-test, accompagnés chacun d'une ou plusieurs instructions par destinataire indiquant la remise ou le test de remise;
3) un ou plusieurs duplicata de l'argument de message ou d'envoi-test, accompagnés chacun d'une ou plusieurs instructions par destinataire indiquant la production de rapport.

14.3.1.3 Erreurs

Aucune. Il est tenu compte des situations d'erreurs dans les résultats décrits ci-dessus.

14.3.1.4 Description de la procédure

1) Message ou envoi-test sans instructions:

   On appelle d'abord la procédure de face-avant (Front-end) pour effectuer une initialisation de trace et quelques vérifications par message telles que l'expiration d'un message et la détection de boucle d'acheminement.

   Si en retour la procédure envoie une instruction de rapport signalant un problème avec le message, le traitement se poursuit à l'étape 11.

   Dans tous les autres cas de retour, le traitement se poursuit à l'étape ci-dessous.

2) La procédure de décision d'acheminement et de conversion (Routing-and-conversion-decision) est appelée pour calculer les instructions d'acheminement et de conversion pour chaque destinataire. (Il s'agit d'instructions complètes destinées à orienter le message ou l'envoi-test à travers les procédures restantes.)

   Si une instruction de réacheminement apparaît [par exemple, destinataire suppléant désigné par le destinataire (**recipient-assigned-alternate-recipient**)], le traitement se poursuit à l'étape 3.

   Sinon, le traitement se poursuit à l'étape 4 (aiguilleur).

3) La procédure de réacheminement (Redirection) est appelée. Dans le cas d'un retour avec succès, le traitement se poursuit à l'étape 2.

   Dans le cas d'un retour avec échec, le traitement se poursuit à l'étape 10 (procédure de traitement d'erreurs, Error-handler).

4) Aiguilleur (Dispatcher): l'aiguilleur agit sur les instructions produites et passe le contrôle à la première procédure applicable parmi les suivantes:
   - duplication (Splitter) (étape 5);
   - conversion (étape 6);
   - développement de liste (Distribution-list-expansion) (étape 7);
   - double enveloppement (étape 8);
   - extraction de double enveloppe (étape 9);
   - traitement d'erreurs (étape 10) dans le cas où le processus de décision se heurte à un problème, par exemple une erreur d'acheminement;
   - sortie (étape 12).

5) La procédure de duplication (Splitter) est appelée lorsqu'une duplication est indiquée par les instructions produites pour chaque destinataire dans la procédure de décision d'acheminement et de conversion (Routing-and-conversion-decision). Le traitement se poursuit alors séparément pour chaque duplicata à l'étape 4 (aiguilleur).

6) La procédure de conversion est appelée pour chaque message ou envoi-test nécessitant une conversion.

   Dès retour avec succès du message ou de l'envoi-test, le traitement se poursuit à l'étape 4 (aiguilleur).

   Dès retour avec une mention de rapport signalant une erreur de conversion, le traitement se poursuit à l'étape 10 (procédure de traitement d'erreurs).

7) La procédure de développement de liste (DL-expansion) est appelée.

   Dès retour du message avec succès, le traitement se poursuit à l'étape 2 de manière à appliquer au message le traitement correspondant à chacun des destinataires membres de cette liste.

   Si une copie du message accompagnée d'instructions de rapport de remise est retournée à la place ou en plus du retour mentionné ci-dessus, le traitement dudit message se poursuit à l'étape 11.

   Un envoi-test retourné avec succès sera accompagné d'instructions de rapport; le traitement se poursuit alors à l'étape 11 (production de rapport Report-generation).

Lors de l'envoi en retour d'un message ou d'un envoi-test accompagné d'une instruction de rapport indiquant un problème de développement de liste de distribution, le traitement d'erreurs se poursuit à l'étape 10.

8) La procédure de création de double enveloppe est appelée si l'instruction de routage exige que le message soit imbriqué dans un type de contenu à enveloppe interne (**inner-envelope content-type**).

   Dès retour avec succès, la procédure se termine car l'agent MTA n'a plus d'autre traitement à effectuer sur le message original.

   Dès retour sans succès, le traitement se poursuit à l'étape 10 (traitement d'erreur).

9) La procédure d'extraction de double enveloppe est appelée si l'instruction de routage vise à extraire l'enveloppe interne du contenu (**content**).

   Dès retour avec succès d'un message ou d'un envoi-test extrait, le traitement du message ou envoi-test extrait reprend à l'étape 1. Dès retour avec succès d'un rapport extrait, le traitement de ce rapport se poursuit comme spécifié au § 14.4.1. Par ailleurs, le traitement des instructions de rapport au sujet du message original se poursuit dans chaque cas à l'étape 11.

   Dès retour sans succès, le traitement se poursuit à l'étape 10 (traitement d'erreur).

10) C'est le point de rassemblement qu'atteint le traitement lorsqu'il constate qu'un message ou un envoi-test ne peut pas être traité par les procédures de la ligne de traitement principale. La procédure de traitement d'erreurs (Error-processing) est appelée pour rechercher une autre méthode de remise ou un destinataire suppléant. Dans un retour avec succès, la procédure de traitement d'erreurs (Error-processing) indique le nouveau destinataire dans une instruction à la procédure de décision d'acheminement et de conversion (Routing-and-conversion-decision procedure) (étape 2), à laquelle le traitement se poursuit.

    Si un réacheminement s'avère impossible, le message ou l'envoi-test est transmis au générateur de rapport étape 11.

11) La procédure de commande prend fin à ce stade et renvoie un message ou un envoi-test avec des instructions de production de rapport.

12) Lorsqu'un message ou un envoi-test atteint ce stade, la procédure de commande prend fin.

14.3.2 Procédure de face-avant (Front-end)

Cette procédure effectue l'initialisation de trace, la détection d'expiration de message, la vérification de sécurité initiale, la détection de boucles et la vérification de criticité.

14.3.2.1 Arguments

Le message ou l'envoi-test plus une estampille facultative de l'heure d'arrivée.

14.3.2.2 Résultats

Le message ou l'envoi-test, assorti d'une information de trace initialisée pour cet agent MTA.

14.3.2.3 Erreurs

Le message ou l'envoi-test, assorti d'instructions de production de rapport détaillant le problème rencontré.

14.3.2.4 Description de la procédure

1) Si le message a franchi une limite de domaine, un élément d'information de trace **trace-information-element** pour ce domaine est ajouté avec **relay** (relais) comme indication d'action. Si le message est accompagné d'un temps d'arrivée, c'est qu'il y a eu remise différée; l'heure différée **deferred-time** est donc réglée sur le temps courant et l'heure d'arrivée **arrival-time** est réglée sur la valeur de l'estampille de l'heure qui accompagne le message. Sinon, il n'y a pas eu de remise différée et l'heure d'arrivée **arrival-time** est réglée sur le temps courant. Un élément d'information de trace interne **internal-trace-information-element** est également ajouté, que le message ait franchi ou non une limite de domaine.

2) Si la politique de sécurité en vigueur l'exige ou si le contrôle d'authentification d'origine de message **message-origin-authentication-check** est incorrect, la procédure renvoie une instruction de production de rapport. Les valeurs du code de motif de non-remise **non-delivery-reason-code** et du code de diagnostic de non-remise **non-delivery-diagnostic-code** sont fixées respectivement à **unable-to-transfer** (impossibilité de transfert) et à **secure-messaging-error** (erreur de sécurité de messagerie).

3) Si l'un quelconque des champs d'extension propres à chaque message, ou des champs d'extension propres à des destinataires pour lesquels l'argument **responsibility** (responsabilité) a la valeur **responsible** (responsable), porte la mention **critical-for-transfer** (critique pour le transfert) mais n'est pas sémantiquement compris par l'agent MTA, la procédure renvoie pour ces destinataires une instruction de production de rapport. Si les instructions de production de rapport ont été produites pour certains destinataires (mais pas pour tous) pour lesquels l'argument responsabilité **responsibility** a la valeur **responsible**, alors une instruction de duplication du message est renvoyée. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **unsupported-critical-function** (fonction critique non prise en charge). La procédure prend alors fin.

   NOTE – Les implémentations plus anciennes peuvent utiliser une autre valeur de code de motif de non-remise spécifiée dans une édition antérieure de la présente Définition de service.

4) Si l'heure limite de remise **latest-delivery-time** a expiré ou si le délai maximal de transit du système a été dépassé pour la **priority** (priorité) du message, la procédure renvoie une instruction de production de rapport. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **transfer-failure** (échec de transfert) ou à **unable-to-transfer** (impossibilité de transfert) selon le cas, et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **maximum-time-expired** (expiration du délai maximal). La procédure prend alors fin.

5) Une détection de boucle est effectuée. L'algorithme de détection de boucle sort du cadre de la présente Définition de service. On trouvera cependant au § 14.3.11 un exemple d'algorithme combiné d'acheminement et de détection de boucle. Si une boucle est détectée, la procédure renvoie une instruction de production de rapport. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **transfer-failure** (échec de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **loop-detected** (bouclage). La procédure prend alors fin.

6) Suivant la politique adoptée, l'agent MTA peut s'assurer au moment du dépôt que la valeur de l'argument de type de notification **notification-type** correspond bien au contenu. Si l'agent MTA n'effectue pas cette vérification, ou si le type de notification indiqué correspond bien au contenu, la procédure prend alors fin avec succès. Si l'agent MTA vérifie la valeur du type de notification et si cette valeur ne correspond pas au contenu, une des dispositions suivantes est prise en fonction de la politique choisie:

   a) la contradiction est ignorée et la procédure prend fin avec succès;

   b) si le type de notification **notification-type** n'a pas l'une des valeurs type-1, type-2 ou type-3, la valeur correcte lui est affectée et la procédure prend fin;

   c) si le type de notification **notification-type** est mis incorrectement à l'une des valeurs type-1, type-2 ou type-3, la procédure renvoie une instruction de production de rapport avec le code de motif de non-remise **non-delivery-reason-code** fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **incorrect-notification-type** (type de notification incorrecte). Puis la procédure prend fin.

L'agent MTA peut vérifier les messages de service **service-message** par des procédures similaires.

14.3.3 Procédure de décision d'acheminement et de conversion (routing-and-conversion-decision)

Pour chaque destinataire d'un message ou d'un envoi-test dont l'agent MTA est responsable, cette procédure détermine les actions d'acheminement et de conversion éventuelles que doit effectuer cet agent MTA. Ces actions sont enregistrées comme instructions par destinataire associées au message. Elles sont ensuite exécutées par d'autres sous-procédures au sein de la procédure interne, ou ailleurs dans l'agent MTA.

NOTE – Cette procédure peut être appelée plusieurs fois pour un même message. En pareil cas, la procédure ignore les instructions par destinataire produites par des appels antérieurs à cette procédure et qui n'auraient pas encore été traitées ailleurs.

14.3.3.1 Arguments

1) Un message ou un envoi-test dont l'argument **responsibility** (responsabilité) a la valeur **responsible** (responsable) pour les destinataires intéressant cet agent MTA.

14.3.3.2 Résultats

Le message ou l'envoi-test formant l'argument de la procédure, plus les instructions nouvelles ou révisées par destinataire, indiquant les actions d'acheminement et d'éventuelle conversion que doit effectuer cet agent MTA.

14.3.3.3 Erreurs

Aucune. Les situations d'erreur éventuelles sont notées dans les instructions par destinataire.

14.3.3.4 Description de la procédure

Chaque destinataire est pris en considération à tour de rôle. Si l'argument de responsabilité **responsibility** a la valeur **not-responsible** (non responsable), le destinataire est ignoré. Sinon, les procédures de décision d'acheminement Routing-decision et de décision de conversion Conversion-decision sont appelées à tour de rôle pour ce destinataire. Lorsque tous les destinataires ont été pris en considération de cette manière, la procédure prend fin. Voir Figure 9.

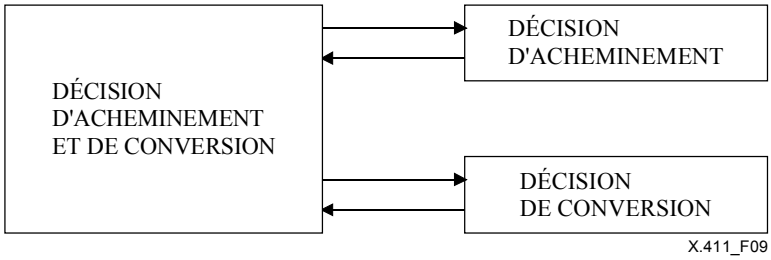


Figure 9 – Organisation des sous-procédures de la procédure de décision d'acheminement et de conversion

14.3.4 Procédure de décision d'acheminement Routing-decision

Cette procédure produit une instruction d'acheminement pour un destinataire unique de message.

14.3.4.1 Arguments

1) Un destinataire de message, plus l'éventuelle instruction par destinataire qui lui est applicable.
2) L'instruction éventuelle par message, applicable à ce message. Les autres champs de message sont également accessibles à la procédure selon les besoins.

14.3.4.2 Résultats

Une instruction d'acheminement nouvelle ou éventuellement révisée, applicable à ce destinataire. Les instructions possibles sont les suivantes:

a) relayer vers un autre agent MTA;
b) remettre à un destinataire local;
c) développer la liste de distribution représentée par ce destinataire;
d) produire un rapport indiquant un échec de remise. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** sont inclus dans l'instruction;
e) réacheminer vers une adresse préférée ou vers un destinataire suppléant désigné par le destinataire.

14.3.4.3 Erreurs

Aucune. Les situations d'erreur sont enregistrées dans l'instruction d'acheminement.

14.3.4.4 Description de la procédure

La procédure est décrite dans les étapes suivantes.

NOTE – Pour s'assurer que la politique de sécurité n'est pas enfreinte durant l'acheminement, il convient de vérifier l'adéquation de l'étiquette de sécurité de message **message-security-label** par rapport au contexte de sécurité **security-context**.

1) S'il existe une instruction par message indiquant l'échec d'un relais antérieur, la procédure s'efforce de calculer une destination de bond suivant de substitution pour ce destinataire. Le choix de l'algorithme d'acheminement sort du cadre de la présente Définition de service. Toutefois, on trouvera au § 14.3.11 un exemple d'algorithme applicable dans ce cas. En cas de succès, l'information de trace interne **internal-trace-information** du message est mise à jour avec comme mention d'action d'acheminement **rerouted** indiquant que le message a été réacheminé (voir § 12.3.1). Si le message est censé franchir une limite de domaine, l'information de trace **trace-information** est alors mise à jour en conséquence. La procédure renvoie une instruction de relais à la destination de remplacement et prend fin.

S'il n'existe aucun bond suivant de remplacement ou si tous les bonds suivants disponibles ont déjà été essayés en vain ou sont interdits, la procédure renvoie une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **transfer-failure** (échec de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à une valeur correspondant au type d'échec de relais subi. La procédure prend alors fin.

2) Si l'instruction par destinataire indique un échec de remise, alors la procédure renvoie une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** sont fournis par la procédure de remise de message *Message-delivery* ou d'essai de remise d'envoi-test *Probe-delivery-test*. La procédure prend alors fin.

3) Si le destinataire est spécifié par un nom **OR-name** qui ne contient qu'un nom d'annuaire **directory-name** (ce qui peut arriver après un développement de liste de distribution, si un membre de la liste n'est spécifié que par un nom d'annuaire), l'agent MTA tente de déterminer l'adresse **OR-address** à partir de l'annuaire. S'il n'y parvient pas, la procédure renvoie une instruction de production de rapport pour ce destinataire et prend fin. Le code de motif de non-remise **non-delivery-reason-code** prend la valeur **directory-operation-unsuccessful** (échec de recherche d'annuaire) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** peut prendre une valeur selon le problème rencontré.

   Dans tous les autres cas, les opérations suivantes sont effectuées.

4) Si l'adresse **OR-address** du destinataire spécifie de manière non ambiguë un destinataire effectif mais qui n'est pas une adresse préférée de ce destinataire, une instruction de réacheminement est produite avec le nom **OR-name** préféré du destinataire et avec pour motif de renvoi **alias**, et la procédure prend fin.

5) Si le destinataire est une liste de distribution pour laquelle l'agent MTA sert de point de développement, on examine alors l'argument d'interdiction de développement **DL-expansion-prohibited** du message. S'il contient la valeur **DL-expansion-allowed** (développement de liste autorisé), la procédure renvoie une instruction d'acheminement (sous réserve de la politique de sécurité en vigueur) afin de développer la liste. La procédure prend alors fin.

   Si la valeur est **DL-expansion-prohibited (**développement de liste interdit), ou si la politique de sécurité interdit l'utilisation d'une liste de distribution, la procédure renvoie une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **DL-expansion-prohibited** (développement de liste interdit). La procédure prend alors fin.

6) Si le nom **OR-name** du destinataire désigne un extracteur de double enveloppe dans cet agent MTA et si le type de contenu **content-type** du message est à enveloppe interne **inner-envelope**, la procédure renvoie une instruction de routage afin d'extraire l'enveloppe interne du contenu **content**. La procédure se termine ensuite.

7) Si le destinataire s'avère être local, c'est-à-dire s'il s'agit d'un utilisateur MTS pris en charge par cet agent MTA, les étapes suivantes sont effectuées:

   a) si l'adresse **OR-address** ne désigne pas sans équivoque un destinataire effectif, la procédure renvoie une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** à **unrecognized-OR-name** (nom d'OR inconnu) ou **ambiguous-OR-name** (nom d'OR ambigu), selon le cas. La procédure prend alors fin;

   b) si l'adresse **OR-address** désigne sans équivoque un destinataire local effectif, les paramètres d'enregistrement du destinataire sont examinés pour y déceler l'existence d'un réacheminement indiqué par le destinataire **recipient-assigned-redirections.** Lors de la recherche d'un destinataire suppléant, l'étiquette de sécurité d'utilisateur **user-security-label** doit être comparée à l'étiquette de sécurité de message **message-security-label** pour s'assurer que la politique de sécurité n'est pas enfreinte.

      Si un réacheminement indiqué par le destinataire a été enregistré pour ce destinataire, qu'un tel suppléant soit autorisé par le champ d'interdiction de réassignation de destinataire **recipient-reassignment-prohibited**, et si la politique de sécurité le permet, alors les arguments types d'information codée **encoded-information-types**, longueur du contenu **content-length**, type de contenu **content-type**, étiquettes de sécurité **message-security-labels**, priorité **priority**, nom d'expéditeur **originator-name**, chronologie de réacheminement **redirection-history** et chronologie de développement **DL-expansion-history** du message sont comparés tour à tour avec chaque classe de réacheminement **redirection-class** de destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient**, jusqu'à trouver une classe de réacheminement dont les valeurs spécifiées correspondent à celles du message. Si une telle classe est trouvée, le destinataire

suppléant associé forme le premier argument d'un appel à la procédure de réacheminement. Les autres arguments indiquent le destinataire remplacé, le message et le motif de réacheminement.

Si la procédure de réacheminement s'achève normalement, elle repasse la main à la procédure de décision d'acheminement *Routing Decision*. Si la procédure de réacheminement signale une erreur de bouclage, le contrôle est pris par la procédure de traitement d'erreur;

c) si le message n'a pas été réacheminé par une instruction **recipient-assigned-redirections**, et qu'une ou plusieurs classes de remise **deliverable-classes** aient été enregistrées, le système MTS déterminera si le message satisfait aux critères d'au moins une de ces classes et s'il peut donc être remis.

Pour chaque classe de remise, les types d'information codée du message sont comparés avec les contraintes de type **encoded-information-types-constraints** du destinataire, le type du contenu avec les types livrables **deliverable-content-types**, la longueur du contenu avec la longueur maximale livrable **deliverable-maximum-content-length**, et les étiquettes de sécurité avec les étiquettes livrables **deliverable-security-labels**.

La composante des contraintes de type **encoded-information-types-constraints** est utilisée avec le paramètre de types d'information **encoded-information-types** du message (les types convertis **converted-encoded-information-types** du dernier élément d'information de trace qui contient ce paramètre, sinon les types d'origine **original-encoded-information-types**) pour décider de la possibilité de remettre le message:

si aucun type d'information codée n'est spécifié dans le message, ou en l'absence de contraintes **encoded-information-types-constraints**, le message satisfait aux contraintes de type d'information codée de cette classe livrable;

sinon, et si des types inacceptables **unacceptable-encoded-information-types** ont été spécifiés et que le message contienne au moins l'un d'entre eux, le message ne satisfait pas aux contraintes de type d'information codée de la classe livrable;

sinon, et si des types acceptables **acceptable-encoded-information-types** ont été spécifiés, et que le message contienne au moins l'un d'entre eux, le message satisfait aux contraintes de type d'information codée de la classe livrable;

sinon, et si des types exclusivement acceptables **exclusively-acceptable-encoded-information-types** ont été spécifiés, et que le message contienne au moins un type qui n'appartient pas à cette liste, le message ne satisfait pas aux contraintes de type d'information codée de la classe livrable;

sinon, le message satisfait aux contraintes de type d'information codée de la classe livrable.

Le système MTS ne remettra le message que s'il satisfait aux contraintes d'au moins une des classes livrables enregistrées;

d) le paramètre d'enregistrement de remise restreinte **restricted-delivery** est utilisé pour décider si un message peut être remis:

si aucun paramètre de remise restreinte **restricted-delivery** n'est enregistré, le message peut être remis;

si une ou plusieurs restrictions **restriction** sont enregistrées, le nom d'expéditeur **originator-name**, le nom **OR-name** de chaque élément de la chronologie de développement de la liste de distribution **DL-expansion-history** et le nom **OR-name** de chaque élément de la chronologie de réacheminement **redirection-history** du message sont tour à tour comparés avec chaque **restriction** enregistrée (dont le paramètre **objects** a pour valeur **messages** ou **both**), jusqu'à coïncidence. Si la remise est permise par la restriction correspondante, le système renvoie une instruction de remise; sinon, il renvoie une instruction de production de rapport.

La procédure de comparaison des noms **OR-name** est décrite au § 12.4.4 pour la correspondance exacte et au § 12.4.5 de la Rec. UIT-T X.413 | ISO/CEI 10021-5 pour la correspondance par masque;

e) en l'absence de problème, la procédure de décision d'acheminement retourne une instruction de remise pour ce destinataire et prend fin.

S'il existe une contradiction entre le message et les paramètres d'enregistrement, la procédure retourne une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prend la valeur correspondant au problème rencontré. La procédure prend alors fin.

8) Si le destinataire n'est pas un destinataire local de l'agent MTA, les considérations de l'étape 6 relatives à la possibilité de remise peuvent être prises en compte. S'il n'en résulte aucune instruction, la procédure de décision d'acheminement s'efforce de déterminer une instruction de bond suivant (sous réserve de la politique de sécurité en vigueur) pour ce destinataire. En cas de succès, une instruction de relais pour le bond suivant est retournée et la procédure prend fin.

   Si la politique de sécurité spécifie qu'une double enveloppe est requise pour le prochain bond identifié et si le type de contenu **content-type** du message n'est pas à enveloppe interne **inner-envelope**, la procédure renvoie une instruction de routage afin d'imbriquer le message actuel dans le contenu **content** d'un nouveau message au moyen de la procédure spécifiée au § 14.3.13. La procédure se termine ensuite.

   Si le bond suivant ne peut pas être déterminé, la procédure envoie en retour une instruction de production de rapport pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** est fixé à **unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prend la valeur correspondant au problème rencontré. La procédure prend alors fin.

14.3.5 Procédure de décision de conversion Conversion-decision

Cette procédure produit une instruction de conversion pour un destinataire unique de message.

14.3.5.1 Arguments

1) Un destinataire de message ou d'envoi-test plus l'instruction éventuelle par destinataire applicable à ce destinataire.
2) D'autres champs de message sont également pris en considération par la procédure:
   a) types d'information codée **encoded-information-types** en cours, déduits de la dernière valeur du champ des types convertis d'information codée **converted-encoded-information-types** lorsqu'un tel champ existe dans l'information de trace **trace-information**, donnés sinon par le champ des types d'origine d'information codée **original-encoded-information-types**;
   b) interdiction de conversion implicite **implicit-conversion-prohibited**;
   c) interdiction de conversion avec perte **conversion-with-loss-prohibited**;
   d) conversion explicite **explicit-conversion**.

14.3.5.2 Résultats

1) une instruction de conversion de contenu applicable à ce destinataire, plus éventuellement:
2) une instruction d'acheminement révisée indiquant un transfert en sortie de message ou d'envoi-test vers un agent MTA capable d'effectuer la conversion requise ou, à la place des points 1 et 2 ci-dessus:
3) une instruction de production d'un rapport indiquant un échec de remise. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** sont inclus dans l'instruction.

14.3.5.3 Erreurs

Aucune. Les situations d'erreur sont prises en compte dans l'instruction d'acheminement.

14.3.5.4 Description de la procédure

NOTE – Les conditions dans lesquelles un agent MTA donné effectue une conversion pouvant faire l'objet d'une future normalisation, il n'est pas réaliste de décrire une procédure qui déterminerait les types d'information codée nécessaires en sortie de conversion. Ainsi, si la conversion est effectuée par un agent MTA intermédiaire, il n'existe pas de méthode normalisée permettant de déterminer les types d'information codée que peut traiter un utilisateur MTS. Il a donc été admis dans les points suivants que les types d'information codée de conversion étaient connus de l'agent MTA.

1) Si une conversion explicite est requise pour ce destinataire, la procédure commence à l'étape 6;
2) si une conversion implicite est nécessaire mais que le destinataire n'ait pas souscrit au service de conversion implicite, la procédure retourne une instruction de rapport négative avec le code de motif de non-remise **non-delivery-reason-code conversion-not-performed** (conversion non effectuée) et le code de diagnostic de non-remise **non-delivery-diagnostic-code implicit-conversion-not-subscribed** (non-abonnement à la conversion implicite). La procédure prend alors fin;
3) si la conversion requise est irréalisable, la procédure produit une instruction de rapport négative avec le code de motif de non-remise **non-delivery-reason-code conversion-not-performed** (conversion non effectuée) et le code de diagnostic de non-remise **non-delivery-diagnostic-code conversion-impractica**l (conversion impossible). La procédure prend alors fin;

4) si la conversion est requise mais interdite pour le message, la procédure produit une instruction de rapport négative avec le code de motif de non-remise **non-delivery-reason-code conversion-not-performed** (conversion non effectuée) et le code de diagnostic de non-remise **non-delivery-diagnostic-code conversion-prohibited** (conversion interdite). La procédure prend alors fin;

5) si la conversion requise peut entraîner une perte d'information et que le champ interdiction de conversion avec perte **conversion-with-loss-prohibited** ait la valeur **conversion-with-loss-prohibited** (conversion avec perte interdite), la procédure produit une instruction de rapport négative avec le code de motif de non-remise **non-delivery-reason-code conversion-not-performed** (conversion non effectuée) et l'un des codes de diagnostic de non-remise **non-delivery-diagnostic-codes** suivants, selon le cas:

   line-too-long (ligne trop longue);

   page-split (coupure de page);

   pictorial-symbol-loss (perte de symbole graphique);

   punctuation-symbol-loss (perte de symbole de ponctuation);

   alphabetical-character-loss (perte de caractère alphabétique);

   multiple-information-loss (perte d'information multiple).

   La procédure prend alors fin;

6) si la conversion requise ne peut être effectuée par cet agent MTA, et qu'un autre agent MTA est réputé pouvoir l'effectuer, aucune instruction de conversion n'est générée. L'instruction d'acheminement qui avait été générée antérieurement est modifiée en transfert sortant ou envoi-test sortant, avec une destination de bond suivant vers l'agent MTA en question. Il faut toutefois prendre garde à éviter un éventuel bouclage. La procédure prend alors fin;

7) si la conversion requise peut être effectuée par cet agent MTA, la procédure retourne une instruction pour effectuer la conversion et prend fin.

14.3.6 Procédure de traitement d'erreurs Error-processing

Lorsqu'une autre procédure rencontre une erreur de possibilité de remise ou d'acheminement, cette procédure est appelée pour déterminer si la remise ou l'acheminement peuvent être assurés par la désignation d'un nouveau destinataire ou par le choix d'une adresse **OR-address** différente pour le même destinataire. Sinon, la non-remise doit être signalée au module de rapport. Parmi les erreurs provoquant un appel dans le cadre de cette procédure, on peut citer:

- nom de destinataire **recipient-name** ne désignant pas un utilisateur MTS ou une liste de distribution DL;
- échec de remise;
- agent MTA incapable d'effectuer la conversion nécessaire;
- problèmes de trajet de transfert;
- problèmes de développement de liste DL;
- infractions à la sécurité;
- contradiction avec les paramètres d'enregistrement.

NOTE – Les mesures prises en traitement d'erreur seront sujettes à la politique de sécurité en vigueur.

14.3.6.1 Arguments

1) un message ou envoi-test, avec les champs par destinataire à l'origine du problème;
2) instructions de rapport indiquant l'erreur.

14.3.6.2 Résultats

Le message ou l'envoi-test en question, avec un champ de nom de destinataire **recipient-name** actualisé;

1) le message ou l'envoi-test en question;
2) instructions de rapport.

14.3.6.3 Erreurs

Aucune.

14.3.6.4 Description de procédure

NOTE – Cette procédure peut être appelée à de multiples reprises pour un même destinataire. Toutes les possiblités seront éventuellement explorées et l'étape 5 sera exécutée pour présenter un rapport d'échec.

1) Les arguments sont examinés à la recherche d'un nom d'annuaire **directory-name**. Si un tel nom est trouvé, la procédure de résolution de nom d'annuaire (voir § 14.3.12) est lancée pour déterminer une nouvelle adresse **OR-address**. Si celle-ci est différente de l'adresse originale, elle est combinée avec le nom d'annuaire **directory-name** pour former le nom **OR-name** d'un destinataire suppléant. La procédure de réacheminement (Redirection) est alors appelée pour réacheminer le message vers ce destinataire, avec comme motif de réacheminement **directory-look-up** (recherche par l'annuaire).

2) Sinon, la procédure détermine si un destinataire suppléant demandé par l'expéditeur **originator-requested-alternate-recipient** a été spécifié pour le destinataire en question. Si tel est le cas et si ce suppléant est différent du nom du destinataire actuel **recipient-name**, la procédure de réacheminement (Redirection) est appelée avec pour arguments le message et les champs pertinents renseignés. Après retour avec succès de la procédure de réacheminement, la procédure de traitement d'erreurs prend fin, le message réacheminé étant retourné en guise de résultat.

3) Sinon, la procédure vérifie s'il existe une erreur de remise, et si oui, elle vérifie la cause de l'erreur en examinant le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code**. Si l'adresse **OR-address** du destinataire n'identifiait pas un utilisateur MTS ou une liste de distribution, les indicateurs propres au message **per-message-indicators** sont examinés à la recherche d'un argument d'autorisation de destinataire suppléant **alternate-recipient-allowed**. Si la valeur constatée est **alternate-recipient-allowed** (destinataire suppléant autorisé), et que l'agent MTA ait été configuré pour cette classe de destinataire avec un destinataire suppléant différent du destinataire actuel, la procédure de réacheminement (Redirection) est appelée pour réacheminer le message vers le destinataire suppléant. Dès retour avec succès de la procédure de réacheminement, la procédure de traitement d'erreurs prend fin, renvoyant comme résultat le message à présent réacheminé.

4) Le traitement des erreurs qui peuvent être résolues mais qui ne sont pas imputables à des problèmes d'adressage est du ressort local, par exemple l'acheminement vers un autre agent MTA à l'intérieur du domaine pour cause de problèmes de conversion.

5) Si l'erreur de remise est d'un type autre que cité ci-dessus, ou si la valeur de l'argument d'autorisation de destinataire suppléant **alternate-recipient-allowed** est **alternate-recipient-prohibited** (destinataire suppléant interdit), ou s'il n'existe pas de destinataire suppléant adéquat spécifié par le domaine de gestion, la procédure retourne une instruction de rapport et prend fin.

14.3.7 Procédure de réacheminement (redirection)

Cette procédure réachemine un message.

NOTE – L'utilisation de services de réacheminement doit être assujettie à la politique de sécurité en vigueur.

14.3.7.1 Arguments

1) Le nom **OR-name** du destinataire suppléant vers lequel le message doit être réacheminé.

2) Les champs de message propres à chaque destinataire pour le destinataire devant être remplacés par un suppléant.

3) Le message ou l'envoi-test à réacheminer.

4) Le motif du réacheminement.

14.3.7.2 Résultats

Le message ou l'envoi-test fourni dans le troisième argument après remplacement du destinataire identifié dans le deuxième argument par le destinataire suppléant spécifié dans le premier argument.

14.3.7.3 Erreurs

Indication selon laquelle une boucle de réacheminement a été détectée.

14.3.7.4 Description de la procédure

1) La procédure veille en premier lieu à ce que le réacheminement vers le destinataire suppléant spécifié ne provoque pas une boucle de réacheminement. L'adresse **OR-address** du destinataire suppléant fourni dans l'argument 1 est comparée avec chaque nom de destinataire prévu **intended-recipient-name** à partir de la séquence de l'historique de réacheminement **redirection-history** des champs par destinataires identifiés dans l'argument 2. Lorsqu'il y a concordance, la procédure prend fin en indiquant qu'une boucle de réacheminement a été détectée.

2) Un élément est joint à l'historique du réacheminement **redirection-history** (qui est créé s'il n'existe pas déjà), en utilisant le nom de destinataire **recipient-name** de l'argument 2 pour former le nom de destinataire prévu **intended-recipient-name**, en déduisant le motif de réacheminement **redirection-reason** de l'argument 4 et en indiquant l'heure à laquelle ce réacheminement est effectué. Le nom **OR-name** fourni dans le premier argument est alors remplacé par le nom de destinataire **recipient-name**.

3) Si l'opération de liste DL **dl-operation** n'est pas déjà indiquée dans le champ des autres actions **other-actions** de l'information de trace **trace-information** et de trace interne **internal-trace-information** courantes, la valeur **redirected** (réacheminé) y est inscrite. Sinon, de nouveaux éléments d'information de trace et d'information de trace interne (**trace-information** and **internal-trace-information**) sont créés avec la valeur **redirected** (réacheminé).

4) L'enveloppe de transfert du message est actualisée comme suit:

recipient-name: (nom de destinataire)	remplacé
trace-information/**internal-trace-information**: (information de trace/de trace interne)	indication **redirected** (réacheminé)
redirection-history: (chronologie de réacheminement)	ajouter le nom de destinataire **recipient-name** et le motif de réacheminement **redirection-reason** précédents
originator-requested-alternate-recipient: (destinataire suppléant demandé par l'expéditeur)	supprimé si, et seulement si, le motif de réacheminement indique **originator-requested-alternate-recipient** (destinataire suppléant demandé par l'expéditeur).

14.3.8 Procédure de duplication (splitter)

Cette procédure reproduit les messages et les envois-tests selon les besoins pour le traitement ultérieur. Les arguments des duplicata sont modifiés afin d'indiquer les nouvelles valeurs de responsabilité **responsibility** pour les divers destinataires. Chaque duplicata est accompagné d'une instruction par message indiquant son traitement ultérieur au sein de l'agent MTA.

NOTE – L'utilisation des moyens de duplication est sujette à la politique de sécurité en vigueur.

14.3.8.1 Arguments

Un message ou un envoi-test. Pour chaque destinataire dont l'argument responsabilité **responsibility** a pour valeur **responsible** (responsable), une instruction d'acheminement et de conversion par destinataire accompagne le message.

14.3.8.2 Résultats

Un ou plusieurs duplicata du message ou de l'envoi-test original, avec indication appropriée de responsabilité **responsibility**, et une instruction par message indiquant le traitement ultérieur du duplicata à l'intérieur de l'agent MTA.

14.3.8.3 Erreurs

Aucune.

14.3.8.4 Description de la procédure

Le duplicateur (splitter) examine les instructions produites par la procédure de décision d'acheminement et de conversion Routing-and-conversion-decision afin de trier (conceptuellement) par groupes les destinataires ayant **responsible** (responsable) comme valeur d'argument de responsabilité **responsibility**. Un duplicata est créé pour chaque groupe. Le traitement ultérieur de ce duplicata (par d'autres procédures) dépend des instructions d'acheminement et de conversion applicables au groupe concerné.

NOTE 1 – La duplication du message est nécessaire dans l'agent MTA en raison des possibles différences de traitement suivant les destinataires. Ces différences proviennent de la nécessaire multiplicité des trajets d'acheminement sortant d'un agent MTA, de la nécessaire multiplicité de conversion du contenu de message, et du développement nécessaire des listes de distribution. Lorsqu'il existe par exemple plus d'un trajet d'acheminement, un duplicata distinct doit être créé pour chaque trajet, avec les valeurs appropriées de responsabilité **responsibility** pour chacun des destinataires situés sur ce trajet.

NOTE 2 – La détermination des duplicata nécessaires est du ressort local et entreprise de manière à minimiser leur nombre total. L'approche décrite dans les paragraphes suivants n'est qu'une suggestion qui n'a aucun caractère obligatoire ou contraignant pour une réalisation effective.

NOTE 3 – Pour simplifier l'exposé, le système de duplication (Splitter) est décrit comme un algorithme monopasse. Autrement dit, tous les duplicata nécessaires sont créés préalablement à tout autre traitement. Une optimisation importante serait d'effectuer une duplication minimale aux fins de conversion, puis de compléter la reproduction nécessaire des duplicata convertis.

1) La procédure prend d'abord en considération les destinataires pour lesquels existent des instructions de conversion de contenu. Ces destinataires sont regroupés par type de conversion requise. Un duplicata est créé pour chacun de ces groupes avec un argument de responsabilité (**responsibility**) ayant la valeur **responsible** (responsable) pour les destinataires de ce groupe, et **not-responsible** (non responsable) pour tous les autres.

2) On recherche alors parmi les destinataires ceux pour lesquels existent des instructions de développement de liste DL. Un duplicata est créé pour chaque liste de distribution destinataire avec un argument de responsabilité (**responsibility**) ayant la valeur **not-responsible** (non responsable) pour tous les destinataires, sauf la liste DL pour laquelle le duplicata a été réalisé.

3) Les groupes sont encore subdivisés en fonction des instructions d'acheminement par destinataire pour les procédures de transfert sortant (Transfer-out) ou d'envoi-test sortant (Probe-out). Ces destinataires sont regroupés de telle manière que chaque groupe ayant une même destination de bond suivant. Un duplicata est créé pour chaque groupe ayant une valeur d'argument de responsabilité (**responsibility**) égale à **responsible** (responsable) pour les destinataires de ce groupe, et **not-responsible** (non responsable) pour tous les autres. Pour tous les destinataires du groupe, il s'agira soit de la première tentative de transfert ou d'une tentative de réacheminement. Dans ce dernier cas, l'information de trace (trace-information) du message ou de l'envoi-test est modifiée de manière à indiquer qu'il s'agit d'un premier réacheminement ou d'un réacheminement ultérieur.

4) Enfin, les instructions d'acheminement de certains destinataires feront appel à la procédure de remise de message (Message-delivery) ou de production de rapport (Report-generation). Un duplicata est créé pour chacun de ces sous-groupes avec une valeur d'argument de responsabilité (**responsibility**) égale à **responsible** (responsable) pour les destinataires de ce groupe et **not-responsible** (non responsable) pour tous les autres.

5) Si la divulgation d'autres destinataires (**disclosure-of-other-recipients**) n'est pas demandée, les indications relatives aux destinataires dont la valeur d'argument de responsabilité est **not-responsible** (non responsable) pourront être supprimées.

6) Tout développement se faisant pour un destinataire dont l'argument de **responsibilité** a pour valeur **not-responsible** (non responsable) peut être supprimé.

7) La procédure prend alors fin.

14.3.9 Procédure de conversion

Cette procédure convertit les messages et indique pour les envois-tests les conversions qui auraient eu lieu.

14.3.9.1 Arguments

Un message ou un envoi-test avec indication de la ou des conversions requises.

14.3.9.2 Résultats

Le message ou l'envoi-test avec les conversions effectuées et signalées (seulement signalées dans le cas d'un envoi-test).

14.3.9.3 Erreurs

Le message ou l'envoi-test avec les instructions de rapport détaillant le problème de conversion rencontré.

14.3.9.4 Description de la procédure

1) Pour un message, les procédures de conversion des types d'information codée intégrés sont effectuées comme défini dans la Rec. CCITT X.408. Les procédures de conversion entre types d'information codée définis extérieurement ainsi qu'entre types d'information codée intégrés et définis extérieurement sortent du cadre de la présente Définition de service.

2) Après conversion, l'information de trace **trace-information** pour ce domaine ou de trace interne **internal-trace-information** pour cet agent MTA est mise à jour afin de signaler les types d'information codée convertis du message ou de l'envoi-test. La procédure prend alors fin.

14.3.10 Procédure de développement de liste Distribution-list-expansion

Cette procédure reçoit un message avec une liste DL destinataire unique et retourne un message dont la liste de destinataires comporte les membres de la liste DL. Pour un envoi-test, la procédure se contente de vérifier s'il y aurait eu le cas échéant développement de liste DL.

NOTE – L'utilisation de la procédure de développement de liste est sujette à la politique de sécurité en vigueur.

14.3.10.1 Arguments

1) Un message avec une information signalant la liste DL destinataire à développer;
2) un envoi-test avec une information signalant la liste DL destinataire dont le développement doit être vérifié.

14.3.10.2 Résultats

1) Le message avec zéro destinataire ou plus représentant les membres de la liste DL. D'autres champs peuvent être mis à jour comme indiqué dans la description de procédure ci-dessous;
2) facultativement, le message assorti d'instructions de production de rapport pour indiquer une remise avec succès;
3) l'envoi-test avec une instruction de production de rapport.

14.3.10.3 Erreurs

1) Une instruction de rapport indiquant un échec de remise. Les valeurs du code de motif de non-remise **non-delivery-reason-code** et du code de diagnostic de non-remise **non-delivery-diagnostic-code** sont indiquées dans la description de procédure ci-dessous.
2) En cas de récurrence de liste DL, la procédure prend fin sans retour d'erreurs ou de résultats.

14.3.10.4 Description de la procédure

1) Pour un message (mais non pour un envoi-test), effectuer une détection de récurrence: on recherche parmi les composantes du champ de la chronologie de développement **DL-expansion-history** l'occurrence du nom de la liste DL destinataire. Le développement de la liste est soit réalisé au moyen d'une entrée enregistrée dans l'annuaire, soit par traitement local de la liste DL. Quand la liste est développée à l'aide de l'annuaire, le nom d'annuaire **directory-name** distinctif obtenu doit être comparé, après résolution des éventuels alias, avec le nom d'annuaire de chaque nom **OR-name** figurant dans la chronologie de développement **DL-expansion-history**, sans tenir compte des adresses **OR-addresses**. Quand la liste est développée par traitement local, chaque agent MTA capable de développer la liste doit avoir connaissance de toutes les adresses **OR-addresses** de la liste, la détection du bouclage étant effectuée par comparaison des adresses.

   La présence du nom de la liste DL destinataire dans la chronologie de développement **DL-expansion-history** signifie que la liste DL est définie de façon récurrente et ne doit plus être développée. Le message est supprimé et aucun rapport ou autre résultat n'est renvoyé. La procédure de développement prend fin.

2) Acquisition de la liste DL: la procédure de développement tente d'acquérir les attributs de la liste DL.

   En cas d'échec, la procédure renvoie une instruction de rapport avec le code de motif de non-remise **non-delivery-reason-code unable-to-transfer** (impossibilité de transfert) accompagné du code adéquat de diagnostic de non-remise **non-delivery-diagnostic-code**. La procédure prend alors fin.

3) Vérification d'autorisation de dépôt: pour un message (et non un envoi-test), le dernier élément du champ de la chronologie de développement **DL-expansion-history** s'il existe, sinon le nom d'expéditeur **originator-name** est considéré comme l'envoyeur du message. Pour un envoi-test, l'expéditeur d'origine est considéré comme l'envoyeur.

   Le nom de l'envoyeur est alors comparé avec les composantes de l'argument d'autorisation de dépôt à la liste DL **DL-submit-permission**. S'il n'y a pas concordance, renvoyer une instruction de rapport avec le code de motif de non-remise **non-delivery-reason-code unable-to-transfer** (impossibilité de transfert) et le code de diagnostic de non-remise **non-delivery-diagnostic-code no-DL-submit-permission** (pas de permission de dépôt à la liste DL). La procédure prend alors fin.

4) Pour un envoi-test: si aucune autre politique locale ne fait obstacle à une tentative de remise, renvoyer une instruction de rapport pour obtenir une indication de remise réussie. La procédure prend alors fin.

5) Pour un message: l'indicateur de responsabilité (**responsibility)** de la liste DL destinataire reçoit la valeur **not-responsible** (non responsable). Si l'agent MTA effectuant le développement de la liste DL prend en charge l'argument destinataires exemptés de liste DL **DL-exempted-recipients**, alors les membres de la liste DL sont comparés aux valeurs de cet argument. S'il manque un composant d'adresse **OR-address** d'une valeur de l'argument destinataires exemptés de liste DL **DL-exempted-recipients**, alors celui-ci est obtenu à partir de l'attribut OR-addresses du système MHS de l'entrée d'annuaire de cet argument. Si plusieurs adresses OR-addresses sont présentes dans cet attribut d'annuaire, chaque valeur est incorporée dans l'argument. La comparaison de l'égalité de l'adresse **OR-address** et des composants du nom d'annuaire **directory-name** de l'attribut destinataires exemptés de liste DL **DL-exempted-recipients**, avec les valeurs de l'adresse **OR-address** ou du nom d'annuaire **directory-name** (en utilisant la règle **OR-name-match** décrite dans le § 12.4.4 de la Rec. UIT-T X.413 | ISO/CEI 10021-5), est effectuée pour chaque membre de la liste DL. Si l'adresse **OR-address** ou le composant du nom d'annuaire **directory-name** correspond à un membre de la liste DL, alors ce membre ne doit pas être ajouté comme nouveau destinataire du message. L'argument destinataire exempté de liste DL **DL-exempted-recipients** devra demeurer inchangé dans l'enveloppe quel que soit le nombre d'éléments qui ont été mis avec succès, en correspondance avec les membres de la liste DL. Tous les membres de la liste DL ne correspondant pas à une valeur de destinataires exemptés de liste DL **DL-exempted-recipients** doivent être ajoutés comme nouveaux destinataires du message. Les champs d'information de chacun de ces nouveaux destinataires sont recopiés à partir des champs correspondants de la liste DL destinataire aux exceptions suivantes près:

   recipient-name (nom de destinataire): membre de la liste DL.

   Les champs d'information suivants sont recopiés ou modifiés suivant la politique locale de traitement des listes DL:

   originating-MTA-report-request (demande de rapport du MTA expéditeur) (voir la Note 1);

   originator-report-request (demande de rapport par l'expéditeur) (voir la Note 1);

   originator-requested-alternate-recipient (destinataire suppléant demandé par l'expéditeur) (voir la Note 2);

   explicit-conversion (conversion explicite);

   proof-of-delivery-request (demande de preuve de remise) (voir la Note 4);

   requested-delivery-method (méthode de remise demandée);

   message-token (voir la Note 6);

   body-part-encryption-token (voir la Note 6);

   forwarded-content-token (voir la Note 6).

   NOTE 1 – Doit être recopié sans modification si la politique de traitement des listes DL est de renvoyer les rapports vers l'arrière; peut être modifié si la politique de traitement des listes est de ne pas renvoyer les rapports vers l'arrière.

   NOTE 2 – L'indication de destinataire suppléant demandé par l'expéditeur **originator-requested-alternate-recipient** peut être supprimée ou remplacée, suivant la politique locale de traitement de liste DL, ou recopiée, mais seulement si la politique de traitement de liste DL l'exige explicitement.

   NOTE 3 – Tout membre de la liste DL désignant une liste DL déjà présente dans la chronologie de développement **DL-expansion-history** peut être exclu du développement de la liste DL et ne pas être inclus comme nouveau destinataire du message.

   NOTE 4 – Qu'une demande de preuve de remise **proof-of-delivery-request** aboutisse à une preuve de remise **proof-of-delivery** émanant du point de développement de liste, des membres de la liste DL, des deux ou d'aucun des deux dépend de la politique de traitement de listes et de la politique de sécurité en vigueur.

   NOTE 5 – Quand un membre de la liste DL n'est identifié que par un nom d'annuaire, le traitement nécessaire pour obtenir une adresse **OR-address** est décrit dans la procédure de décision d'acheminement.

   NOTE 6 – Lorsqu'un message est développé et contient des données chiffrées dans un jeton pour le destinataire de la liste DL, ces données sont déchiffrées au moyen de la clé privée de la liste DL et un nouveau jeton est créé pour chaque membre destinataire, les données déchiffrées étant à nouveau chiffrées au moyen du premier algorithme figurant dans l'argument token-encryption-algorithm preference qui est pris en charge à la fois par l'agent MTA de développement DL et par le membre de la liste DL concerné. Le nouveau jeton est signé en utilisant le premier algorithme figurant dans l'argument token-signature-algorithm preference qui est pris en charge à la fois par l'agent MTA de développement DL et par le membre de la liste DL concerné.

6) Dans le champ des autres actions **other-actions** de l'information courante de trace **trace-information** et de trace interne **internal-trace-information**, si **redirected** (réacheminé) n'est pas déjà indiqué, la valeur **dl-operation** (développement) est alors indiquée. Sinon les nouveaux éléments d'information de trace et d'information de trace interne (**trace-information** and **internal-trace-information**) sont créés avec la valeur **dl-operation** (développement) indiquée.

7) La valeur du nom **recipient-name** du destinataire de la liste de distribution (qui comprend son nom d'annuaire **directory-name** distinctif après résolution des alias le cas échéant) et l'heure à laquelle le développement a eu lieu sont ajoutées au champ chronologie de développement **DL-expansion-history** du message.

NOTE 7 – La valeur courante du nom de destinataire **recipient-name** sera une valeur préférée, par suite des actions spécifiées au § 14.3.4.4, point 3.

8) Si les nouvelles valeurs de demande de rapport (déterminées à l'étape 5) ou la politique locale de traitement de listes DL empêchent l'expéditeur de recevoir de la part des membres de la liste DL un rapport de remise qu'il aurait demandé, le point de développement renvoie, en même temps que le message, une copie du message accompagnée d'instructions de demande de rapport de remise pour la liste DL développée.

Dans ce cas (où la politique de liste DL n'enverra pas à l'expéditeur de rapports de la part des membres de la liste DL), si le contexte initiateur de réinitialisation de liste DL DL-reset-originator (voir Rec. UIT-T X.402 | ISO/CEI 10021-2) est associé à un des membres de la liste DL, alors une procédure apparentée à la procédure de doubleur est utilisée pour faire deux copies du message: une pour les membres sans le contexte Réinitialisation d'expéditeur de liste DL (DL-reset-originator), et une autre pour les membres ayant le contexte Réinitialisation d'expéditeur de liste DL (DL-reset-originator). Dans la copie pour les membres ayant le contexte Réinitialisation d'expéditeur de liste DL (DL-reset-originator), le champ nom d'expéditeur (originator-name) est remplacé par le nom (OR-name) d'expéditeur/destinataire du propriétaire de la liste DL.

9) La procédure retourne le message révisé et la demande de rapport facultative, puis prend fin.

14.3.11 Algorithme de détection de boucle (loop detection) et d'acheminement (routing)

Les algorithmes d'acheminement et de détection de boucle pour utilisation entre domaines et à l'intérieur de ceux-ci sortent du cadre de la présente Définition de service. Afin d'exposer les sujets à prendre en considération, le présent paragraphe décrit une approche possible pour l'acheminement et la détection de boucle. Mais ces éléments n'ont qu'un caractère d'illustration.

Le présent paragraphe décrit une méthode simple de détection de boucle ainsi qu'un algorithme d'acheminement minimal. L'algorithme est minimal en ce sens qu'il ne présuppose qu'une connaissance minimale de chaque domaine de gestion MD et effectue des étapes de transfert qui évitent les boucles (au sens indiqué ci-dessous). Bien entendu, cet algorithme peut être amélioré chaque fois qu'un domaine MD en connaît davantage sur la topologie du réseau des domaines MD.

L'algorithme reconnaît le fait qu'il est généralement légitime (c'est-à-dire qu'aucun bouclage ne doit en résulter) de repasser par un domaine MD si, depuis le dernier passage, une opération spécifique a été effectuée par un autre domaine MD. Les opérations légitimes sont les suivantes: conversion, développement de liste DL et renvoi.

1) Notation: La séquence d'information de trace est constituée d'éléments d'information de trace **trace-information-elements** notés de façon simplifiée par le groupe (MD, action d'acheminement, opération), où MD est le nom d'un domaine de gestion, où l'action d'acheminement est 'relayed' (relayé) ou 're-routed' (réacheminé) et où l'opération est 'conversion', 'DL-operation' (développement), 'redirection' (réacheminement) ou 'nil' (néant). M désigne le message à transférer. MD(o) indique le domaine de gestion courant (celui qui effectue la détection de boucle au moment considéré). Voisinage est un ensemble de domaines de gestion adjacents choisis (voisins de MD(o)), qui représentent des domaines relais possibles pour le message M. Trace-info* est la séquence constituée des dernières informations de trace commençant par le dernier élément d'information [MD, r, op] pour lequel op n'est pas 'nil' (néant) (nil indique qu'aucune opération n'a été effectuée par un domaine MD).

2) Détection de boucle: recherche de boucle dans l'information de trace. Une boucle est détectée si la séquence d'information de trace contient une sous-séquence finale [MD(o), relayé, op(o)] . . . [MD(p), relayé, op(p)] dans laquelle MD(p) = MD(o) et où pour tout $o < j \leq p$ l'élément d'information de trace associé est [MD(j), relayé, op(j)] avec op(j) = nil (néant). Autrement dit, une boucle est détectée lorsque M parvient à un domaine de gestion MD qui l'a déjà relayé et après lequel chaque domaine rencontré l'a également relayé sans lui appliquer d'opération autre que d'acheminement. Si une boucle est détectée, l'algorithme retourne une erreur indiquant le problème, et prend fin.

3) Elaboration de l'acheminement: si aucune boucle n'est détectée, l'ensemble Voisinage est, si nécessaire, ajusté pour éviter la formation de boucles dans les étapes de transfert, dans le contexte du message courant (cet ajustement n'affecte pas les autres messages).

   a) S'il n'existe ni boucle ni élément [MD(o), r, op] dans la séquence Trace-info*, l'ensemble Voisinage reste inchangé.

b) S'il n'existe pas de boucle, mais qu'il existe une occurrence de l'élément [MD(o), r, op] dans Trace-info*, éliminer de l'ensemble Voisinage tous les domaines MD apparaissant dans la sous-séquence de Trace-info*, commençant par [MD(o), r, op]. Modifier l'élément d'information de trace correspondant au domaine courant en indiquant "re-routed" (réacheminé) comme action d'acheminement. Ajouter un paramètre de domaine antérieur "previous-MD" déterminé comme suit: on localise le dernier élément [MD(o), r, op] dans la séquence d'information de trace. Le "domaine antérieur" est le domaine MD apparaissant dans le premier élément d'information de trace après cet élément [MD(o), r, op].

c) Dans les cas a) et b), si l'ensemble Voisinage est vide, l'algorithme retourne une erreur indiquant le problème puis prend fin.

4) Action d'acheminement. Un bond suivant est sélectionné dans l'ensemble Voisinage pour chacun des destinataires.

14.3.12 Procédure de résolution de nom d'annuaire (Directory Name Resolution)

Cette procédure produit une adresse **OR-address** pour un utilisateur identifié par un nom d'annuaire.

14.3.12.1 Arguments

Nom d'annuaire de l'utilisateur, méthode de remise demandée **requested-delivery-method** si elle est spécifiée, et chronologie de renvoi **redirection-history** le cas échéant.

14.3.12.2 Résultats

Adresse **OR-address** de l'utilisateur.

14.3.12.3 Erreurs

Indication établissant que la recherche à partir du nom d'annuaire n'a pas donné de résultat.

14.3.12.4 Description de la procédure

1) L'agent MTA accède à l'annuaire à l'aide du nom d'annuaire fourni. Si ce nom ne correspond pas à une entrée de l'annuaire, la procédure renvoie une indication d'erreur et prend fin.

2) Si l'argument de méthode de remise demandée **requested-delivery-method** n'est pas fourni, ou s'il a pour valeur **any-delivery-method** (méthode indifférente), l'agent MTA essaie d'obtenir l'attribut de méthode de remise préférée *preferred-delivery-method* à partir de l'entrée d'annuaire. Si les étapes restantes permettent de construire plusieurs types d'adresses, le choix entre ceux-ci sera déterminé conjointement par la méthode de remise demandée **requested-delivery-method** (ou par la méthode préférée *preferred-delivery-method*) et la politique locale. S'il faut choisir entre plusieurs adresses **OR-addresses**, et qu'il existe un argument de chronologie de renvoi **redirection-history**, toute adresse **OR-address** existant déjà dans la chronologie de renvoi sera préalablement exclue du choix.

3) En présence de l'attribut *mhs-or-addresses* (adresse OR de messagerie), une valeur de cet attribut peut être renvoyée. On considère qu'une telle valeur satisfait à la méthode de remise MHS **mhs-delivery**. Si l'attribut a plusieurs valeurs, le choix entre celles-ci est du ressort local. Ce choix peut être influencé par les fonctionnalités d'agent utilisateur destinataire (déterminées à partir d'autres attributs d'annuaire ou de connaissances locales) et par les caractéristiques du message.

4) L'agent MTA peut être configuré avec des informations sur diverses unités d'accès qu'il lui est permis d'utiliser lors de la construction d'une adresse **OR-address** à partir des informations fournies par l'annuaire. Les informations configurées comprennent les valeurs d'attribut **OR-address** – qui peuvent être combinées avec les informations obtenues dans l'annuaire pour former une adresse **OR-address** complète – ainsi que la méthode de remise imposée par une telle adresse. Si l'agent MTA est configuré avec les détails de plusieurs unités d'accès de même type, le choix entre celles-ci est du ressort local. L'agent MTA peut être configuré avec des informations relatives à zéro, un ou plusieurs des types suivants d'unités d'accès:

a) remise physique: les valeurs des arguments suivants sont configurées: **country-name** (nom de pays), **administration-domain-name** (domaine d'administration), **private-domain-name** (domaine privé – facultatif), et **pds-name** (système de remise physique). L'adresse **OR-address** est construite à partir des éléments configurés, des valeurs **unformatted-postal-address** (adresse postale non formatée) et **postal-code** (code postal) déduites des attributs d'annuaire *postalAddress* et *postalCode*, ainsi qu'à partir du nom du pays de remise physique **physical-delivery-country-name** obtenu de l'élément *countryName* du nom distinctif de l'entrée d'annuaire. On considère que cela satisfait à la méthode de remise physique;

b) remise de télécopie de Groupe 3: les valeurs des arguments suivants peuvent être configurées: **country-name** (nom de pays), **administration-domain-name** (domaine d'administration), **private-domain-name** (domaine privé – facultatif). L'adresse **OR-address** est construite à partir des éléments configurés, le cas échéant et de l'adresse réseau **network-address** obtenue à partir de la valeur de l'attribut d'annuaire *facsimileTelephoneNumber* et **terminal-type** (type de terminal – facultatif) mis à la valeur *g3-facsimile*. On considère que cela satisfait à la méthode de remise de télécopie de Groupe 3.

c) remise télex: les valeurs des arguments suivants peuvent être configurées: **country-name** (nom de pays), **administration-domain-name** (nom de domaine d'administration) et **private-domain-name** (nom de domaine privé – facultatif). L'adresse **OR-address** est construite à partir des éléments configurés ainsi que de l'adresse réseau **network-address** obtenue à partir des valeurs des éléments telexNumber et countryCode de l'attribut d'annuaire *telexNumber*, de l'identificateur de terminal **terminal-identifier** obtenu à partir de la valeur de l'élément answerback de l'attribut d'annuaire *telexNumber* et d'un type **Terminal type** mis à la valeur *telex*. On considère que cela satisfait à la méthode de remise télex **telex-delivery**.

14.3.13 Mise sous double enveloppe

Par cette procédure, un message, un envoi-test ou un rapport est placé comme objet complet dans le contenu d'un nouveau message adressé à un extracteur de double enveloppe distant et soumis comme nouveau message ayant un contenu de type à enveloppe interne.

14.3.13.1 Arguments

1) Un message, un envoi-test ou un rapport qui doit être placé dans une enveloppe externe.
2) Le nom **OR-name** de l'extracteur de double enveloppe distant.
3) Le nom **OR-name** du dispositif de mise sous double enveloppe.
4) Les services de sécurité qu'il convient d'appliquer pour protéger le contenu de l'enveloppe interne et l'information spécifique sur l'algorithme ou les préférences en matière d'algorithme pour ceux-ci (pour la confidentialité content-confidentiality, les données message-token-encrypted-data, les données de type message-token-signed-data et le contrôle message-origin-authentication-check).

14.3.13.2 Résultats

Aucun, l'agent MTA n'ayant pas à poursuivre le traitement du message original.

NOTE – Cette procédure comporte deux événements de sortie: l'un est le dépôt d'un nouveau message contenant l'enveloppe interne, le second est un état contenant suffisamment d'informations pour permettre au dispositif de mise sous double enveloppe de construire un rapport de non-remise du message original au cas où il reçoit un rapport de non-remise du nouveau message.

14.3.13.3 Erreurs

Indication d'une erreur de sécurité si un service demandé n'a pas pu être fourni.

NOTE – L'occurrence d'une telle erreur de sécurité peut indiquer soit une erreur de configuration (lorsqu'il est impossible d'obtenir un algorithme configuré ou la clé privée de l'agent MTA pour celui-ci), soit une erreur dans le certificat de l'extracteur de double enveloppe.

14.3.13.4 Description de la procédure

L'ensemble de l'unité MTS-APDU contenant le message, l'envoi-test ou le rapport est placé dans le contenu d'un nouveau message dont l'expéditeur est le nom **OR-name** de ce dispositif de mise sous double enveloppe et dont le destinataire est le nom **OR-name** de l'extracteur de double enveloppe distant. La demande originator-report-request pour ce demandé est mise à "rapport" et le type de contenu est mis à "enveloppe interne".

Si les préférences en matière d'algorithme sont spécifiées pour les services de sécurité demandés et que le nom directory-name soit présent dans le nom **OR-name** de l'extracteur double-envelope-extractor distant, cette entrée d'annuaire est lue afin d'obtenir les algorithmes et l'attribut Certificat d'utilisateur acceptés. L'algorithme de niveau le plus élevé dans l'ordre de préférence qui est accepté par cet agent MTA et par l'extracteur double-envelope-extractor distant est sélectionné pour chaque service de sécurité demandé (c'est-à-dire confidentialité content-confidentiality, données message-token-encrypted-data, données message-token-signed-data, et contrôle message-origin-authentication-check). Ces informations sur l'algorithme contiennent un identificateur (algorithm-identifier) et, facultativement, des informations permettant de sélectionner un certificat approprié pour cet algorithme pour l'expéditeur, pour le destinataire ou pour les deux (selon les critères de l'algorithme). Les informations certificate-selector ne sont requises que si l'entrée d'annuaire peut contenir plus d'un certificat pour l'algorithme identifié. En l'absence de nom d'annuaire, c'est la préférence de niveau le plus élevé qui est sélectionnée et il faudra une configuration locale de la clé de cryptage publique de l'extracteur double-envelope-extractor.

Le contenu est crypté au moyen de l'algorithme content-confidentiality-algorithm sélectionné (ou configuré), qui peut être un algorithme asymétrique. S'il est symétrique, une clé content-confidentiality-key aléatoire est produite et utilisée pour crypter le contenu, et un jeton message-token créé au moyen de ce contenu est crypté au moyen de l'algorithme message-token-encryption-algorithm sélectionné (ou configuré) (qui doit être un algorithme asymétrique) et signé au moyen de l'algorithme message-token-signature-algorithm sélectionné (ou configuré) (qui doit être un algorithme de signature). La clé publique utilisée avec l'algorithme de cryptage asymétrique est trouvée au moyen de l'identificateur algorithm-identifier et du sélecteur recipient-certificate-selector pour choisir un certificat approprié dans l'entrée d'annuaire.

Si l'authentification message-origin-authentication est spécifiée, un contrôle message-origin-authentication-check est calculé; il contient une signature du contenu crypté utilisant l'algorithme sélectionné (ou configuré) avec la clé privée de cet agent MTA, correspondant à son certificat identifié par le sélecteur originator-certificate-selector.

Le nouveau message contenant l'enveloppe interne est soumis et son identificateur message-submission-identifier est consigné avec suffisamment d'informations pour permettre au dispositif de mise sous double enveloppe d'établir un rapport de non-remise relatif au message original s'il reçoit un rapport de non-remise relatif au nouveau message.

14.3.14 Procédure de l'extracteur double-envelope-extractor

Par cette procédure, un message à contenu de type à enveloppe interne extrait du contenu un message, un envoi-test ou un rapport que l'agent MTA traite ensuite comme s'il avait été transféré normalement.

14.3.14.1 Arguments

Message dont le contenu est de type à enveloppe interne.

14.3.14.2 Résultats

Message, envoi-test ou rapport.

14.3.14.3 Erreurs

L'indication d'une erreur de sécurité si la vérification d'un argument de sécurité n'a pas eu de résultat favorable.

En réponse à un envoi-test ou à un message ayant un type de contenu autre qu'une enveloppe interne, une instruction de production d'un rapport d'incapacité de transférer un nom-OR non reconnu.

14.3.14.4 Description de la procédure

La procédure suit celle de remise de message message-delivery (voir § 14.7.1) s'il y a lieu, y compris la production d'une instruction de rapport en cas de nécessité.

En présence du contrôle message-origin-authentication-check, ce contrôle est effectué. Le contenu est décrypté et le message, l'envoi-test ou le rapport est extrait et transmis à la procédure frontale (ou à la procédure frontale de rapport).

14.4 Module de rapport (Report)

Le module de rapport peut être invoqué par:

1) le module de rapport entrant (Report-in), qui transmet un rapport;
2) le module principal (Main), qui transmet un message ou un envoi-test avec des instructions de rapport;
3) le module de rapport sortant (Report-out), qui transmet un rapport avec une description de défaillance.

Si les procédures internes à ce module détectent une erreur, elles ne produisent pas de sortie. Sinon, le module de rapport appelle le module de rapport sortant ou de remise de rapport en transmettant un rapport avec des instructions respectivement de transfert ou de remise (voir la Figure 10).

NOTE – L'utilisation de rapports est sujette à la politique de sécurité en vigueur.

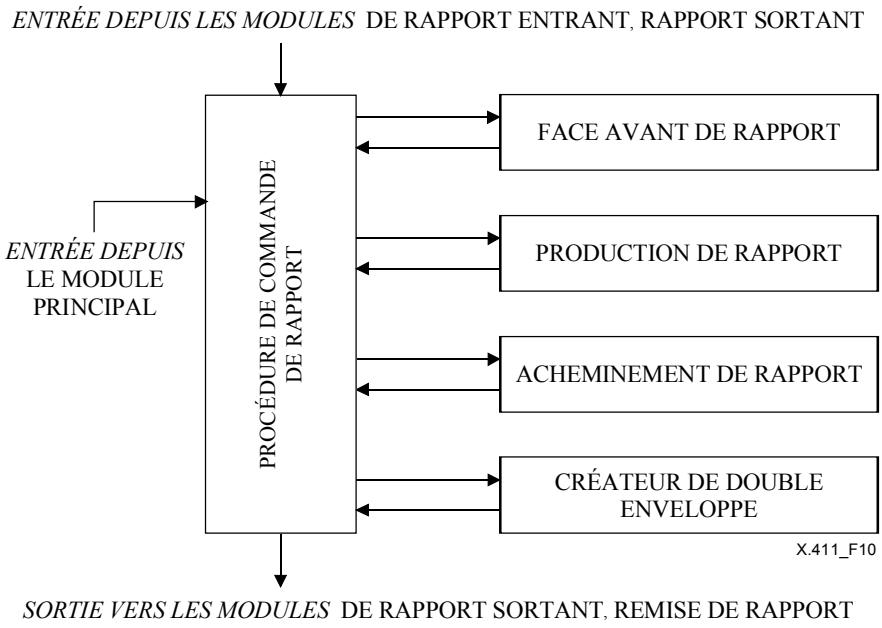


Figure 10 – Organisation des procédures à l'intérieur du module de rapport

14.4.1 Procédure de commande (Control)

14.4.1.1 Arguments

1) Un rapport;
2) un message ou un envoi-test avec des instructions de rapport.

14.4.1.2 Résultats

1) Un rapport avec des instructions de transfert ou de remise;
2) aucun résultat en cas d'erreur trouvée.

14.4.1.3 Erreurs

Aucune. Le rapport, le message ou l'envoi-test est ignoré si une erreur est rencontrée.

14.4.1.4 Description de la procédure

1) Pour un rapport provenant du module de rapport entrant (Report-in), la procédure de face avant (Report-front-end) est d'abord appelée pour initialiser l'information de trace et procéder à plusieurs étapes de vérification initiale. Un retour vide indique une erreur; le rapport est ignoré et le traitement prend fin. Sinon, le traitement se poursuit à l'étape 3 ci-dessous.
2) Pour un message ou un envoi-test, la procédure de production de rapport (Report-generation) est d'abord appelée pour créer un rapport. Un retour vide indique une erreur; le message ou l'envoi-test est ignoré et le traitement prend fin. Si un rapport est renvoyé, le traitement se poursuit à l'étape 3 ci-dessous.
3) La procédure d'acheminement de rapport (Report-routing) est appelée pour produire une instruction d'acheminement de rapport. Un retour vide indique une erreur; le rapport est alors ignoré et le traitement prend fin. La procédure de commande retourne le rapport complété, accompagné d'une instruction d'acheminement puis prend fin, sous réserve de la politique de sécurité.

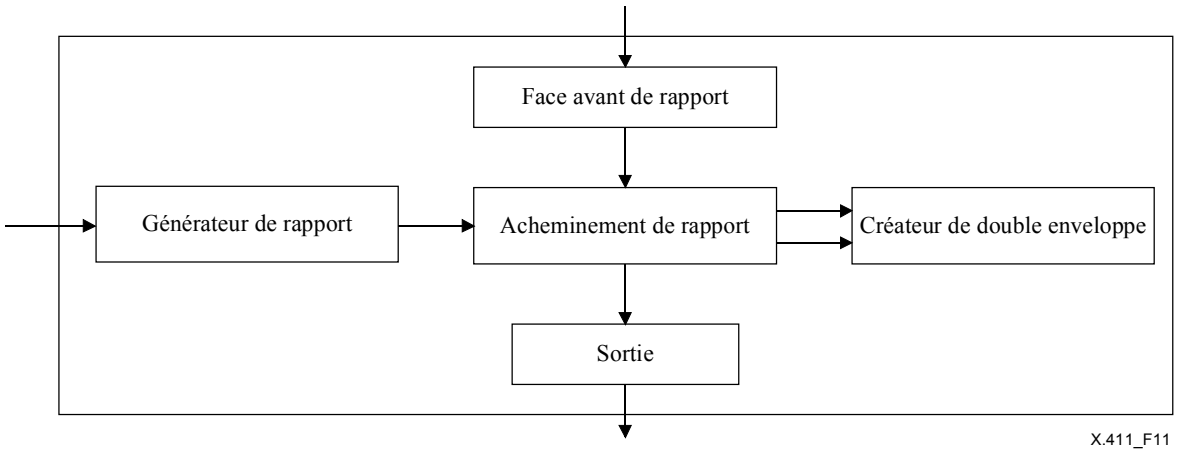


Figure 11 – Flux d'informations à l'intérieur du module de rapport

14.4.2 Procédure de face avant de rapport (Report-front-end)

Cette procédure effectue l'initialisation de trace, la détection des expirations de délais de messages, les contrôles initiaux de sécurité, la détection de boucles et la vérification de criticité.

14.4.2.1 Arguments

Un rapport.

14.4.2.2 Résultats

Le rapport, avec les informations de trace **trace-information** initialisées pour cet agent MTA.

14.4.2.3 Erreurs

Aucune. Le rapport est écarté si une erreur est détectée.

14.4.2.4 Description de la procédure

1) Si le rapport a franchi une limite de domaine, un élément d'informations de trace **trace-information-element** est ajouté pour ce domaine, avec indication du temps courant comme valeur d'heure d'arrivée **arrival-time** et de la valeur **relay** (relais) comme action (**action**). Un élément d'informations de trace interne **internal-trace-information-element** est également ajouté, que le rapport ait ou non franchi une limite de domaine.
2) Si la politique de sécurité en vigueur l'impose, ou si le contrôle d'authentification d'origine de rapport **report-origin-authentication-check** est incorrect, le rapport est ignoré et le traitement prend fin.
3) Si l'un quelconque des champs d'extension est marqué comme étant critique pour le transfert, sans être sémantiquement compris par l'agent MTA, le rapport est ignoré et la procédure prend fin.
4) La détection de boucle est effectuée. L'algorithme de détection de boucle sort du cadre de la présente Définition de service. Toutefois, le § 14.3.11 donne un exemple d'algorithme combiné d'acheminement et de détection de boucle. Si une boucle est détectée, le rapport est ignoré et la procédure prend fin.

14.4.3 Procédure de production de rapport

Cette procédure produit un rapport qui décrit le succès ou l'échec des opérations entreprises par l'agent MTA.

14.4.3.1 Arguments

Un message ou un envoi-test. Pour chaque destinataire dont l'argument de responsabilité **responsibility** a pour valeur **responsible** (responsable), une instruction est ajoutée indiquant le succès de l'opération ou le problème à signaler.

14.4.3.2 Résultats

Rapport décrivant le succès ou l'échec à signaler.

14.4.3.3 Erreurs

Aucune.

14.4.3.4 Description de la procédure

Lorsque le champ de demande de rapport de l'agent MTA expéditeur **originating-MTA-report-request** du sujet le spécifie, le rapport est établi avec les arguments énumérés dans le Tableau 32 et est enrichi par les éléments suivants:

Les arguments de remise (heure de remise de message **message-delivery-time**, type d'utilisateur **type-of-MTS-user**) ou de non-remise (code de motif de non-remise **non-delivery-reason-code**, code de diagnostic de non-remise **non-delivery-diagnostic-code**) sont recopiés pour chaque destinataire à partir des instructions par destinataire qui accompagnent le message sujet. En cas de remise avec succès à une liste DL destinataire, la valeur de l'argument type d'utilisateur **type-of-MTS-user** est mise à **DL**. Le nom de destination de rapport **report-destination-name** est le dernier élément de la chronologie de développement **DL-expansion-history** s'il existe. Pour les messages sans chronologie de développement et pour tous les envois-tests, le nom de destination de rapport **report-destination-name** sera le nom d'expéditeur **originator-name** du sujet. L'argument expéditeur de développement **originator-and-DL-expansion** contiendra le nom d'expéditeur **originator-name** et l'heure de dépôt de message **message-submission-time** du sujet suivis du contenu de la chronologie de développement **DL-expansion-history**. Un élément d'information de trace **trace-information-element** est créé pour ce domaine avec le temps courant comme valeur de temps d'arrivée **arrival-time** et **relay** (relais = transfert) comme valeur d'action (**action**). Un élément d'information de trace interne est également créé. Si le sujet contient un argument de chronologie de renvoi **redirection-history** ou de chronologie de développement de liste **dl-expansion-history**, le nom de destinataire initialement prévu **originally-intended-recipient-name** est recopié à partir du premier élément de la chronologie de renvoi ou de la chronologie de développement de liste, selon celui de ces événements qui a eu lieu en premier (la séquence de ces événements est déterminée à partir des informations de trace **trace-information**).

NOTE – Le nom de liste DL au rapport **reporting-DL-name** n'est produit dans aucune de ces conditions.

Lorsque les instructions rendent compte d'échecs multiples, le rapport doit signaler le problème initial plutôt que l'échec des actions ultérieures de reprise.

L'agent MTA établit les valeurs de criticité **criticality** des champs copiés à partir du sujet. Ces nouvelles valeurs reflètent une criticité de rapport et non pas de sujet. L'agent MTA ne copiera pas dans le rapport une fonction critique s'il ne la prend pas en charge.

14.4.4 Procédure d'acheminement du rapport (Report-routing)

Cette procédure détermine l'opération d'acheminement à appliquer s'il y a lieu au rapport. L'acheminement de rapport correspond aux situations particulières qui nécessitent une procédure d'acheminement différente de la procédure applicable aux messages ou aux envois-tests:

1) un rapport n'a qu'un seul destinataire: l'expéditeur du message qui constitue le sujet du rapport, un point de développement de liste DL ou, lorsque la politique locale le permet, un titulaire de liste DL;
2) un échec insurmontable dans l'acheminement d'un rapport se traduira par l'abandon de ce rapport. On ne tentera pas de produire un autre rapport sur le problème rencontré.

Les traitements nécessaires correspondants sont décrits dans ce qui suit. Il convient de noter que l'acheminement des rapports est soumis à la politique de sécurité.

14.4.4.1 Arguments

L'un des arguments suivants:

1) rapport en provenance d'un autre agent MTA acheminé vers l'agent MTA présent et traité avec succès par la procédure de face avant **Report-front-end**;
2) rapport créé par la procédure de production de rapport interne à l'agent MTA présent;
3) rapport renvoyé par la procédure de sortie de rapport, accompagné d'une description du problème d'acheminement survenu.

14.4.4.2 Résultats

L'un des résultats suivants:

1) le rapport, avec les instructions de transfert vers le prochain agent MTA;
2) le rapport, avec indication de l'utilisateur MTS pris en charge localement, auquel le rapport doit être remis.

14.4.4.3 Erreurs

Aucune. Faute de pouvoir déterminer le destinataire local ou le prochain bond, le rapport est supprimé.

14.4.4.4 Description de la procédure

1) Les rapports envoyés à cet agent MTA ou produits localement reçoivent le traitement d'acheminement normal suivant:

   a) lorsque la destination du rapport n'est pas locale à cet agent MTA, il faut prévoir un transfert. La procédure d'acheminement de rapport tente de déterminer l'adresse du bond suivant. A cette fin, l'étiquette de sécurité de message **message-security-label** est vérifiée au vu du contexte de sécurité **security-context**, afin de prévenir toute infraction à la politique de sécurité. Si cet examen est positif, la procédure renvoie en guise de résultat le rapport accompagné de cette information, puis elle prend fin. Le rapport est ensuite passé à la procédure de rapport sortant **Report-out**.

      Si la politique de sécurité spécifie qu'une double enveloppe est requise pour le prochain bond identifié, la procédure renvoie une instruction visant à imbriquer le rapport dans le contenu **content** d'un nouveau message au moyen de la procédure spécifiée au § 14.3.13. La procédure se termine ensuite.

      S'il n'est pas possible de déterminer l'adresse du bond suivant, le rapport est abandonné et la procédure prend fin sans renvoi de résultat;

   b) si la destination du rapport spécifie sans ambiguïté un destinataire existant sans qu'il s'agisse de l'adresse préférée de ce destinataire, une instruction de renvoi est produite avec le nom **OR-name** préféré du destinataire et avec le motif de renvoi **alias**, puis procédure prend fin.

      Si la destination du rapport spécifie sans ambiguïté un destinataire local existant, les paramètres d'enregistrement du destinataire sont examinés pour trouver un destinataire suppléant désigné par le destinataire **recipient-assigned-redirections**; s'il existe, la longueur du contenu renvoyé est comparée, le cas échéant, avec la longueur de contenu **content-length.** Le type de contenu, s'il est présent, est comparé avec le type de contenu **content-type** de chaque classe de réacheminement **redirection-class** du réacheminement assigné par le destinataire **recipient-assigned-redirections** (qui a des objets positionnés vis-à-vis des rapports ou inversement) et ce tour à tour jusqu'à ce que l'on trouve une classe de réacheminement dont les valeurs spécifiées pour ces champs correspondent à celles du rapport, les classes de réacheminement avec des valeurs spécifiées pour d'autres composantes étant ignorées; si une classe de réacheminement correspond, une instruction de renvoi est produite et la procédure prend fin;

   c) si la destination du rapport est un utilisateur MTS local à cet agent MTA et que le champ de demande de rapport par l'expéditeur **originator-report-request** l'indique, la remise du rapport est requise (sous réserve de la politique de sécurité en vigueur). La procédure d'acheminement du rapport tente de déterminer l'adresse OR-address de la destination du rapport. En cas de succès, la procédure renvoie en guise de résultat le rapport accompagné de cette information, puis elle prend fin. Le rapport est ensuite passé à la procédure de remise de rapport Report-delivery.

      Si la destination du rapport n'identifie pas d'utilisateur MTS et que l'agent MTA ait été configuré avec l'adresse d'un destinataire suppléant pour cette classe de destination, une instruction de réacheminement est produite avec comme motif de réacheminement recipient-MD-assigned-alternate-recipient (destinataire suppléant désigné par le domaine destinataire) et la procédure prend fin.

      Si le rapport n'était pas demandé ou s'il n'a pas été possible d'en déterminer l'adresse de destination, ce rapport est abandonné et la procédure prend fin sans renvoi de résultat;

   d) si le nom de destination de rapport **report-destination-name** est une liste DL locale à cet agent MTA, le rapport fait l'objet d'un acheminement vers l'amont selon un trajet de points successifs de développement de liste. La valeur **dl-operation** (développement) est inscrite dans le champ autres actions **other-actions** de l'élément courant d'informations de trace **trace-information-element** et de trace interne **internal-trace-information-element**.

      Tout traitement reposant sur une politique locale de traitement de listes interviendrait à ce niveau; par exemple, une copie du rapport peut être établie et envoyée au titulaire de la liste DL. Dans ce cas, le nom de destination de rapport **report-destination-name** est celui du titulaire de la liste DL et le nom de liste DL au rapport **reporting-DL-name** comprend le nom de la liste DL sujet. Cette copie du rapport ne contiendra pas le contenu renvoyé **returned-content**. Par ailleurs, la suppression des rapports peut avoir lieu ici.

   NOTE 1 – La possibilité qu'un titulaire de liste DL soit lui-même une liste DL pourra faire l'objet d'une normalisation.

NOTE 2 – L'autorisation de dépôt de liste DL n'est pas prise en compte lors du traitement d'un rapport.

S'il ne faut pas supprimer le rapport, l'agent MTA remplace alors le nom **OR-name** qui se trouve dans le champ nom de destination de rapport **report-destination-name** par le nom **OR-name** le précédant immédiatement dans le champ expéditeur et chronologie de développement **originator-and-DL-expansion-history**. Ainsi, le rapport acquiert une nouvelle destination, à savoir l'entrée juste en amont dans la chaîne des entrées du champ d'expéditeur et de chronologie de développement **originator-and-DL-expansion-history**:

nom de destination de rapport: **report-destination-name**	copier le nom **OR-name** précédent de liste DL du champ expéditeur et chronologie de développement **originator-and-DL-expansion-history**.
nom de liste DL au rapport: **reporting-DL-name**	ne le produire qu'en cas de rapport fait au titulaire de la liste DL.

Pour acheminer le rapport vers cette nouvelle destination, la procédure d'acheminement de rapport s'appelle elle-même récursivement. Le résultat éventuel est retourné et la procédure prend fin;

e) si le nom de destination de rapport **report-destination-name** désigne un extracteur de double enveloppe dans cet agent MTA, la procédure du § 14.4.5 s'applique et la procédure se termine. Tout nouveau rapport résultant est traité à partir du début de cette procédure.

2) Lorsqu'un rapport renvoyé en amont par la procédure de rapport sortant est bloqué par un échec de transfert vers un autre agent MTA, la procédure d'acheminement de rapport tente de réacheminer ce rapport, c'est-à-dire de calculer une adresse de bond suivant de remplacement (sous réserve de la politique de sécurité en vigueur). Si une adresse de remplacement est trouvée, la procédure renvoie en guise de résultat le rapport accompagné de cette information et d'une information de trace adéquatement modifiée, puis elle prend fin. Le rapport est ensuite passé à la procédure de rapport sortant.

S'il est impossible de trouver une adresse de remplacement, le rapport est abandonné et la procédure prend fin sans renvoi de résultat.

14.4.5 Procédure de mise sous double enveloppe

Cette procédure examine le rapport relatif à un message (créé par cet agent MTA) qui avait un contenu de type à enveloppe interne et, s'il s'agit d'un rapport de non-remise, substitue un rapport de non-remise au message qui était dans l'enveloppe interne.

14.4.5.1 Arguments

Rapport.

14.4.5.2 Résultats

Autre rapport si argument est un rapport de non-remise, aucun dans le cas contraire.

14.4.5.3 Erreurs

Aucune.

14.4.5.4 Description de la procédure

Si le rapport est un rapport de non-remise, la consignation des messages sous double enveloppe qui ont été soumis est lue pour obtenir les informations nécessaires à la création d'un rapport de non-remise relatif au message de l'enveloppe interne. Ce nouveau rapport de non-remise remplace le rapport de non-remise relatif à l'enveloppe externe.

Si le rapport est un rapport de remise, il n'est pas nécessaire de poursuivre le transfert.

Dans les deux cas, la consignation des messages sous double enveloppe qui ont été soumis est complétée des informations relatives au rapport de remise ou de non-remise. L'agent MTA peut mettre en œuvre une procédure additionnelle, lancée à l'expiration de la temporisation, pour produire un rapport de non-remise relatif au message de l'enveloppe interne si aucun rapport de remise n'a été reçu pour le message de l'enveloppe externe.

14.5 Rattachement MTS-bind et détachement MTS-unbind

14.5.1 Procédure de rattachement MTS-bind demandée par l'utilisateur MTS

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'un rattachement MTS-bind est invoqué par un utilisateur MTS.

14.5.1.1 Arguments

Les arguments de rattachement sont définis au § 8.1.1.1.1.

14.5.1.2 Résultats

Les résultats du rattachement sont définis au § 8.1.1.1.2.

14.5.1.3 Erreurs

Les erreurs de rattachement sont définies au § 8.1.2.

14.5.1.4 Description de la procédure

1) Si les ressources de l'agent MTA ne peuvent prendre en charge l'établissement d'une nouvelle association, la procédure retourne une erreur de rattachement (occupé) et prend fin.

2) Dans le cas contraire, si une authentification est requise par la politique de sécurité en vigueur, l'agent MTA cherche à la fois à authentifier l'utilisateur MTS au moyen des pouvoirs du demandeur **initiator-credentials** fournis, et à vérifier l'acceptabilité du contexte de sécurité **security-context**.

   Si les pouvoirs du demandeur **initiator-credentials** contiennent des pouvoirs renforcés **strong-credentials**, la signature du jeton de rattachement du demandeur est vérifiée au moyen de la clé publique du certificat d'utilisateur du système MTS pour l'algorithme de signature identifié. Le certificat d'utilisateur du système MTS peut être inclus dans les pouvoirs du demandeur de l'argument de rattachement Bind, ou être identifié par un sélecteur de certificat et, à moins qu'il ne soit déjà à la disposition de l'agent MTA, être obtenu à partir de l'attribut User Certificate de l'utilisateur du système MTS. La validité du certificat et son trajet de certification sont également vérifiés. De plus, le nom d'annuaire figurant dans le champ du sujet de ce certificat est vérifié pour établir qu'il s'agit effectivement du nom de l'utilisateur du système MTS. Le nom **OR-name** contenu dans le champ de variante nominative d'entité de ce certificat est vérifié en ce qui concerne sa correspondance avec le nom **OR-name** de l'utilisateur du système MTS figurant dans le champ initiator-name et avec le nom **OR-name** du rattachement Bind. Le nom **mta-name** et l'identificateur global-domain-identifier contenus dans le jeton initiator-bind-token sont vérifiés pour établir qu'ils sont effectivement ceux de cet agent MTA. L'heure indiquée dans le jeton est comparée à celle du moment pour garantir que la période de validité du jeton, pouvant être acceptée par cet agent MTA, n'a pas pris fin.

   Le jeton responder-bind-token est produit au moyen du même algorithme de signature (à moins qu'un autre algorithme qui lui est préféré ne soit réputé être accepté par l'utilisateur du système MTS) et de la clé privée de cet agent MTA pour signer un jeton qui comprend l'identificateur d'algorithme pour l'algorithme de signature, le nom **OR-name** de l'utilisateur du système MTS, l'heure actuelle et un nombre aléatoire en tant que données bind-token-signed-data. Ce jeton responder-bind-token et le **certificate-selector** ou le **certificate** (et les certificats additionnels indiquant son trajet de certification) pour cette clé publique d'agent MTA pour cet algorithme constituent les pouvoirs du demandé dans le résultat du rattachement Bind.

   S'il n'est pas possible d'authentifier les pouvoirs du demandeur **initiator-credentials**, la procédure renvoie une erreur d'authentification et prend fin. Si le contexte de sécurité **security-context** n'est pas acceptable, la procédure renvoie une erreur de rattachement (contexte de sécurité non acceptable) et prend fin.

3) Si l'authentification se déroule avec succès et si le contexte de sécurité **security-context** est acceptable, l'agent MTA accepte l'association demandée. La procédure renvoie le nom **MTA-name** et les pouvoirs du demandé **responder-credentials**. Une indication **messages-waiting** (messages en instance) est également renvoyée lorsque l'utilisateur MTS a souscrit à l'élément de service de mise en instance de remise. La procédure prend fin.

4) Si l'authentification n'est pas requise, une indication **messages-waiting** (messages en instance) est retournée lorsque l'utilisateur MTS a demandé l'élément de service de mise en instance de remise et la procédure prend fin.

14.5.2 Procédure de détachement MTS-unbind demandée par l'utilisateur MTS

Le rpésent paragraphe décrit le comportement de l'agent MTA lorsqu'un utilisateur MTS invoque un détachement MTS-unbind pour libérer une association précédemment établie par cet utilisateur.

14.5.2.1 Arguments

Néant.

14.5.2.2 Résultats

La procédure de détachement retourne un résultat vide comme indication de libération de l'association.

14.5.2.3 Erreurs

Aucune.

14.5.2.4 Description de la procédure

La procédure libère l'association, renvoie un résultat vide et prend fin.

14.5.3 Procédure de rattachement MTS-bind demandée par l'agent MTA

Le présent paragraphe décrit les opérations effectuées par un agent MTA chargé d'établir une association avec un utilisateur MTS.

14.5.3.1 Arguments

Les arguments de rattachement MTS-bind sont définis au § 8.1.1.1.1.

14.5.3.2 Résultats

Identificateur interne pour l'association établie.

14.5.3.3 Erreurs

La procédure renvoie une indication d'échec lorsque l'association n'a pas pu être établie.

14.5.3.4 Description de la procédure

1) La procédure établit des valeurs pour les arguments définis au § 8.1.1.1.1. Une indication **messages-waiting** (messages en instance) peut être fournie lorsque l'utilisateur MTS a souscrit à l'élément de service de mise en instance de remise **Hold for Delivery**. Les valeurs des arguments **initiator-name** (nom du demandeur), **security-context** (contexte de sécurité) et **initiator-credentials** (pouvoirs du demandeur) sont extraites de l'information interne.

   Si les pouvoirs du demandeur **initiator-credentials** contiennent des pouvoirs renforcés **strong-credentials**, l'agent MTA sélectionne un algorithme de signature qui est accepté par l'utilisateur MTS et emploie celui-ci pour signer un jeton initiator-bind-token comprenant l'identificateur d'algorithme pour cet algorithme, le nom **OR-name** de l'utilisateur MTS, l'heure actuelle et un nombre aléatoire en tant que données de type bind-token-signed-data. Ce jeton initiator-bind-token et le sélecteur **certificate-selector** ou le **certificate** (et les certificats additionnels indiquant le trajet de certification) pour cette clé publique d'agent MTA pour cet algorithme constituent les pouvoirs du demandeur dans l'argument de rattachement Bind.

2) La procédure détermine l'adresse d'utilisateur **user-address** de l'utilisateur MTS et tente d'établir une association avec les arguments du § 8.1.1.1.1. En cas d'échec, une indication d'échec est renvoyée et la procédure prend fin.

3) En cas de succès, les résultats renvoyés par l'utilisateur MTS (définis au § 8.1.1.1.2) sont examinés. L'exactitude du nom du demandé **responder-name** est vérifiée et la procédure tente d'authentifier l'utilisateur MTS au moyen des pouvoirs du demandé **responder-credentials** retournés.

   Dès réception du résultat du rattachement Bind, la signature du jeton responder-bind-token est vérifiée au moyen de la clé publique du **certificate** de l'utilisateur MTS pour l'algorithme de signature identifié (il s'agit éventuellement d'un algorithme de signature différent de celui qui a été utilisé pour signer le jeton initiator-bind-token). Le **certificate** de l'utilisateur MTS peut être inclus dans le résultat du rattachement Bind ou être identifié par un sélecteur **certificate-selector** et, à moins qu'il ne soit déjà à la disposition de l'agent MTA, doit être obtenu à partir de l'attribut User Certificate de l'utilisateur MTS dans l'annuaire. La validité du **certificate** et son trajet de certification sont également vérifiés. De plus, le nom d'annuaire figurant dans le champ du sujet de ce **certificate** est vérifié pour établir qu'il est effectivement celui de l'utilisateur MTS (c'est-à-dire pour s'assurer que l'utilisateur MTS demandé est l'objectif visé par le rattachement Bind). Le nom **OR-name** du champ subject-alternative-name de ce **certificate** est vérifié en ce qui concerne sa correspondance avec le nom **OR-name** de l'utilisateur MTS et avec le nom **OR-name** du champ responder-name du résultat du rattachement Bind. Le nom *mta-name* et l'identificateur global-domain-identifier contenus dans le jeton responder-bind-token sont vérifiés pour établir qu'ils sont effectivement ceux de cet agent MTA. L'heure indiquée dans le jeton est comparée à celle du moment pour garantir que la période de validité du jeton, pouvant être acceptée par cet agent MTA, n'a pas pris fin.

Si l'une des deux vérifications aboutit à un échec, la procédure libère la connexion, retourne une indication d'échec et prend fin.

4) Si les vérifications aboutissent toutes deux à un succès, la procédure retourne l'identificateur d'association et prend fin.

14.5.4 Procédure de détachement MTS-unbind demandée par l'agent MTA

Cette procédure est appelée pour libérer une association avec un utilisateur MTS.

14.5.4.1 Arguments

Identificateur interne de l'association à libérer.

14.5.4.2 Résultats

La procédure de détachement retourne un résultat vide en guise d'indication de libération de l'association.

14.5.4.3 Erreurs

Aucune.

14.5.4.4 Description de la procédure

La procédure libère l'association, renvoie un résultat vide et prend fin.

14.6 Point d'accès de dépôt submission-port

14.6.1 Procédure de dépôt de message Message-submission

Le présent paragraphe décrit le comportement de l'agent MTA lorsque l'utilisateur MTS invoque une opération abstraite de dépôt de message **Message-submission** au point d'accès de dépôt **submission-port**.

14.6.1.1 Arguments

Les arguments de dépôt de message sont énumérés au Tableau 3, qui spécifie les paragraphes où ils sont décrits.

14.6.1.2 Résultats

1) Les résultats de l'opération de dépôt de message **Message-submission**, énumérés au Tableau 5 et décrits aux paragraphes indiqués dans ce tableau, sont renvoyés à l'utilisateur MTS.
2) La procédure appelle le module de remise différée et lui passe le message déposé.

14.6.1.3 Erreurs

Voir § 8.2.1.1.3, qui décrit les erreurs abstraites se rapportant à la procédure.

14.6.1.4 Description de la procédure

1) Recherche d'erreur

   La procédure de dépôt de message **Message-submission** recherche d'éventuelles conditions d'erreur. Si une telle condition est décelée, l'erreur abstraite indiquée est renvoyée. Tout traitement ultérieur est interrompu. La responsabilité du message visé n'est pas acceptée par l'agent MTA.

   Erreurs présentant un intérêt particulier:

   a) erreurs de sécurité: si l'étiquette de sécurité de message **message-security-label** n'est pas compatible avec le contexte de sécurité **security-context** ou si, lorsqu'il est demandé, le contrôle d'authentification d'origine de message **message-origin-authentication-check** n'est pas correct, une erreur de sécurité **security-error** est produite;

   b) erreurs de criticité: si l'un des champs d'extension porte la valeur **critical-for-submission** (critique pour le dépôt) et qu'il n'est pas sémantiquement compris par l'agent MTA, la procédure retourne l'erreur fonction critique non prise en charge.

      Si aucune erreur n'est décelée à ce stade, le traitement se poursuit à l'étape 2. D'autres erreurs peuvent être décelées dans les étapes suivantes, auquel cas l'agent MTA agit comme exposé plus haut.

2) Traitement du nom

Sauf indication contraire, la procédure suivante s'applique aux arguments de nom d'expéditeur **originator-name**, de nom de destinataire **recipient-name** et de destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient**.

a) Lorsque le nom **OR-name** ne contient qu'un nom d'annuaire **directory-name**, l'agent MTA recherche l'adresse **OR-address**.

S'il s'agit d'un nom de destinataire **recipient-name**, la procédure de résolution de nom d'annuaire (voir § 14.3.12) est appelée pour déterminer une nouvelle adresse **OR-address**.

S'il n'est pas trouvé d'adresse **OR-address**, la procédure renvoie à l'expéditeur du message une indication d'erreur abstraite **recipient-improperly-specified** (destinataire incorrectement spécifié) ou un rapport de non-remise.

b) Si le nom **OR-name** contient à la fois le nom d'annuaire **directory-name** et l'adresse **OR-address**, il n'est pas nécessaire de valider leur association.

c) La validation de l'adresse **OR-address**, qu'elle ait été indiquée dans l'argument de dépôt de message ou obtenue par résolution du nom d'annuaire **directory-name**, se déroule en deux temps. La première étape confirme que l'adresse **OR-address** visée comporte la combinaison d'attributs nécessaires à la validation (voir § 8.5.5). La seconde étape, qui ne s'applique qu'au nom d'expéditeur **originator-name**, confirme que l'adresse **OR-address** est bien celle de l'utilisateur MTS ayant déposé le message.

3) Transfert de responsabilité, renvoi des résultats

Si aucune erreur n'est détectée au cours du traitement ci-dessus, l'agent MTA accepte la responsabilité du message et le signifie en retournant à l'utilisateur MTS les résultats de dépôt de message **Message-submission**. Ces résultats sont décrits au § 8.2.1.1.2. L'agent MTA établit de manière appropriée les arguments d'identificateur de dépôt de message **message-submission-identifier** et d'heure de dépôt de message **message-submission-time**. L'identificateur de contenu **content-identifier** est identique à l'argument correspondant de dépôt de message **Message-submission**. Si l'expéditeur en a fait la demande, l'agent MTA d'origine produit la preuve de dépôt **proof-of-submission** en utilisant l'algorithme identifié par l'identificateur d'algorithme de preuve de dépôt **proof-of-submission-algorithm-identifier** et les arguments définis au § 8.2.1.1.2.4. Par ailleurs, il renvoie le certificat d'agent MTA d'origine **originating-MTA-certificate**.

4) Constitution du message

Un message est alors constitué par l'assemblage des arguments de dépôt de message, éventuellement modifiés dans les étapes décrites ci-dessus, ainsi que des arguments additionnels (spécifiés au § 12.2.1.1) fournis par l'agent MTA.

Lorsque cette opération est terminée, la procédure de dépôt de message prend fin et le message est transféré au module de remise différée pour la suite du traitement.

14.6.2 Procédure de dépôt d'envoi-test Probe-submission

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'un utilisateur MTS invoque l'opération abstraite de dépôt d'envoi-test à partir d'un point d'accès de dépôt **submission-port**.

14.6.2.1 Arguments

Les arguments de dépôt d'envoi-test sont énumérés au Tableau 7 et décrits aux paragraphes indiqués dans ce tableau.

14.6.2.2 Résultats

1) Les résultats de dépôt d'envoi-test énumérés au Tableau 8 et décrits aux paragraphes indiqués dans ce tableau sont renvoyés à l'utilisateur MTS.

2) Le module principal est invoqué; l'envoi-test déposé lui est passé.

14.6.2.3 Erreurs

Le § 8.2.1.2.3 décrit les erreurs abstraites correspondantes.

14.6.2.4 Description de la procédure

1) Recherche d'erreur

   La procédure de dépôt d'envoi-test recherche les conditions d'erreur. Si elle en détecte une, l'erreur abstraite indiquée est renvoyée. L'agent MTA refuse la responsabilité de l'envoi-test proposé.

   Erreurs présentant un intérêt particulier:

   a) erreurs de sécurité: si l'étiquette de sécurité de message **message-security-label** n'est pas compatible avec le contexte de sécurité ou si le contrôle d'authentification d'origine d'envoi-test **probe-origin-authentication-check** est négatif, une erreur de sécurité est produite;

   b) erreurs de criticité: lorsqu'un champ d'extension quelconque prend la valeur **critical-for-submission** (critique pour le dépôt) mais n'est pas sémantiquement compris par l'agent MTA, ce dernier renvoie l'erreur fonction critique non prise en charge.

      Si aucune erreur n'est détectée à ce stade, le traitement se poursuit à l'étape 2. D'autres erreurs peuvent être décelées dans le traitement ultérieur, auquel cas l'agent MTA agit comme décrit plus haut.

2) Traitement du nom

   Sauf indication contraire, la procédure suivante s'applique aux arguments de nom d'expéditeur **originator-name**, de nom de destinataire **recipient-name** et de destinataire suppléant désigné par l'expéditeur **originator-requested-alternate-recipient**.

   a) Si le nom **OR-name** ne contient qu'un nom d'annuaire **directory-name**, l'agent MTA recherche l'adresse **OR-address**.

      S'il s'agit d'un nom de destinataire **recipient-name**, la procédure de résolution de nom d'annuaire (voir § 14.3.12) est appelée pour déterminer une nouvelle adresse **OR-address**.

      S'il n'est pas trouvé d'adresse **OR-address**, la procédure renvoie à l'expéditeur du message une indication d'erreur abstraite **recipient-improperly-specified** (destinataire incorrectement spécifié) ou un rapport de non-remise.

   b) Si le nom **OR-name** contient à la fois le nom d'annuaire **directory-name** et l'adresse **OR-address**, il n'est pas nécessaire de valider leur association.

   c) La validation de l'adresse **OR-address**, qu'elle ait été indiquée dans l'argument de dépôt d'envoi-test ou obtenue par résolution du nom d'annuaire **directory-name**, se déroule en deux temps. La première étape confirme que l'adresse **OR-address** visée comporte la combinaison d'attributs nécessaires à la validation (voir § 8.5.5). La seconde étape, qui ne s'applique qu'au nom d'expéditeur **originator-name**, confirme que l'adresse **OR-address** est bien celle de l'utilisateur MTS ayant déposé le message.

3) Transfert de responsabilité, retour des résultats

   Si aucune erreur n'est détectée au cours du traitement ci-dessus, l'agent MTA accepte la responsabilité de l'envoi-test et le signifie en retournant à l'utilisateur MTS les résultats de dépôt d'envoi-test. Ces résultats sont décrits au § 8.2.1.2.2. L'agent MTA établit de manière appropriée les arguments d'identificateur de dépôt d'envoi-test **probe-submission-identifier** et d'heure de dépôt d'envoi-test **probe-submission-time**. L'identificateur de contenu **content-identifier** est identique à l'argument correspondant de dépôt d'envoi-test.

4) Constitution de l'envoi-test

   Un envoi-test est alors constitué à partir des arguments de dépôt d'envoi-test, éventuellement modifiés dans les étapes décrites ci-dessus, ainsi que des arguments additionnels fournis par l'agent MTA.

   Lorsque cette opération est achevée, la procédure de dépôt d'envoi-test prend fin et l'envoi-test est transféré au module principal pour la suite du traitement.

14.6.3 Procédure d'annulation de remise différée Cancel-deferred-delivery

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'un utilisateur MTS invoque l'opération abstraite d'annulation de remise différée **Cancel-deferred-delivery** à partir d'un point d'accès de dépôt **submission-port**, afin d'annuler la remise différée d'un message déposé précédemment auprès de l'agent MTA.

14.6.3.1 Arguments

Les arguments d'annulation de remise différée sont énumérés au Tableau 10 et décrits aux paragraphes spécifiés par ce tableau.

14.6.3.2 Résultats

Un résultat vide est envoyé à l'utilisateur MTS pour lui signaler le succès de l'annulation.

14.6.3.3 Erreurs

Le § 8.2.1.3.3 décrit les erreurs abstraites correspondantes.

14.6.3.4 Description de la procédure

1) Si une preuve de dépôt **proof-of-submission** a déjà été fournie, l'agent MTA renvoie l'erreur abstraite trop tard pour annuler. La remise différée du message n'est pas annulée.
2) Si l'agent MTA estime que la valeur de l'argument identificateur de dépôt de message **message-submission-identifier** est valide et qu'elle est associée à un message qu'il retient pour remise différée, il supprime le message et n'en assume plus la responsabilité.
3) Lorsque l'agent MTA reconnaît que la valeur de l'argument identificateur de dépôt de message **message-submission-identifier** est valide mais qu'elle se réfère à un message déjà remis ou transféré à un autre agent MTA, il renvoie l'erreur abstraite trop tard pour annuler. La remise différée du message n'est pas annulée.
4) Lorsque la valeur de l'argument identificateur de dépôt de message **message-submission-identifier** n'est pas reconnue comme valide (soit que l'agent MTA n'ait jamais affecté de telle valeur, soit qu'il ne dispose plus de la chronologie d'un message à remise différée qui aurait été transféré ou remis), l'agent MTA renvoie l'erreur abstraite identificateur de dépôt de message non valide ou trop tard pour annuler le choix étant du ressort local.

14.6.4 Procédure de commande de dépôt Submission-control

Le présent paragraphe décrit le comportement de l'agent MTA lors de l'appel de l'opération abstraite de commande de dépôt pour limiter temporairement les opérations abstraites de point d'accès de dépôt que l'utilisateur MTS peut demander à partir de ce point. Ces commandes restent en vigueur pendant la durée de l'association en cours sauf nouvelle opération abstraite de commande de dépôt.

NOTE – L'utilisation de la commande de dépôt est soumise aux dispositions de la politique de sécurité en vigueur. La valeur contexte de sécurité permis **permissible-security-context** de l'argument de commande de dépôt limite le contexte de sécurité **security context** constitué pendant l'établissement de l'association.

14.6.4.1 Arguments

Les arguments de commande de dépôt sont énumérés au Tableau 12 et décrits aux paragraphes indiqués dans ce tableau.

14.6.4.2 Résultats

L'utilisateur MTS renvoie à l'agent MTA les résultats de commande de dépôt énumérés au Tableau 13 et décrits aux paragraphes spécifiés par ce tableau.

14.6.4.3 Erreurs

Une erreur de sécurité peut être renvoyée par l'utilisateur MTS. Le § 8.2.1.4.3 décrit cette erreur abstraite.

14.6.4.4 Description de la procédure

Les circonstances qui peuvent amener un agent MTA à appeler l'opération abstraite de commande de dépôt sont du ressort local, tout comme les actions menées pendant et après cette opération.

14.7 Point d'accès de remise

14.7.1 Procédure de remise de message Message-delivery

Le présent paragraphe décrit les opérations effectuées par un agent MTA lorsqu'il est chargé de remettre un message à un ou plusieurs utilisateurs MTS.

La plupart des dispositions décrites ci-dessous s'appliquent également au cas dans lequel l'agent MTA a reçu un envoi-test adressé à un ou plusieurs destinataires locaux. Sauf indication contraire, toutes les étapes de la procédure à l'exception de la remise physique s'appliquent au traitement des envois-tests.

NOTE – L'établissement de rapports est soumis aux dispositions de la politique de sécurité.

14.7.1.1 Arguments

1) Un message émanant du module principal accompagné d'instructions propres à chaque destinataire à remettre à un ou plusieurs utilisateurs MTS locaux.

2) Les arguments de remise de message énumérés au Tableau 15 et décrits aux paragraphes indiqués dans ce tableau sont transmis à l'utilisateur MTS destinataire.

14.7.1.2 Résultats

1) Si un rapport n'est pas requis, la remise avec succès est signalée par le retour d'un résultat vide ou, sur demande, d'une preuve de remise **proof-of-delivery** et d'un certificat de destinataire **recipient-certificate** facultatif de l'utilisateur MTS.

2) Si un rapport est requis, le module principal est appelé et un message lui est transféré, accompagné d'indications propres à chaque destinataire décrivant les éventuels problèmes de remise rencontrés et signalant les remises avec succès dont il est demandé de rendre compte.

14.7.1.3 Erreurs

Le § 8.3.1.1.3 décrit les erreurs abstraites de remise de message **Message-delivery** que l'utilisateur MTS peut retourner à l'agent MTA. Ces conditions d'erreur sont signalées au module principal dans les résultats décrits ci-dessus.

14.7.1.4 Description de la procédure

1) Lorsque le message parvient à expiration, une instruction de rapport est produite pour chaque destinataire local. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent respectivement les valeurs **unable-to-transfer** (impossibilité de transfert) et **maximum-time-expired** (expiration du délai maximal). La procédure prend alors fin.

2) Lorsqu'un des champs d'extension **extension-fields** propres à chaque message porte la valeur **critical-for-delivery** (critique pour la remise) sans être sémantiquement compris par l'agent MTA, une instruction de rapport est produite pour chaque destinataire local. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent respectivement les valeurs **unable-to-transfer** (impossibilité de transfert) et **unsupported-critical-function** (fonction critique non prise en charge).

3) Sinon, des valeurs sont établies pour les arguments applicables à tous les destinataires de l'opération abstraite de remise de message (les arguments de cette opération abstraite sont décrits au § 8.3.1.1.1).

4) Les étapes 5 à 16 sont exécutées pour chaque destinataire dont l'argument de responsabilité **responsibility** porte la valeur **responsible** (responsable). La procédure prend alors fin.

5) Pour garantir le respect de la politique de sécurité pendant la remise, l'étiquette de sécurité de message **message-security-label** est comparée au contexte de sécurité **security-context**. Lorsque la remise est interdite par la politique de sécurité, une instruction de rapport pour ce destinataire est établie, sous réserve des dispositions de la politique de sécurité. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent respectivement les valeurs **unable-to-transfer** (impossibilité de transfert) et **secure-messaging-error** (erreur de sécurité de messagerie).

6) Lorsque la remise est interdite par des commandes de remise imposées au cours d'une opération abstraite antérieurement appelée de commande d'enregistrement ou de commande de remise, l'agent MTA, sous réserve des dispositions de la politique de sécurité en vigueur, gardera le message en attente, jusqu'à la levée des commandes applicables. Les commandes de remise ne sont pas applicables aux messages d'essai.

7) Si le délai maximal de rétention d'un message est dépassé (le choix de ce délai étant du ressort local, sauf que l'heure limite de remise **latest-delivery-time** sera respectée si elle est indiquée et si elle porte la mention de criticité **critical-for-delivery**) et que les restrictions applicables soient toujours en vigueur, une instruction de rapport est produite pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent alors respectivement les valeurs **unable-to-transfer** (impossibilité de transfert) et **recipient-unavailable** (destinataire occupé). Le traitement prend alors fin pour ce destinataire.

NOTE 1 – Les étapes de traitement (6 et 7 ci-dessus) associées aux restrictions de commande ne s'appliquent pas aux envois-tests.

8) Lorsqu'une restriction de remise est en vigueur et que l'expéditeur appartient à la catégorie des expéditeurs non autorisés, une instruction de rapport est produite pour le destinataire. Le code de motif de non-remise **non-delivery-reason-code** prend la valeur **restricted-delivery** (remise restreinte). Le traitement prend alors fin pour ce destinataire.

9) L'agent MTA détermine les arguments de l'opération abstraite de remise de message qui ne s'appliquent qu'à un destinataire individuel: l'identificateur de remise de message **message-delivery-identifier** et l'heure de remise de message **message-delivery-time** reçoivent des valeurs comme indiqué aux § 8.3.1.1.1.1 et 8.3.1.1.1.2. Si le message contient une chronologie de réacheminement **redirection-history** ou une chronologie de développement de liste **dl-expansion-history**, le nom du destinataire initialement prévu **originally-intended-recipient-name** sera recopié à partir du premier élément de la chronologie de réacheminement ou de la chronologie de développement de liste, selon l'événement qui a eu lieu en premier (l'ordre de ces événements est déterminé à partir des informations de trace **trace-information**). Tous les autres arguments sont directement recopiés à partir des champs correspondants du message à remettre. Aux exceptions près indiquées ci-dessous, tous les arguments du Tableau 15 sont inclus dans chaque appel de la procédure de remise de message.

10) Si l'argument de divulgation des autres destinataires **disclosure-of-other-recipients** a la valeur **disclosure-of-other-recipients-requested** (divulgation des autres destinataires demandée), l'argument de nom d'autre destinataire **other-recipient-name** reçoit les informations suivantes:

    a) le nom **OR-name** de tous les destinataires initialement spécifiés ayant un numéro **originally-specified-recipient-number** différent de celui du destinataire en cours. Pour chaque destinataire pour lequel il y a eu renvoi, le nom **OR-name** de destinataire initialement spécifié correspond à la première entrée de la chronologie de renvoi associée;

    b) si un développement de liste de distribution a eu lieu, le nom **OR-name** de la première entrée de la chronologie de développement **DL-expansion-history**.

    Si le destinataire appartient à une liste de distribution, les autres membres de cette liste ne doivent pas être inscrits dans l'argument **other-recipient-name** (autre destinataire). Le destinataire est membre d'une liste de distribution si le champ de chronologie de développement de liste **DL-expansion-history** n'est pas vide.

11) Lorsqu'un des champs d'extension propres à chaque destinataire a la valeur **critical-for-delivery** (critique pour la remise), mais n'est pas sémantiquement compris par l'agent MTA, une instruction de rapport est produite pour ce destinataire. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent respectivement les valeurs **unable-to-transfer** (impossibilité de transfert) et **unsupported-critical-function** (fonction critique non prise en charge).

12) En cas de remise à une unité d'accès de remise physique PDAU, les arguments de remise physique sont compris dans la remise de message. Ces arguments sont décrits aux § 8.2.1.1.1.14 à 8.2.1.1.1.23.

13) Lorsque toutes les conditions de succès sont réunies, l'agent MTA remet physiquement le message. L'accomplissement de la remise à un utilisateur MTS destinataire local à l'agent MTA est du ressort local. Dans le cas d'un utilisateur MTS destinataire distant, l'agent MTA établit une association avec cet utilisateur MTS (ou utilise une association existante) et appelle à travers cette association l'opération abstraite de remise de message. Après remise distante ou locale avec succès, la responsabilité du message passe de l'agent MTA à l'utilisateur MTS destinataire.

14) Après une remise avec succès et si la demande de rapport de remise de l'agent MTA d'origine **originating-MTA-delivery-report-request** a la valeur **report** (rapport) ou **audited-report** (rapport vérifié), une instruction de rapport est produite afin de rendre compte du succès de remise. Le traitement prend alors fin pour ce destinataire.

15) Dans le cas d'un utilisateur MTS destinataire distant, si aucune association initiale n'existe ou ne peut être établie, ou s'il y a défaillance de transfert à travers l'association, l'agent MTA peut répéter la tentative de transfert ou d'établissement de l'association, le nombre maximal ou la durée maximale des tentatives relevant d'un choix local (sauf que l'heure limite de remise **latest-delivery-time** doit être respectée si elle est indiquée et si elle porte la mention de criticité **critical-for-delivery**). Si, après des tentatives répétées, le transfert n'a toujours pas eu lieu, le message est considéré comme impossible à remettre et une instruction de rapport est produite, sous réserve des dispositions de la politique de sécurité en vigueur. Le code de motif de non-remise **non-delivery-reason-code** et le code de diagnostic de non-remise **non-delivery-diagnostic-code** prennent respectivement les valeurs **transfer-failure** (échec de transfert) et **recipient-unavailable** (destinataire occupé). Le traitement prend alors fin pour ce destinataire.

NOTE 2 – Les étapes de traitement associées au transfert physique d'un message vers un utilisateur MTS destinataire ne s'appliquent pas à l'envoi-test.

16) Retour des résultats et des erreurs par l'utilisateur MTS

    Lorsque l'opération abstraite de remise de message aboutit, l'utilisateur MTS retourne comme indication de succès, soit un résultat vide soit, sur demande, une preuve de remise **proof-of-delivery** et un certificat de destinataire **recipient-certificate** facultatif.

Lorsque l'opération abstraite de remise de message enfreint un ou plusieurs contrôles imposés par une opération abstraite antérieure de commande de remise ou d'enregistrement Registre, l'utilisateur MTS renvoie l'erreur (commande de remise enfreinte). Lorsque le contexte de sécurité **security-context** interdit à l'utilisateur MTS de prendre en charge l'opération abstraite demandée car cela enfreindrait la politique de sécurité, l'utilisateur MTS retourne une erreur de sécurité. Dans ce cas, l'appel de la procédure de remise de message échoue et l'agent MTA conserve la responsabilité du message en ce qui concerne ce destinataire. Le message est soit retenu pour tenter ultérieurement une nouvelle remise, soit transféré au module principal pour l'établissement d'un rapport. Le traitement prend alors fin pour ce destinataire.

14.7.2 Procédure d'essai de remise d'envoi-test Probe-delivery-test

Le présent paragraphe décrit les étapes suivies par un agent MTA chargé de s'assurer qu'un envoi-test peut être remis.

NOTE – L'utilisation des rapports est soumise aux dispositions de la politique de sécurité en vigueur.

14.7.2.1 Arguments

1) Un envoi-test provenant de la procédure interne avec des instructions propres à chaque destinataire, pour un essai de remise d'envoi-test à un ou plusieurs utilisateurs MTS locaux.

14.7.2.2 Résultats

Le module principal est invoqué pour lui transférer l'envoi-test avec les instructions propres à chaque destinataire précisant si la remise hypothétique aurait eu lieu, ou sinon, pourquoi.

14.7.2.3 Erreurs

Aucune.

14.7.2.4 Description de la procédure

La logique de la procédure de remise de message est décrite au § 14.7.1. Toutes les étapes sont ici exécutées sauf celles pour lesquelles il est explicitement mentionné qu'elles ne s'appliquent pas à l'envoi-test.

14.7.3 Procédure de remise de rapport Report-delivery

Le présent paragraphe décrit les étapes suivies par un agent MTA chargé de remettre un rapport à un utilisateur MTS. La procédure de remise de rapport est appelée lorsqu'un agent MTA reçoit un rapport provenant du module de rapport entrant ou produit dans l'agent MTA lui-même et dont le champ de nom d'expéditeur **originator-name** spécifie un utilisateur MTS desservi par cet agent MTA.

14.7.3.1 Arguments

1) Un rapport émanant du module de rapport avec des instructions propres à chaque destinataire pour la remise à un destinataire local.
2) Les arguments de remise de rapport énumérés au Tableau 18 et décrits aux paragraphes indiqués dans ce tableau sont transmis à l'utilisateur MTS destinataire.

14.7.3.2 Résultats

Un résultat vide est retourné par l'utilisateur MTS, en guise d'indication de remise avec succès.

14.7.3.3 Erreurs

Le § 8.3.1.2.3 décrit les erreurs de remise de rapport pouvant être retournées à l'agent MTA par l'utilisateur MTS.

14.7.3.4 Description de la procédure

1) Pour garantir le respect de la politique de sécurité pendant la remise de rapport, l'étiquette de sécurité de message **message-security-label** est comparée au contexte de sécurité. Si la remise du rapport est interdite par la politique de sécurité, le rapport est supprimé.
2) Si la remise de rapport est interdite par des restrictions imposées lors d'une opération abstraite antérieure d'enregistrement (Register) ou de commande de remise, l'agent MTA, sous réserve de la politique de sécurité en vigueur, retiendra le rapport jusqu'à la levée des restrictions applicables. Ces restrictions sont établies par les arguments de l'opération abstraite d'enregistrement ou de commande de remise décrits au § 8.3.1.3.1.

   Si le délai maximal de rétention d'un rapport (dont la fixation est du ressort local) est écoulé et si les restrictions sont toujours en vigueur, le rapport est ignoré.

3) Les arguments de l'opération abstraite de remise de rapport sont recopiés à partir des champs correspondants du rapport.

4) Si un champ d'extension quelconque propre à un message ou à un destinataire porte la valeur **critical-for-delivery** (critique pour la remise) sans être sémantiquement compris par l'agent MTA, le rapport est supprimé.

5) L'accomplissement d'une remise de rapport à un utilisateur MTS local est du ressort local. Dans le cas d'un utilisateur MTS distant, l'agent MTA établit avec lui une association (ou utilise une association existante) et invoque l'opération abstraite de remise de rapport via cette association. Lorsque la remise de rapport locale ou distante s'achève avec succès, la responsabilité du rapport passe de l'agent MTA à l'utilisateur MTS.

6) Si, dans le cas d'un utilisateur MTS distant, une association ne peut être initialement établie, l'agent MTA peut renouveler la tentative, le nombre et la durée maximale des tentatives étant du ressort local. Si, à l'issue des tentatives répétées, aucune association n'a été établie, le rapport, considéré comme impossible à remettre, est ignoré.

7) Renvoi des résultats et des erreurs par l'utilisateur MTS

   Si l'opération abstraite de remise de rapport s'achève avec succès, l'utilisateur MTS le signale en retournant un résultat vide.

   Si l'opération abstraite de remise de rapport enfreint un ou plusieurs contrôles imposés par une opération abstraite antérieure d'enregistrement ou de commande de remise, l'utilisateur MTS retourne l'erreur commande de remise enfreinte. Dans ce cas, la procédure de demande de remise de rapport a échoué et l'agent MTA conserve la responsabilité du rapport.

14.7.4 Procédure de commande de remise Delivery-control

Le présent paragraphe décrit le comportement de l'agent MTA lorsque l'opération abstraite de commande de remise est appelée par un utilisateur MTS desservi par cet agent MTA. La commande de remise impose et lève les restrictions concernant les opérations abstraites de remise de message et de remise de rapport. Ces commandes demeurent en vigueur pendant toute la durée de l'association en cours, sauf modification par une commande de remise ultérieure. Les commandes de remise limitent temporairement le contexte de sécurité **security-context** mais ne peuvent pas enfreindre la politique de sécurité.

Ces commandes ne s'appliquent pas au traitement des envois-tests par l'agent MTA.

14.7.4.1 Arguments

Les arguments de commande de remise énumérés au Tableau 20 et décrits au § 8.3.1.3.1.

14.7.4.2 Résultats

1) L'agent MTA renvoie à l'utilisateur MTS les résultats de commande de remise énumérés au Tableau 21 et décrits au § 8.3.1.3.2.

2) Divers paramètres de commande de l'utilisateur MTS consignés par cet agent MTA sont remplacés par les valeurs correspondantes véhiculées par les arguments de commande de remise.

14.7.4.3 Erreurs

Les erreurs abstraites correspondantes sont décrites au § 8.3.1.3.3.

14.7.4.4 Description de la procédure

1) Si la valeur de l'argument de restriction **restrict** est **remove** (supprimer), toutes les commandes établies par une quelconque commande de remise antérieure sont supprimées; l'opération abstraite est achevée et le résultat est renvoyé à l'utilisateur MTS.

2) Si la valeur de l'argument de restriction **restrict** est **update** (mettre à jour) et qu'aucun autre argument ne soit présent, la requête est considérée comme valide et le résultat est renvoyé à l'utilisateur MTS.

   Dans ce cas, toutes les valeurs de commande en vigueur restent inchangées.

3) Si la valeur de l'argument de restriction **restrict** est **update** (mettre à jour) et que d'autres arguments soient présents, il est procédé à la vérification de la compatibilité de ces arguments avec les conditions à long terme spécifiées pour le point d'accès d'administration **administration-port** par l'opération abstraite d'enregistrement (Register) appelée en dernier (voir § 14.4.1). Si aucune incompatibilité n'est décelée, et que la mise à jour soit autorisée dans le cadre de la politique de sécurité, les mises à jour indiquées sont effectuées; l'opération abstraite est achevée et le résultat est renvoyé à l'utilisateur MTS.

4) Si l'une des incompatibilités suivantes avec les conditions à long terme est décelée, l'agent MTA renvoie l'erreur abstraite (infraction aux paramètres d'enregistrement par la commande):

   a) les types permis d'information codée **permissible-encoded-information-types** ne sont pas spécifiés parmi les types autorisés à long terme;

   b) les types permis de contenu **permissible-content-types** ne sont pas spécifiés parmi les contenus admis à long terme;

   c) la longueur maximale permise de contenu **permissible-maximum-content-length** dépasse la longueur admise à long terme;

   d) le contexte de sécurité permis **permissible-security-context** n'est pas respecté.

   Dans chacun de ces cas d'erreur, la commande de remise est rejetée et n'est pas effectuée.

14.8 Accès d'administration

14.8.1 Procédure enregistrement (Register)

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'un utilisateur MTS desservi par cet agent MTA invoque l'opération abstraite d'enregistrement (Register).

14.8.1.1 Arguments

Les arguments de la procédure d'enregistrement énumérés dans le Tableau 23 et décrits aux paragraphes indiqués dans ce tableau.

14.8.1.2 Résultats

1) Si l'argument **retrieve-registrations (**extraction d'enregistrements) est présent, les informations enregistrées demandées sont renvoyées dans le résultat. Un argument Register extension (extension d'enregistrement) peut également entraîner le renvoi d'informations complémentaires; dans le cas contraire, un résultat vide est renvoyé.

2) Divers paramètres relatifs à l'utilisateur MTS consignés par l'agent MTA sont remplacés par des valeurs figurant dans les arguments de la procédure d'enregistrement.

14.8.1.3 Erreurs

Voir § 8.4.1.1.3 pour une description des erreurs abstraites pertinentes.

14.8.1.4 Description de la procédure

1) L'exactitude de la spécification des arguments d'enregistrement est vérifiée. En cas d'erreur, la procédure renvoie l'erreur Register-rejected (rejet d'enregistrement) et prend fin. Selon la politique locale ou des dispositions d'abonnement, l'agent MTA peut imposer des restrictions supplémentaires aux enregistrements qui peuvent être effectués par l'utilisateur MTS; si ces restrictions ne sont pas respectées, une erreur abstraite est renvoyée à l'utilisateur MTS et aucune étape supplémentaire n'est traitée.

2) Si les arguments d'enregistrement sont correctement spécifiés, les valeurs des paramètres d'utilisateur MTS sont remplacées par celles des arguments de l'enregistrement. Si l'argument **recipient-assigned-redirections** (réacheminement désigné par le destinataire) contient une seule **restriction** dans laquelle tous les types de source sont permis et dans laquelle le nom de source est omis (dans le contexte d'application de la Norme de 1994) ou contient le nom OR (**OR-name**) de l'utilisateur MTS (dans le contexte d'application de la Norme de 1988), aucun destinataire de ce type n'est enregistré. Si l'argument **retrieve-registrations** (extraction enregistrements) est présent, les informations enregistrées demandées sont renvoyées.

14.8.2 Procédure de modification des pouvoirs Change-credentials à l'initiative de l'utilisateur MTS

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'une opération abstraite de modification des pouvoirs **Change-credentials** est invoquée par l'utilisateur MTS.

NOTE – Toutes les modifications de pouvoirs sont soumises à la politique de sécurité en vigueur.

14.8.2.1 Arguments

Les arguments de modification de pouvoirs sont énumérés dans le Tableau 25 et décrits au § 8.4.1.2.1.

14.8.2.2 Résultats

1) La procédure de modification des pouvoirs **Change-credentials** renvoie un résultat vide à l'utilisateur MTS pour signaler la réussite de l'opération.
2) Les pouvoirs de l'utilisateur MTS consignés par cet agent MTA sont modifiés conformément à l'argument de nouveaux pouvoirs **new-credentials**.

14.8.2.3 Erreurs

Les erreurs abstraites nouveaux pouvoirs inacceptables ou anciens pouvoirs incorrectement spécifiés, telles qu'elles sont indiquées au Tableau 26 et décrites au § 8.4.1.2.3.

14.8.2.4 Description de la procédure

NOTE – Toutes les modifications de pouvoirs sont sujettes à la politique de sécurité en vigueur.

1) Si la valeur de l'argument anciens pouvoirs **old-credentials** n'est pas identique aux pouvoirs consignés par l'agent MTA pour l'utilisateur MTS invoquant l'opération abstraite, l'erreur anciens pouvoirs incorrectement spécifiés est retournée à l'utilisateur MTS et la procédure de modification des pouvoirs prend fin.
2) Sinon, la validité de l'argument nouveaux pouvoirs **new-credentials** est vérifiée. S'il n'est pas valide (il s'agit d'une question du ressort local liée à la politique de sécurité), une erreur nouveaux pouvoirs inacceptables est renvoyée à l'utilisateur MTS et la procédure de modification des pouvoirs prend fin.
3) Sinon, les pouvoirs de l'utilisateur MTS consignés par cet agent MTA sont modifiés à la valeur de l'argument de nouveaux pouvoirs **new-credentials** et un résultat vide est renvoyé à l'utilisateur MTS comme indication de succès; la procédure de modification des pouvoirs prend alors fin.

14.8.3 Procédure de modification des pouvoirs à l'initiative de l'agent MTA

Le présent paragraphe décrit le comportement d'un agent MTA lors de la modification de ses pouvoirs consignés par un utilisateur MTS local.

NOTE – Toutes les modifications de pouvoirs sont assujetties à la politique de sécurité en vigueur.

14.8.3.1 Arguments

Les arguments de modification des pouvoirs sont énumérés dans le Tableau 25 et décrits au § 8.4.1.2.1.

14.8.3.2 Résultats

L'utilisateur MTS renvoie un résultat vide à la procédure de modification des pouvoirs comme indication de succès.

14.8.3.3 Erreurs

L'utilisateur MTS peut renvoyer l'erreur nouveaux pouvoirs inacceptables ou anciens pouvoirs incorrectement spécifiés, comme cela est indiqué au § 8.4.1.2.3 et spécifié dans le Tableau 26.

14.8.3.4 Description de la procédure

NOTE – Toutes les modifications de pouvoirs sont assujetties à la politique de sécurité en vigueur.

1) La procédure invoque l'opération abstraite de modification des pouvoirs afin de modifier les pouvoirs de l'agent MTA consignés par un utilisateur MTS local. Les conditions amenant un agent MTA à modifier ses pouvoirs sont du ressort local.
2) S'il reçoit de l'utilisateur MTS l'erreur nouveaux pouvoirs inacceptables ou anciens pouvoirs incorrectement spécifiés, l'agent MTA doit comprendre que ses pouvoirs n'ont pas été modifiés. D'autres mesures, d'un ressort local, peuvent être prises et la procédure prend fin.
3) Si l'utilisateur MTS répond par un résultat vide, l'agent MTA en déduira que la procédure a abouti et que ses pouvoirs sont modifiés. La procédure prend fin.

14.9 Rattachement MTA-bind et détachement MTA-unbind

14.9.1 Procédure de rattachement en entrée MTA-bind-in

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'une procédure de rattachement est invoquée par un autre agent MTA.

14.9.1.1 Arguments

Les arguments de rattachement sont définis au § 12.1.1.1.1 et énumérés au Tableau 28.

14.9.1.2 Résultats

Les résultats de rattachement sont définis au § 12.1.1.1.2 et énumérés au Tableau 29.

14.9.1.3 Erreurs

Les erreurs de rattachement sont définies au § 12.1.2.

14.9.1.4 Description de la procédure

1) Si les ressources de l'agent MTA ne peuvent assurer, sur le moment, l'établissement d'une nouvelle association, la procédure retourne l'erreur de rattachement occupé et prend fin.

2) Sinon, et si la politique de sécurité impose une authentification, l'agent MTA tente à la fois d'authentifier le MTA appelant par le biais des pouvoirs du demandeur **initiator-credentials** tels qu'ils sont fournis dans la demande, et de vérifier l'acceptabilité du contexte de sécurité.

   Si les pouvoirs du demandeur **initiator-credentials** contiennent des pouvoirs renforcés **strong-credentials**, la signature du jeton initiator-bind-token est vérifiée au moyen de la clé publique du **certificate** de l'agent MTA demandeur pour l'algorithme de signature identifié. Le **certificate** de l'agent MTA demandeur peut être inclus dans les pouvoirs du demandeur dans l'argument de rattachement Bind, ou être identifié par le sélecteur **certificate-selector** et, à moins qu'il ne soit déjà à la disposition de l'agent MTA, être obtenu à partir de l'attribut User Certificate de l'agent MTA contenu dans l'annuaire. La validité du **certificate** et son trajet de certification sont également vérifiés. De plus, le nom d'annuaire contenu dans le champ de ce certificat est vérifié pour établir qu'il est effectivement celui de l'agent MTA. Le nom mta-name du champ subject-alternative-name de ce certificat est vérifié relativement à sa correspondance avec le nom MTA de l'agent MTA demandeur et de l'identificateur Global Domain Identifier et avec le nom **mta-name** contenu dans le champ initiator-name du rattachement Bind. Le nom mta-name et l'identificateur global-domain-identifier contenu dans le jeton initiator-bind-token sont vérifiés pour établir qu'ils sont effectivement ceux de cet agent MTA. L'heure indiquée dans le jeton est comparée à celle du moment pour garantir que la période de validité du jeton, pouvant être acceptée par cet agent MTA, n'a pas pris fin.

   Le jeton responder-bind-token est produit au moyen du même algorithme de signature (à moins qu'un autre algorithme, qui lui est préféré, ne soit réputé être accepté par le demandeur), et de la clé privée de cet agent MTA pour signer un jeton qui comprend l'identificateur d'algorithme pour l'algorithme de signature, le nom mta-name et l'identificateur global domain identifier de l'agent MTA demandeur, l'heure actuelle et un nombre aléatoire en tant que données de type bind-token-signed-data. Le jeton responder-bind-token et le sélecteur **certificate-selector** ou le **certificate** (et les certificats additionnels qui indiquent le trajet de certification) pour cette clé publique d'agent MTA dans cet algorithme forment les pouvoirs du demandé dans le résultat du rattachement Bind.

   Si les pouvoirs du demandeur **initiator-credentials** ne peuvent être authentifiés, la procédure renvoie une erreur d'authentification et prend fin. Si le contexte de sécurité **security-context** n'est pas acceptable, la procédure retourne une erreur de contexte de sécurité inacceptable et prend fin.

3) Si l'authentification est positive et si le contexte de sécurité **security-context** est acceptable, l'agent MTA établit l'association demandée. La procédure retourne le nom **MTA-name** et les pouvoirs du demandé **responder-credentials**. La procédure prend alors fin.

4) Si l'authentification n'est pas exigée, aucun résultat n'est à renvoyer et la procédure prend fin.

14.9.2 Procédure de détachement en entrée MTA-unbind-in

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'une procédure de détachement est invoquée par un autre agent MTA pour libérer une association existante.

14.9.2.1 Arguments

Aucun.

14.9.2.2 Résultats

La procédure de détachement en entrée retourne un résultat vide pour indiquer la libération de l'association.

14.9.2.3 Erreurs

Aucune.

14.9.2.4 Description de la procédure

La procédure libère l'association, retourne un résultat vide et prend fin.

14.9.3 Procédure de rattachement en sortie MTA-bind-out

Le présent paragraphe décrit les opérations exécutées par un agent MTA chargé d'établir une association avec un autre agent MTA.

14.9.3.1 Arguments

1) Le nom **MTA-name** de l'agent MTA avec lequel l'association doit être établie.
2) Le contexte de sécurité **security-context** de cette association.

14.9.3.2 Résultats

Un identificateur interne pour l'association établie.

14.9.3.3 Erreurs

La procédure retourne une indication d'échec si l'association ne peut être établie.

14.9.3.4 Description de la procédure

1) La procédure procède à la valuation des arguments définis au § 12.1.1.1.1. Les valeurs des arguments **initiator-name** (nom du demandeur), **security-context** (contexte de sécurité) et **initiator-credentials** (pouvoirs du demandeur) sont reprises des informations internes.

   Si les pouvoirs du demandeur **initiator-credentials** contiennent des pouvoirs renforcés **strong-credentials**, l'agent MTA sélectionne un algorithme de signature qui est accepté par l'agent MTA visé et utilise cet algorithme pour signer un jeton initiator-bind-token comprenant l'identificateur d'algorithme pour cet algorithme, le nom mta-name et l'identificateur Global Domain Identifier de l'agent MTA visé, l'heure actuelle et un nombre aléatoire en tant que données de type bind-token-signed-data. Ce jeton initiator-bind-token et le sélecteur **certificate-selector** ou le **certificate** (et les certificats additionnels qui indiquent le trajet de certification) pour cette clé publique d'agent MTA dans cet algorithme forment les pouvoirs du demandeur dans l'argument de rattachement Bind.

2) La procédure détermine l'adresse de l'agent MTA et tente d'établir une association avec les arguments décrits au § 12.1.1.1.1. Si le résultat est négatif, une indication d'échec est retournée et la procédure prend fin.

3) En cas de succès, les résultats (définis au § 12.1.1.1.2) retournés par l'agent MTA appelé sont examinés. Le nom du demandé **responder-name** est vérifié et une authentification de l'agent MTA est tentée au moyen des pouvoirs du demandé **responder-credentials** qui ont été retournés. Si l'une des vérifications aboutit à un échec, la procédure retourne au demandeur une indication d'échec, met fin à l'association et s'achève.

   Dès réception du résultat du rattachement Bind, la signature du jeton responder-bind-token est vérifiée au moyen de la clé publique du **certificate** de l'utilisateur MTS pour l'algorithme de signature identifié (il s'agit éventuellement d'un algorithme de signature différent de celui qui a été utilisé pour signer le jeton initiator-bind-token). Le **certificate** de l'utilisateur MTS peut être inclus dans le résultat du rattachement Bind ou être identifié par un sélecteur **certificate-selector** et, à moins qu'il ne soit déjà à la disposition de l'agent MTA, être obtenu à partir de l'attribut User Certificate de l'agent MTA contenu dans l'annuaire. La validité du **certificate** et son trajet de certification sont également vérifiés. De plus, le nom d'annuaire figurant dans le champ du sujet de ce **certificate** est vérifié pour établir qu'il s'agit bien du nom de l'agent MTA (c'est-à-dire pour s'assurer que l'agent MTA demandé est l'objectif visé par le rattachement Bind). Le nom mta-name du champ subject-alternative-name de ce **certificate** est vérifié en ce qui concerne sa correspondance avec le nom MTA et l'identificateur Global Domain Identifier de l'agent MTA et avec le

nom mta-name du champ responder-name du résultat du rattachement Bind. Le nom mta-name et l'identificateur global-domain-identifier, contenus dans le jeton responder-bind-token, sont vérifiés pour établir qu'ils sont bien ceux de cet agent MTA. L'heure indiquée dans le jeton est comparée à celle du moment pour garantir que la période de validité des jetons, pouvant être acceptée par cet agent MTA, n'a pas pris fin. Si l'une de ces vérifications échoue, la procédure renvoie à l'appelant une indication d'échec, met fin à l'association et s'arrête.

4) Si toutes les vérifications aboutissent à un succès, la procédure retourne un identificateur d'association et prend fin.

14.9.4 Procédure de détachement en sortie MTA-unbind-out

Cette procédure est appelée pour libérer une association existant avec un autre agent MTA.

14.9.4.1 Arguments

L'identificateur interne de l'association à libérer.

14.9.4.2 Résultats

La procédure de détachement en sortie retourne un résultat vide comme indication de libération de l'association.

14.9.4.3 Erreurs

Aucune.

14.9.4.4 Description de la procédure

La procédure libère l'association, retourne un résultat vide et prend fin.

14.10 Accès de transfert

NOTE – Les actions entreprises au niveau de l'accès de transfert sont assujetties à la politique de sécurité en vigueur.

14.10.1 Procédure de message entrant Message-in

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'une opération abstraite de transfert de message est invoquée par un autre agent MTA à un accès de transfert.

14.10.1.1 Arguments

Les arguments de la procédure de transfert de message sont énumérés dans le Tableau 30 et décrits aux paragraphes indiqués dans ce tableau.

14.10.1.2 Résultats

Le module de remise différée est appelé et le message transféré en entrée lui est passé.

14.10.1.3 Erreurs

Aucune.

14.10.1.4 Description de la procédure

Dès réception d'un message à l'occasion d'une opération abstraite de transfert de message (appelée par un agent MTA voisin), la procédure de message entrant est invoquée. Celle-ci passe simplement le message au module de remise différée afin de déterminer la suite à donner par cet agent MTA.

La responsabilité du message passe à l'agent MTA appelé une fois ce transfert réussi.

14.10.2 Procédure d'envoi-test entrant Probe-in

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'une opération abstraite de transfert d'envoi-test **Probe-transfer** est invoquée par un autre agent MTA au niveau d'un accès de transfert.

14.10.2.1 Arguments

Les arguments de la procédure de transfert d'envoi-test sont énumérés au Tableau 31 et décrits aux paragraphes indiqués dans ce tableau.

14.10.2.2 Résultats

Le module principal est appelé et l'envoi-test en entrée lui est passé.

14.10.2.3 Erreurs

Aucune.

14.10.2.4 Description de la procédure

Dès réception d'un envoi-test à l'occasion d'une opération abstraite de transfert d'envoi-test (invoquée par un agent MTA voisin), la procédure d'envoi-test entrant est invoquée. Elle passe simplement l'envoi-test au module principal afin de déterminer la suite à donner par cet agent MTA.

La responsabilité de l'envoi-test passe à l'agent MTA récepteur une fois ce transfert réussi.

14.10.3 Procédure de rapport entrant Report-in

Le présent paragraphe décrit le comportement de l'agent MTA lorsqu'il reçoit un rapport à un accès de transfert à l'occasion d'une opération abstraite de transfert de rapport appelée par un autre agent MTA, ou lorsqu'il reçoit d'une unité d'accès (une PDAU par exemple) une indication l'invitant à produire un rapport.

14.10.3.1 Arguments

Les arguments de rapport sont énumérés dans le Tableau 32 et décrits aux paragraphes indiqués dans ce tableau.

14.10.3.2 Résultats

Le module de rapport est appelé et le rapport transféré en entrée lui est passé.

14.10.3.3 Erreurs

Aucune.

14.10.3.4 Description de la procédure

Dès réception d'un rapport à l'occasion d'une opération abstraite de transfert de rapport (invoquée par un agent MTA voisin) ou dès réception d'une indication l'invitant à produire un rapport depuis une unité d'accès (une PDAU par exemple), la procédure de rapport entrant est invoquée. Elle passe simplement le rapport au module de rapport afin de déterminer la suite à donner par cet agent MTA.

La responsabilité du rapport passe à l'agent MTA appelé une fois le transfert réussi.

14.10.4 Procédure de message sortant Message-out

Le présent paragraphe décrit les actions effectuées par un agent MTA chargé de transférer un message à un autre agent MTA.

14.10.4.1 Arguments

Un message provenant de la procédure interne avec des instructions d'acheminement pour le transfert à un autre agent MTA. Les champs de ce message constituent les arguments de l'opération abstraite de transfert de message tels qu'ils sont énumérés au Tableau 30.

14.10.4.2 Résultats

Aucun.

14.10.4.3 Erreurs

En cas d'échec du transfert, le module principal est invoqué et le message lui est passé avec une instruction propre à chaque message indiquant le motif de l'échec.

14.10.4.4 Description de la procédure

Le message à transférer fournit les arguments de l'opération abstraite de transfert de message. A noter que le message peut refléter le traitement (conversion de contenu, réacheminement ou développement de liste de distribution par exemple) effectué dans l'agent MTA courant ou dans les agents MTA précédents.

1) Pour garantir que la politique de sécurité n'est pas enfreinte au cours du transfert, l'étiquette de sécurité de message **message-security-label** est comparée au contexte de sécurité **security-context**. Si le transfert est interdit par la politique de sécurité ou par des restrictions temporaires, le processus se poursuit à l'étape 3 ci-dessous.

2) Sinon, l'agent MTA établit une association avec l'agent MTA récepteur (ou utilise une association existante) et invoque l'opération abstraite de transfert de message à travers cette association. L'achèvement de la procédure de message sortant indique le succès du transfert et que l'agent MTA récepteur accepte désormais la responsabilité du message. La procédure de message sortant prend alors fin.

   Si l'agent MTA expéditeur reçoit du système récepteur l'instruction de faire avorter le transfert, le traitement se poursuit à l'étape 3 ci-dessous.

   S'il n'existe pas d'association et si aucune autre ne peut être établie au départ, ou s'il y a échec du transfert à travers une association, l'agent MTA peut tenter à nouveau d'établir une association ou d'effectuer le transfert, le nombre maximal et la durée maximale des tentatives étant du ressort local, sauf que l'heure limite de remise **latest-delivery-time** sera respectée si elle est indiquée et si elle porte la mention de criticité **critical-for-transfer**.

3) Si après plusieurs tentatives, le transfert n'a pas eu lieu, ou si une infraction aux règles de sécurité a été détectée au cours de l'étape 1, ou si l'agent MTA expéditeur reçoit une instruction pour mettre fin au transfert au cours de l'étape 2, le message, jugé non transférable, est retourné, avec indication du motif de l'échec au module principal pour un possible réacheminement ou renvoi. L'agent MTA émetteur garde la responsabilité du message. La procédure message sortant prend alors fin.

NOTE – L'ordre de faire avorter le transfert est produit par le fournisseur de l'élément de service de transfert fiable (RTSE) récepteur lorsqu'il est dans l'impossibilité permanente de mener le transfert à bonne fin, par exemple lorsque l'élément à transférer est d'une longueur telle qu'il ne puisse jamais être accepté.

14.10.5 Procédure d'envoi-test sortant Probe-out

Le présent paragraphe décrit les opérations effectuées par un agent MTA chargé de transférer un envoi-test à un autre agent MTA.

14.10.5.1 Arguments

Un envoi-test provenant de la procédure interne avec les instructions d'acheminement pour transfert vers un autre agent MTA. Les champs de cet envoi-test constituent les arguments de l'opération abstraite de transfert d'envoi-test, tels qu'ils sont énumérés dans le Tableau 31.

14.10.5.2 Résultats

Aucun.

14.10.5.3 Erreurs

En cas d'échec du transfert, le module principal est appelé et l'envoi-test lui est transféré avec des instructions par message indiquant le motif de l'échec.

14.10.5.4 Description de la procédure

L'envoi-test à transférer fournit les arguments de l'opération abstraite de transfert d'envoi-test. A noter que l'envoi-test peut refléter le traitement (un réacheminement par exemple) effectué dans cet agent MTA ou dans les agents MTA précédents.

1) Pour s'assurer que la politique de sécurité n'est pas enfreinte au cours du transfert, l'étiquette de sécurité de message **message-security-label** est comparée au contexte de sécurité **security-context**. Si le transfert est interdit soit par la politique de sécurité, soit par des restrictions temporaires, le traitement se poursuit à l'étape 3 ci-dessous.

2) L'agent MTA établit une association avec l'agent MTA récepteur (ou utilise une association existante) et invoque l'opération abstraite de transfert d'envoi-test sur cette association. L'achèvement de la procédure d'envoi-test sortant indique que le transfert a été mené à bonne fin et que l'agent MTA récepteur accepte maintenant la responsabilité de l'envoi-test. La procédure d'envoi-test sortant prend alors fin.

Si l'agent MTA expéditeur reçoit du système récepteur l'instruction de faire avorter le transfert, le traitement se poursuit à l'étape 3 ci-dessous.

S'il n'existe pas d'association et si aucune autre ne peut être établie au départ, ou s'il y a échec du transfert à travers une association, l'agent MTA peut tenter à nouveau d'établir une association ou d'effectuer le transfert, le nombre maximal et la durée maximale des tentatives étant du ressort local.

3) Si après plusieurs tentatives, le transfert n'a pas eu lieu, ou si une infraction aux règles de sécurité a été détectée au cours de l'étape 1, ou si l'agent MTA expéditeur reçoit une instruction pour mettre fin au transfert au cours de l'étape 2, le message, jugé non transférable, est retourné avec indication du motif de l'échec au module principal pour un possible réacheminement ou renvoi. L'agent MTA expéditeur garde la responsabilité de l'envoi-test. La procédure d'envoi-test sortant **Probe-out** prend alors fin.

NOTE – L'ordre de faire avorter le transfert est produit par le fournisseur de l'élément de service de transfert fiable (RTSE) récepteur lorsqu'il est dans l'impossibilité permanente de mener le transfert à bonne fin, par exemple lorsque l'élément à transférer est d'une longueur telle qu'il ne puisse jamais être accepté.

14.10.6 Procédure de rapport sortant Report-out

Le présent paragraphe décrit les opérations effectuées par un agent MTA chargé de transférer un rapport à un autre agent MTA.

14.10.6.1 Arguments

Un rapport provenant de la procédure interne avec instructions de transfert vers un autre agent MTA. Les champs de ce rapport constituent les arguments de l'opération abstraite de transfert de rapport tels qu'ils sont énumérés dans le Tableau 32.

14.10.6.2 Résultats

Aucun.

14.10.6.3 Erreurs

Le rapport, accompagné du motif de l'échec de transfert, est retourné au module de rapport.

14.10.6.4 Description de la procédure

Le rapport à transférer fournit les arguments de l'opération abstraite de transfert de rapport. A noter que le rapport peut refléter le traitement (par exemple, le réacheminement) exécuté dans cet agent MTA ou dans des agents MTA précédents.

1) Pour s'assurer que la politique de sécurité n'est pas enfreinte au cours du transfert, l'étiquette de sécurité de message **message-security-label** est comparée au contexte de sécurité **security-context**. Si le transfert est interdit soit par la politique de sécurité, soit par des restrictions temporaires, le traitement se poursuit à l'étape 3 ci-dessous.

2) L'agent MTA établit une association avec l'agent MTA récepteur (ou utilise une association existante) et invoque l'opération abstraite de transfert de rapport sur cette association. L'achèvement de la procédure de rapport sortant indique que le transfert a été mené à bonne fin et que l'agent MTA récepteur accepte désormais la responsabilité du rapport. La procédure de rapport sortant prend alors fin.

   Si l'agent MTA expéditeur reçoit du système récepteur l'instruction de faire avorter le transfert, le traitement se poursuit à l'étape 3 ci-dessous.

   S'il n'existe pas d'association et si aucune autre ne peut être établie au départ, ou s'il y a échec du transfert à travers une association, l'agent MTA peut tenter à nouveau d'établir une association ou d'effectuer le transfert, la fixation du nombre maximal et de la durée maximale des tentatives étant du ressort local.

3) Si après plusieurs tentatives, le transfert n'a pas eu lieu, ou si une infraction aux règles de sécurité a été détectée au cours de l'étape 1 ci-dessus, ou si l'agent MTA expéditeur reçoit une instruction pour mettre fin au transfert au cours de l'étape 2, le rapport, jugé non transférable, est retourné avec indication du motif de l'échec au module principal pour un possible réacheminement. L'agent MTA expéditeur garde la responsabilité du rapport. La procédure de rapport sortant prend alors fin.

NOTE – L'ordre de faire avorter le transfert est produit par le fournisseur de l'élément de service de transfert fiable (RTSE) récepteur lorsqu'il est dans l'impossibilité permanente de mener le transfert à bonne fin, par exemple lorsque l'élément à transférer est d'une longueur telle qu'il ne puisse jamais être accepté.

Annexe A

Définition de référence des identificateurs d'objet MTS

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

La présente annexe définit, aux fins de référence, les divers identificateurs d'objet cités dans les modules ASN.1 contenues dans le corps de la présente Définition de service. Ces identificateurs d'objet sont assignés conformément à la Figure A.1.

Tous les identificateurs d'objet assignés par la présente Définition de service le sont dans la présente annexe, qui a un caractère définitif pour tous les éléments, exception faite des modules ASN.1 et du système de transfert de messages proprement dit. Les assignations définitives des modules sont faites dans les modules mêmes; d'autres références les concernant apparaissent dans les déclarations IMPORT. Le système MTS, quant à lui, est figé.

```
MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0) object-identifiers(0)
              version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

--      Prologue

--      Exporte tout

IMPORTS-- rien --  ;

ID ::= OBJECT IDENTIFIER

--      Système de transfert de messages

id-mts ID ::= { joint-iso-itu-t mhs(6) mts(3) } -- provisoire

--      Catégories d'identificateurs d'objet

id-mod  ID ::= { id-mts 0 } -- modules
id-ot   ID ::= { id-mts 1 } -- types d'objets
id-pt   ID ::= { id-mts 2 } -- types d'accès
id-cont ID ::= { id-mts 3 } -- types de contenu
id-eit  ID ::= { id-mts 4 } -- types d'information codée
id-att  ID ::= { id-mts 5 } -- attributs
id-tok  ID ::= { id-mts 6 } -- types de jetons
id-sa   ID ::= { id-mts 7 } -- types d'agents fiabilisés
id-ct   ID ::= { id-mts 8 } -- contrats
id-cp   ID ::= { id-mts 9 } -- blocs de connexion

--      Modules

id-mod-object-identifiers   ID ::= { id-mod 0 } -- provisoire
id-mod-mts-abstract-service ID ::= { id-mod 1 } -- provisoire
id-mod-mta-abstract-service ID ::= { id-mod 2 } -- provisoire
id-mod-upper-bounds         ID ::= { id-mod 3 } -- provisoire


--      Types d'objets

id-ot-mts      ID ::= { id-ot 0 }
id-ot-mts-user ID ::= { id-ot 1 }
id-ot-mta      ID ::= { id-ot 2 }
```

Figure A.1 – Définition de syntaxe abstraite des identificateurs d'objet MTS (partie 1 de 2)

```
--      Types d'accès

id-pt-submission    ID  ::= { id-pt 0 }
id-pt-delivery      ID  ::= { id-pt 1 }
id-pt-administration ID ::= { id-pt 2 }
id-pt-transfer      ID  ::= { id-pt 3 }

--      Types de contenu

id-cont-unidentified   ID ::= { id-cont 0 } -- A l'usage de la mémoire de messages et de l'annuaire
id-cont-inner-envelope ID ::= { id-cont 1 }

--      Types d'information codée

id-eit-unknown      ID ::= { id-eit 0 }
        -- la valeur { id-eit 1 } n'est plus définie
id-eit-ia5-text     ID ::= { id-eit 2 }
id-eit-g3-facsimile ID ::= { id-eit 3 }
id-eit-g4-class-1   ID ::= { id-eit 4 }
id-eit-teletex      ID ::= { id-eit 5 }
id-eit-videotex     ID ::= { id-eit 6 }
id-eit-voice        ID ::= { id-eit 7 }
id-eit-sfd          ID ::= { id-eit 8 }
id-eit-mixed-mode   ID ::= { id-eit 9 }

--      Attributs

id-att-physicalRendition-basic         ID ::= { id-att 0 }
id-att-physicalRendition-no-cover-page ID ::= { id-att 1 }

--      Types de jetons

id-tok-asymmetricToken ID ::= { id-tok 0 }

--      Types d'agents fiables

id-sa-ua ID ::= { id-sa 0 }
id-sa-ms ID ::= { id-sa 1 }

--      Contrats

id-ct-mts-access        ID ::= {id-ct 0}
id-ct-mts-forced-access ID ::= {id-ct 1}
id-ct-mta-transfer      ID ::= {id-ct 2}

--      Paquetages de connexion

id-cp-mts-connect       ID ::= {id-cp 0}
id-cp-mta-connect       ID ::= {id-cp 1}

END     -- Fin des identificateurs d'objet MTS MTSObjectIdentifiers
```

Figure A.1 – Définition de syntaxe abstraite des identificateurs d'objet MTS (partie 2 de 2)

Annexe B

Définition de référence des limites supérieures des paramètres MTS

(Cette annexe fait partie intégrante de la Recommandation UIT-T mais ne fait pas partie intégrante de la Norme internationale ISO/CEI)

La présente annexe présente, aux fins de référence, les limites supérieures de divers types de données de longueur variable dont les syntaxes abstraites sont définies dans les modules ASN.1 figurant dans le corps de la présente Définition de service. Ces limites supérieures sont définies dans la Figure B.1.

```
MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3) version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- Prologue

-- Exporte tout

IMPORTS-- rien -- ;

-- Limites supérieures

ub-additional-info INTEGER ::= 1024

ub-bilateral-info INTEGER ::= 1024

ub-bit-options INTEGER ::= 16

ub-built-in-content-type INTEGER ::= 32767

ub-built-in-encoded-information-types INTEGER ::= 32

ub-certificates INTEGER ::= 64

ub-common-name-length INTEGER ::= 64

ub-content-correlator-length INTEGER ::= 512

ub-content-id-length INTEGER ::= 16

ub-content-length INTEGER ::= 2147483647          -- le plus grand entier 32 bits

ub-content-types INTEGER ::= 1024

ub-country-name-alpha-length INTEGER ::= 2

ub-country-name-numeric-length INTEGER ::= 3

ub-diagnostic-codes INTEGER ::= 32767

ub-deliverable-class INTEGER ::= 256

ub-dl-expansions INTEGER ::= 512

ub-domain-defined-attributes INTEGER ::= 4
```

Figure B.1 – Définition de syntaxe abstraite des limites supérieures du système MTS (partie 1 de 3)

```
ub-domain-defined-attribute-type-length INTEGER ::= 8

ub-domain-defined-attribute-value-length INTEGER ::= 128

ub-domain-name-length INTEGER ::= 16

ub-encoded-information-types INTEGER ::= 1024

ub-extension-attributes INTEGER ::= 256

ub-extension-types INTEGER ::= 256

ub-e163-4-number-length INTEGER ::= 15

ub-e163-4-sub-address-length INTEGER ::= 40

ub-generation-qualifier-length INTEGER ::= 3

ub-given-name-length INTEGER ::= 16

ub-initials-length INTEGER ::= 5

ub-integer-options INTEGER ::= 256

ub-labels-and-redirections INTEGER ::= 256

ub-local-id-length INTEGER ::= 32

ub-mta-name-length INTEGER ::= 32

ub-mts-user-types INTEGER ::= 256

ub-numeric-user-id-length INTEGER ::= 32

ub-organization-name-length INTEGER ::= 64

ub-organizational-unit-name-length INTEGER ::= 32

ub-organizational-units INTEGER ::= 4

ub-orig-and-dl-expansions INTEGER ::= 513   -- ub-dl-expansions plus un

ub-password-length INTEGER ::= 62

ub-pds-name-length INTEGER ::= 16

ub-pds-parameter-length INTEGER ::= 30

ub-pds-physical-address-lines INTEGER ::= 6

ub-postal-code-length INTEGER ::= 16

ub-privacy-mark-length INTEGER ::= 128

ub-queue-size INTEGER ::= 2147483647       -- le plus grand entier 32 bits

ub-reason-codes INTEGER ::= 32767

ub-recipient-number-for-advice-length INTEGER ::= 32

ub-recipients INTEGER ::= 32767

ub-redirection-classes INTEGER ::= 256

ub-redirections INTEGER ::= 512
```

Figure B.1 – Définition de syntaxe abstraite des limites supérieures du système MTS (partie 2 de 3)

```
ub-restrictions INTEGER ::= 1024

ub-security-categories INTEGER ::= 64

ub-security-labels INTEGER ::= 256

ub-security-problems INTEGER ::= 256

ub-supplementary-info-length INTEGER ::= 256

ub-surname-length INTEGER ::= 40

ub-teletex-private-use-length INTEGER ::= 128

ub-terminal-id-length INTEGER ::= 24

ub-transfers INTEGER ::= 512

ub-tsap-id-length INTEGER ::= 16

ub-unformatted-address-length INTEGER ::= 180

ub-universal-generation-qualifier-length INTEGER ::= 16

ub-universal-given-name-length INTEGER ::= 40

ub-universal-initials-length INTEGER ::= 16

ub-universal-surname-length INTEGER ::= 64

ub-x121-address-length INTEGER ::= 16

END     -- Fin de limites supérieures MTS MTSUpperBounds
```

Figure B.1 – Définition de syntaxe abstraite des limites supérieures du système MTS (partie 3 de 3)

NOTE – Comme il est spécifié au § 45.5.4 de la Rec. X.680 | ISO/CEI 8824-1, les limites supérieures de la chaîne télétex sont mesurées en caractères. Un nombre sensiblement plus élevé d'octets sera nécessaire pour contenir une telle valeur. Un nombre miminal de 16 octets ou une valeur égale à deux fois la limite supérieure spécifiée (la plus élevée de ces deux valeurs étant retenue) doivent être autorisés.

Annexe C

Définition du service abstrait pour le système de transfert de messages de 1988

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

La présente annexe définit une version du service abstrait MTS qui, au niveau de la mise en œuvre du protocole, interagit avec la version correspondante de protocole définie dans l'édition précédente de cette Recommandation | Norme internationale. Elle est fournie à seule fin de transition. Il est prévu que la présente annexe soit supprimée de la prochaine édition.

Le service abstrait du système de transfert de messages 1988 est identique à la version 1994 définie à l'article 8, sauf pour les opérations d'enregistrement Register et de commande de remise Delivery-control qui sont définies ci-dessous, et pour les attributs suivants définis dans la Figure 2: MTSBindArgument, MTSBindResult, InitiatorCredentials, ResponderCredentials, MessageDeliveryResult, et ReportDeliveryResult, dans lesquels les composantes venant à la suite des points de suspension "..." ne sont pas définies dans les contextes d'application de 1988.

C.1 Enregistrement-88 Register-88

L'opération abstraite d'enregistrement-88 Register-88 permet à l'utilisateur MTS d'apporter des modifications à long terme aux divers paramètres d'utilisateur MTS consignés par le MTS chargé de la remise de messages à l'utilisateur MTS.

De telles modifications restent en vigueur jusqu'à ce qu'elles soient supplantées par une nouvelle invocation de l'opération abstraite d'enregistrement-88 Register-88. Toutefois, certains paramètres peuvent être momentanément annulés et remplacés par appel de l'opération abstraite de commande de remise-88 Delivery-control-88.

NOTE 1 – Cette opération abstraite doit être appelée avant de pouvoir utiliser toute autre opération abstraite de point d'accès de dépôt (submission-port), de remise (delivery-port) ou d'administration (administration-port), et avant qu'un enregistrement équivalent par des moyens locaux ait eu lieu.

NOTE 2 – Cette opération abstraite n'englobe pas les paramètres de base auxquels fait appel l'élément de service de désignation de destinataire suppléant Alternate Recipient Assignment défini dans la Rec. UIT-T X.400 | ISO/CEI 10021-1. La manière dont ces paramètres sont fournis et modifiés est du ressort local.

C.1.1 Arguments

Le Tableau C.1 énumère les arguments de l'opération abstraite d'enregistrement-88 Register-88, en qualifie la présence et identifie les paragraphes où ils sont définis.

Tableau C.1 – Arguments d'enregistrement-88 Register-88

Argument	Présence	Paragraphe
Arguments d'enregistrement		
Nom d'utilisateur *user-name*	O	8.4.1.1.1.1
Adresse d'utilisateur *user-address*	O	8.4.1.1.1.2
Types d'information codée pouvant être remis *deliverable-encoded-information-types*	O	C.1.1.1
Types de contenu pouvant être remis *deliverable-content-types*	O	C.1.1.2
Longueur maximale de contenu pouvant être remise *deliverable-maximum-content-length*	O	C.1.1.3
Destinataire suppléant désigné par le destinataire *recipient-assigned-alternate-recipient*	O	C.1.1.4
Etiquettes de sécurité d'utilisateur *user-security-labels*	O	C.1.1.5
Arguments de commande de remise par défaut		8.4.1.1.1.7
Restriction *restrict*	O	8.3.1.3.1.1
Opérations permises *permissible-operations*	O	8.3.1.3.1.2
Plus faible priorité permise *permissible-lowest-priority*	O	8.3.1.3.1.3
Types permis d'information codée *permissible-encoded-information-types*	O	C.2.1.1
Types permis de contenu *permissible-content-types*	O	8.3.1.3.1.5
Longueur maximale permise de contenu *permissible-maximum-content-length*	O	8.3.1.3.1.6

C.1.1.1 Types d'information codée pouvant être remis deliverable-encoded-information-types

Cet argument indique, s'il y a lieu de les changer, les types d'information codée **encoded-information-types** autorisés par le système MTS à figurer dans les messages remis à l'utilisateur MTS. Il peut être produit par l'utilisateur MTS.

Si un message comporte un ou plusieurs types d'information codée pour la remise desquels l'utilisateur MTS n'a pas souscrit, il doit être rejeté par le système MTS comme ne pouvant être remis. L'utilisateur MTS peut se faire enregistrer pour recevoir le type d'information codée inconnu **unknown-encoded-information-type**. Les types d'information codée pouvant être remis indiquent également les types d'information codée dont la conversion implicite peut être utile.

En l'absence de cet argument, les types d'information codée pouvant être remis **deliverable-encoded-information-types** restent inchangés.

C.1.1.2 Types de contenu pouvant être remis deliverable-content-types

Cet argument indique, s'il y a lieu de les modifier, les types de contenu **content-types** autorisés par le système MTS à figurer dans les messages remis à l'utilisateur MTS. Il peut être produit par l'utilisateur MTS.

Si un message comporte des types de contenu à la remise desquels l'utilisateur MTS n'a pas souscrit, ce message doit être rejeté par le système MTS comme ne pouvant être remis. L'utilisateur MTS peut se faire enregistrer pour recevoir le type de contenu **unidentified content-type** (non identifié).

En l'absence de cet argument, les types de contenu pouvant être remis **deliverable-content-types** restent inchangés.

C.1.1.3 Longueur maximale de contenu pouvant être remise deliverable-maximum-content-length

Cet argument contient, s'il y a lieu de la modifier, la longueur de contenu **content-length** en octets, du contenu le plus long autorisé par le système MTS à figurer dans les messages remis à l'utilisateur MTS. Il peut être produit par l'utilisateur MTS.

Si la longueur d'un message excède celle à laquelle l'utilisateur MTS a souscrit, ce message doit être rejeté par le système MTS comme ne pouvant être remis.

En l'absence de cet argument, la longueur maximale de contenu pouvant être remise **deliverable-maximum-content-length** reste inchangée.

C.1.1.4 Destinataire suppléant désigné par le destinataire recipient-assigned-alternate-recipient

Cet argument, utilisé pour changer de destinataire suppléant, contient le nom **OR-name** d'un destinataire suppléant spécifié par l'utilisateur MTS, vers lequel les messages devront être réacheminés. Il peut être produit par l'utilisateur MTS. Une valeur différente de cet argument pourra être spécifiée pour chaque valeur de l'étiquette **user-security-labels**.

Si un destinataire suppléant désigné par le destinataire est enregistré et associé à une valeur d'étiquettes **user-security-labels**, les messages portant une étiquette **message-security-label** correspondant à cette valeur doivent être réacheminés vers le destinataire suppléant. Les messages portant une étiquette **message-security-label** pour laquelle aucun destinataire suppléant désigné par le destinataire n'a été enregistré ne doivent pas être réacheminés vers un tel suppléant.

Si un seul destinataire suppléant désigné par le destinataire est enregistré et que ce destinataire ne soit pas associé à une valeur d'étiquettes **user-security-labels**, tous les messages doivent être réacheminés vers lui.

L'argument **recipient-assigned-alternate-recipient** (suppléant désigné par le destinataire) contient le nom **OR-name** du destinataire suppléant. S'il contient le nom **OR-name** de l'utilisateur MTS (voir § 8.4.1.1.1.1), cela signifie qu'aucun destinataire suppléant n'est désigné par le destinataire.

En l'absence de cet argument, le destinataire suppléant désigné par le destinataire, s'il y en a un, reste inchangé.

C.1.1.5 Etiquettes de sécurité d'utilisateur user-security-labels

Cet argument contient, s'il y a lieu de les modifier, les étiquettes de sécurité **security-labels** de l'utilisateur MTS. Il peut être produit par l'utilisateur MTS.

Un destinataire suppléant désigné par le destinataire **recipient-assigned-alternate-recipient** peut être enregistré pour n'importe quelle valeur d'étiquettes de sécurité d'utilisateur **user-security-labels**.

En l'absence de cet argument, les étiquettes de sécurité d'utilisateur **user-security-labels** restent inchangées.

Certaines politiques de sécurité peuvent n'autoriser une telle modification des étiquettes de sécurité d'utilisateur **user-security-labels** que lorsqu'une liaison sûre est utilisée. D'autres moyens locaux et sûrs de modifier les étiquettes de sécurité d'utilisateur pourront être fournis.

C.1.2 Résultats

L'opération abstraite d'enregistrement-88 Register-88 renvoie un résultat vide pour indiquer le succès de l'opération.

C.1.3 Erreurs abstraites abstract-errors

Le Tableau C.2 énumère les erreurs abstraites qui peuvent interrompre l'opération abstraite d'enregistrement-88 Register-88 et identifie les paragraphes dans lesquels elles sont définies.

Tableau C.2 – Erreurs abstraites d'enregistrement-88 Register-88

Erreur abstraite abstract-error	Paragraphe
Rejet d'enregistrement *register-rejected*	8.4.2.1
Erreur de rattachement distant *remote-bind-error*	8.2.2.10

C.2 Commande de remise-88 Delivery-control-88

L'opération abstraite de commande de remise-88 Delivery-control-88 permet à l'utilisateur MTS de limiter temporairement les opérations abstraites que le système MTS peut invoquer au point d'accès de remise delivery-port, ainsi que les messages que le système MTS peut remettre à l'utilisateur MTS par une opération abstraite de remise de message Message-delivery.

Le système MTS doit suspendre, plutôt que de les abandonner, les opérations abstraites et les messages actuellement interdits.

La réussite de l'opération abstraite signifie que les commandes spécifiées sont maintenant en vigueur. Ces commandes annulent et remplacent toutes les autres commandes précédemment en vigueur et restent en cours jusqu'à ce que l'association soit libérée, que l'utilisateur MTS re-invoque l'opération abstraite de commande de remise-88 Delivery-control-88 ou qu'il invoque l'opération abstraite d'enregistrement-88 de l'accès administration-port pour imposer des contraintes plus sévères que les commandes précédemment spécifiées.

L'opération abstraite renvoie une indication signalant toute opération abstraite que le MTS aurait pu invoquer, et tout type de message que le système MTS aurait pu remettre ou signaler en l'absence des commandes en vigueur.

C.2.1 Arguments

Le Tableau C.3 énumère les arguments de l'opération abstraite de commande de remise-88 Delivery-control-88, en qualifie la présence et identifie les paragraphes où ils sont définis.

Tableau C.3 – Arguments de la commande de remise-88 Delivery-control-88

Argument	Présence	Paragraphe
Arguments de commande de remise		
Restriction *restrict*	O	8.3.1.3.1.1
Opérations permises *permissible-operations*	O	8.3.1.3.1.2
Plus faible priorité permise *permissible-lowest-priority*	O	8.3.1.3.1.3
Types permis d'information codée *permissible-encoded-information-types*	O	C.2.1.1
Types permis de contenu *permissible-content-types*	O	8.3.1.3.1.5
Longueur maximale permise de contenu *permissible-maximum-content-length*	O	8.3.1.3.1.6
Contexte de sécurité permis *permissible-security-context*	O	8.3.1.3.1.7

C.2.1.1 Types permis d'information codée permissible-encoded-information-types

Cet argument indique les types d'information codée **encoded-information-types** qui apparaissent dans les messages que le système MTS fournit à l'utilisateur MTS par l'opération abstraite de remise Message-delivery. Il peut être produit par l'utilisateur MTS.

Les types permis d'information codée **permissible-encoded-information-types** spécifiés doivent appartenir aux types qui ont reçu une autorisation à long terme suite à une demande antérieure de l'opération abstraite d'enregistrement de l'accès d'administration (types d'information codée pouvant être remis **deliverable-encoded-information-types**).

En l'absence de cet argument, les types permis d'information codée **permissible-encoded-information-types** que le MTS peut remettre à l'utilisateur MTS restent inchangés. Si aucune invocation de l'opération abstraite de commande de remise Delivery-control n'a antérieurement eu lieu sur l'association, la commande par défaut enregistrée par le système MTS par l'opération abstraite d'enregistrement Register de l'accès d'administration doit s'appliquer.

C.2.2 Résultats

Les résultats de l'opération abstraite de commande de remise-88 Delivery-control-88 sont identiques aux résultats de l'opération abstraite de commande de remise définis au § 8.3.1.3.2.

C.2.3 Erreurs abstraites

Le Tableau C.4 énumère les erreurs abstraites pouvant interrompre l'opération abstraite de commande de remise-88, et identifie pour chacune d'elles le paragraphe qui la définit.

Tableau C.4 – Erreurs abstraites de commande de remise-88

Erreur abstraite *abstract-error*	Paragraphe
Paramètres d'enregistrement enfreints par la commande *control-violates-registration*	8.3.2.2
Erreur de sécurité *security-error*	8.3.2.3

```
MTSAbstractService88 { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
              version-1988(1988) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exporte tout

IMPORTS

        -- Opérations distantes

        CONTRACT
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
                        remote-operations(4) informationObjects(5) version1(0) }

        -- Paramètres du service abstrait MTS

        ABSTRACT-OPERATION, change-credentials, ContentLength, ContentTypes, Controls,
        control-violates-registration, DefaultDeliveryControls, EncodedInformationTypes,
        message-delivery, MHS-OBJECT, mts-connect, operationObject1, PORT,
        RecipientAssignedAlternateRecipient, register-rejected, report-delivery, SecurityLabel,
        security-error, submission, UserAddress, UserName, Waiting
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- Identificateurs d'objet

        id-ct-mts-access, id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user,
        id-pt-administration, id-pt-delivery
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }

        -- Codes d'opérations

        op-delivery-control, op-register
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                        mts-access-protocol(1) version-1999(1) }
```

```
        -- Limites supérieures

        ub-content-types, ub-labels-and-redirections
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                        version-1999(1) };

--      Objets

mts-88 MHS-OBJECT ::= {
        INITIATES       { mts-forced-access-contract-88 }
        RESPONDS        { mts-access-contract-88 }
        ID              {id-ot-mts 88} }

mts-user-88 MHS-OBJECT ::= {
        INITIATES       { mts-access-contract-88 }
        RESPONDS        { mts-forced-access-contract-88 }
        ID              { id-ot-mts-user 88 } }
```

Figure C.1 – Définition de syntaxe abstraite du service abstrait MTS de 1988 (partie 1 de 2)

-- Contrats

```
mts-access-contract-88 CONTRACT ::= {
       CONNECTION              mts-connect
       INITIATOR CONSUMER OF   { submission | delivery-88 | administration-88 }
       ID                      { id-ct-mts-access 88 } }

mts-forced-access-contract-88 CONTRACT ::= {
       CONNECTION              mts-connect
       RESPONDER CONSUMER OF   { submission | delivery-88 | administration-88 }
       ID                      { id-ct-mts-forced-access 88 } }
```

-- Accès

```
delivery-88 PORT ::= {
       OPERATIONS {operationObject1,...} /* Cet ensemble d'objets informationels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       CONSUMER INVOKES {delivery-control-88,...} -- Cette interruption IOS doit être
extensible afin de tenir compte de l'opération de réacheminement Forward{} telle que définie
dans la Rec. UIT-T X.880--
       SUPPLIER INVOKES {message-delivery | report-delivery,...} -- Cette interruption IOS
doit être extensible afin de tenir compte de l'opération de réacheminement Forward{} telle que
définie dans la Rec. UIT-T X.880--
       ID {id-pt-delivery 88}}

administration-88 PORT ::= {
       OPERATIONS {change-credentials,...} /* Cet ensemble d'objets informationels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       CONSUMER INVOKES {register-88,...} /* Cet ensemble d'objets informationels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       SUPPLIER INVOKES {operationObject1,...} /* Cet ensemble d'objets informationels doit
être extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       ID {id-pt-administration 88}
  }
```

-- Accès de remise

```
delivery-control-88 ABSTRACT-OPERATION ::= {
       ARGUMENT          DeliveryControls88
       RESULT            Waiting
       ERRORS            { control-violates-registration | security-error }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-delivery-control }

DeliveryControls88 ::= SET {
       COMPONENTS OF Controls (WITH COMPONENTS {
              ... ,
              permissible-encoded-information-types ABSENT } ),
       permissible-encoded-information-types-88 EncodedInformationTypes OPTIONAL }
```

-- Accès d'administration

```
register-88 ABSTRACT-OPERATION ::= {
       ARGUMENT          Register88
       RESULT            NULL
       ERRORS            { register-rejected }
       LINKED {operationObject1,...} /* Cet ensemble d'objets informationnels doit être
extensible parce qu'il est utilisé par l'opération de réacheminement Forward{} (telle que
définie dans la Rec. UIT-T X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }
```

```
Register88 ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-encoded-information-types EncodedInformationTypes OPTIONAL,
       deliverable-maximum-content-length [1] EXPLICIT ContentLength OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       deliverable-content-types [3] ContentTypes OPTIONAL,
       labels-and-redirections [4] SET SIZE (1..ub-labels-and-redirections) OF
              LabelAndRedirection OPTIONAL }

LabelAndRedirection ::= SET {
       user-security-label [0] UserSecurityLabel OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                    OPTIONAL }

UserSecurityLabel ::= SecurityLabel

END     -- du service abstrait de 1988 MTSAbstractService88
```

Figure C.1 – Définition de syntaxe abstraite du service abstrait MTS de 1988 (partie 2 de 2)

Annexe D

Différences entre la Norme ISO/CEI 10021-4 et la Recommandation UIT-T X.411

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

La présente annexe indique les différences techniques entre la Rec. UIT-T X.411 et l'ISO/CEI 10021-4.

Ces différences sont les suivantes:

1) dans la Rec. UIT-T X.411, des contraintes de taille s'appliquent à un certain nombre de champs de protocole (voir l'Annexe B). Dans l'ISO/CEI 10021-4, les valeurs effectives des contraintes ne font pas partie intégrante de la Norme.

Annexe E

Index

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

La présente annexe constitue un index de la présente Définition de service. 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.

Cette annexe renvoie aux items figurant (le cas échéant) dans les catégories suivantes:

a) Abréviations;
b) Termes;
c) Définition des paramètres du système MTS;
d) Modules ASN.1;
e) Classes d'objets informationnels ASN.1;
f) Types ASN.1;
g) Valeurs ASN.1.

Abbreviations
- MTA 102
- MTS 4

Terms
- administration-port 5, 102
- application-context 104
- Cancel-deferred-delivery 6, 27
- Change-credentials 6, 54
- Criticality Mechanism 62
- Delivery-control 6, 45
- Delivery-control-88 171
- delivery-port 5, 102
- Extension Mechanism 62
- Message Transfer System 4, 102
- Message-delivery 6, 33
- Message-submission 6, 10
- Message-transfer 103
- message-transfer-agent 102
- MTA-bind 103, 104
- MTA-unbind 103
- MTS-bind 6, 7
- MTS-unbind 6, 9
- Probe-submission 6, 25
- Probe-transfer 103
- Register 6, 50
- Register-88 169
- Report-delivery 6, 37
- Report-transfer 103
- security-context 104
- Submission-control 6, 28
- submission-port 5, 102
- transfer-port 102

Definitions of the MTS parameters
- Actual-recipient-name 38
- Additional-information 113
- Algorithm-identifier 61
- alphabetic-character-loss (non-delivery-diagnostic-code) 41
- Alternate-recipient-allowed 11
- ambiguous-OR-name (non-delivery-diagnostic-code) 40
- Arrival-time 113
- asymmetric-token 60
- Authentication-error (bind-error) 10, 106
- authentication-failure-on-subject-message 49
- authentication-failure-on-subject-message (non-delivery-diagnostic-code) 43

basic encoded-information-types 57
built-in content-type 20
built-in-domain-defined-attributes 57
built-in-encoded-information-types 58
built-in-standard-attributes 57
Busy (bind-error) 10, 106
Certificate 58
certificates 59
certificate-selector 8, 9, 105, 106
Certificate-selectors 23
Certificate-selectors-override 23
certification-path 59
Content 21
Content-confidentiality-algorithm-identifier 17
content-confidentiality-key 17
Content-correlator 21
Content-identifier 21
content-integrity-algorithm-identifier 18
Content-integrity-check 18
content-integrity-key 17
Content-length 26
Content-return-request 16
content-syntax-error (non-delivery-diagnostic-code) 41
content-too-long (non-delivery-diagnostic-code) 41
Content-type 20, 44
content-type-not-supported (non-delivery-diagnostic-code) 41
conversion-not-performed (non-delivery-reason-code) 40
Conversion-with-loss-prohibited 13
conversion-with-loss-prohibited (non-delivery-diagnostic-code) 41
Converted-encoded-information-types 36, 39
credentials 7, 9, 55, 104, 105
critical-for-delivery 63
critical-for-submission 63
critical-for-transfer 63
decryption-failed 49
decryption-failed (non-delivery-diagnostic-code) 43
decryption-key-unobtainable 49
decryption-key-unobtainable (non-delivery-diagnostic-code) 43
Default-delivery-control-arguments 54
deferred-delivery-not-performed (non-delivery-reason-code) 40
Deferred-delivery-time 14, 109
deliverable-class 51
Deliverable-classes 51
Deliverable-content-types 52, 170
Deliverable-encoded-information-types 170
Deliverable-maximum-content-length 52, 170
Deliverable-security-labels 53
directory-name 57
directory-operation-unsuccessful (non-delivery-reason-code) 40
Disclosure-of-other-recipients 13
DL-exempted-recipients 22
DL-expansion-failure (non-delivery-diagnostic-code) 41
DL-expansion-history 36
DL-expansion-prohibited 13
DL-expansion-prohibited (non-delivery-diagnostic-code) 41
DL-expansion-prohibited-by-security-policy (non-delivery-diagnostic-code) 42
domain-defined-attributes 57
double-envelope-creation-failure (non-delivery-diagnostic-code) 43
double-enveloping-message-restoring-failure (non-delivery-diagnostic-code) 43
edi-messaging (content-type) 21
Encoded-information-types 57
Encoded-information-types-constraints 51
encoded-information-types-unsupported (non-delivery-diagnostic-code) 41
encrypted-data 8, 9, 17, 60, 104, 105
Explicit-conversion 14, 110
extended content-type 21
extended-encoded-information-types 58
extension-domain-defined-attributes 57
extension-standard-attributes 57
external (content-type) 20
externally-defined encoded-information-type 58

failure-of-proof-of-message 49
failure-of-proof-of-message (non-delivery-diagnostic-code) 43
forbidden-alternate-recipient (non-delivery-diagnostic-code) 42
forbidden-user-security-label-register 56
Global-domain-identifier 57
implicit-conversion-not-subscribed (non-delivery-diagnostic-code) 41
Implicit-conversion-prohibited 13
implicit-conversion-prohibited (non-delivery-diagnostic-code) 41
improperly-specified-recipients 31
Inadequate-association-confidentiality (bind-error) 10, 106
incompatible-change-with-original-security-context 32, 49
incorrect-notification-type (non-delivery-diagnostic-code) 42
initiator-bind-token 8, 104
initiator-certificate 8, 104
Initiator-credentials 7, 104
Initiator-name 7, 104
inner-envelope (content-type) 21
integrity-failure-on-subject-message 49
integrity-failure-on-subject-message (non-delivery-diagnostic-code) 43
internal-trace-information 113
Internal-trace-information 109
interpersonal-messaging-1984 (content-type) 21
interpersonal-messaging-1988 (content-type) 21
invalid-arguments (non-delivery-diagnostic-code) 41
invalid-security-label 32, 49
invalid-security-label (non-delivery-diagnostic-code) 43
invalid-security-label-update 56
key-failure 49
key-failure (non-delivery-diagnostic-code) 43
Latest-delivery-time 14
line-too-long (non-delivery-diagnostic-code) 41
loop-detected (non-delivery-diagnostic-code) 40
mandatory-parameter-absence 32, 49, 56
mandatory-parameter-absence (non-delivery-diagnostic-code) 43
maximum-time-expired (non-delivery-diagnostic-code) 40
Message-delivery-identifier 34
Message-delivery-time 34, 39
Message-identifier 107
message-origin-authentication-algorithm-identifier 19
Message-origin-authentication-check 19
Message-security-label 19
message-sequence-number 17
Message-submission-identifier 24, 28
Message-submission-time 24
Messages-waiting 8, 9
Message-token 17
MTA-name 57
MTS-congestion (non-delivery-diagnostic-code) 40
MTS-identifier 56
multiple-information-loss (non-delivery-diagnostic-code) 41
Multiple-originator-certificates 22
New-credentials 55
no-bilateral-agreement (non-delivery-diagnostic-code) 41
no-DL-submit-permission (non-delivery-diagnostic-code) 41
Non-basic-parameters 58
Non-delivery-diagnostic-code 40
Non-delivery-reason-code 40
Notification-type 21
Old-credentials 55
operation-security-failure 32, 49, 56
operation-security-failure (non-delivery-diagnostic-code) 43
OR-address 57
Original-encoded-information-types 20
Originally-intended-recipient-name 35
Originally-specified-recipient-number 109
Originating-MTA-certificate 24
Originating-MTA-report-request 109
Originator-and-DL-expansion-history 38

Originator-certificate 16
Originator-name 11
Originator-report-request 16
Originator-requested-alternate-recipient 13
Originator-return-address 16
OR-name 57
Other-recipient-names 35
page-split (non-delivery-diagnostic-code) 41
password 7, 9, 55, 61, 104, 105
Per-domain-bilateral-information 107
Permissible-content-types 46
Permissible-encoded-information-types 46, 171
Permissible-lowest-priority 29, 46
Permissible-maximum-content-length 29, 47
Permissible-operations 29, 46
Permissible-security-context 29, 47
Physical-delivery-modes 15
physical-delivery-not-performed (non-delivery-reason-code) 40
Physical-delivery-report-request 16
Physical-forwarding-address 39
Physical-forwarding-address-request 15
Physical-forwarding-prohibited 14
Physical-rendition-attributes 15
physical-rendition-attributes-not-supported (non-delivery-diagnostic-code) 41
physical-rendition-not-performed (non-delivery-reason-code) 40
pictorial-symbol-loss (non-delivery-diagnostic-code) 41
Priority 13
privacy-mark 61
Probe-identifier 110
probe-origin-authentication-algorithm-identifier 26
Probe-origin-authentication-check 26
Probe-submission-identifier 27
Probe-submission-time 27
Proof-of-delivery 36
proof-of-delivery-algorithm-identifier 36
Proof-of-delivery-request 20
Proof-of-submission 24
proof-of-submission-algorithm-identifier 24
Proof-of-submission-request 20
protocol-violation (non-delivery-diagnostic-code) 41
punctuation-symbol-loss (non-delivery-diagnostic-code) 41
random-number 8, 9, 104, 105
recipient-assigned-alternate-recipient 53
Recipient-assigned-alternate-recipient 170
Recipient-assigned-redirections 53
Recipient-certificate 22, 36
Recipient-name 11
Recipient-number-for-advice 15
Recipient-reassignment-prohibited 12
recipient-reassignment-prohibited (non-delivery-diagnostic-code) 41
recipient-unavailable (non-delivery-diagnostic-code) 40
redirection-class 53
Redirection-history 35, 39
redirection-loop-detected (non-delivery-diagnostic-code) 41
redirection-prohibited 56
redirection-reason 35
refused-alternate-recipient-name 56
Registered-mail-type 15
Report-destination-name 112
Report-identifier 112
Reporting-DL-name 39
Reporting-MTA-certificate 43
report-origin-authentication-algorithm-identifier 44
Report-origin-authentication-check 44
repudiation-failure-of-message 49
repudiation-failure-of-message (non-delivery-diagnostic-code) 43
Requested-delivery-method 14
responder-bind-token 9, 105
responder-certificate 9, 105
Responder-credentials 9, 105
Responder-name 8, 105
Responsibility 109
Restrict 29, 46

Restricted-delivery 53
restricted-delivery (non-delivery-reason-code) 40
restriction 53
Retrieve-registrations 54
Returned-content 44
secure-messaging-error (non-delivery-diagnostic-code) 42
security-attributes 61
security-categories 61
security-classification 61
Security-context 8, 105
security-context-failure 32, 49
security-context-failure-message (non-delivery-diagnostic-code) 43
Security-label 60
security-policy-identifier 61
security-policy-violation 32, 49, 56
security-policy-violation (non-delivery-diagnostic-code) 42
security-problem 32, 48, 56
security-services-refusal 32, 49, 56
security-services-refusal (non-delivery-diagnostic-code) 42
Service-message 21
signed-data 8, 9, 17, 60, 104, 105
size-constraint-violation (non-delivery-diagnostic-code) 41
standard-attributes 57
Subject-identifier 113
Subject-intermediate-trace-information 113
subject-public-key 58
Subject-submission-identifier 38
Supplementary-information 39
This-recipient-name 34
Time 57
Token 60
token-decryption-failed 49
token-decryption-failed (non-delivery-diagnostic-code) 43
token-error 49
token-error (non-delivery-diagnostic-code) 43
token-type-identifier 60
too-many-recipients (non-delivery-diagnostic-code) 41
Trace-information 107, 113
transfer-attempts-limit-reached (non-delivery-diagnostic-code) 42
transfer-failure (non-delivery-reason-code) 40
transfer-failure-for-security-reason (non-delivery-reason-code) 40
Type-of-MTS-user 39
unable-to-complete-transfer (non-delivery-diagnostic-code) 42
unable-to-downgrade (non-delivery-diagnostic-code) 42
unable-to-transfer (non-delivery-reason-code) 40
Unacceptable-dialogue-mode 106
Unacceptable-dialogue-mode (bind-error) 10
Unacceptable-security-context (bind-error) 10, 106
unauthorised-DL-member (non-delivery-diagnostic-code) 42
unauthorised-dl-name 32
unauthorised-DL-name (non-delivery-diagnostic-code) 42
unauthorised-originally-intended-recipient-name 49
unauthorised-originally-intended-recipient-name (non-delivery-diagnostic-code) 43
unauthorised-originator-name 32, 49
unauthorised-originator-name (non-delivery-diagnostic-code) 43
unauthorised-recipient-name 32, 49
unauthorised-recipient-name (non-delivery-diagnostic-code) 43
unauthorised-security-label-update 56
unauthorised-user-name 56
undeliverable-mail-new-address-unknown (non-delivery-diagnostic-code) 42
undeliverable-mail-organization-expired (non-delivery-diagnostic-code) 42
undeliverable-mail-originator-prohibited-forwarding (non-delivery-diagnostic-code) 42
undeliverable-mail-physical-delivery-address-incomplete (non-delivery-diagnostic-code) 42
undeliverable-mail-physical-delivery-address-incorrect (non-delivery-diagnostic-code) 41
undeliverable-mail-physical-delivery-office-incorrect-or-invalid (non-delivery-diagnostic-code) 42

undeliverable-mail-recipient-changed-address-permanently (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-changed-address-temporarily (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-changed-temporary-address (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-deceased (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-did-not-claim (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-did-not-want-forwarding (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-refused-to-accept (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-unknown (non-delivery-diagnostic-code) 42
unidentified (content-type) 20
unknown-security-label 32, 49
unknown-security-label (non-delivery-diagnostic-code) 43
unrecognised-OR-name (non-delivery-diagnostic-code) 40
unreliable-system (non-delivery-diagnostic-code) 43
unsupported-algorithm-identifier 49
unsupported-algorithm-identifier (non-delivery-diagnostic-code) 43
unsupported-critical-function (non-delivery-diagnostic-code) 41
unsupported-security-policy 49
unsupported-security-policy (non-delivery-diagnostic-code) 43
User-address 51
User-name 51
User-security-labels 170
voice-messaging (content-type) 21
Waiting-content-types 30, 48
Waiting-encoded-information-types 30, 48
Waiting-messages 30, 47
Waiting-operations 30, 47

Definitions of the MTS parametersconversion-impractical
(non-delivery-diagnostic-code) 41

ASN.1 modules
MTAAbstractService 116
MTSAbstractService 65
MTSAbstractService88 172
MTSObjectIdentifiers 164
MTSUpperBounds 166

ASN.1 information object classes
ABSTRACT-ERROR 68
ABSTRACT-OPERATION 68
ADDITIONAL 121
ALGORITHM - see ISO/IEC 9594-8
BILATERAL 121
CONNECTION-PACKAGE - see ISO/IEC 13712-1
CONTRACT - see ISO/IEC 13712-1
ENCRYPTED { } - see ISO/IEC 9594-8
ERROR - see ISO/IEC 13712-1
EXTENSION 85
EXTENSION-ATTRIBUTE 93
IPMPerRecipientEnvelopeExtensions - see ISO/IEC 10021-7
MHS-OBJECT 66
OPERATION - see ISO/IEC 13712-1
OPERATION-PACKAGE - see ISO/IEC 13712-1
PORT 68
ROS-OBJECT-CLASS - see ISO/IEC 13712-1
SECURITY-CATEGORY 101
SIGNATURE { } - see ISO/IEC 9594-8
SIGNED { } - see ISO/IEC 9594-8
TOKEN 100
TOKEN-DATA 100

ASN.1 types
ActualRecipientName 82, 121
AdditionalActions 122
AdditionalInformation 121
AdministrationDomainName 93
AlgorithmIdentifier - see ISO/IEC 9594-8
ArrivalTime 123
AsymmetricToken 100
BilateralDomain 121
BindTokenEncryptedData 101
BindTokenSignedData 101

BuiltInContentType 81
BuiltInDomainDefinedAttribute 93
BuiltInDomainDefinedAttributes 93
BuiltInEncodedInformationTypes 98
BuiltInStandardAttributes 92
CancelDeferredDeliveryArgument 71
CancelDeferredDeliveryResult 71
CertificateAssertion - see ISO/IEC 9594-8
Certificates - see ISO/IEC 9594-8
CertificateSelectors 91
ChangeCredentialsArgument 76
CommonName 94
Content 92
ContentConfidentialityAlgorithmIdentifier 87
ContentCorrelator 88
ContentIdentifier 81
ContentIntegrityAlgorithmIdentifier 88
ContentIntegrityCheck 88
ContentLength 82
ContentType 81
ContentTypes 81
Controls 76
ConversionWithLossProhibited 86
ConvertedEncodedInformationTypes 82
CountryName 93
Credentials 70
Criticality 85
DefaultDeliveryControls 77
DeferredDeliveryTime 82
DeferredTime 123
DeliverableClass 77
DeliveredContentType 81
DeliveredOriginatorName 81
DeliveryControlArgument 74
DeliveryControlExtensions 74
DeliveryControlResult 75
DeliveryControlResultExtensions 75
DeliveryControls 75
DeliveryControls88 173
DeliveryFlags 82
DeliveryQueue 70
DeliveryReport 81
DLExemptedRecipients 91
DLExpansion 89
DLExpansionHistory 89
DLExpansionProhibited 85
DomainSuppliedInformation 122
EncodedInformationTypes 98
EncodedInformationTypesConstraints 77
EncryptionKey 101
ExactOrPattern 77
ExplicitConversion 82
ExtendedCertificate 91
ExtendedCertificates 91
ExtendedContentType 81
ExtendedEncodedInformationType 99
ExtendedEncodedInformationTypes 99
ExtendedNetworkAddress 98
ExtensionAttribute 93
ExtensionAttributes 93
ExtensionAttributeTable 94
ExtensionField 85
ExtensionORAddressComponents 96
ExtensionPhysicalDeliveryAddressComponents 96
ExtensionType 85
G3FacsimileNonBasicParameters 100
GlobalDomainIdentifier 92
ID 164
ImproperlySpecifiedRecipients 72
InitiatorCredentials 70
IntendedRecipientName 89
InternalAdditionalActions 122
InternalTraceInformation 122
InternalTraceInformationElement 122
LabelAndRedirection 174
LastTraceInformation 122
LatestDeliveryTime 86
LocalIdentifier 92
LocalPostalAttributes 97
Message 118

MessageClass 77
MessageClassExtensions 77
MessageDeliveryArgument 74
MessageDeliveryEnvelope 79
MessageDeliveryExtensions 80
MessageDeliveryIdentifier 82
MessageDeliveryResult 74
MessageDeliveryResultExtensions 74
MessageDeliveryTime 82
MessageIdentifier 120
MessageOriginAuthenticationAlgorithm Identifier 88
MessageOriginAuthenticationCheck 88
MessageOrProbeIdentifier 121
MessageSecurityLabel 88
MessageSubmissionArgument 71
MessageSubmissionEnvelope 78
MessageSubmissionIdentifier 73
MessageSubmissionResult 71
MessageSubmissionResultExtensions 71
MessageSubmissionTime 73
MessagesWaiting 70
MessageToken 87
MessageTokenEncryptedData 101
MessageTokenSignedData 101
MessageTransferEnvelope 118
MessageTransferExtensions 118
MTABindArgument 117
MTABindResult 117
MTAName 92
MTASuppliedInformation 122
MTSBindArgument 68
MTSBindExtensions 68
MTSBindResult 68
MTSBindResultExtensions 68
MTSIdentifier 92
Name - see ISO/IEC 9594-2
NetworkAddress 93
NonBasicParameters 99
NonDeliveryDiagnosticCode 83
NonDeliveryReasonCode 83
NonDeliveryReport 81
NumericUserIdentifier 93
ObjectName 70
Operations 74
ORAddress 92
ORAddressAndOptionalDirectoryName 92
ORAddressAndOrDirectoryName 92
OrganizationalUnitName 93
OrganizationalUnitNames 93
OrganizationName 93
OriginalEncodedInformationTypes 81
OriginallyIntendedRecipientName 82, 122
OriginallySpecifiedRecipientNumber 121
OriginatingMTACertificate 90
OriginatorAndDLExpansion 89
OriginatorAndDLExpansionHistory 89
OriginatorCertificate 87
OriginatorName 81, 120
OriginatorReportRequest 82
OriginatorRequestedAlternateRecipient 85, 122
OriginatorReturnAddress 87
ORName 92
OtherActions 123
OtherMessageDeliveryFields 79
OtherRecipientName 82
OtherRecipientNames 82
Password 70
PDSName 95
PDSParameter 98
PerDomainBilateralInformation 121
PerMessageIndicators 81
PerMessageSubmissionExtensions 78
PerMessageSubmissionFields 78
PerMessageTransferFields 118
PermissibleEncodedInformationTypes 76
PerProbeSubmissionExtensions 79
PerProbeSubmissionFields 79
PerProbeTransferFields 119
PerRecipientDeliveryReportFields 90

PerRecipientIndicators 121
PerRecipientMessageSubmissionExtensions 78
PerRecipientMessageSubmissionFields 78
PerRecipientMessageTransferExtensions 119
PerRecipientMessageTransferFields 118
PerRecipientNonDeliveryReportFields 90
PerRecipientProbeSubmissionExtensions 79
PerRecipientProbeSubmissionFields 79
PerRecipientProbeTransferExtensions 119
PerRecipientProbeTransferFields 119
PerRecipientReportDeliveryExtensions 80
PerRecipientReportDeliveryFields 80
PerRecipientReportFields 90
PerRecipientReportTransferExtensions 120
PerRecipientReportTransferFields 120
PerReportDeliveryFields 80
PerReportTransferFields 120
PersonalName 93
PhysicalDeliveryCountryName 96
PhysicalDeliveryModes 86
PhysicalDeliveryOfficeName 96
PhysicalDeliveryOfficeNumber 96
PhysicalDeliveryOrganizationName 96
PhysicalDeliveryPersonalName 96
PhysicalDeliveryReportRequest 87
PhysicalForwardingAddress 89
PhysicalForwardingAddressRequest 86
PhysicalForwardingProhibited 86
PhysicalRenditionAttributes 87
PostalCode 96
PosteRestanteAddress 97
PostOfficeBoxAddress 97
PresentationAddress - see ISO/IEC 9594-6
Priority 82
PrivacyMark 101
PrivateDomainIdentifier 92
PrivateDomainName 93
PrivateExtensions 85
Probe 118
ProbeIdentifier 121
ProbeOriginAuthenticationAlgorithmIdentifier 89
ProbeOriginAuthenticationCheck 89
ProbeResultExtensions 71
ProbeSubmissionArgument 71
ProbeSubmissionEnvelope 79
ProbeSubmissionIdentifier 73
ProbeSubmissionResult 71
ProbeSubmissionTime 73
ProbeTransferEnvelope 119
ProbeTransferExtensions 119
ProofOfDelivery 75
ProofOfDeliveryAlgorithmIdentifier 75
ProofOfDeliveryRequest 88
ProofOfSubmission 90
ProofOfSubmissionAlgorithmIdentifier 90
ProofOfSubmissionRequest 88
ProtectedPassword 70
PSAPAddress 77
RandomNumber 101
RecipientAssignedAlternateRecipient 77
RecipientCertificate 75
RecipientName 81, 121
RecipientNumberForAdvice 87
RecipientReassignmentProhibited 85
RecipientRedirection 77
Redirection 89
RedirectionClass 77
RedirectionHistory 89
RedirectionReason 89
Redirections 77
RefusalReason 75
RefusedArgument 75
RefusedOperation 75
Register88 174
RegisterArgument 76
RegisteredMailType 87
RegisterExtensions 76
RegisterResult 76
RegisterResultExtensions 76
RegistrationTypes 78

Report 118
ReportDeliveryArgument 74
ReportDeliveryEnvelope 80
ReportDeliveryExtensions 80
ReportDeliveryResult 74
ReportDeliveryResultExtensions 74
ReportDestinationName 121
ReportIdentifier 121
ReportingDLName 90
ReportingMTACertificate 90
ReportingMTAName 90
ReportOriginAuthenticationAlgorithmIdentifier 90
ReportOriginAuthenticationCheck 90
ReportTransferContent 120
ReportTransferContentExtensions 120
ReportTransferEnvelope 120
ReportTransferEnvelopeExtensions 120
ReportType 81
RequestedDeliveryMethod 86
ResponderCredentials 70
RestrictedDelivery 77
Restriction 77
RoutingAction 122
SecurityCategories 101
SecurityCategoriesTable 101
SecurityCategory 101
SecurityClassification 101
SecurityContext 70
SecurityLabel 101
SecurityPolicyIdentifier 101
SecurityProblem 72
StreetAddress 97
StrongCredentials 70
SubjectIdentifier 121
SubjectIntermediateTraceInformation 121
SubjectSubmissionIdentifier 82
SubmissionControlArgument 71
SubmissionControlResult 71
SubmissionControls 73
SupplementaryInformation 84
TeletexCommonName 94
TeletexDomainDefinedAttribute 98
TeletexDomainDefinedAttributes 98
TeletexNonBasicParameters 100
TeletexOrganizationalUnitName 95
TeletexOrganizationalUnitNames 95
TeletexOrganizationName 94
TeletexPersonalName 94
TerminalIdentifier 93
TerminalType 98
ThisRecipientName 82
Time 92
Token 100
TokenData 100
TokenDataTable 101
TokensTable 100
TraceInformation 122
TraceInformationElement 122
TypeOfMTSUser 82
UnformattedPostalAddress 97
UniquePostalName 97
UniversalCommonName 94
UniversalDomainDefinedAttribute 98
UniversalDomainDefinedAttributes 98
UniversalExtensionORAddressComponents 96
UniversalExtensionPhysicalDeliveryAddressComponents 96
UniversalLocalPostalAttributes 98
UniversalOrBMPString 95
UniversalOrganizationalUnitName 95
UniversalOrganizationalUnitNames 95
UniversalOrganizationName 94
UniversalPDSParameter 98
UniversalPersonalName 95
UniversalPhysicalDeliveryOfficeName 96
UniversalPhysicalDeliveryOfficeNumber 96
UniversalPhysicalDeliveryOrganizationName 96
UniversalPhysicalDeliveryPersonalName 96
UniversalPosteRestanteAddress 97
UniversalPostOfficeBoxAddress 97

UniversalStreetAddress 97
UniversalUnformattedPostalAddress 97
UniversalUniquePostalName 97
UserAddress 77
UserName 77
UserSecurityLabel 174
Waiting 73
WaitingMessages 74
X121Address 93

ASN.1 values

alias (RedirectionReason) 89
alphabetic-character-loss (NonDeliveryDiagnosticCode) 83
alternate-recipient-allowed 81
ambiguous-OR-name (NonDeliveryDiagnosticCode) 83
any-delivery-method (RequestedDeliveryMethod) 86
assemby-instructions-conflict-with-security-services (SecurityProblem) 72
asymmetric-token 100
authentication-error (Bind-Error) 69, 117
authentication-failure-on-subject-message (NonDeliveryDiagnosticCode) 83
authentication-failure-on-subject-message (SecurityProblem) 72
authentication-problem (SecurityProblem) 72
bind-token-encrypted-data 101
bind-token-signed-data 101
bit-5 81
bit-6 81
bureau-fax-delivery (PhysicalDeliveryModes) 86
busy (Bind-Error) 69, 117
cancel-deferred-delivery 71
certificate-selectors 91
certificate-selectors-override 91
change-credentials 76
common-name 94
confidential (SecurityClassification) 101
confidentiality-association-problem (SecurityProblem) 72
content-confidentiality-algorithm-identifier 87
content-correlator 88
content-integrity-check 88
content-return-request 81
content-syntax-error (NonDeliveryDiagnosticCode) 83
content-too-long (NonDeliveryDiagnosticCode) 83
content-type-not-supported (NonDeliveryDiagnosticCode) 83
control-violates-registration 75
conversion-impractical (NonDeliveryDiagnosticCode) 83
conversion-not-performed (NonDeliveryReasonCode) 83
conversion-with-loss-prohibited 85
conversion-with-loss-prohibited (NonDeliveryDiagnosticCode) 83
counter-collection (PhysicalDeliveryModes) 86
counter-collection-with-telephone-advice (PhysicalDeliveryModes) 86
counter-collection-with-teletex-advice (PhysicalDeliveryModes) 86
counter-collection-with-telex-advice (PhysicalDeliveryModes) 86
decryption-failed (NonDeliveryDiagnosticCode) 84
decryption-failed (SecurityProblem) 72
decryption-key-unobtainable (NonDeliveryDiagnosticCode) 84
decryption-key-unobtainable (SecurityProblem) 72
deferred-delivery-cancellation-rejected 72
deferred-delivery-not-performed (NonDeliveryReasonCode) 83
delivery-control 74
delivery-control-88 173
delivery-control-violated 75
directory-look-up (RedirectionReason) 89
directory-operation-unsuccessful (NonDeliveryReasonCode) 83
disclosure-of-other-recipients 81
dl (TypeOfMTSUser) 82
dl-exempted-recipients 91
dl-expansion-failure (NonDeliveryDiagnosticCode) 83
dl-expansion-history 89

dl-expansion-prohibited 85
dl-expansion-prohibited (NonDeliveryDiagnosticCode) 83
dl-expansion-prohibited-by-security-policy (NonDeliveryDiagnosticCode) 83
double-envelope-creation-failure (NonDeliveryDiagnosticCode) 84
double-enveloping-message-restoring-failure (NonDeliveryDiagnosticCode) 84
e163-4-address 98
element-of-service-not-subscribed 72
emptyUnbind - see ISO/IEC 13712-1
encoded-information-types-unsupported (NonDeliveryDiagnosticCode) 83
err-control-violates-registration - see ISO/IEC 10021-6
err-deferred-delivery-cancellation-rejected - see ISO/IEC 10021-6
err-delivery-control-violated - see ISO/IEC 10021-6
err-element-of-service-not-subscribed - see ISO/IEC 10021-6
err-inconsistent-request - see ISO/IEC 10021-6
err-message-submission-identifier-invalid - see ISO/IEC 10021-6
err-new-credentials-unacceptable - see ISO/IEC 10021-6
err-old-credentials-incorrectly-specified - see ISO/IEC 10021-6
err-operation-refused - see ISO/IEC 10021-6
err-originator-invalid - see ISO/IEC 10021-6
err-recipient-improperly-specified - see ISO/IEC 10021-6
err-register-rejected - see ISO/IEC 10021-6
err-remote-bind-error - see ISO/IEC 10021-6
err-security-error - see ISO/IEC 10021-6
err-submission-control-violated - see ISO/IEC 10021-6
err-unsupported-critical-function - see ISO/IEC 10021-6
express-mail (PhysicalDeliveryModes) 86
extended-network-address 98
extension-OR-address-components 96
extension-physical-delivery-address-components 96
failure-of-proof-of-message (NonDeliveryDiagnosticCode) 84
failure-of-proof-of-message (SecurityProblem) 72
forbidden-alternate-recipient (NonDeliveryDiagnosticCode) 83
forbidden-user-security-label-register (SecurityProblem) 72
forwarding-request - see ISO/IEC 10021-5
g3-facsimile (EncodedInformationType) 98
g3-facsimile-delivery (RequestedDeliveryMethod) 86
g4-class-1 (EncodedInformationType) 98
g4-facsimile-delivery (RequestedDeliveryMethod) 86
generation-qualifier 93, 94
given-name 93, 94
ia5-terminal-delivery (RequestedDeliveryMethod) 86
ia5-text (EncodedInformationType) 98
id-att 164
id-att-physicalRendition-basic 165
id-att-physicalRendition-no-cover-page 165
id-cont 164
id-cont-inner-envelope 165
id-cont-unidentified 165
id-cp 164
id-cp-mta-connect 165
id-cp-mts-connect 165
id-ct 164
id-ct-mta-transfer 165
id-ct-mts-access 165
id-ct-mts-forced-access 165
id-eit 164
id-eit-g3-facsimile 165
id-eit-g4-class-1 165
id-eit-ia5-text 165
id-eit-mixed-mode 165
id-eit-teletex 165
id-eit-unknown 165
id-eit-videotex 165
id-eit-voice 165
id-mod 164
id-mod-mta-abstract-service 164
id-mod-mts-abstract-service 164

id-mod-object-identifiers 164
id-mod-upper-bounds 164
id-mts 164
id-ot 164
id-ot-mta 164
id-ot-mts 164
id-ot-mts-user 164
id-pt 164
id-pt-administration 165
id-pt-delivery 165
id-pt-submission 165
id-pt-transfer 165
id-sa 164
id-sa-ms 165
id-sa-ua 165
id-tok 164
id-tok-asymmetricToken 165
implicit-conversion-allowed 82
implicit-conversion-not-subscribed (NonDeliveryDiagnosticCode) 83
implicit-conversion-prohibited 81, 82
implicit-conversion-prohibited (NonDeliveryDiagnosticCode) 83
inadequate-association-confidentiality (Bind-Error) 69, 117
incompatible-change-with-original-security-context (SecurityProblem) 72
inconsistent-request 72
incorrect-notification-type (NonDeliveryDiagnosticCode) 83
initials 93, 94
integrity-failure-on-subject-message (NonDeliveryDiagnosticCode) 84
integrity-failure-on-subject-message (SecurityProblem) 72
internal-trace-information 122
invalid-arguments (NonDeliveryDiagnosticCode) 83
invalid-security-label (NonDeliveryDiagnosticCode) 84
invalid-security-label (SecurityProblem) 72
invalid-security-label-update (SecurityProblem) 72
key-failure (NonDeliveryDiagnosticCode) 84
key-failure (SecurityProblem) 72
latest-delivery-time 86
line-too-long (NonDeliveryDiagnosticCode) 83
local-postal-attributes 97
loop-detected (NonDeliveryDiagnosticCode) 83
mandatory-parameter-absence (NonDeliveryDiagnosticCode) 84
mandatory-parameter-absence (SecurityProblem) 72
maximum-time-expired (NonDeliveryDiagnosticCode) 83
message-delivery 74
message-origin-authentication-check 88
message-security-label 88
message-submission 70
message-submission-identifier-invalid 72
message-token 87
message-token-encrypted-data 101
message-token-signed-data 101
message-transfer 118
mhs-delivery (RequestedDeliveryMethod) 86
mixed-mode (EncodedInformationType) 98
ms (TypeOfMTSUser) 82
mta 117
mta-bind 117
mta-bind-error 117
mta-connect 117
mta-transfer 117
mta-unbind 117
mts 66
mts-88 172
mts-access-contract 66
mts-access-contract-88 173
mts-bind 68
mts-bind-error 69
mts-congestion (NonDeliveryDiagnosticCode) 83
mts-connect 68
mts-forced-access-contract 67
mts-forced-access-contract-88 173
mts-unbind 69
mts-user 66
mts-user-88 173

multiple-information-loss (NonDeliveryDiagnosticCode) 83
multiple-originator-certificates 91
new-credentials-unacceptable 76
no-bilateral-agreement (NonDeliveryDiagnosticCode) 83
no-dl-submit-permission (NonDeliveryDiagnosticCode) 83
non-registered-mail (RegisteredMailType) 87
non-urgent (Priority) 82
normal (Priority) 82
old-credentials-incorrectly-specified 77
op-cancel-deferred-delivery - see ISO/IEC 10021-6
op-change-credentials - see ISO/IEC 10021-6
op-delivery-control - see ISO/IEC 10021-6
operation-refused 75
operation-security-failure (NonDeliveryDiagnosticCode) 84
operation-security-failure (SecurityProblem) 72
op-message-delivery - see ISO/IEC 10021-6
op-message-submission - see ISO/IEC 10021-6
op-probe-submission - see ISO/IEC 10021-6
op-register - see ISO/IEC 10021-6
op-report-delivery - see ISO/IEC 10021-6
op-submission-control - see ISO/IEC 10021-6
ordinary-mail (PhysicalDeliveryModes) 86
originating-MTA-certificate 90
originating-MTA-non-delivery-report 121
originating-MTA-report 121
originator-and-DL-expansion-history 89
originator-certificate 87
originator-invalid 72
originator-non-delivery-report 121
originator-report 121
originator-requested-alternate-recipient 85, 122
originator-requested-alternate-recipient (RedirectionReason) 89
originator-return-address 87
other (TypeOfMTSUser) 82
page-split (NonDeliveryDiagnosticCode) 83
pdau (TypeOfMTSUser) 82
pds-name 95
physical-delivery (RequestedDeliveryMethod) 86
physical-delivery-country-name 95
physical-delivery-modes 86
physical-delivery-not-performed (NonDeliveryReasonCode) 83
physical-delivery-office-name 96
physical-delivery-office-number 96
physical-delivery-organization-name 96
physical-delivery-personal-name 96
physical-delivery-report-request 87
physical-forwarding-address 89
physical-forwarding-address-request 86
physical-forwarding-prohibited 86
physical-recipient (TypeOfMTSUser) 82
physical-rendition-attributes 87
physical-rendition-attributes-not-supported (NonDeliveryDiagnosticCode) 83
physical-rendition-not-performed (NonDeliveryReasonCode) 83
pictorial-symbol-loss (NonDeliveryDiagnosticCode) 83
postal-code 96
poste-restante-address 97
post-office-box-address 97
private (TypeOfMTSUser) 82
private-extension 85
probe-origin-authentication-check 88
probe-submission 71
probe-transfer 118
proof-of-delivery 89
proof-of-delivery-request 88
proof-of-submission 90
proof-of-submission-request 88
protocol-violation (NonDeliveryDiagnosticCode) 83
psap-address 98
public (TypeOfMTSUser) 82
punctuation-symbol-loss (NonDeliveryDiagnosticCode) 83
recipient-assigned-alternate-recipient (RedirectionReason) 89
recipient-certificate 89
recipient-improperly-specified 72

recipient-MD-assigned-alternate-recipient (RedirectionReason) 89
recipient-number-for-advice 87
recipient-reassignment-prohibited 85
recipient-reassignment-prohibited (NonDeliveryDiagnosticCode) 83
recipient-unavailable (NonDeliveryDiagnosticCode) 83
redirection-history 89
redirection-loop-detected (NonDeliveryDiagnosticCode) 83
redirection-prohibited (SecurityProblem) 72
refused-alternate-recipient-name (SecurityProblem) 72
register 76
register-88 173
registered-mail (RegisteredMailType) 87
registered-mail-to-addressee-in-person (RegisteredMailType) 87
registered-mail-type 87
register-rejected 76
remote-bind-error 73
report-delivery 74
reporting-DL-name 90
reporting-MTA-certificate 90
reporting-MTA-name 90
report-origin-authentication-check 90
report-transfer 118
repudiation-failure-of-message (NonDeliveryDiagnosticCode) 84
repudiation-failure-of-message (SecurityProblem) 72
requested-delivery-method 86
responder-credentials-checking-problem (SecurityProblem) 72
responsibility 121
restricted (SecurityClassification) 101
restricted-delivery (NonDeliveryReasonCode) 83
return-of-notification-by-MHS (PhysicalDeliveryReportRequest) 87
return-of-notification-by-MHS-and-PDS (PhysicalDeliveryReportRequest) 87
return-of-notification-by-PDS (PhysicalDeliveryReportRequest) 87
return-of-undeliverable-mail-by-PDS (PhysicalDeliveryReportRequest) 87
secret (SecurityClassification) 101
secure-messaging-error (NonDeliveryDiagnosticCode) 83
security-context-failure (NonDeliveryDiagnosticCode) 84
security-context-failure (SecurityProblem) 72
security-context-problem (SecurityProblem) 72
security-error 72
security-policy-violation (NonDeliveryDiagnosticCode) 83
security-policy-violation (SecurityProblem) 72
security-services-refusal (NonDeliveryDiagnosticCode) 83
security-services-refusal (SecurityProblem) 72
service-message 81
size-constraint-violation (NonDeliveryDiagnosticCode) 83
special-delivery (PhysicalDeliveryModes) 86
standard-extension 85
street-address 97
submission-control 71
submission-control-violated 72
surname 93, 94
telephone-delivery (RequestedDeliveryMethod) 86
teletex (EncodedInformationType) 98
teletex-common-name 94
teletex-delivery (RequestedDeliveryMethod) 86
teletex-domain-defined-attributes 98
teletex-organizational-unit-names 95
teletex-organization-name 94
teletex-personal-name 94
telex-delivery (RequestedDeliveryMethod) 86
terminal-type 98
token-decryption-failed (NonDeliveryDiagnosticCode) 84
token-decryption-failed (SecurityProblem) 72
token-error (NonDeliveryDiagnosticCode) 84
token-error (SecurityProblem) 72
too-many-recipients (NonDeliveryDiagnosticCode) 83
top-secret (SecurityClassification) 101

trace-information 122
transfer 117
transfer-attempts-limit-reached (NonDeliveryDiagnosticCode) 83
transfer-failure (NonDeliveryReasonCode) 83
transfer-failure-for-security-reason (NonDeliveryReasonCode) 83
ub-additional-info 166
ub-bilateral-info 166
ub-bit-options 166
ub-built-in-content-type 166
ub-built-in-encoded-information-types 166
ub-certificates 166
ub-common-name-length 166
ub-content-correlator-length 166
ub-content-id-length 166
ub-content-length 166
ub-content-types 166
ub-country-name-alpha-length 166
ub-country-name-numeric-length 166
ub-deliverable-class 166
ub-diagnostic-codes 166
ub-dl-expansions 166
ub-domain-defined-attributes 166
ub-domain-defined-attribute-type-length 167
ub-domain-defined-attribute-value-length 167
ub-domain-name-length 167
ub-e163-4-number-length 167
ub-e163-4-sub-address-length 167
ub-encoded-information-types 167
ub-extension-attributes 167
ub-extension-types 167
ub-generation-qualifier-length 167
ub-given-name-length 167
ub-initials-length 167
ub-integer-options 167
ub-labels-and-redirections 167
ub-local-id-length 167
ub-mta-name-length 167
ub-mts-user-types 167
ub-numeric-user-id-length 167
ub-organizational-unit-name-length 167
ub-organizational-units 167
ub-organization-name-length 167
ub-orig-and-dl-expansions 167
ub-password-length 167
ub-pds-name-length 167
ub-pds-parameter-length 167
ub-pds-physical-address-lines 167
ub-postal-code-length 167
ub-privacy-mark-length 167
ub-queue-size 167
ub-reason-codes 167
ub-recipient-number-for-advice-length 167
ub-recipients 167
ub-redirection-classes 167
ub-redirections 167
ub-restrictions 168
ub-security-categories 168
ub-security-labels 168
ub-security-problems 168
ub-supplementary-info-length 168
ub-surname-length 168
ub-teletex-private-use-length 168
ub-terminal-id-length 168
ub-transfers 168
ub-tsap-id-length 168
ub-unformatted-address-length 168
ub-universal-generation-qualifier-length 168
ub-universal-given-name-length 168
ub-universal-initials-length 168
ub-universal-surname-length 168
ub-x121-address-length 168
unable-to-aggregate-security-labels (SecurityProblem) 72
unable-to-complete-transfer (NonDeliveryDiagnosticCode) 83
unable-to-downgrade (NonDeliveryDiagnosticCode) 83
unable-to-transfer (NonDeliveryReasonCode) 83
unacceptable-dialogue-mode (Bind-Error) 69, 117

unacceptable-security-context (Bind-Error) 69, 117
unauthorised-dl-member (NonDeliveryDiagnosticCode) 83
unauthorised-dl-name (NonDeliveryDiagnosticCode) 83
unauthorised-dl-name (SecurityProblem) 72
unauthorised-entry-class (SecurityProblem) 72
unauthorised-originally-intended-recipient-name (SecurityProblem) 72
unauthorised-originally-intended-recipient-name (NonDeliveryDiagnosticCode) 83
unauthorised-originator-name (NonDeliveryDiagnosticCode) 83
unauthorised-originator-name (SecurityProblem) 72
unauthorised-recipient-name (NonDeliveryDiagnosticCode) 83
unauthorised-recipient-name (SecurityProblem) 72
unauthorised-security-label (SecurityProblem) 72
unauthorised-user-name (SecurityProblem) 72
unclassified (SecurityClassification) 101
undeliverable-mail-new-address-unknown (NonDeliveryDiagnosticCode) 83
undeliverable-mail-organization-expired (NonDeliveryDiagnosticCode) 83
undeliverable-mail-originator-prohibited-forwarding (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-address-incomplete (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-address-incorrect (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-office-incorrect-or-invalid (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-address-permanently (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-address-temporarily (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-temporary-address (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-deceased (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-did-not-claim (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-did-not-want-forwarding (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-refused-to-accept (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-unknown (NonDeliveryDiagnosticCode) 83
unformatted-postal-address 97
unique-postal-name 97
universal-domain-defined-attributes 98
universal-extension-OR-address-components 96
universal-extension-physical-delivery-address-components 96
universal-local-postal-attributes 98
universal-organizational-unit-names 95
universal-physical-delivery-office-name 96
universal-physical-delivery-office-number 96
universal-physical-delivery-organization-name 96
universal-physical-delivery-personal-name 96
universal-poste-restante-address 97
universal-post-office-box-address 97
universal-street-address 97
universal-unformatted-postal-address 97
universal-unique-postal-name 97
unknown (EncodedInformationType) 98
unknown-security-label (NonDeliveryDiagnosticCode) 84
unknown-security-label (SecurityProblem) 72
unmarked (SecurityClassification) 101
unrecognised-OR-name (NonDeliveryDiagnosticCode) 83
unreliable-system (NonDeliveryDiagnosticCode) 83
unsupported-algorithm-identifier (NonDeliveryDiagnosticCode) 84
unsupported-algorithm-identifier (SecurityProblem) 72
unsupported-critical-function 72
unsupported-critical-function (NonDeliveryDiagnosticCode) 83
unsupported-security-policy (NonDeliveryDiagnosticCode) 84
unsupported-security-policy (SecurityProblem) 72
urgent (Priority) 82
videotex (EncodedInformationType) 98
videotex-delivery (RequestedDeliveryMethod) 86
voice (EncodedInformationType) 98

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
Série X	**Réseaux de données et communication entre systèmes ouverts**
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

Imprimé en Suisse
Genève, 2004