UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.812

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(02/2004)

SÉRIE Q: COMMUTATION ET SIGNALISATION

Interface Q3

Profils des protocoles des couches supérieures pour les interfaces Q et X

Recommandation UIT-T Q.812

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4, 5, 6, R1 ET R2	Q.120–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	**Q.800–Q.849**
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
SPÉCIFICATIONS DE LA SIGNALISATION RELATIVE À LA COMMANDE D'APPEL INDÉPENDANTE DU SUPPORT	Q.1900–Q.1999
RNIS À LARGE BANDE	Q.2000–Q.2999

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

Recommandation UIT-T Q.812

Profils des protocoles des couches supérieures pour les interfaces Q et X

Résumé

La présente Recommandation fournit les profils des protocoles des couches supérieures (5-7) pour les interfaces Q et X définies dans les Recommandations UIT-T de la série M.3000.

Source

La Recommandation Q.812 de l'UIT-T a été approuvée le 13 février 2004 par la Commission d'études 4 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), 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 l'AMNT.

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

© UIT 2005

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

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références normatives	1
3	Définitions	5
4	Abréviations	6
5	Spécifications des protocoles des couches supérieures pour le paradigme de l'OSI	8
	5.1 Introduction	8
	5.2 Spécifications des protocoles des couches supérieures pour les services de classe interactive	8
	5.3 Spécifications des protocoles des couches supérieures pour les services de classe orientée fichier	10
	5.4 Spécifications du protocole de couche supérieure pour les services d'annuaire	11
	5.5 Spécifications des protocoles de couche supérieure pour les services d'enregistrement et retransmission	11
6	Spécifications des protocoles des couches supérieures pour les services de classe interactive utilisant le paradigme de l'OSI	11
	6.1 Profils de couche Transport	11
	6.2 Couche Session	17
	6.3 Couche Présentation	17
	6.4 Couche Application	18
	6.5 Prise en charge de la sécurité pour des applications interactives	20
7	Spécification des protocoles de couche supérieure pour les fonctions de classe orientée fichier utilisant le paradigme de l'OSI	21
	7.1 Couche Session	21
	7.2 Couche Présentation	21
	7.3 Profil de la couche Application	22
	7.4 Prise en charge de la sécurité pour les services FTAM	24
8	Spécifications du protocole de couche supérieure pour les services d'annuaire utilisant le paradigme de l'OSI	24
	8.1 Couche Session	24
	8.2 Couche Présentation	24
	8.3 Couche Application	25
	8.4 Prise en charge de la sécurité pour les services d'annuaire	26
9	Conformité pour le paradigme de l'OSI	26
10	Profil de protocole pour les services basés sur l'architecture CORBA	27
	10.1 Domaine du profil du protocole CORBA	27
	10.2 Aperçu général des profils pour les services basés sur l'architecture CORBA	27
	10.3 Définition du service	28

Page

10.4 Spécification du GIOP 28
10.5 Spécification du protocole IOP sécurisé 28
10.6 Spécification du protocole IIOP 28
10.7 Profil du protocole TCP/IP à utiliser avec le protocole IIOP 28
11 Profil de protocole pour services axés sur la norme EDI/EDIFACT 29
11.1 Cadre du profil de protocole EDI/EDIFACT 29
11.2 Résumé 29
11.3 Profil de protocole TCP/IP à utiliser avec l'agent IA 29
11.4 Profil de protocole TLS à utiliser avec l'agent IA 29
11.5 Profil de l'agent IA 30
11.6 Module de sécurité pour le profil de protection complète du message 30
11.7 Protocole du traducteur EDI/EDIFACT 31
12 Profil de protocole pour le paradigme SNMP 31
13 Profil de protocole pour le paradigme de langage de balisage des télécommunications (tML) 32
Appendice I – Directives pour l'utilisation de la gestion allomorphique 32
I.1 Introduction 32
I.2 Opérations du protocole CMIP 34
I.3 Notifications CMIP 44
I.4 Considérations relatives à l'implémentation 45
I.5 Exemples d'utilisation de l'allomorphisme 48
Appendice II – Modifications des prescriptions de conformité ISP 51

Recommandation UIT-T Q.812

Profils des protocoles des couches supérieures pour les interfaces Q et X

1 Domaine d'application

La présente Recommandation définit les caractéristiques des profils des protocoles pour les interfaces Q et X définies dans la série de Recommandations UIT-T de la série M.3000. L'interface prendra en charge le transfert de données bidirectionnel pour la gestion des systèmes de télécommunication.

Si la nécessité d'une fonction de sécurité est bien connue, celle-ci n'est toutefois pas traitée dans sa totalité dans la présente Recommandation et nécessite un complément d'étude. Les utilisateurs devront éventuellement recourir à des mécanismes qui sont hors du domaine de la présente Recommandation pour répondre à leurs besoins de sécurité particuliers. Ces mécanismes pourront être choisis en fonction de la configuration du réseau.

La présente Recommandation définit:

– les profils des services de couche;

– les profils des protocoles de couche;

– le service d'application et les profils de protocole;

– les besoins de conformité à respecter par une mise en œuvre de cette interface.

La présente Recommandation ne définit pas:

– la structure ou le sens des informations de gestion transmises au moyen de la suite de protocoles;

– la manière dont la gestion est accomplie par suite de l'application des échanges de protocole;

– les interactions qui résultent de l'utilisation des protocoles des couches Application.

Les profils contenus dans la présente Recommandation sont alignés sur les profils ISP équivalents.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[1] ISO/CEI/TR 10000-1:1995, *Technologies de l'information – Cadre et taxonomie des profils normalisés internationaux – Partie 1: Principes généraux et cadre de documentation*.

[2] Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base*.

[3] Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications*.

[4] Recommandation UIT-T X.224 (1995) | ISO/CEI 8073:1997, *Technologies de l'information – Interconnexion des systèmes ouverts (OSI) – Protocole assurant le service de transport en mode connexion*.

[5] Recommandation UIT-T X.225 (1995) | ISO/CEI 8327-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de session en mode connexion: spécification, plus* Amendement 1 (1997), *Amélioration de l'efficacité*.

[6] ISO/CEI ISP 11183-1:1992, *Technologies de l'information – Profil normalisé international AOM1n pour la gestion OSI – Communications d'informations de gestion – Partie 1: Spécification des protocoles d'ACSE, de présentation et de session utilisés par ROSE et CMISE*.

[7] Recommandation UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de présentation*.

[8] Recommandation UIT-T X.226 (1994) | ISO/CEI 8823-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de présentation en mode connexion: spécification du protocole*.

[9] Recommandation UIT-T X.209 (1988), *Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un (ASN.1)*.

ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro UNE (ASN.1)*.

[10] Recommandation UIT-T X.680 (1994) | ISO/CEI 8824-1:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base*.

[11] Recommandation UIT-T X.681 (1994) | ISO/CEI 8824-2:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels*.

[12] Recommandation UIT-T X.682 (1994) | ISO/CEI 8824-3:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes*.

[13] Recommandation UIT-T X.683 (1994) | ISO/CEI 8824-4:1995, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un*.

[14] Recommandation UIT-T X.208 (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1)*.

ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts, spécification de la syntaxe abstraite numéro un (ASN.1)*.

[15] ISO/CEI 9545:1994, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Structure de la couche application*.

[16] Recommandation UIT-T X.217 (1995) | ISO/CEI 8649:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition de service applicable à l'élément de service de contrôle d'association*.

[17] Recommandation UIT-T X.227 (1995) | ISO/CEI 8650-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: spécification du protocole*.

[18] Recommandation UIT-T X.219 (1988), *Opérations distantes: modèle, notation et définition du service*.

ISO/CEI 9072-1:1989, *Systèmes de traitement de l'information – Communication de texte – Opérations à distance – Partie 1: Modèle, notation et définition du service*.

[19] Recommandation UIT-T X.229 (1988), *Opérations distantes: spécification du protocole*.

ISO/CEI 9072-2:1989, *Systèmes de traitement de l'information – Communication de texte – Opérations à distance – Partie 2: Spécification du protocole*.

[20] Recommandation UIT-T X.710 (1991), *Définition du service commun de transfert d'informations de gestion pour les applications du CCITT*.

ISO/CEI 9595:1991, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service commun d'informations de gestion*.

[21] Recommandation UIT-T X.711 (1991), *Opérations distantes: Modèle, notation et définition du service*.

ISO/CEI 9596-1:1991, *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole commun d'information de gestion – Partie 1: Spécification du protocole*.

[22] ISO/CEI ISP 11183-3:1992, *Technologies de l'information – Profil normalisé international AOM1n pour la gestion OSI – Communications d'informations de gestion – Partie 3: CMISE/ROSE pour AOM11 – Communications de base d'informations de gestion*.

[23] ISO/CEI ISP 11183-2:1992, *Technologies de l'information – Profil normalisé international AOM1n pour la gestion OSI – Communications d'informations de gestion – Partie 2: CMISE/ROSE pour AOM12 – Communications étendues d'informations de gestion*.

[24] ISO/CEI ISP 10607-1:1995, *Technologies de l'information – Profils normalisés internationaux AFTnn – Transfert, accès et gestion de fichier – Partie 1: Spécifications des protocoles ACSE, de présentation et de session pour emploi par FTAM*.

[25] ISO 8571-1:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Transfert, accès et gestion de fichiers – Partie 1: Introduction générale*.

[26] ISO 8571-2:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Transfert, accès et gestion de fichiers – Partie 2: Détermination du système de fichiers virtuel*.

[27] ISO 8571-3:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Transfert, accès et gestion de fichiers – Partie 3: Définition du service de fichiers*.

[28] ISO 8571-4:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Transfert, accès et gestion de fichiers – Partie 4: Spécification du protocole de fichiers*.

[29] 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*.

[30] Recommandation UIT-T X.501 (1997) | ISO/CEI 9594-2:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*.

[31] 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*.

[32] 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*.

[33] Recommandation UIT-T X.519 (1997) | ISO/CEI 9594-5:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécifications du protocole*.

[34] 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*.

[35] 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*.

[36] Recommandation UIT-T X.509 (1997) | ISO/CEI 9594-8:1998, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification*.

[37] Recommandation UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Technologies de l'information – Opérations distantes: concepts, modèle et notation*.

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

[39] Recommandation UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: aperçu général, modèles et notation*.

[40] ISO/CEI ISP 10607-3:1995, *Technologies de l'information – Profils normalisés internationaux AFTnn – Transfert, accès et gestion de fichier – Partie 3: AFT11 – Service de transfert simple de fichier (non structuré)*.

[41] Recommandation UIT-T X.214 (1995) | ISO/CEI 8072:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service de transport*.

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

[43] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

ISO/CEI 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

[44] Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures*.

[45] Recommandation UIT-T X.811 (2004), *Profils des protocoles des couches inférieures pour les interfaces Q et X*.

[46] Recommandation UIT-T Q.814 (2000), *Spécification d'un agent interactif d'échange informatisé de données*.

[47] Recommandation UIT-T X.815 (2000), *Spécification d'un modèle de sécurité pour la protection globale des messages*.

[48] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.

[49] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[50] IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

[51] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[52] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[53] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[54] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[55] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[56] IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

[57] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

[58] IETF RFC 3430 (2002), *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping*.

[59] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

[60] ISO/CEI ISP 10608-1:1992, *Technologies de l'information – Profil normalisé international TAnnnn – Service de transport en mode connexion sur le service de réseau en mode sans connexion – Partie 1: Introduction générale et spécifications indépendantes du sous-réseau*.

[61] ISO/CEI ISP 10609-1:1992, *Technologies de l'information – Profils normalisés internationaux TB, TC, TD et TE – Service de transport en mode connexion sur un service de réseau en mode connexion – Partie 1: Spécifications indépendantes du type de sous-réseau pour groupe TB*.

[62] CORBA GIOP Specification, Chapter 15 of *The Common Object Request Broker: Architecture and Specification*, Revision 2.3, Object Management Group (OMG Doc. Number: Formal/98-12-01).

[63] CORBA Security Service Specification, Chapter 15 of *CORBA services: Common Object Services Specification*, Object Management Group (OMG Doc. Number: Formal/98-12-17).

[64] Recommandation UIT-T M.3030 (2002), *Langage de balisage pour les télécommunications (tML): cadre général*.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 profil international normalisé (ISP, *international standardized profile)*: document homogène, approuvé sur le plan international, qui définit une norme ou un groupe de normes ainsi que les options et les paramètres nécessaires à l'accomplissement d'une fonction ou d'un ensemble de fonctions [1].

3.2 agent interactif (IA, *interactive agent*) (Rec. UIT-T Q.814): l'agent interactif prend en charge les transactions d'échange informatisé de données (UN/EDIFACT ou ASC X12 EDI) entre des entités homologues. L'agent IA fonctionne comme une interface entre son utilisateur direct

(généralement un traducteur ou un module de sécurité EDIFACT/ASC X12 EDI) et la sécurité de la couche de transport. Plusieurs approches concernant l'implémentation peuvent être envisagées, allant d'une simple interface de programme d'application (API) jusqu'à un programme autonome. L'agent IA est décrit dans la Rec. UIT-T Q.814 et le module de sécurité est décrit dans la Rec. UIT-T Q.815.

3.3 sécurité de la couche de transport (TLS, *transport layer security*) (Rec. UIT-T Q.814): le protocole TLS fournit en option la confidentialité des communications. Ce protocole permet aux applications client/serveur de communiquer de manière à empêcher toute écoute illégale, altération ou intrusion. Le protocole TLS permet également une authentification d'homologues et une intégrité de circulation des données efficaces.

3.4 règles de codage distinctives (DER, *distinguished encoding rule*) (Rec. UIT-T X.690): les règles DER de l'ASN.1 sont un sous-ensemble des règles de codage de base (BER) qui donne une manière et une seule de représenter une valeur ASN.1 sous la forme d'une chaîne d'octets. Les règles DER sont destinées aux applications qui nécessitent un codage unique en chaîne d'octets, comme c'est le cas lorsqu'un message ASN.1 est codé en vue du transport sécurisé TLS. Les règles DER sont présentées dans la Rec. UIT-T X.690. Dans le présent profil il faut utiliser la méthode de construction de longueur définie pour les messages IA.

3.5 protocole de transfert d'agent interactif (IATP, *interactive agent transfer protocol*) (Rec. UIT-T Q.814): le protocole IATP est utilisé entre des agents interactifs homologues voulant effectuer des transactions/envoyer des messages d'échanges informatisé de données via le protocole de commande de transmission/protocole Internet (TCP/IP) en utilisant la sécurité de la couche de transport. Le protocole IATP est décrit dans la Rec. UIT-T Q.814.

3.6 traducteur (EDI, *electronic data interchange*) (Rec. UIT-T .814): programme ou module logiciel qui convertit des formats et des représentations de données privés en formats et en représentations normalisés, tels que ceux spécifiés dans l'ISO 9735 et l'ANSI ASC X12, et vice versa.)

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ACSE élément de service de contrôle d'association (*association control service element*)

AE entité d'application (*application entity*)

APDU unité de données protocolaire d'application (*application protocol data unit*)

ASE élément de service d'application (*application service element*)

ASN.1 notation de syntaxe abstraite numéro un (*abstract syntax notation one*)

ASO objet de service d'application (*application service object*)

BER règles de codage de base (*basic encoding rules*)

CCITT Comité consultatif international télégraphique et téléphonique

CEI Commission électrotechnique internationale

CF fonction de commande (*control function*)

CMIP protocole commun d'informations de gestion (*common management information protocol*)

CMISE élément du service commun d'informations de gestion (*common management information service element*)

CLNS service de couche réseau en mode sans connexion (*connectionless-mode network layer service*)

CONS service de couche réseau en mode connexion (*connection-mode network layer service*)

CORBA architecture de courtier commun de requêtes d'objets (*common object request broker architecture*)

COTS service de transport en mode connexion (*connection-mode transport service*)

DAP protocole d'accès à l'annuaire (*directory access protocol*)

DER règles de codage distinctives (*distinguished encoding rules*)

DSA agent de système d'annuaire (*directory system agent*)

DUA agent d'utilisateur d'annuaire (*directory user agent*)

EDI échange informatisé de données (*electronic data interchange*)

EDIFACT échange informatisé de données pour l'administration, le commerce et le transport (*electronic data interchange for administration, commerce and transport*)

FTAM transfert, accès et gestion de fichiers (*file transfer, access and management*)

GULS sécurité générique des couches supérieures (*generic upper layer security*)

IA agent interactif (*interactive agent*)

IATP protocole de transfert d'agent interactif (*interactive agent transfer protocol*)

IDL langage de définition d'interface (*interface definition language*)

IETF Groupe de travail d'ingéniérie Internet (*Internet engineering task force*)

IP protocole Internet (internet protocol)

IPSec architecture de sécurité pour le protocole IP (*security architecture for the IP protocol*)

ISO Organisation Internationale de Normalisation (*International Organization for Standardization*)

ISP profil normalisé international (*international standardized profile*)

NBS Bureau national de normalisation (*National Bureau of Standards*)

NCMS sous-protocole de gestion de connexion réseau (*network connection management subprotocol*)

NE élément de réseau (*network element*)

OS système d'exploitation (*operations system*)

OSI interconnexion des systèmes ouverts (*open systems interconnection*)

PDU unité de données protocolaire (*protocol data unit*)

RCD réseau de communication de données

RFC demande de commentaires (*request for comments*)

RGT réseau de gestion des télécommunications

ROS service d'opérations distantes (*remote operations service*)

ROSE élément du service d'opérations distantes (*remote operations service element*)

SACF fonction de contrôle d'association unique (*single association control function*)

SMASE élément de service d'application de gestion-systèmes (*systems management application service element*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SPDU unité de données protocolaire de session (*session protocol data unit*)

TCP protocole de commande de transmission (*transmission control protocol*)

TLS sécurité de la couche de transport (*transport layer security*)

tML langage de balisage des télécommnications (*telecommunication markup language*)

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

UIT Union internationale des télécommunications

UIT-T Union internationale des télécommunications – Secteur de la normalisation de télécommunications

USM modèle de sécurité fondé sur l'utilisateur (*user-based security model*)

5 Spécifications des protocoles des couches supérieures pour le paradigme de l'OSI

5.1 Introduction

Les services et protocoles de communication dont traite la présente Recommandation sont conformes au modèle de référence pour l'interconnexion des systèmes ouverts (OSI, *open systems interconnection*) [2].

Les protocoles pour les différentes couches sont fondés sur les Recommandations pertinentes de l'UIT-T et sur les normes appropriées de l'ISO, le formulaire de spécifications CORBA du groupe OMG et les spécifications du protocole Internet de l'IETF.

La présente Recommandation définit trois types de profil de protocole:

– les profils de protocole de couche supérieure pour les services de classe interactive;

– les profils de protocole de couche supérieure pour les services de classe orientée fichier;

– les spécifications de protocole de couche supérieure pour les services d'annuaire.

Ces trois profils de protocole peuvent être utilisés pour des applications faisant appel à des réseaux RCD, selon la définition de la Rec. UIT-T M.3010 [3].

L'interface Q est définie en vue de la connexion, au moyen d'un réseau RCD, des dispositifs de médiation aux systèmes d'exploitation (OS), des adaptateurs Q aux OS, des éléments NE aux OS et des OS aux OS. L'interface X est définie en vue de connecter les RGT de deux Administrations.

D'autres éléments ASE seront ajoutés dans les profils de protocole identifiés à mesure que de nouveaux besoins apparaîtront.

5.2 Spécifications des protocoles des couches supérieures pour les services de classe interactive

La Figure 1 illustre la pile de protocoles du profil de protocole de couche supérieure pour les services de classe interactive. Le profil des ensembles de fonctions du RGT correspondant à l'élément SMASE pour les services de classe interactive peut être spécifié dans le cadre des Recommandations définissant les modèles et les services d'information.

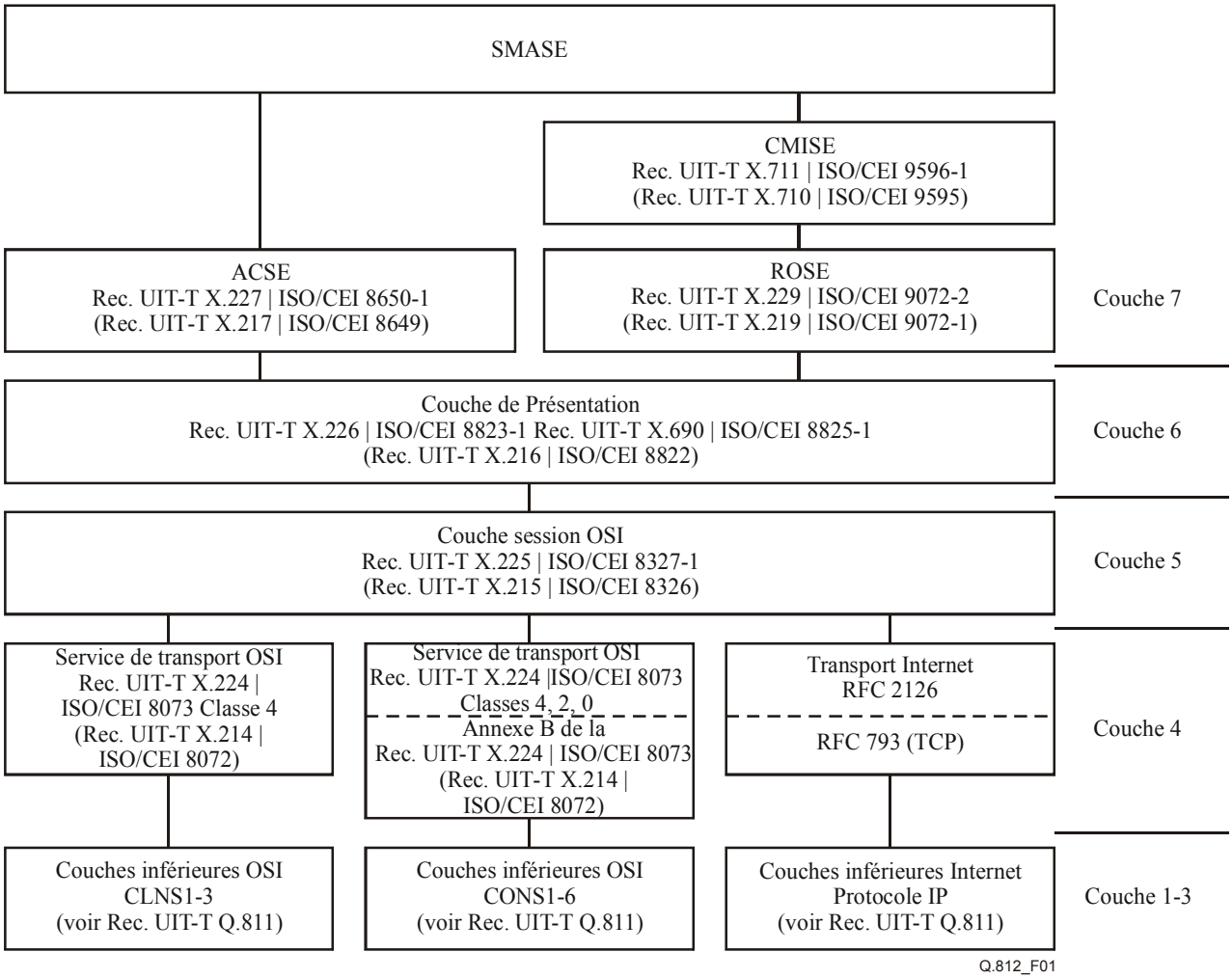

Figure 1/Q.812 – Pile de protocoles du profil de protocole de couche supérieure pour les services de classe interactive pour le paradigme de l'OSI

5.3 Spécifications des protocoles des couches supérieures pour les services de classe orientée fichier

La Figure 2 illustre la pile de protocoles du profil de protocole de couche supérieure pour les services de classe orientée fichier.

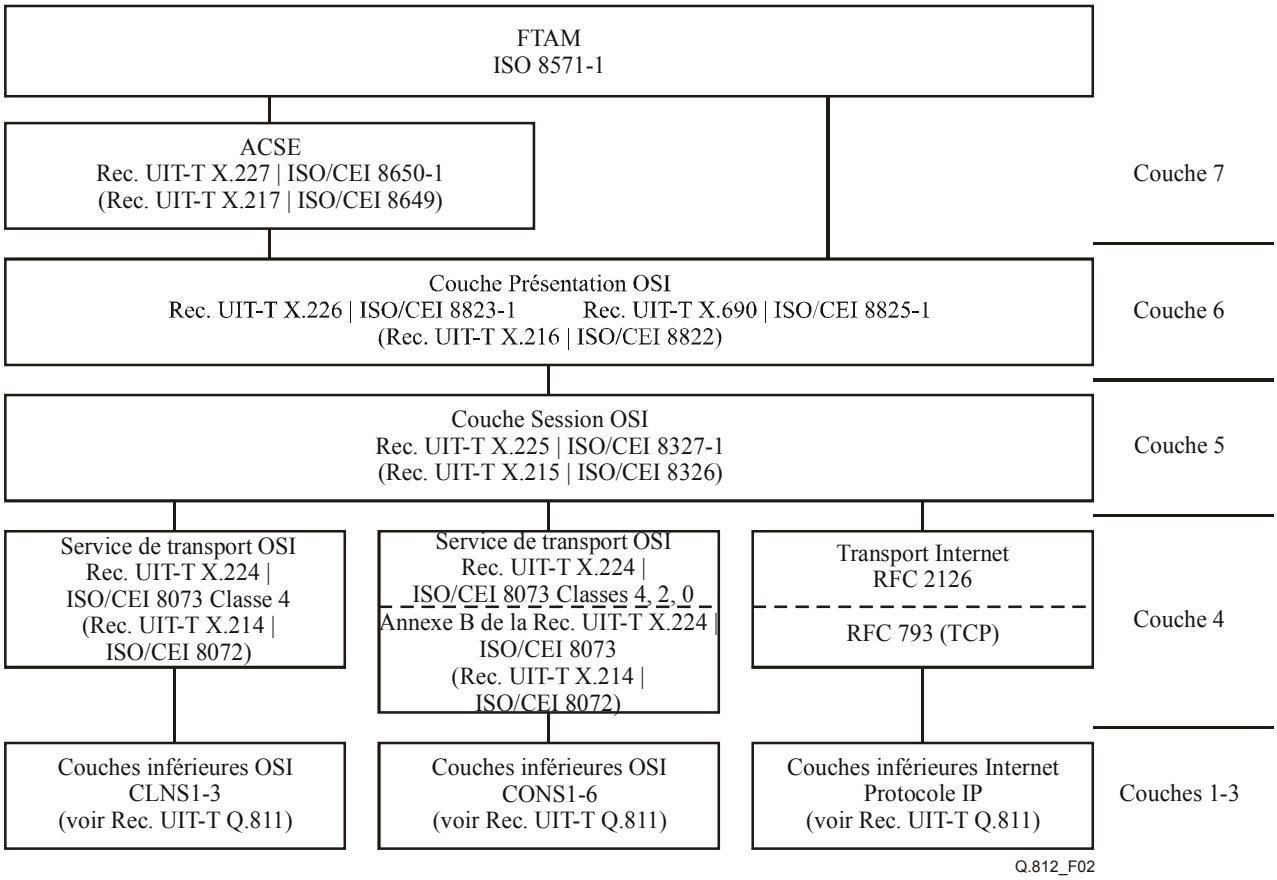

Figure 2/Q.812 – Pile de protocoles du profil de protocole de couche supérieure pour les services de classe orientée fichier pour le paradigme de l'OSI

5.4 Spécifications du protocole de couche supérieure pour les services d'annuaire

La Figure 3 illustre la pile de protocoles du profil de protocole de couche supérieure pour les services d'annuaire.

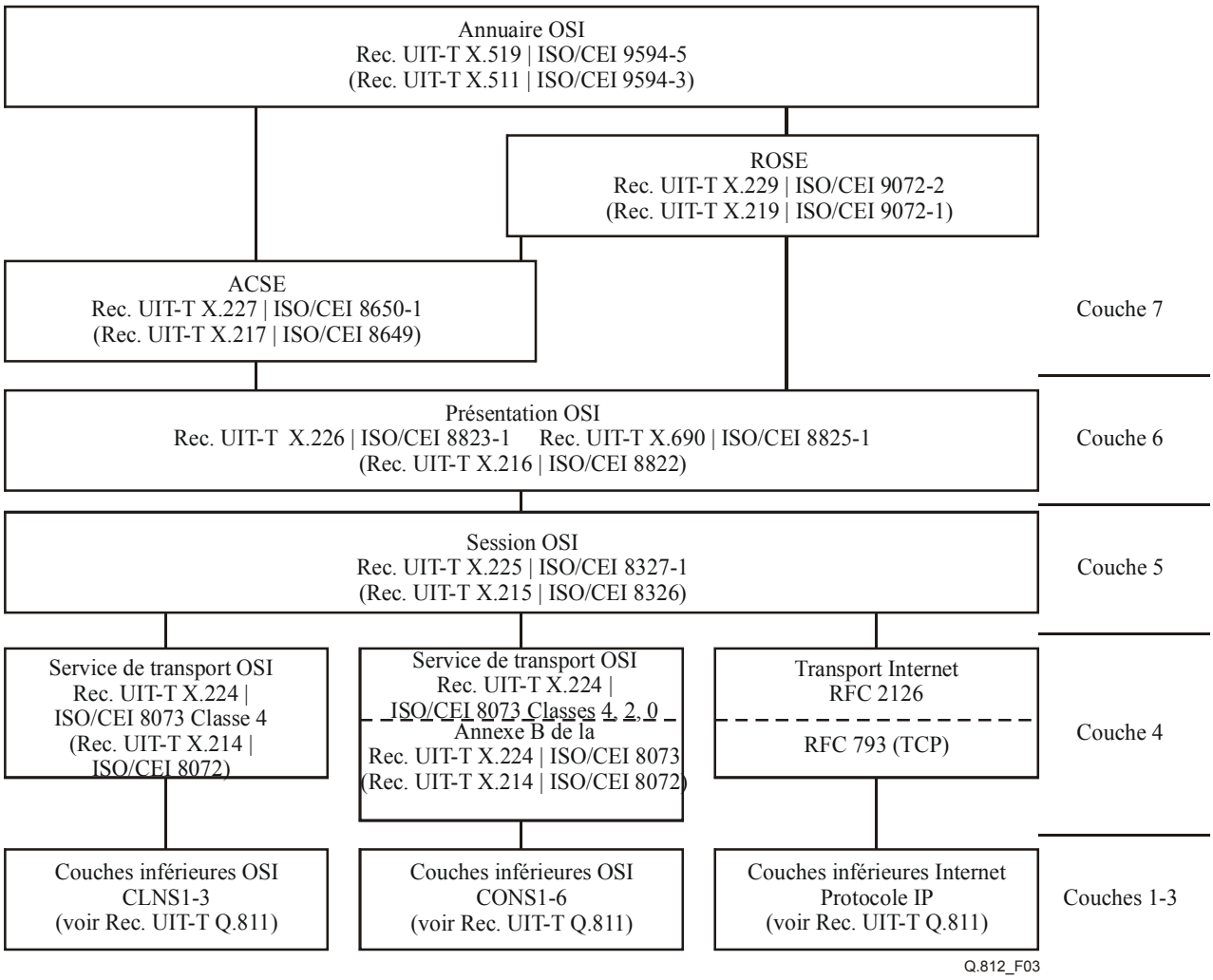

Figure 3/Q.812 – Pile de protocoles du profil de protocole de couche supérieure pour les services d'annuaire pour le paradigme de l'OSI

5.5 Spécifications des protocoles de couche supérieure pour les services d'enregistrement et retransmission

Les protocoles de couche supérieure à utiliser pour les services d'enregistrement et retransmission (par exemple, pour l'échange d'information au format EDI) nécessitent un complément d'étude.

6 Spécifications des protocoles des couches supérieures pour les services de classe interactive utilisant le paradigme de l'OSI

6.1 Profils de couche Transport

6.1.1 Profil de couche Transport pour services CLNS1, CLNS2 et CLNS3

Le présent paragraphe définit le profil de couche Transport à utiliser avec les services CLNS1, CLNS2 et CLNS3 définis dans la Rec. UIT-T Q.811 [45].

6.1.1.1 Profil des services

Pour le service de réseau en mode sans connexion, il est indispensable que le service de transport soit conforme aux prescriptions de la Rec. UIT-T X.214 | ISO/CEI 8072 [41].

6.1.1.2 Profil de protocole

Le fonctionnement avec le protocole de transport sur le service de réseau en mode sans connexion (CLNS, *connectionless-mode network layer service*), défini dans la Rec. UIT-T X.213 | ISO/CEI 8348, utilisera les éléments de la Rec. UIT-T X.224 | ISO/CEI 8073 [4], "Caractéristiques du protocole de transport en Classe 4 dans l'exploitation du service CLNS". Les dispositions des 6.1.2.1.2, 6.1.2.1.3, 6.1.2.1.4, 6.1.2.2.4, 6.1.2.2.6, 6.1.2.2.7 et 6.1.2.2.8 du protocole de transport de profil CONS1 s'appliquent également dans ce cas.

6.1.1.3 Classe de service

La prise en charge du fonctionnement en Classe 4 de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] est obligatoire.

6.1.1.4 Attributs de couche Transport

Les attributs de la couche Transport pour le fonctionnement en Classe 4 sur le service de réseau en mode sans connexion sera conforme aux prescriptions du Tableau 1.

Tableau 1/Q.812 – Attributs de couche Transport
[pour emploi avec le service de réseau en mode sans connexion (CLNS)]

	valeur/gamme/option	**valeur par défaut**
Maximum d'unités TPDU (octets)	128, 256, 512, 1024 (2048, 4096, 8192 en option)	(128)
TSAP-ID (Note 1)	Jusqu'à 32 octets	–
Classe de service	4	–
Classe préférée	4	–
Autre classe possible	Aucun	–
Données exprès	Non-utilisation	–
Options:		
paramètres de sécurité	En option	–
numérotation des unités TPDU de données (Note 2)	Normale, étendue	(Normale)
total de contrôle (Note 3)	Utilisation, non-utilisation	(Non-utilisation)
Paramètres:		
T1 – Temps de retransmission	0,25-64 secondes (Note 4)	(8)
N – Retransmissions	2-15	(2)
L – Référence liée	1-256 secondes	(32)
I – Temps d'inactivité	2-512 secondes	(64)

Tableau 1/Q.812 – Attributs de couche Transport
[pour emploi avec le service de réseau en mode sans connexion (CLNS)]

NOTE 1 – Certains systèmes peuvent avoir besoin d'identificateurs de point TSAP (TSAP-ID), mais tous auront la capacité de générer des TSAP-ID appelés dans des unités CR TPDU et de recevoir des TSAP-ID appelants et appelés dans les unités CR TPDU et CC TPDU, respectivement.

NOTE 2 – L'option de format étendu sera implémentée. La non-utilisation de cette option sera négociable. Dans la mesure du possible, l'appelé donnera suite à la requête de l'appelant. Les négociations relatives à des éléments autres que ceux demandés ne pourront se faire que dans des conditions anormales, par exemple en cas de fort encombrement, dans les limites fixées par le réalisateur. Les appelants seront prêts à fonctionner dans le mode confirmé par l'appelé.

NOTE 3 –Pour les unités CR TPDU, il faut utiliser le total de contrôle. Une prescription additionnelle est que toutes les implémentations prennent en charge la "non-utilisation" négociée du total de contrôle. Les appelants demanderont et les appelés accepteront la "non-utilisation" du total de contrôle.

NOTE 4 – La valeur du temporisateur T1 de la couche Transport doit toujours être supérieure à celle du temporisateur T1 de la couche Liaison.

6.1.2 Profil de la couche Transport pour les services CONS1, CONS2, CONS3 et CONS5

Le présent paragraphe définit le profil de la couche Transport à utiliser avec les services à utiliser avec les services CONS1, CONS2, CONS3, CONS4 et CONS5 définis dans la Rec. UIT-T Q.811 [45].

6.1.2.1 Profil des services

Les profils de protocole décrits dans la présente Recommandation assurent le service de transport en mode connexion (COTS, *connection-mode transport service*) aux couches supérieures de l'OSI défini dans la Rec. UIT-T X.214 | ISO/CEI 8072 [41].

6.1.2.1.1 Interruptions

Les appelés peuvent refuser les connections du réseau qui pourraient restreindre inutilement la capacité d'établir des connexions sortantes. Pour empêcher les tentatives infructueuses pendant les interruptions, les appelants éviteront de demander immédiatement des connexions de réseau additionnelles après qu'une connexion de réseau ait été refusée. Le temps qu'il convient d'attendre avant de demander de nouvelles connexions de réseau nécessite un compléments d'étude.

6.1.2.1.2 Négociation de la qualité de service

La négociation de la qualité de service ne fait pas partie du domaine de la présente Recommandation. Si la négociation de la qualité de service n'est pas prise en charge, la réception des paramètres "débit", "taux d'erreurs résiduelles ", "priorité" et "temps de transit " dans les demandes CR et les confirmations CC TPDU devront être ignorés.

6.1.2.1.3 Négociation de la taille des unités TPDU

On obtient l'interopérabilité en faisant en sorte que l'appelant propose une taille d'unité TPDU de l'ensemble spécifié dans le Tableau 2 et que l'appelé sélectionne la taille d'unité TPDU la plus appropriée entre 128 et la taille proposée. Les règles à respecter pour la négociation de la taille de l'unité TPDU dans une instance donnée de communication sont spécifiées dans la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

Le choix de la taille de l'unité TPDU est une question d'implémentation locale.

6.1.2.1.4 Négociation de la protection

La négociation de la protection ne fait pas partie du domaine de la présente Recommandation. Si elle n'est pas prise en charge, la réception des paramètres de protection dans toute CR TPDU ou CC TPDU sera ignorée.

6.1.2.2 Profil de protocole

Pour le service réseau en mode connexion, le protocole de transport sera obligatoirement conforme à la Rec. UIT-T X.224 | ISO/CEI 8073 [4] s'appliquant à l'utilisation du service de couche réseau en mode connexion (CONS, *connection-mode network layer service*).

6.1.2.2.1 Classe de service

Comme le montre le Tableau 2, les Classes 4, 2 et 0 seront prises en charge dans les pays nécessitant les caractéristiques de la couche Transport de Classe 4. En cas de spécification de celle-ci, les règles de conformité de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] requièrent la prise en charge simultanée des Classes 0 et 2. Pour les équipements existants et dans les pays qui ne requièrent pas la Classe 4, la prise en charge de la Classe 0 est obligatoire et celle de la Classe 2 est facultative.

Les valeurs par défaut feront partie de l'offre par défaut du fournisseur. Autrement dit, sauf spécification autre par l'utilisateur, les paramètres par défaut seront les valeurs fournies initialement. Elles peuvent être modifiées ultérieurement par l'utilisateur à l'intérieur de la plage spécifiée.

En plus des critères spécifiés dans la Rec. UIT-T X.224 | ISO/CEI 8073 [4], l'équipement doit satisfaire à la condition suivante: si l'appelé reçoit une classe autre que "aucune", il répondra au moyen de la classe préférée. Les règles s'appliquant aux appelés sont spécifiées dans le Tableau 3.

Des options de l'utilisateur seront proposées pour désigner les classes préférées et les classes de substitution (voir le Tableau 3/X.224 | ISO/CEI 8073 [4]). Lorsque toutes les classes sont prises en charge, la classe préférée pour la connexion est la Classe 4.

Tableau 2/Q.812 – Attributs de la couche Transport [pour le service de couche réseau en mode connexion (CONS)]

Attribut	Gamme	Par défaut
Maximum d'unités TPDU (octets)	128, 256, 512, 1024 (2048, 4096, 8192 en option)	(128)
Classe de service	4, 2, 0	
Class préférée	4, 2, 0	(4)
Autre classe possible	4, 2, 0, aucune	(Aucune)
Données exprès	Non-utilisation	
Options pour la Classe 4		
Numérotation des unités TPDU de données (Note 2)	Normale, étendue	(Normale)
Options pour la Classe 2		
Numérotation des unité TPDU de données (Note 2)	Normale, étendue	(Normale)
Contrôle du flux	Explicite	
Paramètres pour la Classe 4		
T1 – Temps de retransmission	0,25-64 secondes (Note 4)	(8)
N – Retransmissions	2 (autres valeurs: à étudier)	
L – Référence liée	1-256 secondes	(32)
I – Temps d'inactivité	2-512 secondes	(64)

Tableau 2/Q.812 – Attributs de la couche Transport
[pour le service de couche réseau en mode connexion (CONS)]

NOTE 1 – Certains systèmes peuvent avoir besoin d'identificateurs de point TSAP (TSAP-ID), mais tous auront la capacité de générer des TSAP-ID appelés dans des unités CR TPDU et de recevoir des TSAP-ID appelants et appelés dans les unités CR TPDU et CC TPDU, respectivement.

NOTE 2 – L'option de format étendu sera implémentée. La non-utilisation de cette option sera négociable. Dans la mesure du possible, l'appelé donnera suite à la requête de l'appelant. Les négociations relatives à des éléments autres que ceux demandés ne pourront se faire que dans des conditions anormales, par exemple en cas de fort encombrement, dans les limites fixées par le réalisateur. Les appelants seront prêts à fonctionner dans le mode confirmé par l'appelé.

NOTE 3 –Pour les unités CR TPDU, il faut utiliser le total de contrôle. Une prescription additionnelle est que toutes les implémentations prennent en charge la "non-utilisation" négociée du total de contrôle. Les appelants demanderont et les appelés accepteront la "non-utilisation" du total de contrôle.

NOTE 4 – La valeur du temporisateur T1 de la couche Transport doit toujours être supérieure à celle du temporisateur T1 de la couche Liaison.

Tableau 3/Q.812 – Réponse valable correspondant au classes préférées et autres classes possibles proposées dans l'unité CR TPDU

Classe préférée	Autre classe possible			
	0	**2**	**4**	**Aucun**
0	Pas valable	Pas valable	Pas valable	Classe 0
2	Classes 0 et 2	Classe 2	Pas valable	Classe 2
4	Classes 0, 2 et 4	Classe 2 ou 4	Classe 4	Classe 2 ou 4

6.1.2.2.2 Identification du protocole

On utilisera, pour identifier le protocole de la couche Transport, les procédures spécifiées dans l'Annexe B de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] ainsi que dans la Rec. UIT-T X.264 | ISO/CEI 11570. Il conviendra de respecter les conventions relatives à l'identification du protocole énoncées dans la Rec. UIT-T X.263 | ISO/CEI TR 9577. La sélection des codes qui ne sont pas spécifiés dans les normes mentionnées nécessite un complément d'étude. L'absence de données sur l'utilisateur dans un paquet de demande d'appel ou d'acceptation d'appel de la Rec. UIT-T X.25 et de l'ISO/CEI 8208 indique l'utilisation des procédures de la couche Transport de la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

6.1.2.2.3 Attributs

Les attributs de la couche Transport réservés aux services CONS sont résumés dans le Tableau 2. Le choix des valeurs proposées dans les gammes de valeurs requises et des valeurs en option dépend des caractéristiques des messages.

NOTE – La nécessité de prendre en charge des messages à priorité élevée qui requièrent un faible temps de transit sur une connexion de Transport donnée doit apparaître dans les paramètres de qualité de service indiqués à l'établissement de la connexion de Transport. Une entité de Transport correctement implémentée ne devrait pas multiplexer des messages à priorité élevée qui nécessitent un faible temps de transit si elle ne peut pas assurer la qualité de service voulue. Etant donné qu'il s'agit ici d'un détail d'implémentation, il ne fait pas l'objet d'une normalisation.

6.1.2.2.4 Données d'utilisateur dans les unités TPDU de demande de connexion et de confirmation de connexion

Les données d'utilisateur dans les unités TPDU de demande de connexion et de confirmation de connexion sont facultatives dans la Rec. UIT-T X.224 | ISO/CEI 8073 [4]. Aucun utilisateur du service de Transport ne les enverra; toutes les implémentations de protocole seront prêtes à les recevoir et toutes peuvent les ignorer, autrement dit ne causeront pas de déconnexion.

6.1.2.2.5 Unité TPDU d'erreur de Classe 0

Lorsque c'est la classe de Transport 0 qui a été négociée, on peut utiliser la TPDU d'erreur (ER-TPDU, *error transport protocol data unit*) à tout moment, et à sa réception elle requiert que le destinataire déconnecte la connexion de réseau et, par voie de conséquence, la connexion de Transport.

6.1.2.2.6 Paramètres de CR TPDU inconnus

Un paramètres inconnu dans une unité CR TPDU reçue sera ignoré.

Quand toutes les classes sont prises en charge, la classe préférée sera, au lancement d'une unité CR TPDU, la Classe 4.

Si un appelé reçoit une classe autre que "aucune", la négociation implicite est appliquée.

6.1.2.2.7 Valeurs non valables d'unités CR TPDU connues

Les paramètres connus ayant la longueur voulue mais une valeur non valable dans une unité CR TPDU seront traités comme indiqué dans le Tableau 4.

Tableau 4/Q.812 – Paramètres d'unité TPDU

Paramètre	Action
TSAP-ID	Envoyer DR TPDU
Taille d'unité TPDU	Ignorer le paramètre, utiliser valeur par défaut
Version	Ignorer le paramètre, utiliser la valeur par défaut
Total de contrôle	Ignorer la CR TPDU
Autres classes de protocole possibles	Erreur de protocole

6.1.2.2.8 Paramètres d'options additionnelles

Les bits non reconnus ou non applicables des "options additionnelles " seront ignorés.

6.1.2.2.9 Sous-protocole de gestion de connexion de réseau (NCMS, *network connection management subprotocol*)

L'emploi du NCMS spécifié dans l'Annexe B de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] est facultatif. Les implémentations qui prennent en charge le NCMS auront la capacité de communiquer avec celles qui ne le font pas.

6.1.3 Profil TP0/TCP/IP de l'ISO destiné au service IP

Le présent paragraphe définit le profil de transport à adopter avec le paradigme de l'OSI en cas d'utilisation du service IP de couche inférieure défini dans la Rec. UIT-T Q.811 [45].

– Pour le haut de la couche 4 – Norme STD0035 "ISO Transport Service on top of the TCP (Version 3)" mars 1997. (Inclut RFC 2126). Ce document définit comment fournir le TP0, ISO Transport Services au moyen du protocole TCP.

– Pour le bas de la couche 4 – Norme STD0007 "Transmission Control Protocol", septembre 1981. (Inclut RFC 793.)

Il convient de noter que la Norme STD0035 (RFC 2126) implémente le protocole ISO TP0 avec le protocole TCP/IP et non avec le protocole de réseau ISO/UIT-T. Etant donné que le protocole de classe 0 de Transport s'utilise sur la connexion TCP/IP, il assure la même fonction que la classe 4 de Transport. Dès lors, les couches ISO/UIT-T de niveau supérieur (toutes des entités de session, de présentation et d'application) peuvent fonctionner normalement sans se rendre compte qu'elles fonctionnent sur un protocole TCP/IP interréseau.

6.2 Couche Session

6.2.1 Définition du service

La couche Session est conforme à la définition du service de la Rec. UIT-T X.215 | ISO/CEI 8326.

Les valeurs par défaut doivent faire partie de l'offre du fournisseur. Autrement dit, à moins qu'il ne soit spécifié autrement par l'utilisateur, les paramètres par défaut seront les valeurs initialement fournies. Ces valeurs pourront être ultérieurement modifiées par l'utilisateur dans les limites de la gamme de valeurs spécifiées.

Il existe un désaccord entre l'ISO et l'UIT-T en ce qui concerne les valeurs de code pour la confirmation des numéros subséquents et de la commande de flux. Le problème devrait être résolu conformément aux dispositions de la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

6.2.1.1 Unités fonctionnelles

Deux unités fonctionnelles (FU, *functional unit*) de couche Session sont nécessaires dans la présente Recommandation:

1) noyau;

2) duplex.

6.2.2 Spécification du protocole

La couche Session sera conforme à la définition de protocole contenue dans la Rec. UIT-T X.225 | ISO/CEI 8327-1 [5]. Les options et valeurs de paramètre spécifiques qui seront prises en charge pour l'application de gestion des systèmes de télécommunication sont définies dans l'ISP 11183-1 de l'ISO/CEI [6].

6.2.2.1 Données d'utilisateur

La longueur maximale des données d'utilisateur de la session sera de 10 240 octets. Cette restriction sous-entend que les unités SPDU d'acceptation de débordement et de débordement de données de connexion ne doivent pas être prises en charge. Les valeurs du paramètre "sélecteur de session" auront une longueur maximale de 16 octets.

6.3 Couche Présentation

6.3.1 Définition du service

La couche Présentation doit obligatoirement être conforme aux services spécifiés dans la Rec. UIT-T X.216 | ISO/CEI 8822 [7].

6.3.1.1 Unités fonctionnelles

Une unité fonctionnelle (FU) de couche Présentation est nécessaire dans la présente Recommandation:

– noyau.

6.3.2 Spécification du protocole

La couche Présentation doit obligatoirement être conforme aux protocoles spécifiés dans la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (mode normal). Les options et valeurs de paramètre spécifiques qui seront prises en charge pour l'application de gestion des systèmes de télécommunication sont définies dans l'ISO/CEI ISP 11183-1 [6].

6.3.3 Règles de codage pour la syntaxe de transfert

Les règles de codage définies dans la Rec. UIT-T X.209 | ISO/CEI 8825 [9] seront appliquées pour établir la syntaxe de transfert pour les unités de données protocolaire d'application (APDU, *application protocol data unit*). L'IDENTIFICATEUR D'OBJET [joint-iso-itu-t asn1 (1) basic-encoding (1)] ASN.1 [10] à [13] sera utilisé comme valeur pour le nom de syntaxe de transfert. La valeur maximale d'une étiquette de codage de base ASN.1 devant être traitée aux fins de conformité avec la présente Recommandation est de 16 383. Il s'agit du nombre entier sans signe le plus grand qui puisse être représenté par 14 bits. De ce fait, les octets de l'identificateur se composeront d'un octet initial suivi de deux octets au maximum, occupant ainsi un nombre maximal de trois octets. De même, le nombre d'octets le plus grand de la composante "octets de contenu" du codage de valeur de données ASN.1 devant être traité aux fins de conformité avec la présente Recommandation est 4 294 967 295. Il s'agit du nombre entier sans signe le plus grand qui puisse être représenté par 32 bits. Ainsi, dans le codage "de forme longue", les octets de longueur se composeront d'un octet initial suivi de quatre autres octets au maximum et occuperont un nombre maximal de cinq octets (à noter que cette restriction ne s'applique pas au codage de "longueur non définie").

6.4 Couche Application

La présentation de l'unité de données protocolaire de la couche Application est décrite au moyen de la notation de syntaxe abstraite numéro un (ASN.1) selon la définition de la Rec. UIT-T X.208 | ISO/CEI 8824 [14].

6.4.1 Architecture de la couche Application

La couche Application doit obligatoirement être conforme à l'architecture de la couche Application décrite dans l'ISO/CEI 9545 [15].

Les concepts d'entité d'application (AE, *application entity*), d'invocation d'entité d'application, d'objet de service d'application (ASO, *application service object*), de fonction de commande (CF, *control function*) et de contexte d'application serviront à décrire les relations entre les éléments ROSE, ACSE, CMISE et SMASE.

6.4.2 Elément de service de contrôle d'association

6.4.2.1 Définition du service

La description du service ACSE est donnée en détail dans la Rec. UIT-T X.217 | ISO/CEI 8649 [16]. Tous les services ACSE définis (voir Tableau 5) sont obligatoires. La valeur du paramètre de mode A-ASSOCIATE sera "normale".

6.4.2.2 Spécification du protocole

La spécification du protocole pour l'ACSE sera conforme à la Rec. UIT-T X.227 | ISO/CEI 8650-1 [17]. Les cinq unités APDU (voir Tableau 5) spécifiées dans la norme sont obligatoires. Les options spécifiques et les valeurs de paramètre qui seront prises en charge pour l'application de gestion des systèmes de télécommunication de classe interactive sont définies dans l'ISO/CEI ISP 11183-1 [6].

Tableau 5/Q.812 – Services ACSE et unités APDU associées

Service ACSE	APDU associées	Service-P connexe
A-ASSOCIATE	AARQ, AARE	P-CONNECT
A-RELEASE	RLRQ, RLRE	P-RELEASE
A-ABORT	ABRT	P-U-ABORT
A-P-ABORT	(Aucune)	P-P-ABORT

6.4.2.3 Utilisation de la fonction SACF pour le contrôle d'association

La fonction CF sert à contrôler les interactions entre éléments ASE et/ou objet ASO dans l'ASO contenant défini dans l'ISO/CEI 9545 [15] avec le projet de modification DAM 1.

De ce fait, elle commande l'établissement de l'association, sa libération et son interruption dans le cadre des règles définies dans le contexte d'application disponible pour l'association.

Elle permet donc l'utilisation conjointe de plusieurs éléments ASE dans la même association.

6.4.2.4 Nom de syntaxe abstraite

Le nom de syntaxe abstraite d'élément ACSE a l'IDENTIFICATEUR D'OBJET du type ASN.1. La valeur suivante sera utilisée pour identifier la définition de syntaxe abstraite d'élément ACSE:

```
{
joint-iso-itu-t association-control (2)
abstract-syntax (1) apdu's (0) version (1)

}
```

6.4.3 Opérations distantes

6.4.3.1 Définition du service

L'élément de service d'opérations distantes (ROSE, *remote operations service element*) sera un élément de service obligatoire. La description du service ROSE est donnée en détail dans la Rec. UIT-T X.219 | ISO/CEI 9072-1 [18]. Tous les services ROSE définis (voir Tableau 6) sont obligatoires.

6.4.3.2 Spécification du protocole

La spécification du protocole pour le service ROSE sera conforme à la Rec. UIT-T X.229 | ISO/CEI 9072-2 [19]. Les quatre unités APDU spécifiées dans la norme (voir Tableau 6) sont obligatoires. De plus, l'aptitude à accepter une source et une réception correctes de l'élément de protocole identificateur de lien est nécessaire.

La condition spécifiée dans le Tableau 6 sous-entend la Classe d'association 3 dans le service ROSE.

Tableau 6/Q.812 – Services ROSE et unités APDU associées

Service ROSE	APDU associées	Service connexe sous-jacent
RO-INVOKE	ROIV	P-DATA
RO-RESULT	RORS	P-DATA
RO-ERROR	RORE	P-DATA
RO-REJECT-U	RORJ	P-DATA
RO-REJECT-P	RORJ	P-DATA

6.4.4 Information de gestion commune

Les applications de gestion de réseau doivent utiliser l'élément de service commun des informations de gestion (CMISE, *common management information service element*).

6.4.4.1 Définition du service

La description du service CMISE est donnée en détail dans la Rec. UIT-T X.710 | ISO/CEI 9595 [20]. Les services CMISE sont énumérés dans le Tableau 7.

Les unités fonctionnelles sélection d'objets multiples, filtre, réponse multiple et obtention d'annulation, définies dans la Rec. UIT-T X.710 | ISO/CEI 9595 [20] sont facultatives. Leur utilisation dépend de l'application. Pendant l'établissement de l'association, la négociation sur leur utilisation ou leur non-utilisation sera acceptée.

La prise en charge de l'unité fonctionnelle de service élargi définie dans la Rec. UIT-T X.710 | ISO/CEI 9595 [20] n'est pas nécessaire pour la conformité avec la présente Recommandation et la négociation de sa non-utilisation au moment de l'établissement de l'association sera acceptée.

Tableau 7/Q.812 – Services CMISE

Service	Type
M-EVENT-REPORT	Confirmé/non confirmé
M-GET	Confirmé
M-SET	Confirmé/non confirmé
M-ACTION	Confirmé/non confirmé
M-CREATE	Confirmé
M-DELETE	Confirmé
M-CANCEL-GET	Confirmé

6.4.4.2 Spécification du protocole

Les opérations définies dans la Rec. UIT-T X.711 | ISO/CEI 9596-1 [21], nécessaires pour des applications spécifiques, seront prises en charge lors de la mise en œuvre. Tous les paramètres obligatoires définis dans la Rec. UIT-T X.711 | ISO/CEI 9596-1 [21] pour les opérations requises sont des paramètres obligatoires dans le cadre de la présente Recommandation. Les options spécifiques et les valeurs de paramètre qui seront prises en charge sont définies dans l'ISO/CEI ISP 11183-3 [22] pour la gestion de base des systèmes de télécommunication ainsi que dans l'ISO/CEI ISP 11183-2 [23] pour la gestion améliorée des systèmes de télécommunication.

6.4.4.3 Syntaxe abstraite

Le nom de syntaxe abstraite pour CMISE est {joint-iso-ccitt ms(9) cmip(1) abstract syntax(4)}

6.5 Prise en charge de la sécurité pour des applications interactives

La prise en charge des services d'authentification et de sécurité du contrôle d'accès est obligatoire pour l'interface X; elle est facultative pour l'interface Q. Le service d'authentification sera pris en charge au moyen de l'unité fonctionnelle d'authentification spécifiée dans l'élément ACSE. Le choix du ou des mécanismes utilisés pour l'interface X nécessite un complément d'étude.

Le service du contrôle d'accès sera pris en charge au moyen du paramètre de contrôle d'accès défini dans les opérations CMIP. La syntaxe de ce paramètre dépend de mécanismes spécifiques et nécessite un complément d'étude. Lorsque des mécanismes spécifiques seront définis, une syntaxe abstraite supplémentaire définissant la syntaxe du contrôle d'accès sera incluse dans l'ensemble des contextes définis (DCS, *definition context text*) pour le protocole de présentation.

7 Spécification des protocoles de couche supérieure pour les fonctions de classe orientée fichier utilisant le paradigme de l'OSI

Les profils pour chaque couche sont les mêmes que ceux décrits dans le § 6; le présent paragraphe ne fait que documenter les différences nécessaires pour la prise en charge de la gestion FTAM.

7.1 Couche Session

7.1.1 Profil du service

7.1.1.1 Unités fonctionnelles

Quatre unités fonctionnelles (FU) de la couche Session sont nécessaires dans la présente Recommandation:

1) noyau;
2) duplex;
3) synchronisation mineure;
4) resynchronisation.

7.1.2 Profil du protocole

Les options spécifiques et les valeurs de paramètre qui seront prises en charge par le service de transfert de fichier sont spécifiées dans l'ISO/CEI ISP 10607-1 [24].

7.2 Couche Présentation

7.2.1 Définition du service

La couche Présentation doit obligatoirement être conforme aux services définis dans la Rec. UIT-T X.216 | ISO/CEI 8822 [7].

7.2.1.1 Unités fonctionnelles

Une unité fonctionnelle (FU) de couche Présentation est nécessaire dans la présente Recommandation:

– noyau.

7.2.2 Spécification du protocole

La couche Présentation doit obligatoirement être conforme aux protocoles spécifiés dans la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (mode normal). Les options spécifiques et les valeurs de paramètre qui seront prises en charge pour l'application de gestion des systèmes de télécommunication sont définies dans l'ISO/CEI ISP 11183-1 [6].

7.2.3 Règles de codage pour la syntaxe de transfert

Les règles de codage définies dans la Rec. UIT-T X.209 | ISO/CEI 8825 [9] seront appliquées pour établir la syntaxe de transfert pour les unités de données protocolaire d'application (APDU). L'IDENTIFICATEUR D'OBJET [joint-iso-itu-t asn1 (1) basic-encoding (1)] ASN.1 sera utilisé comme valeur pour le nom de syntaxe de transfert. La valeur maximale d'une étiquette de codage de base ASN.1 devant être traitée aux fins de conformité avec la présente Recommandation est de 16 383. Il s'agit du nombre entier sans signe le plus grand qui puisse être représenté par 14 bits. De ce fait, les octets de l'identificateur se composeront d'un octet initial suivi de deux octets au maximum, occupant ainsi un nombre maximal de trois octets. De même, le nombre d'octets le plus grand de la composante "octets de contenu" du codage de valeur de données ASN.1 devant être traité aux fins de conformité avec la présente Recommandation est 4 294 967 295. Il s'agit du nombre entier non signé le plus grand qui puisse être représenté par 32 bits. Ainsi, dans le codage "de forme longue", les octets de longueur se composeront d'un octet initial suivi de

quatre autres octets au maximum et occuperont un nombre maximal de cinq octets. (A noter que cette restriction ne s'applique pas au codage de "longueur non définie".)

7.3 Profil de la couche Application

7.3.1 Architecture de la couche Application

La description de l'élément ACSE et du service FTAM dans le cadre de l'architecture de la couche Application reste à établir.

7.3.2 Transfert, accès et gestion de fichiers

7.3.2.1 Profil du service

La classe de service de fichier obligatoire est la classe transfert de fichier.

Dans cette classe, les unités fonctionnelles suivantes sont obligatoires:

– noyau;
– lecture et écriture;
– gestion de fichier limitée;
– groupement;
– et, dans le service de fichier interne, récupération et facultativement réinitialisation.

7.3.2.2 Profil du protocole

Les unités fonctionnelles du protocole de fichier sont équivalentes aux unités fonctionnelles du service pris en charge décrit ci-dessus.

Les unités fonctionnelles conservées et les unités PDU associées sont indiquées dans le Tableau 8.

Le présent fichier de protocole admet les services de session décrits au § 7.1.1.1 avec les détails suivants:

– l'unité fonctionnelle de récupération ou de réinitialisation sous-entend l'utilisation du service de session synchronisation mineure;
– l'unité fonctionnelle de réinitialisation sous-entend l'adjonction du service de session resynchronisation au service de session synchronisation mineure.

Tableau 8/Q.812 – Unités fonctionnelles FTAM et unités PDU associées

Nom	Unité fonctionnelles
demande F-INITIALIZE	Noyau
réponse F-INITIALIZE	Noyau
demande F-TERMINATE	Noyau
réponse F-TERMINATE	Noyau
demande F-P-ABORT	Noyau
demande F-U-ABORT	Noyau
demande F-SELECT	Noyau
réponse F-SELECT	Noyau
demande F-DESELECT	Noyau
réponse F-DESELECT	Noyau
demande F-CREATE	Gestion de fichier limitée
réponse F-CREATE	Gestion de fichier limitée
demande F-DELETE	Gestion de fichier limitée
réponse F-DELETE	Gestion de fichier limitée
demande F-READ-ATTRIB	Gestion de fichier limitée
réponse F-READ-ATTRIB	Gestion de fichier limitée

Tableau 8/Q.812 – Unités fonctionnelles FTAM et unités PDU associées

Nom	Unité fonctionnelles
demande F-OPEN	Lecture, écriture
réponse F-OPEN	Lecture, écriture
demande F-CLOSE	Lecture, écriture
réponse F-CLOSE	Lecture, écriture
demande F-READ	Lecture
demande F-WRITE	écriture
demande F-DATA-END	Lecture, écriture
demande F-TRANSFER-END	Lecture, écriture
réponse F-TRANSFER-END	Lecture, écriture
demande F-CANCEL	Lecture, écriture
réponse F-CANCEL	Lecture, écriture
demande F-BEGIN-GROUP	groupement
réponse F-BEGIN-GROUP	groupement
demande F-END-GROUP	groupement
réponse F-END-GROUP	groupement
demande F-RECOVER	Reprise
réponse F-RECOVER	Reprise
demande F-RESTART	Réinitialisation
réponse F-RESTART	Réinitialisation

7.3.2.3 Syntaxe abstraite

Les noms de syntaxe abstraite pour le service FTAM sont les suivants:

{iso standard 8571 abstract syntax(2) ftam-fadu(2)}

{iso standard 8571 abstract syntax(2) ftam-pci(1)}

{iso standard 8571 abstract syntax(2) unstructured-text(3)}

{iso standard 8571 abstract syntax(2) unstructured-binary(4)}

7.3.2.4 Prise en charge de types de documents

La nature de la structure des fichiers à transférer sous-entend l'utilisation de types de documents appropriés.

Trois types de structures de fichiers sont retenus:

– dossiers binaires non structurés;

– dossiers texte non structurés;

– dossiers à ordonnancement séquentiel (ils sont constitués d'une séquence de dossiers sans possibilité d'accès direct à un dossier donné, chaque dossier se composant de domaines de types différents).

En conséquence, trois types de documents au moins sont nécessaires:

– texte ISO FTAM non structuré (FTAM.1);

– ISO FTAM binaire non structuré (FTAM.3);

– fichier séquentiel NBS (NBS-6).

Les types FTAM.1 et FTAM.3 sont autorisés par le modèle de fichier hiérarchique FTAM défini dans l'ISO 8571-2 [26] comme étant limité par l'ensemble de restrictions non structurées.

Le type NBS-6 est autorisé par le modèle de fichier hiérarchique FTAM défini dans l'ISO 8571-2 [26] comme étant limité par l'ensemble de restrictions séquentielles uniformes.

7.4 Prise en charge de la sécurité pour les services FTAM

La prise en charge du service d'authentification est obligatoire pour l'interface X; elle est facultative pour l'interface Q. Le service d'authentification sera pris en charge au moyen de l'unité fonctionnelle d'authentification spécifiée dans l'élément ACSE. Le choix du ou des mécanismes utilisés pour l'interface X nécessite un complément d'étude.

La prise en charge de la sécurité pour les services FTAM dans le RGT nécessite un complément d'étude.

8 Spécifications du protocole de couche supérieure pour les services d'annuaire utilisant le paradigme de l'OSI

Les profils pour chaque couche sont les mêmes que ceux décrits au § 6. Ce paragraphe énumère seulement les différences requises pour la prise en charge de l'annuaire.

8.1 Couche Session

8.1.1 Définition du service

La couche Session est conforme à la définition du service de la Rec. UIT-T X.215 | ISO/CEI 8326.

8.1.1.1 Unités fonctionnelles

Deux unités fonctionnelles (FU) de couche Session sont nécessaires dans la présente Recommandation:

a) noyau;

b) duplex.

8.1.2 Spécification du protocole

Le protocole de la couche Session sera conforme à la définition de protocole contenue dans la Rec. UIT-T X.225 | ISO/CEI 8327-1 [5].

8.1.3 Données d'utilisateur

Les agents d'utilisateur d'annuaire (DUA) pourront envoyer des unités APDU de demande ayant une longueur de 32 767 (32k – 1) octets au maximum. Ces agents DSA seront capables d'accepter et de traiter des unités APDU de demande ayant une longueur de fonctionnement de 32 767 octets au maximum. Ils pourront envoyer des unités APDU de réponse ayant une longueur de 262 143 (256k – 1) octets au maximum. Ils auront la possibilité d'accepter et de traiter des unités APDU de réponse ayant une longueur de 262 143 octets au maximum et pourront envoyer des unités APDU de demande ayant une longueur de 32 767 octets au maximum.

8.2 Couche Présentation

8.2.1 Définition du service

La Rec. UIT-T X.216 | ISO/CEI 8822 [7] définissent le service de présentation.

L'élément ACSE est l'utilisateur exclusif des services P-CONNECT, P-RELEASE, P-U-ABORT et P-P-ABORT du service de présentation.

L'élément ROSE est l'utilisateur exclusif du service P-DATA du service de présentation.

Le contexte par défaut de présentation, le rétablissement de contexte et la gestion de contexte ne sont pas utilisés.

8.2.2 Spécification du protocole

La couche Présentation sera conforme aux protocoles spécifiés dans la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (mode normal).

8.3 Couche Application

8.3.1 Architecture de la couche Application

La couche Application doit obligatoirement être conforme à l'architecture de la couche Application décrite dans les Recommandations UIT-T de la série X.500.x | ISO/CEI 9594 [29] à [36].

8.3.2 Syntaxes abstraites du protocole d'annuaire

Le type ASN.1 dont les valeurs des syntaxes abstraites sont dérivées est spécifié au moyen de types paramétrés d'opérations ROS {DAP-InvokeIDSet | DAP-Invokable | DAP-Returnable | DSP-InvokeIDSet | DSP-Invokable | DSP-Returnable}, d'opérations Bind {dSABind | directoryBind} et d'opérations Unbind{dSAUnbind | directoryUnbind} définis dans la Rec. UIT-T X.880 | ISO/CEI 13712-1 [37].

La syntaxe abstraite du protocole DAP est appelée directoryAccessAbstractSyntax et celle du protocole DSP directorySystemAbstractSyntax.

8.3.3 Contextes d'application d'annuaire

Le contexte d'application du protocole DAP est appelé directoryAccessAC et celui du protocole DSP directorySystemAC.

8.3.4 Elément de service de contrôle d'association

La syntaxe abstraite de l'élément de service de contrôle d'association (ACSE), acse-abstract-syntax, est nécessaire pour les protocoles DAP et DSP.

L'élément ACSE prend en charge l'établissement, la libération et l'interruption d'une association d'application entre une paire d'entités d'application. Les associations entre un agent DUA et un agent DSA peuvent être établies uniquement par un agent DUA. Seul l'initiateur de l'association établie peut la libérer.

8.3.4.1 Définition du service

La description du service d'élément ACSE est donnée en détail dans la Rec. UIT-T X.217 | ISO/CEI 8649 [16].

Les services RO-BIND et RO-UNBIND sont les utilisateurs exclusifs des services A-ASSOCIATE et A-RELEASE de l'élément ACSE. Le processus d'application est l'utilisateur des services A-ABORT et A-P-ABORT de l'élément ACSE.

8.3.4.2 Spécification du protocole

La spécification du protocole pour l'élément ACSE sera conforme à la Rec. UIT-T X.227 | ISO/CEI 8650-1 [17].

8.3.5 Opérations distantes

8.3.5.1 Définition du service

L'élément de service d'opérations distantes (ROSE) sera obligatoire. La description du service ROSE est donnée en détail dans la Rec. UIT-T X.881 | ISO/CEI 13712-2 [38].

Les éléments ASE d'annuaire sont les utilisateurs des services RO-INVOKE, RO-RESULT, RO-ERROR, RO-REJECT-U, et RO-REJECT-P de l'élément ROSE.

8.3.5.2 Spécification du protocole

Le protocole d'accès à l'annuaire (DAP, *directory access protocol*) et le protocole du système d'annuaire (DSP, *directory system protocol*) sont utilisés pour établir les communications entre une paire de processus d'application.

8.4 Prise en charge de la sécurité pour les services d'annuaire

La Rec. UIT-T X.509 | ISO/CEI 9594-8 [36] définit un cadre pour la fourniture des services d'authentification à ses utilisateurs par le biais de l'annuaire. La prise en charge de la sécurité pour les services d'annuaire dans le RGT nécessite un complément d'étude.

Les protocoles de couche supérieure à utiliser pour les services d'enregistrement et retransmission (par exemple, pour l'échange d'information au format EDI) nécessitent un complément d'étude.

La présente Recommandation spécifie une prise en charge partielle des prescriptions de sécurité de part et d'autre des interfaces Q et X. L'utilisation des Recommandations de la série X.830 (sécurité générique des couches supérieures) sera nécessaire pour prendre en charge les services de sécurité tels que l'intégrité des données, la confidentialité, la non-répudiation et la gestion de l'information de sécurité (telles que les procédures et les protocoles de gestion de clés). Les lignes directrices pour l'utilisation de la sécurité GULS dans les applications sont spécifiées dans l'Annexe A/X.830 | ISO/CEI 11586-1 [39]. Les modalités d'utilisation de la sécurité GULS à la fois dans les classes de transfert de fichier et interactives des applications du RGT nécessitent un complément d'étude.

9 Conformité pour le paradigme de l'OSI

Les prescriptions applicables aux éléments qui ne sont pas spécifiquement cités dans la présente Recommandation seront conformes aux profils ISP identifiés ci-dessous:

– Transport:
  - pour le service CLNS1 (voir Rec. UIT-T Q.811 [45]), la couche Transport sera conforme aux prescriptions "Subnetwork Type Independent requirements" de l'ISO/CEI ISP 10608-1 [60];
  - pour le service CLNS2 (voir Rec. UIT-T Q.811 [45]), la couche Transport sera conforme à l'ISO/CEI ISP 10608-1 [60];
  - pour le service CLNS3 (voir Rec. UIT-T Q.811 [45]), la couche Transport sera conforme aux prescriptions "Subnetwork Type Independent requirements" de l'ISO/CEI ISP 10608-1 [60];
  - pour le service CONS1 (voir Rec. UIT-T Q.811 [45], la couche Transport sera conforme à l'ISO/CEI ISP 10609-1 [61] telle que modifiée par le Tableau II.1;
  - pour le service CONS6, la couche Transport sera conforme à l'ISO/CEI ISP 10609-1 [61];
  - pour la pile ISO TP0/TCP/IP, la couche Transport sera conforme à la classe 0 de RFC 2126.
– les couches Session, Présentation et ACSE pour les services de classe interactive seront conformes au profil ISO/CEI ISP 11183-1 [6];
– les couches Session, Présentation et ACSE pour les services de classe orienté fichier seront conformes au profil ISO/CEI ISP 10607-1 [24];
– le protocole CMIP utilisé dans le profil des services de classe interactive sera conforme au profil ISO/CEI ISP 11183-3 [22] pour les services de base et au profil ISO/CEI ISP 11183-2 [23] pour les services améliorés. Les applications peuvent passer outre à la taille de 10K des unités APDU spécifiée dans AOM-12 si une taille plus importante est nécessaire;

– le profil FTAM correspondra à l'ISO/CEI ISP 10607-3 [40] "service de transfert simple de fichier".

10 Profil de protocole pour les services basés sur l'architecture CORBA

10.1 Domaine du profil du protocole CORBA

Les applications de RGT spécifiées utilisant le langage IDL auront un interfonctionnement conforme aux dispositions de ce profil de protocole CORBA.

10.2 Aperçu général des profils pour les services basés sur l'architecture CORBA

La Figure 4 montre la pile de protocoles pour le profil pour les services basés sur l'architecture CORBA.

Les services de RGT ayant des interfaces orientées objet spécifiées utilisant le langage IDL de l'ODP (Rec. UIT-T X.920) sont accessibles par l'utilisation de ce profil.

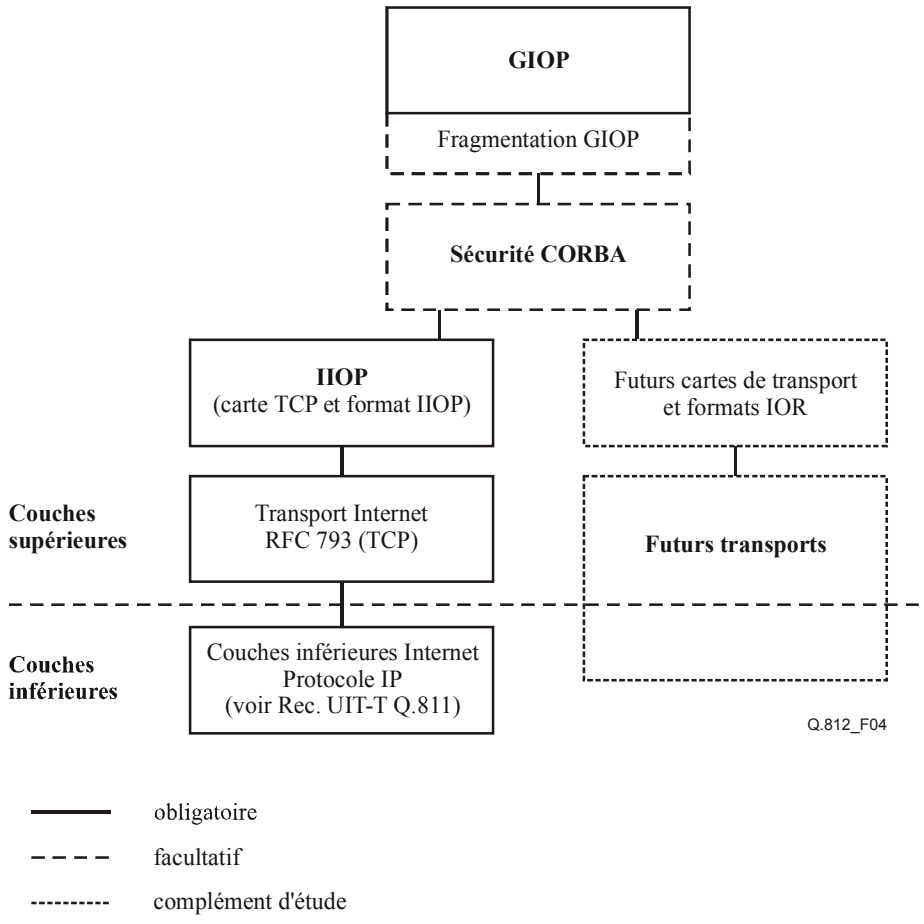

Figure 4/Q.812 – Pile de protocoles de services basés sur l'architecture CORBA de couche supérieure de protocole GIOP

Pour prendre en charge les niveaux CSI 1 et supérieurs il faut utiliser, dans ce profil, le protocole SECIOP. Pour prendre en charge le niveau CSI 0 on peut utiliser, dans ce profil, l'interopérabilité SSL de sécurité CORBA à la place du protocole SECIOP. Les systèmes qui prennent en charge la sécurité CORBA doivent aussi prendre en charge le format version 1.1 du profil IIOR.

Si la fragmentation de l'application est requise, il faut utiliser dans ce profil le protocole GIOP version 1.1 ou plus récente.

Le mappage du protocole GIOP sur des protocoles autres que le TCP nécessite un complément d'étude.

NOTE – Pour le mappage du protocole GIOP sur des profils de protocole, il faut spécifier un format de profil de référence d'objet interopérable (IOR, *interoperable object reference*), associé à ce profil de transport, ainsi que la spécification de la manière dont sont utilisés les services de liaison du profil de transport.

10.3 Définition du service

Les services utilisant l'architecture CORBA auront des interfaces orientées objet spécifiées au moyen du langage IDL du groupe OMG (Rec. UIT-T X.920).

NOTE – Les systèmes basés sur l'architecure CORBA peuvent utiliser des liaisons de langage de programmation courantes pour accéder aux objets CORBA.

10.4 Spécification du GIOP

Les versions 1.0, 1.1 et 1.2 du protocole GIOP seront mises en œuvre comme indiqué dans [CORBA GIOP Specification]. Tous les systèmes qui font fonction de serveurs CORBA prendront en charge au moins la version 1.0.

Les serveurs qui prennent en charge la version 1.1 ou 1.2 doivent aussi assurer le traitement de messages avec toutes les versions antérieures.

10.5 Spécification du protocole IOP sécurisé

Tous les systèmes qui nécessitent les services CORBA sécurisés doivent prendre en charge la version 1.1 ou plus récente du protocole GIOP.

Tous les systèmes qui nécessitent les services CORBA sécurisés prendront en charge le "Secure IOP protocol" ou la "CORBASecurity SSL Interoperability" définis dans [CORBA Security Service Specification].

10.6 Spécification du protocole IIOP

Pour les besoins d'interopérabilité, tous les systèmes CORBA prendront en charge le protocole de mappage IIOP du protocole GIOP sur les services TCP/IP des couches inférieures, comme indiqué dans la spécification [CORBA GIOP Specification].

Les serveurs annonceront qu'ils prennent en charge le protocole GIOP en publiant des IOR contenant un profil IOR Internet (IIOR) avec une version de profil de IIOP mise au niveau le plus élevé de la version du protocole GIOP pris en charge par le système faisant fonction de serveur. Le format du profil IIOR est celui indiqué dans [CORBA GIOP Specification].

10.7 Profil du protocole TCP/IP à utiliser avec le protocole IIOP

Le protocole IIOP est conçu pour être utilisé avec les protocoles axés sur les protocoles TCP/IP des couches inférieures.

Le présent paragraphe définit un profil de protocole à utiliser pour les protocoles des couches inférieures du RGT pour les systèmes axés CORBA utilisant le protocole IIOP. Ce profil est fondé sur l'utilisation des protocoles Internet définis par le groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*). La manière dont ces documents peuvent être utilisés dans la présente Recommandation nécessite un complément d'étude. La pile de protocoles utilise:

- pour la couche 4 – STD0007 "Transmission Control Protocol", septembre 1981. (Inclut RFC 793.)
- pour les couches 3 et au-dessous, on utilise le profil de protocole IP spécifié dans la Rec. UIT-T Q.811 [45].

Les autres mappages de procoles des couches inférieures pour le protocole GIOP nécessitent un complément d'étude.

11 Profil de protocole pour services axés sur la norme EDI/EDIFACT

11.1 Cadre du profil de protocole EDI/EDIFACT

Les applications de RGT qui ont des définitions d'interface X destinées à la couche de gestion du service auront la possibilité d'interfonctionner conformément aux dispositions de ce profil de protocole. La présente Recommandation définit le profil pour l'agent "The Electronic Communication Interactive Agent – IA" et couches de fonctionnalités associées. On trouvera le protocole pour l'agent IA proprement dit dans la Rec. UIT-T Q.814. L'interface IA entre homologues prendra en charge le transfert de données bidirectionnel en temps quasi-réel entre entités homologues.

Le profil global présenté dans le présent paragraphe est modélisé suivant le modèle d'interconnexion à sept couches des systèmes ouverts (OSI); ; autrement dit, les couches des profils décrits ici le sont en termes de couche Transport (4), de couche Session (5), de couche Présentation (6) et de couche Application (7).

L'agent IA décrit ici assure les services de la couche cinq (5). Les autres couches, soit quatre, six et sept, assurent des fonctions qui dialoguent directement ou indirectement avec l'agent IA. Le présent profil décrit l'interaction et les responsabilités de chacune de ces quatre couches.

11.2 Résumé

On se référera, dans l'examen ci-après, à la Figure 5.

11.3 Profil de protocole TCP/IP à utiliser avec l'agent IA

Par conception, l'agent IA doit être utilisé avec un protocole axé sur le TCP/IP des couches inférieures.

Le présent paragraphe définit un profil de protocole à utiliser comme protocoles de RGT des couches inférieures pour l'agent IA. Ce profil est fondé sur l'utilisation de protocoles Internet définis par l'IETF. La manière dont on peut se référer à ces documents peuvent être utilisés dans la présente Recommandation nécessite un complément d'étude. La pile de protocoles utilise:

- pour la couche 4 – STD0007 "Transmission Control Protocol", septembre 1981. (Inclut RFC 793.)
- pour les couches 3 et au-dessous, on utilise le profil de protocole IP spécifié dans la Rec. UIT-T Q.811 [45].

11.4 Profil de protocole TLS à utiliser avec l'agent IA

La couche quatre assure la sécurité de la couche Transport et des services de transport utilisant le protocole de commande de transmission (TCP) (voir ci-dessus).

Le mécanisme de transport spécifié par l'Agent interactif (IA, *interactive agent*) requiert une session TLS individuelle. Celle-ci peut soit être permanente, soit être enclenchée ou reprise pour chaque message individuel. La communication est essentiellement à sens unique, du client au serveur. Le message de situation de l'agent IA est un mécanisme qui permet à des entités homologues d'échanger des informations sur les erreurs et d'autres types d'information sur la commande de flux. Les entités homologues peuvent définir des codes de message spécifiques à l'extérieur du domaine de la présente Recommandation. Le profil TLS assure la sécurité de la prise de contact et du transfert entre entités TLS homologues. La session TLS assure aussi l'intégrité du flux de données, l'authentification des entités homologues et, facultativement, la confidentialité.

11.5 Profil de l'agent IA

L'agent IA assure la fonctionnalité de la couche Session. Il prend en charge les transactions d'échange électronique de données (EDIFACT/ASC X12 EDI/general string) entre entités homologues. Il prend aussi en charge cet échange au moyen de la sécurité de la couche Transport (TLS). Les fonctions de couche Session assurées par l'agent IA sont notamment l'établissement, la gestion et la fermeture des sessions de communication entre entités homologues. L'agent IA effectue aussi la conversion des noms des destinataires EDIFACT/ASC X12 EDI en adresses de réseau et gère la session TLS. A la fin d'une session, l'agent IA détermine s'il doit fermer la session ou la suspendre dans un état qui permet de la *reprendre*.

L'interface d'accord de service IA est définie à la frontière entre l'agent IA et son utilisateur direct.

Le protocole qui prend en charge l'échange de messages IA est appelé le protocole de transfert d'agent interactif (IATP); il est défini dans la Rec. UIT-T Q.814.

11.6 Module de sécurité pour le profil de protection complète du message

Cette fonctionnalité de module de sécurité est facultative en fonction des besoins de la transaction. Toutefois, s'il faut des services de sécurité de l'ensemble du message, il conviendra de suivre les procédures de la Rec. UIT-T Q.815. Les messages confidentiels sont transférés entre les modules de sécurité assurant tant la non-répudiation de l'origine et de la réception que l'intégrité du message.

Le module de sécurité génère/valide les champs de sécurité appropriés et effectue le codage/décodage nécessaire, respectivement selon qu'il envoie ou qu'il reçoit.

Le flux de messages entre le traducteur EDI et l'agent IA peut ou ne peut pas nécessiter des services de sécurité. Le cas dans lequel des éléments de sécurité sont appliqués sont montrés dans la Figure 5.

Le module de sécurité n'est pas sensible au contenu des messages du traducteur EDI et de l'agent IA.

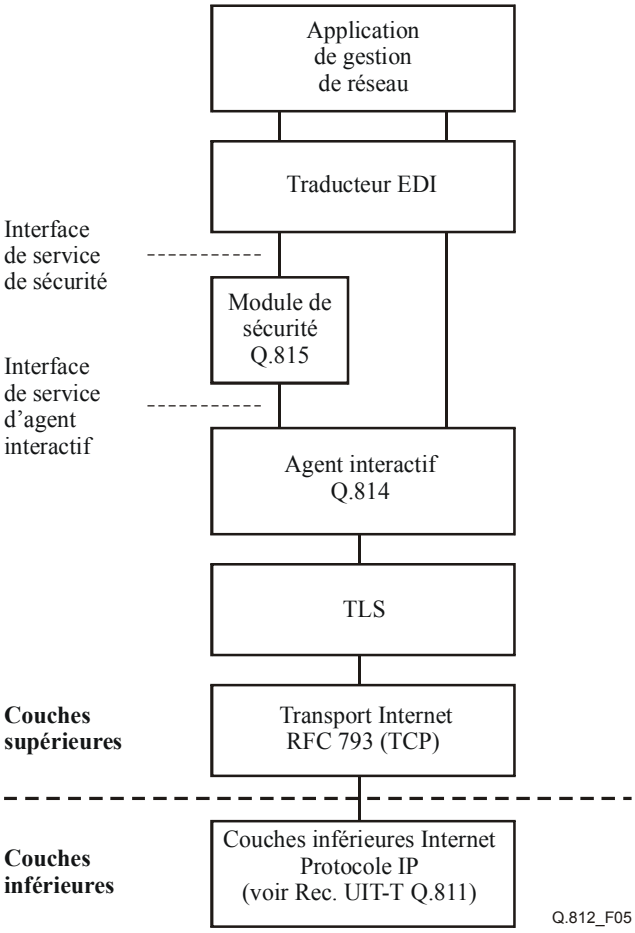

Figure 5/Q.812 – Pile de protocoles des services orientés EDI/EDIFACT de couche supérieure

11.7 Protocole du traducteur EDI/EDIFACT

Le protocole EDI/EDIFACT contient l'application d'utilisateur qui utilise les services de l'Agent IA et, facultativement, du module de sécurité.

Un traducteur/passerelle EDIFACT/ASC X12 EDI est un service d'application qui fournit une combinaison de traductions de formats de données et de fonctions d'échange de données pour les données de messages électroniques.

Un traducteur/passerelle EDIFACT/ASC X12 EDI échange des données de transactions vers et depuis des applications de gestion de réseau au moyen de formats de données intermédiaires. Il traduit ces données, au moyen de tables de correspondances, vers et depuis des formats de données EDIFACT/ASC X12 EDI.

12 Profil de protocole pour le paradigme SNMP

Le paradigme SNMP est représenté à la Figure 6. La version 3 du cadre de gestion Internet est décrit dans le document RFC 3410 de l'IETF. Ce cadre consiste en un langage de définition [57], de définitions des informations de gestion, d'une définition de protocole [54], de la sécurité [52] et [53] et de la gestion [51]. Le protocole est essentiellement utilisé avec le protocole UDP [55], mais peut aussi fonctionner avec le protocole TCP [58]. La coexistence avec des versions antérieures du protocole SNMP est décrite en [56].

En cas d'utilisation du protocole SNMP, c'est la version 3 qui est préférée. Les versions antérieures du cadre de gestion de l' Internet peuvent être sécurisées au moyen de la sécurité IPSec [59].

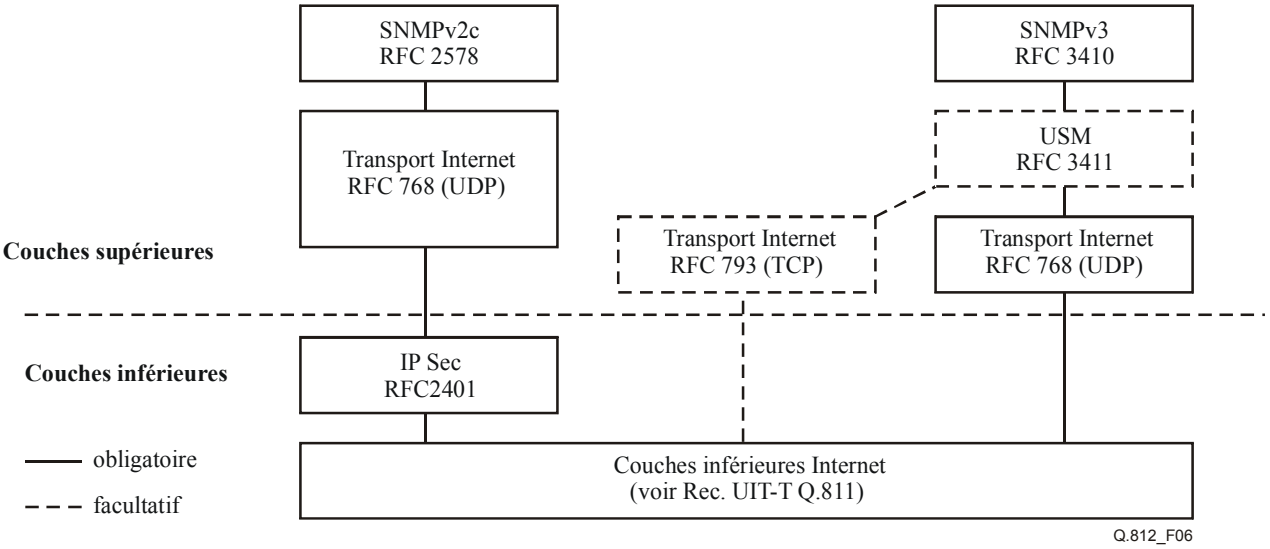

Figure 6/Q.812 – Profil de protocole pour le paradigme SNMP

13 Profil de protocole pour le paradigme de langage de balisage des télécommunications (tML)

Un profil de protocole de prise en charge utilisant les informations de gestion codées [64] sera étudié ultérieurement.

Appendice I

Directives pour l'utilisation de la gestion allomorphique

I.1 Introduction

Le présent appendice vise à donner aux développeurs de gestionnaires et d'agents du protocole CMIP des instructions leur permettant d'utiliser l'allomorphisme. Celui-ci est un outil puissant, dont la valeur s'accroît au fur et à mesure que des RGT sont mis en œuvre. L'allomorphisme peut être utilisé pour résoudre le problème de la façon d'ajouter de nouvelles capacités à des implémentations existantes de gestionnaire et d'agent RGT. Alors que les exigences évoluent et que les modèles sont étendus pour répondre à ces exigences, le logiciel contenu dans le système de gestion tirant parti de l'allomorphisme peut être écrit de manière à ne pas nécessiter de réécriture avant que les nouvelles caractéristiques soient requises dans le modèle.

Le présent appendice tente de préciser la façon de prendre en charge un comportement allomorphique dans des implémentations de systèmes aussi bien gestionnaires qu'agents. Il clarifie la description de l'allomorphisme, donnée dans la Rec. UIT-T X.720 | ISO/CEI 10165-1. En particulier, les gestionnaires doivent toujours être informés de l'allomorphisme pour en bénéficier. Même s'il ne prévoit pas d'utiliser l'allomorphisme, un gestionnaire doit posséder une capacité minimale à assurer l'interface avec des agents qui, eux, implémentent l'allomorphisme. Par exemple, le gestionnaire doit prendre en charge l'attribut "allomorphs" et avoir la capacité de construire des filtres faisant appel à des objets allomorphiques au lieu de la classe des objets réels de l'attribut objectClass.

Le présent appendice analyse les questions relatives à l'allomorphisme pour chaque opération du protocole CMIP, tant du point de vue du gestionnaire que du point de vue de l'agent. Il examine ensuite les questions relatives aux notifications CMIP, de nouveau sous les angles du gestionnaire et

de l'agent. Il propose ensuite quelques réflexions sur les piles de protocoles et leur implémentation. Il répond en conclusion à quelques questions fréquemment posées sur l'allomorphisme.

Dans la suite du texte, on utilisera l'expression "si l'agent prend en charge l'allomorphisme". Cette expression doit être considérée comme signifiant "si l'agent prend en charge l'allomorphisme pour une instance spécifique" car il est possible qu'un agent puisse prendre en charge des révisions pour certaines classes d'objets mais pas pour d'autres. Stricto sensu, deux instances d'une même classe peuvent différer quant à la prise en charge de l'allomorphisme. Toutefois, ce cas est considéré comme extrême et rare dans ce contexte. Il en est de même pour le côté gestionnaire car une version spécifique d'un système gérant peut reconnaître de multiples définitions pour certaines classes de base et pas pour d'autres. Les décisions relatives à l'inclusion des différentes versions sont régies par des objectifs commerciaux (qui sont hors du domaine d'application dans le présent appendice).

I.1.1 Aperçu général

L'allomorphisme est la capacité, pour un objet qui est une instance d'une classe d'objets gérés donnée, à être géré en tant que membre d'une ou de plusieurs autres classes d'objets gérés. L'allomorphisme autorise des instances d'une classe d'objets gérés donnée – appelée classe étendue – représenter des instances d'une autre classe d'objets gérés – appelée classe allomorphique.

Lorsqu'une classe étendue est instanciée, la classe réelle (voir la Rec. UIT-T X.720 | ISO/CEI 10165-1) de l'objet mémorisé dans l'attribut objectClass est la classe étendue. Elle est étendue par rapport à une autre classe d'objets gérés, qui est la classe d'objets gérés avec laquelle elle est compatible. La classe réelle est celle dont un objet géré est une instance. Une classe allomorphique d'un objet géré est une classe d'objets gérés autre que la classe réelle de cette objet géré; elle peut toutefois être gérée comme une instance de cette classe. Un objet géré peut être allomorphique à une ou plusieurs des classes compatibles (c'est-à-dire que des instances de la classe étendue peuvent être gérées comme des instances d'une classe d'objets gérés compatible). Autrement dit, les termes "classe allomorphique" et "classe d'objets gérés compatible" peuvent être utilisés comme des synonymes. Lorsqu'un agent crée un objet géré qui prend en charge l'allomorphisme, le bloc allomorphicPackage (défini comme un bloc conditionnel dans la classe sommitale de la Rec. UIT-T X.721 | ISO/CEI 10165-2) est inclus. Ce bloc contient l'attribut "allomorphs". De type GET seulement, cet attribut a valeur d'ensemble et contient les identificateurs d'objet des classes que cet objet peut représenter (avec lesquelles il est allomorphe). L'attribut "objectClass" possède une valeur de la classe réelle qui a été utilisée pour créer cette instance.

Le principe fondamental qui sous-tend l'allomorphisme est que la classe étendue prend en charge toutes les capacités des classes avec lesquelles elle est allomorphe. Elle peut également prendre en charge des capacités additionnelles. La classe étendue peut être une sous-classe des classes avec lesquelles elle est allomorphique mais cela n'est pas nécessaire. A tous égards, la classe étendue se comporte comme la classe qu'elle est réellement. Cela peut impliquer que le gestionnaire puisse recevoir des informations qui ne sont pas dans la classe allomorphique. Par exemple, si la classe étendue possède de nouveaux attributs, une opération de lecture générale issue du gestionnaire en renverra les valeurs. Le traitement de ce type de problème implique que le gestionnaire soit conscient du fait que la gestion allomorphique est utilisée. La Rec. UIT-T X.724 | ISO/CEI 10165-6 a défini les tables de conformité d'objet géré à utiliser dans les implémentations d'agent comme de gestionnaire. L'utilisation de ces tables pour établir la liste des allomorphes (s'ils sont pris en charge) est recommandée afin de déterminer les niveaux d'interopérabilité.

Les diverses interactions entre gestionnaires et agents utilisant la gestion allomophique sont analysées dans les paragraphes suivants. La Rec. UIT-T X.720 | ISO/CEI 10165-1 traite également de l'interopérabilité lorsque les règles de compatibilité ne sont pas entièrement observées. Le présent appendice ne traite que les scénarios répondant aux règles compatibles définies conformément à la Rec. UIT-T X.720 | ISO/CEI 10165-1 pour prendre en charge l'allomorphisme (voir § 5.2.3.2/X.720 | ISO/CEI 10165-1).

I.2 Opérations du protocole CMIP

Le présent paragraphe étudie l'allomorphisme en liaison avec les opérations m-Create, m-Get, m-Set, m-Action et m-Delete du protocole CMIP. Aucune incidence de l'allomorphisme sur l'opération m-Cancel-Get n'a été déterminée.

I.2.1 Création d'objets gérés

Un objet géré est créé soit par le gestionnaire qui émet une demande explicite de création à l'interface, soit par création automatique à l'intérieur du système agent. Chaque cas est étudié ci-dessous. Une sélection précise de l'attribut et de la structure de nommage est nécessaire. Les questions relatives au nommage sont étudiées ci-dessous dans un paragraphe distinct.

I.2.1.1 Création explicite – Rôle de gestionnaire

Cas 1: le gestionnaire émet une demande de création CMIP introduisant une valeur dans la classe d'objets gérés et un ensemble de valeurs d'attribut appropriées à cette classe. Le gestionnaire fournit le nom réel du nouvel objet. L'action qui en résulte dans l'agent est l'une de celles qui sont définies au § I.2.1.2 – Création explicite – Rôle d'agent – Cas a, b, c. Si la réponse est conforme à la définition du cas c, le gestionnaire doit être en mesure de ne pas tenir compte des attributs inconnus qui sont inclus à la suite de la création d'une classe étendue.

Cas 2: le gestionnaire émet une demande de création CMIP introduisant une valeur dans la classe d'objets gérés et un ensemble de valeurs d'attributs appropriées à cette classe. Le gestionnaire fournit la valeur d'attribut de rattachement de noms. L'action qui en résulte dans l'agent est l'une de celles qui sont définies au § I.2.1.2 – Création explicite – Rôle d'agent – Cas a, b, d. Si la réponse est conforme à la définition du cas d, le gestionnaire doit être en mesure de ne pas tenir compte des attributs inconnus qui sont inclus à la suite de la création d'une classe étendue.

Cas 3: le gestionnaire spécifie la classe sans nom spécifique dans le champ d'instance ni de valeur pour l'attribut de rattachement de noms. L'action qui en résulte dans l'agent est l'une de celles qui sont définies au § I.2.1.2 – Création explicite – Rôle d'agent – Cas a, b, e. Si la réponse est conforme à la définition du cas e, le gestionnaire doit être en mesure de ne pas tenir compte des attributs inconnus qui sont inclus à la suite de la création d'une classe étendue.

Cas 4: le gestionnaire spécifie une classe et demande qu'elle soit une copie d'un autre objet, c'est-à-dire de l'objet de référence. Selon la valeur de la classe, l'un des trois cas ci-dessus est possible.

I.2.1.2 Création explicite – Rôle d'agent

Cas a: l'agent reconnaît la classe d'objets gérés dans la demande et la prend en charge comme classe réelle. Dans ce cas, la classe d'objets gérés demandée est créée et l'allomorphisme n'est pas mis en jeu. L'opération de création réussit ou échoue selon les conditions associées au comportement et aux valeurs d'attribut fournies par le gestionnaire. L'agent utilise le nom fourni dans le cas 1 ci-dessus ou attribue un nom (au moyen de la règle de rattachement de noms du cas 2 ou par génération interne sur la base de la définition du schéma).

Cas b: l'agent ne prend pas en charge la classe demandée (soit en tant que classe réelle prise en charge, soit en tant qu'allomorphe). La classe d'objets gérés indiquée dans la demande n'est pas reconnue. La demande de création est rejetée avec l'erreur "pas de classe d'objets de ce type". Il s'agit d'un échec normal de l'opération de création d'une classe inconnue.

Cas c: l'agent prend en charge l'allomorphisme et crée une classe qui est de type étendu avec le nom fourni par le gestionnaire. Cela suppose que le nom fourni par le gestionnaire est conforme aux règles de structure (rattachement de noms) pour la classe étendue (classe identique ou classe supérieure étendue, ayant le même nom distinctif relatif (RDN, *relative distinguished name*)). Si cette condition n'est pas observée, l'opération de création échouera. Si elle réussit, l'agent répond en indiquant dans le champ de classe d'objets gérés la valeur pour la classe réelle ainsi que tous les

attributs appropriés à la classe réelle. L'objet est créé conformément au comportement de la classe étendue. Si le système agent doit assurer l'interopérabilité (voir § 5.2.3.1/X.720 | ISO/CEI 10165-1), l'agent inclut l'attribut "allomorphs" dans la valeur de la classe fournie dans la demande de création. Si le système gérant assure l'interopérabilité (voir § 5.2.3.2/X.720 | ISO/CEI 10165-1), le gestionnaire peut vérifier l'attribut "allomorphs" et déterminer que la classe d'objets demandée est allomorphique par rapport à la classe réelle.

Cas d: l'agent prend en charge l'allomorphisme et crée une classe qui est de type étendu avec le rattachement de noms fourni par le gestionnaire. Cela implique que le rattachement de noms soit valide pour la classe étendue. Cela est souvent vrai si la classe étendue est une sous-classe et que l'objet GDMO comporte un paragraphe "WITH SUBCLASSES" pour le rattachement des noms. Lorsque l'opération de création réussit, la réponse est la même que pour le cas c. La création échouera si le rattachement de noms n'est pas valide pour la classe étendue (par exemple, un comportement additionnel peut être inclus dans un rattachement de noms différent pour la classe étendue même si l'attribut et la structure de nommage sont les mêmes). Noter que si le gestionnaire reçoit une erreur de valeur invalide pour l'attribut de rattachement de noms sans autres renseignements, cela ne contribuera pas à résoudre le problème. Du point de vue du gestionnaire, la demande vise une classe et le rattachement des noms est valide. Etant donné que la classe étendue nécessite un comportement différent, l'agent ne peut pas utiliser ce rattachement de noms. C'est pourquoi il est recommandé de ne pas fournir le même attribut de rattachement de noms dans la demande de création.

Cas e: l'agent prend en charge l'allomorphisme et crée une classe avec un nom approprié qui est choisi par l'agent (pour le cas 3 du § I.2.1.1 – Création explicite – Rôle de gestionnaire). Le nom assigné peut être compris ou ne pas être compris par le gestionnaire, selon la définition de rattachement de noms choisi. Les autres informations contenues dans la réponse sont les mêmes que dans le cas c.

Pour tous les cas ci-dessus, lorsque le gestionnaire ne fournit pas de valeur pour un attribut et qu'une valeur par défaut existe, la valeur choisie pour cet attribut est en accord avec la classe d'objets créée. Dans les cas c, d et e, il peut en résulter que le gestionnaire reçoive des valeurs pour des attributs qui n'existent que dans la classe étendue. Le gestionnaire peut ne pas comprendre ces types. Il doit pouvoir ne pas tenir compte de ces types sans interrompre l'association. Noter que le gestionnaire peut prendre une décision de gestion additionnelle afin d'enregistrer le fait qu'il rencontre des agents allomorphiques (par exemple des informations d'identification non comprises).

En plus des valeurs par défaut des attributs, les contraintes imposées à la valeur initiale, les valeurs permises et requises peuvent présenter des différences entre la classe allomorphique et la classe étendue. Voir au § I.4 un complément d'analyse à ce sujet.

I.2.1.3 Résumé

Le tableau ci-dessous résume les divers cas de création explicite qui ont été examinés à partir du rôle de gestionnaire et à partir du rôle d'agent, selon que l'allomorphisme est pris ou non pris en charge.

Rôle de gestionnaire	**Rôle d'agent avec allomorphisme**	
	Pris en charge	Non pris en charge
Cas 1	Cas a, b, c	Cas a, b
Cas 2	Cas a, b, d	Cas a, b
Cas 3	Cas a, b, e	Cas a, b
Cas 4	Cas a, b, c, d, e	Cas a, b

I.2.1.4 Création automatique – Rôle d'agent

L'agent peut créer un objet géré sur le plan interne et en informer les gestionnaires au moyen de la notification de création d'objet.

Cas 1: supposons que l'agent ait implémenté la classe étendue et le comportement allomorphique. En plus de tous les attributs appropriés pour la classe créée, l'attribut "allomorphs", contenant toutes les classes d'objets (compatibles) allomorphiques, est inclus dans l'objet géré qui a été créé. L'agent envoie une notification de création pour le nouvel objet.

Dans ce cas, l'agent envoie ensuite une notification à chaque gestionnaire au moyen de la notification de création d'objet contenant la classe réelle. Il inclut tous les attributs de la classe citée en référence dans le champ de classe d'objets gérés de la notification de création. Ce message inclut l'attribut "allomorphs".

Noter que les valeurs par défaut qui sont utilisées sont compatibles avec la classe créée.

Cas 2: l'agent n'implémente que la classe étendue et n'active pas l'allomorphisme pour les classes compatibles. Dans ce cas, la notification de création d'objet ne contient que les renseignements relatifs à la classe étendue et l'attribut "allomorphs" n'est pas présent. Dans un tel environnement, il est recommandé que le système gérant assure l'interopérabilité indépendamment de la prescription ou de la non-prescription des caractéristiques additionnelles. Le rejet de la notification ne sera pas utile pour un environnement RGT concret.

I.2.1.5 Création automatique – Rôle de gestionnaire

Le gestionnaire reçoit la notification de création d'objet avec l'attribut "allomorphs" et une classe étendue dans le champ de classe d'objets gérés. Selon que le gestionnaire prend ou non en charge l'allomorphisme, les cas a à d ci-dessous sont applicables au cas 1 ci-dessus.

Cas a: le gestionnaire est informé de la classe étendue et l'attribut "allomorphs" n'est pas nécessaire car le gestionnaire n'a pas à effectuer de gestion allomorphique. Toutes les caractéristiques associées à la reconnaissance ou à la non-reconnaissance des identificateurs et valeurs d'attribut sont les mêmes lorsque l'allomorphisme n'est pas utilisé.

Cas b: le gestionnaire ne reconnaît pas la valeur de classe d'objets gérés contenue dans la notification. Si le gestionnaire comprend l'identificateur de l'attribut "allomorphs", ce gestionnaire doit, avant de considérer la notification comme une information non reconnue, examiner la valeur de l'attribut "allomorphs" pour déterminer s'il peut effectuer la gestion au moyen d'une des valeurs contenues dans cet attribut. Cela implique qu'au moins une des valeurs de classe d'objet contenues dans l'attribut "allomorphs" soit reconnue par le gestionnaire. Celui-ci doit considérer tous les attributs non reconnus comme appartenant à la classe allomorphique.

Cas c: le gestionnaire ne reconnaît pas la valeur de classe d'objets gérés et n'a pas implémenté la capacité de reconnaître l'identificateur d'attribut "allomorphs". Dans ce cas, le gestionnaire ne peut pas gérer cet objet autocréé. Si la création est envoyée avec une confirmation, une réponse d'erreur peut être donnée par le gestionnaire pour indiquer un objet inconnu.

Cas d: le gestionnaire ne reconnaît pas la valeur de classe d'objets gérés dans la notification. Le gestionnaire comprend l'attribut "allomorphs"; cependant, il ne reconnaît aucune des classes indiquées dans l'attribut "allomorphs". Dans ce cas, le résultat est le même que dans le cas c. La gestion de l'objet autocréé par ce gestionnaire n'est pas possible.

L'agent envoie une notification au moyen de la classe réelle, sans l'attribut "allomorphs" (l'agent n'effectue pas d'allomorphisme). Ce qui correspond au cas a ci-dessus.

Cas e: le gestionnaire comprend la classe étendue et le comportement est comme dans le cas a ci-dessus. L'absence de l'attribut "allomorphs" n'a pas d'incidence et le gestionnaire peut gérer l'objet autocréé.

Cas f: le gestionnaire ne reconnaît pas la classe étendue. Il n'est pas en mesure de gérer cet objet, étant donné que l'attribut "allomorphs" n'est pas pris en charge par l'agent. Cela est vrai, que le gestionnaire prenne ou non en charge l'allomorphisme.

I.2.1.6 Résumé pour l'autocréation

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas d'agent	Cas de gestionnaire
1	a, b, c, d
2	e, f

I.2.2 Opération GET

L'opération GET peut être émise avec un ensemble explicite d'identificateurs d'attribut, une liste vide ou une liste absente. Ces deux derniers cas (liste vide et liste absente font l'objet du même traitement) se différencient également selon que la classe d'objets gérés contenue dans la demande est la classe réelle ou la classe allomorphique pour l'agent. Noter qu'il existe un identificateur d'objet spécial (42) que le gestionnaire peut utiliser dans la demande pour faire référence à la classe réelle de l'objet géré sans avoir à la spécifier.

I.2.2.1 Rôle de gestionnaire

Cas 1: le gestionnaire émet une demande d'opération GET avec une classe qui n'est pas la classe réelle, de l'objet mais un des allomorphes pris en charge par l'agent. La liste des identificateurs d'attribut inclus est appropriée à cette classe allomorphique. La réponse reçue est conforme à l'un des cas a, b ou c ci-dessous. Si l'interopérabilité est prise en charge par le gestionnaire, la réception d'une réponse efficace dans le cas b avec une classe différente sera reconnue comme une réponse valide. Si elle n'est pas prise en charge, le gestionnaire rejettera la réponse (rejet par élément ROSE et non à partir du protocole CMIP).

Cas 2: le gestionnaire émet une demande d'opération GET avec une classe qui est soit la classe réelle, soit l'identificateur d'objet spécial, ce qui implique la classe réelle. La liste des attributs demandés peut être appropriée ou non appropriée à cette classe, car le gestionnaire peut inclure des attributs qui ne sont pas disponibles pour la classe implémentée, soit à titre conditionnel soit au moyen de l'identificateur d'objet spécial. La réponse reçue est conforme au cas d ci-dessous.

Cas 3: le gestionnaire formule la demande en spécifiant une classe, un nom d'objet géré et aucune liste d'attributs. La réponse reçue dépend de la valeur indiquée dans la classe, de la prise en charge de l'allomorphisme par l'agent et de la méthode d'interopérabilité. La réponse reçue est conforme à l'un des cas e, f ou g indiqués ci-dessous. Si la réponse contenue dans f ou g comporte des attributs que le gestionnaire ne reconnaît pas, celui-ci n'en tient pas compte.

Cas 4: le gestionnaire formule la demande en spécifiant soit une classe prise en charge par l'agent et le nom d'un objet géré, soit l'identificateur d'objet spécial décrit ci-dessus et un nom. Il n'inclut pas la liste d'attributs. La réponse reçue est conforme au cas h ci-dessous. Le gestionnaire ne doit pas tenir compte des attributs qui ne sont pas reconnus lorsque la classe indiquée dans la réponse est différente de ce que le gestionnaire reconnaît (en raison de l'utilisation de l'identificateur d'objet spécial).

I.2.2.2 Rôle d'agent

Cas a: l'agent prend en charge l'allomorphisme et reconnaît le nom de l'objet géré. La classe d'objets gérés indiquée dans la demande correspond à l'une des valeurs contenues dans l'attribut "allomorphs". L'agent répond avec les valeurs des attributs demandés et la classe indiquée dans la demande peut être incluse ou non incluse. Si la classe est incluse, il est recommandé que la valeur

de la classe réelle soit utilisée dans la réponse. Cette méthode assure une réponse uniforme et cohérente, que la demande vise un seul objet ou (par détection) plusieurs objets. L'on prévoit également que le paramètre de classe d'objets gérés, contenu dans une réponse CMIP, corresponde à la valeur de l'attribut "objectClass".

Cas b: l'agent ne prend pas en charge l'allomorphisme mais reconnaît le nom de l'objet géré. L'agent peut soit renvoyer une erreur ("aucune classe d'objets de ce type" ou "conflit entre instances de classe") soit renvoyer en réponse les valeurs de l'attribut (interopérabilité assurée par l'agent). C'est ce dernier comportement qui est recommandé. Le champ de classe peut être laissé vide ou recevoir la classe réelle. Si à la fois la classe et le nom ne sont pas reconnus, une réponse d'erreur est produite ("aucune classe d'objets de ce type" ou "conflit entre instances de classe").

Cas c: l'agent ne prend pas en charge l'allomorphisme et ne reconnaît pas la valeur de la classe ou du nom dans la demande. Une erreur de type "aucune classe d'objets de ce type" ou "conflit entre instances de classe" est renvoyée.

Cas d: l'agent reconnaît la classe et le nom, qu'il prenne ou non en charge l'allomorphisme (ce qui correspond au cas 2 où le gestionnaire demande à utiliser une classe qui est compatible et non pas la classe étendue bien qu'il ait connaissance de celle-ci, ou au cas simple où le gestionnaire et l'agent ne connaissent chacun qu'une seule classe). L'agent répond par des valeurs d'attribut (ce qui implique des erreurs si les attributs demandés ne conviennent pas à cette classe ou ont été implémentés en raison d'une opération conditionnelle). Le champ de classe peut être omis ou recevoir la classe réelle.

Cas e: l'agent reconnaît la classe et le nom indiqués dans la demande (que l'allomorphisme soit pris en charge ou non) et renvoie tous les identificateurs et toutes les valeurs d'attribut pour cet objet. La classe et le nom peuvent être omis de la réponse.

Cas f: l'agent prend en charge l'allomorphisme. La valeur de la classe indiquée dans la demande ne correspond pas à la valeur de la classe réelle bien que le nom corresponde à l'un des objets contenus dans le système. La classe correspond à une valeur contenue dans l'attribut "allomorphs". Si l'agent assure l'interopérabilité, cet agent répond avec seulement la valeur des attributs appropriés à la classe demandée. Si la valeur de la classe est incluse dans la réponse (où il n'est pas requis d'inclure la classe ou le nom), c'est la classe réelle qui sera utilisée (voir l'explication ci-dessus concernant le même sujet). Si le gestionnaire assure l'interopérabilité, l'agent renvoie tous les attributs inclus dans l'objet. Si la valeur de la classe indiquée dans la demande ne correspond à aucune des valeurs contenues dans l'attribut "allomorphs", l'agent renvoie au gestionnaire une erreur de type "aucune classe d'objets de ce type". Noter qu'afin d'assurer l'interopérabilité, il est recommandé que l'agent comme le gestionnaire offrent certaines capacités: la prise en charge de l'allomorphisme par l'agent et la non-prise en compte par le gestionnaire des informations inconnues.

Cas g: l'agent ne prend pas en charge l'allomorphisme. La classe demandée n'est pas reconnue mais un objet portant ce nom est disponible. L'agent peut répondre soit par une erreur "aucune classe d'objets de ce type" soit par l'envoi de tous les attributs relatifs à cette classe. Même s'il n'est pas requis que la réponse comporte la classe et l'instance pour une demande d'objet unique, il est recommandé que la classe réelle et le nom soient inclus dans ce cas. Cela indique au gestionnaire que la classe réelle est une classe étendue de la classe compatible que le gestionnaire reconnaît.

Cas h: la classe demandée correspond à la classe réelle chez l'agent ou bien la classe réelle est utilisée parce que la demande contenait la valeur d'identificateur d'objet spécial. Que l'allomorphisme soit ou non pris en charge, toutes les valeurs d'attribut correspondant à la classe réelle mise en œuvre pour cet objet sont renvoyées dans l'hypothèse que l'agent reconnaît le nom. Les champs de classe et de nom peuvent être contenus ou non contenus dans la réponse. Il est toutefois recommandé que la classe réelle et le nom soient inclus dans ce cas lorsque l'identificateur d'objet spécial est utilisé dans la demande. Si le nom n'est pas reconnu, une erreur "aucune instance d'objet de ce type" est renvoyée.

I.2.2.3 Résumé de l'opération GET

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas de gestionnaire	Cas d'agent
1	a, b, c
2	d
3	e, f, g
4	h

I.2.3 Opération SET

L'opération SET peut être émise par différents opérateurs. Elle peut spécifier un remplacement soit par une valeur spécifique, soit par une "mise à la valeur par défaut". Celle-ci peut dépendre, pour un attribut, de la classe réelle. Un attribut peut être spécifié dans une seule classe avec un ensemble de valeurs permises et un ensemble de valeurs requises. Celles-ci doivent toujours être un sous-ensemble ou un ensemble égal des valeurs permises. La classe étendue ne doit pas augmenter les valeurs permises mais peut en supprimer certaines à condition qu'elles ne soient pas dans l'ensemble des valeurs requises (voir la Figure 1). La non-prise en charge d'une valeur permise est autorisée soit dans la classe étendue, soit dans une classe compatible à condition que cette valeur ne soit pas dans la liste requise. Avec une gestion allomorphique, lorsqu'une valeur permise est indiquée pour l'allomorphe et que cette valeur n'est pas incluse dans la classe étendue, cette valeur peut être rejetée sans violer le comportement allomorphique (qui garantit la prise en charge de toutes les valeurs dans la classe compatible; si toutefois la valeur n'est pas dans l'ensemble permis d'une classe compatible, elle ne sera pas prise en charge car la liste ne peut pas être étendue).

I.2.3.1 Rôle de gestionnaire

Cas 1: le gestionnaire émet une demande l'opération SET avec une classe, un nom et la ou les valeurs pour les attributs (opérateur de remplacement/d'addition ou de suppression). La classe de l'objet n'est pas la classe réelle dans l'agent mais une classe compatible. Si une réponse est reçue (seulement si la demande a été confirmée), l'un des cas a, b, c ci-dessous est valide. Si l'interopérabilité est prise en charge par le gestionnaire, la réception d'une réponse efficace dans le cas b avec une classe différente sera reconnue comme une réponse valide. Si ce n'est pas le cas, le gestionnaire rejettera la réponse (par un élément ROSE et non à partir du protocole CMIP).

Cas 2: le gestionnaire émet une demande d'opération SET avec une classe qui est soit la classe réelle soit l'identificateur d'objet spécial, qui implique la classe réelle. La ou les valeurs des attributs (opérateur de remplacement/addition ou suppression) peut ou peuvent être ou ne pas être appropriées pour cette instance en raison d'une opération conditionnelle ou en raison de l'utilisation de l'identificateur d'objet spécial par le gestionnaire, qui peut ainsi fournir des valeurs appropriées pour la classe compatible. Si une réponse est reçue (seulement si la demande a été confirmée), le cas d ci-dessous est valide.

Cas 3: le gestionnaire formule la demande en spécifiant une classe, un nom et un remplacement par une valeur par défaut pour un ou plusieurs attributs. La réponse (si elle est reçue) dépend de la valeur contenue dans la classe, de la prise en charge de l'allomorphisme par l'agent et de la méthode d'interopérabilité. Il s'agit d'un des cas e, f ou g ci-dessous. La réponse reçue peut indiquer des valeurs par défaut pour les attributs qui soient différentes de celles qui sont associées à la classe demandée. Le gestionnaire doit reconnaître ces valeurs comme un résultat différent de la classe réelle chez l'agent.

Cas 4: le gestionnaire formule la demande en spécifiant soit une classe prise en charge par l'agent et un nom, soit l'identificateur d'objet spécial étudié ci-dessus et un nom plus un remplacement par

valeur par défaut pour un ou plusieurs attributs. La réponse, si elle est reçue, est conforme au cas h ci-dessous.

I.2.3.2 Rôle d'agent

Cas a: l'agent prend en charge l'allomorphisme et reconnaît le nom de l'objet géré. La classe d'objets gérés contenue dans la demande correspond à l'une des valeurs contenues dans l'attribut "allomorphs". L'agent modifie ces attributs (en admettant que l'attribut existe et que la valeur fournie est valide). Si la demande est confirmée, l'agent répond soit par un acquittement soit par les valeurs modifiées. Dans ce dernier cas, la valeur du champ de classe (s'il est présent) est la classe réelle (voir ci-dessus le raisonnement pour l'opération GET). Si les attributs ou les valeurs fournies dans la demande sont invalides, une erreur ou un succès partiel (erreur de liste pour l'opération SET) est renvoyé.

Cas b: l'agent ne prend pas en charge l'allomorphisme mais reconnaît le nom de l'objet géré. L'agent peut ne pas effectuer la modification demandée en raison de la non-reconnaissance de la classe. Si la demande n'a pas été confirmée, le gestionnaire n'a pas connaissance du résultat à moins qu'il ne lance une opération GET. Supposons qu'une réponse soit requise. Selon que l'agent a ou non effectué l'opération (avec succès ou autrement), il peut renvoyer l'un des messages suivants: une erreur ("pas de classe d'objets de ce type" ou "conflit entre instances de classe"); une confirmation indiquant le succès ou une erreur avec succès partiel. Il n'est pas nécessaire que les champs de classe et de nom soient inclus dans la réponse. S'ils le sont, il est recommandé d'inclure la classe réelle afin d'informer le gestionnaire de la classe implémentée. Si à la fois la classe et le nom ne sont pas reconnus, une réponse d'erreur est produite ("pas d'instance d'objet de ce type" ou "pas de classe d'objets de ce type").

Cas c: l'agent ne prend pas l'allomorphisme en charge et ne reconnaît pas le nom contenu dans la demande. Un erreur "pas de classe d'objets de ce type" ou "pas d'instance d'objet de ce type" est renvoyée.

Cas d: l'agent reconnaît la classe et le nom, qu'il prenne ou non en charge l'allomorphisme (ce qui correspond au cas 2 où le gestionnaire demande à utiliser une classe qui est compatible et non pas la classe étendue bien qu'il ait connaissance de celle-ci, ou au cas simple où le gestionnaire et l'agent ne connaissent chacun qu'une seule classe). L'agent effectue les modifications pour ces attributs (en supposant que ceux-ci existent et que la valeur fournie soit valide). Si la demande est confirmée, l'agent répond soit par un acquittement, soit par les valeurs modifiées. Dans ce dernier cas, il n'est pas nécessaire que les champs de classe et de nom se trouvent dans la réponse. S'ils y sont, la valeur du champ de classe est la classe réelle (même raisonnement que pour l'opération GET). Si les attributs ou valeurs fournis dans la demande sont non valides, une erreur ou un succès partiel (erreur de liste pour l'opération SET) est renvoyé.

Cas e: l'agent reconnaît la classe et le nom contenus dans la demande (que l'allomorphisme soit pris en charge ou non) puis exécute l'opération. La réponse peut, au besoin, être un acquittement, une erreur due à la non-définition d'une valeur par défaut, ou la valeur modifiée (la valeur par défaut spécifiée pour cette classe).

Cas f: l'agent prend en charge l'allomorphisme. La valeur de la classe dans la demande ne correspond pas à la valeur de la classe réelle bien que le nom corresponde à l'un des objets contenus dans le système. La classe correspond à une valeur de l'attribut "allomorphs". Si l'agent assure l'interopérabilité, soit il exécute la modification conformément à la valeur par défaut pour la classe réelle, soi il détecte une erreur (par exemple non-définition de valeur par défaut pour certains des attributs). Il répond soit par un acquittement, soit par la valeur par défaut assignée, soit par une erreur avec succès partiel. Il n'est pas nécessaire d'inclure les champs de classe et de nom dans la réponse. Si la valeur de la classe est incluse dans la réponse, il s'agit de la classe réelle (voir raisonnement pour l'opération GET). Si la valeur de la classe dans la demande ne correspond à

aucune des valeurs contenues dans l'attribut "allomorphs", l'agent renvoie au gestionnaire une erreur "pas de classe d'objets de ce type".

Cas g: l'agent ne prend pas en charge l'allomorphisme. La classe demandée n'est pas reconnue mais un objet du même nom est disponible. L'agent peut soit exécuter l'opération en remplaçant par des valeurs par défaut appropriées à la classe réelle, soit rejeter la demande. Si celle-ci a été confirmée et que l'agent la rejette, l'agent répond par une erreur "pas de classe d'objets de ce type" ou "conflit entre instances de classe". S'il exécute normalement l'opération, soit un acquittement, soit un succès avec les valeurs modifiées est renvoyé. Les valeurs renvoyées sont appropriées à la classe réelle. Bien qu'il ne soit pas nécessaire que la réponse comporte la classe et l'instance pour la demande d'objet unique, il est recommandé que la classe réelle et le nom soient inclus dans ce cas. Cela donne au gestionnaire l'information que la classe réelle est une classe étendue de la classe compatible reconnue par le gestionnaire (interopérabilité assurée par le gestionnaire). Si la modification est effectuée avec succès partiel, une erreur est envoyée. L'utilisation du champ de classe est la même que pour le cas de succès.

Cas h: la classe demandée correspond à la classe réelle chez l'agent ou la classe réelle est utilisée parce que la demande contenait la valeur d'identificateur d'objet spécial. Que l'allomorphisme soit ou non pris en charge, l'agent remplace par les valeurs par défaut toutes les valeurs correspondant aux identificateurs d'attribut dans la demande (en supposant que tous les attributs contenus dans la demande soient pris en charge par l'agent). S'il exécute normalement l'opération, il renvoie soit un acquittement, soit un succès avec les valeurs modifiées. Bien qu'il ne soit pas nécessaire que la réponse comporte la classe et l'instance pour la demande d'objet unique, il est recommandé que la classe réelle et le nom soient inclus dans ce cas, lorsque l'identificateur d'objet spécial est utilisé dans la demande. Si le nom n'est pas reconnu, une erreur "pas d'instance d'objet de ce type" est renvoyée.

I.2.3.3 Résumé de l'opération SET

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas de gestionnaire	Cas d'agent
1	a, b, c
2	d
3	e, f, g
4	h

I.2.4 Opération ACTION

L'opération ACTION peut, pour toute fonction spécifique, comporter un argument et des réponses ayant chacun des paramètres obligatoires ou facultatifs. Si l'argument de la classe réelle comporte des paramètres obligatoires qui ne font pas partie de la classe compatible, des valeurs par défaut doivent être associées à ces paramètres. Bien que la Rec. UIT-T X.720 | ISO/CEI 10165-1 permette d'ajouter des paramètres obligatoires dans les informations d'action, il n'est pas possible de les spécifier au moyen de la notation abstraite sans créer une nouvelle action. Toutefois, la prescription peut être spécifiée au moyen du comportement. En effet, seules les étiquettes des paramètres peuvent être utilisées afin d'augmenter une spécification d'action. Cela implique que l'action originale possède un champ de type ANY DEFINED BY (ou une classe d'objets d'information selon la Rec. UIT-T X.681 | ISO/CEI 8824-2) et que l'augmentation soit effectuée avec l'étiquette de modèle de paramètre contenue dans une autre classe (ou par création d'un objet informationnel). Si les champs requis doivent être ajoutés à une action, la seule méthode disponible consiste à définir une nouvelle action, ayant un enregistrement différent. En d'autres termes, les modèles ne

permettent pas de construire une action à partir d'une autre action par adjonction de nouveaux champs obligatoires dans une spécification ASN.1 formelle.

I.2.4.1 Rôle de gestionnaire

Cas 1: le gestionnaire émet une demande d'action avec une classe, un nom et la ou les valeurs pour les paramètres de l'argument d'action (s'il est présent). La classe de l'objet n'est pas la classe réelle chez l'agent mais une classe compatible. Si une réponse est reçue (seulement si l'action a été définie comme confirmé), un des cas a, b, c ci-dessous est valide. Si l'interopérabilité est prise en charge par le gestionnaire, la réception d'une réponse de succès dans les cas a et b avec une classe différente et des champs additionnels dans la réponse d'action sera reconnue comme une réponse valide. Sinon, le gestionnaire rejettera la réponse (par élément ROSE et non à partir du protocole CMIP).

Cas 2: le gestionnaire émet une demande d'action avec une classe qui est soit la classe réelle, soit l'identificateur d'objet spécial, ce qui implique l'utilisation de la classe réelle. Tous les champs inclus peuvent être ou ne pas être appropriés pour cette classe. Si une réponse est reçue (seulement si la demande a été confirmée), le cas d ci-dessous est valide.

I.2.4.2 Rôle d'agent

Cas a: l'agent prend en charge l'allomorphisme et reconnaît le nom de l'objet géré. La classe d'objets gérés indiquée dans la demande correspond à l'une des valeurs contenues dans l'attribut "allomorphs". L'agent exécute l'action conformément à sa classe réelle en utilisant les paramètres fournis dans la demande. Noter que s'il existe des champs additionnels qui sont requis pour exécuter l'action, des valeurs par défaut doivent être disponibles car elles ne seront pas fournies par le gestionnaire. Si la demande est confirmée, la réponse de l'agent dépend de deux conditions: le succès d'exécution de l'action et la prise en charge de l'interopérabilité par l'agent. La réponse ne doit pas nécessairement comporter la classe et le nom dans le cas où un objet unique est cité en référence. Si l'opération ne réussit pas, une erreur est renvoyée. L'agent peut inclure la classe réelle afin d'informer le gestionnaire de la classe implémentée ou de la classe demandée (classe allomorphique). Si l'action réussit, l'agent répond soit par un acquittement (ou confirmation du fait que l'action a été correctement exécutée parce que la définition d'action ne comporte pas de champs pour la réponse, soit par la réponse d'action avec les champs appropriés. L'agent peut choisir l'une des deux méthodes suivantes pour répondre. Si l'agent assure l'interopérabilité, il ne peut inclure que les champs appropriés à la classe demandée et non les compléments à la classe réelle. Dans ce cas, la valeur du champ de classe peut être omise. Dans la deuxième méthode, on part du principe que l'interopérabilité est fournie par le gestionnaire. La réponse peut comporter des champs additionnels, qui n'étaient pas dans l'action pour la classe indiquée dans la demande (de nouveaux modèles paramétriques peuvent avoir été inclus pour le champ d'extension ou des règles d'extensibilité peuvent avoir été appliquées en ASN.1). Il est recommandé d'inclure la classe réelle dans le champ de classe, afin que le gestionnaire soit informé de la classe implémentée.

Cas b: l'agent ne prend pas en charge l'allomorphisme mais reconnaît le nom de l'objet géré et l'action est valide pour sa classe réelle. L'agent peut ne pas exécuter l'action demandée en raison d'une non-reconnaissance de la classe dans la demande (classe différente de la classe réelle). Si la définition de l'action indique que celle-ci n'est pas confirmée, le gestionnaire ne sait pas si l'action a été réussie ou non. Selon le type de l'action, l'effet de cette action peut être déduit plus tard (par exemple par exécution d'une opération GET). Dans le cas où l'action est confirmée, l'agent peut, selon qu'il a exécuté l'action (avec succès ou autrement), renvoyer l'un des messages suivants: une erreur ("aucune classe d'objets de ce type" ou "conflit entre instances de classe"); une confirmation indiquant le succès, une erreur spécifique (éventuellement) définie pour cette action ou une erreur générique du protocole CMIP. L'action est exécutée conformément à la classe réelle. Les champs de classe et de nom ne sont pas obligatoirement dans la réponse. S'ils sont présents, il est recommandé d'inclure la classe réelle pour informer le gestionnaire de la classe implémentée. Si aussi bien la

classe que le nom ne sont pas reconnus, une réponse d'erreur est produite ("pas d'instance d'objet de ce type").

Cas c: l'agent ne prend pas en charge l'allomorphisme et ne reconnaît pas le nom dans la demande. Une erreur de type "pas de classe d'objets de ce type" ou "pas d'instance d'objet de ce type" est renvoyée.

Cas d: l'agent reconnaît la classe et le nom sans tenir compte du fait qu'il prend ou non en charge l'allomorphisme (ce qui correspond au cas 2, où le gestionnaire demande à utiliser une classe qui est compatible et non la classe étendue bien que le gestionnaire soit informé de celle-ci, assurant ainsi l'interopérabilité fournie par le gestionnaire ou le simple cas où le gestionnaire et l'agent sont tous deux informés au sujet d'une seule classe). L'agent exécute l'action conformément à sa classe réelle, sans tenir compte du fait que la demande contenait la classe allomorphique ou l'identificateur d'objet spécial. Le résultat de l'action peut être un succès ou une erreur. Si l'action n'a pas été définie comme étant confirmée, aucune réponse n'est produite. Si un succès ou une erreur se produit pendant l'exécution de l'action, une réponse de résultat ou d'erreur est émise, selon le cas. Si l'action est réussie, la réponse est produite conformément à la définition de la classe réelle. Si l'identificateur d'objet spécial est utilisé, il est recommandé d'inclure la valeur de classe pour la classe réelle bien que les champs de classe et de nom ne soient pas requis pour le cas d'un objet unique.

I.2.4.3 Résumé de l'opération ACTION

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas de gestionnaire	Cas d'agent
1	a, b, c
2	d

I.2.5 Opération DELETE

L'opération DELETE (suppression) est définie par deux options: objets confinés dans l'opération de suppression et pas d'opération de suppression autorisée à moins que tous les objets confinés ne soient supprimés. Il faut noter ce qui suit pour l'opération de suppression. Quelle que soit la classe, c'est le nom qui doit être reconnu parce que deux instances de la même classe peuvent avoir des noms différents ou des comportements différents (sur la base du rattachement de noms utilisé pour instancier l'objet).

I.2.5.1 Rôle de gestionnaire

Cas 1: le gestionnaire émet une demande de suppression avec une classe et un nom. La classe de l'objet n'est pas la classe réelle contenue chez l'agent mais est une classe compatible. Un des cas a, b ou c est valide pour la réponse. Si l'interopérabilité est prise en charge par le gestionnaire, la réception d'une réponse de succès dans les cas a et b avec une classe différente sera reconnue comme une réponse valide. Sinon, le gestionnaire rejettera la réponse (par élément ROSE et non à partir du protocole CMIP). Comme indiqué précédemment, l'envoi d'un rejet n'est pas utile (et donc non recommandé) car le gestionnaire doit assurer un certain niveau d'interopérabilité.

Cas 2: le gestionnaire émet une demande de suppression avec une classe qui est soit la classe réelle, soit l'identificateur d'objet spécial qui implique l'utilisation de la classe réelle. La réponse indiquée dans le cas d ci-dessous est valide.

I.2.5.2 Rôle d'agent

Cas a: l'agent prend en charge l'allomorphisme et reconnaît le nom de l'objet géré. La classe d'objets gérés indiquée dans la demande correspond à l'une des valeurs contenues dans l'attribut "allomorphs". L'agent supprime l'objet dans l'hypothèse que les conditions de suppression sont acceptables conformément au rattachement de noms utilisé pour cette instance. Si la suppression n'est pas effectuée, une erreur est produite. Si la suppression réussit, l'agent répond par un acquittement (confirmant que la suppression a bien été effectuée). Il n'est pas nécessaire que la réponse comporte l'indication de la classe et du nom lorsque la référence porte sur un objet unique. Il est recommandé d'inclure la classe réelle dans le champ de classe, afin d'informer le gestionnaire de la classe implémentée (ce qui n'est pas toujours utile au gestionnaire puisque l'objet est supprimé contrairement aux opérations précédentes).

Cas b: l'agent ne prend pas en charge l'allomorphisme mais reconnaît le nom de l'objet géré. L'agent peut ne pas supprimer l'objet en raison de la non-reconnaissance de la classe ("pas de classe d'objets de ce type" ou "conflit entre instances de classe"). Si l'agent effectue la suppression sur la base du nom d'objet (en supposant que les autres conditions de suppression soient satisfaites), un acquittement est renvoyé. Si la suppression n'est pas possible (conditions non satisfaites), une erreur est renvoyée. Dans un cas comme dans l'autre, il n'est pas nécessaire d'inclure la classe et le nom de l'objet. Il est recommandé d'inclure la classe réelle (ce qui n'est pas toujours utile au gestionnaire puisque l'objet est supprimé contrairement aux opérations précédentes).

Cas c: l'agent ne prend pas en charge l'allomorphisme et ne reconnaît pas le nom contenu dans la demande. Une erreur de type "pas de classe d'objets de ce type" ou "pas d'instance d'objet de ce type" est renvoyée.

Cas d: l'agent reconnaît la classe et le nom, qu'il prenne ou non en charge l'allomorphisme (cela correspond au cas 2, où le gestionnaire demande à utiliser une classe qui est compatible et non la classe étendue bien que le gestionnaire soit informé de celle-ci, assurant ainsi l'interopérabilité fournie par le gestionnaire, ou au simple cas où le gestionnaire et l'agent ne sont chacun informés que d'une seule classe). L'agent supprime l'objet dans l'hypothèse que les conditions de suppression sont acceptables en fonction du rattachement de noms applicable à cette instance. Si la suppression n'est pas effectuée, une erreur est produite. Si la suppression réussit, l'agent répond par un acquittement (ou confirmation que la suppression a été effectuée correctement). Il n'est pas nécessaire que la réponse comporte l'indication de la classe et du nom lorsque la référence porte sur un objet unique. Il est recommandé d'inclure la classe réelle dans le champ de classe (si l'identificateur d'objet spécial a été utilisé; sinon, le gestionnaire et l'agent ont la même compréhension de la valeur de classe) afin d'informer le gestionnaire de la classe implémentée (ce qui n'est pas toujours utile au gestionnaire puisque l'objet est supprimé contrairement aux opérations précédentes).

I.2.5.3 Résumé de l'opération DELETE

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas de gestionnaire	Cas d'agent
1	a, b, c
2	d

I.3 Notifications CMIP

Les notifications sont beaucoup plus simples que les opérations mentionnées au paragraphe précédent. Une notification peut être envoyée en mode confirmé ou non confirmé. En mode non confirmé, le gestionnaire peut ne pas tenir compte de ce qu'il reçoit parce que certains des éléments suivants ne sont pas reconnus: classe, nom, type d'événement et tout champ des informations

événementielles. L'utilisation du message RO-Reject est toujours possible mais celui-ci est envoyé au niveau des éléments ROSE et n'est pas reconnu par le protocole CMIP. Toutefois, l'envoi d'un rejet n'assure pas l'interopérabilité des RGT.

I.3.1 Rôle de gestionnaire

Cas a: le gestionnaire reconnaît la classe, le nom, le type de notification et certains des paramètres contenus dans les informations événementielles. Il ne tient pas compte des paramètres inconnus.

Cas b: le gestionnaire n'assure pas l'interopérabilité. Il ne reconnaît pas la classe. Il doit ignorer la notification et peut décider d'envoyer un rejet.

Cas c: le gestionnaire reconnaît le nom, le type de notification et certains des paramètres contenus dans les informations événementielles. Il ne reconnaît pas la classe. Il peut ne pas tenir compte de la notification ou déterminer que la classe est une classe étendue. Il ne tient pas compte des paramètres inconnus (s'il assure l'interopérabilité). Il peut également envoyer un rejet.

Cas d: le gestionnaire ne reconnaît pas la classe ni le nom (dans ce cas, la non-reconnaissance d'autres paramètres de la notification peut ne pas avoir d'importance). Le gestionnaire ne doit pas tenir compte de la notification.

I.3.2 Rôle d'agent

Cas 1: l'agent prend en charge l'allomorphisme. S'il assure l'interopérabilité, la notification peut comporter, dans le champ de classe, une valeur extraite de l'attribut "allomorphs" et toutes les informations événementielles (que les paramètres soient ou non applicables à la classe allomorphique). Normalement, il est prévu que l'agent utilise la classe réelle parce qu'il n'a généralement pas connaissance des allomorphes à mentionner dans les comptes rendus d'événement. Si la notification est confirmée, le cas a, b ou c ci-dessus est applicable.

Cas 2: l'agent ne prend pas en charge l'allomorphisme. Il émet la notification au moyen de la classe réelle et des paramètres relatifs à cette notification. Le cas a, b, c ou d ci-dessus est applicable.

I.3.3 Résumé pour la NOTIFICATION

Le tableau ci-dessous résume la relation entre les cas de gestionnaire et les cas d'agent.

Cas de gestionnaire	Cas d'agent
a	1, 2
b	1, 2
c	1, 2
d	2

I.4 Considérations relatives à l'implémentation

I.4.1 Relations avec les piles protocolaires

A plusieurs étapes de l'analyse de l'allomorphisme, il a fallu que le gestionnaire ait la capacité de ne pas tenir compte des syntaxes en notation ASN.1 (soit à partir des attributs seulement dans la classe étendue, soit à partir des notifications seulement dans la classe étendue). Généralement, ces syntaxes ne sont pas celles qui ont été implémentées dans le gestionnaire (car celui-ci s'efforce d'effectuer une gestion allomorphique). De façon que le gestionnaire réussisse à ne pas tenir compte de ces syntaxes, celles-ci doivent pouvoir traverser la pile de protocoles sans interrompre l'association. Cette fonction est assurée par les protocoles de couche Présentation. Celle-ci comporte normalement une règle d'abandon d'association en cas de réception d'unité PDU inconnue (voir § 6.4.4.3/X.226 | ISO/CEI 8823-1). Toutefois, le § 7.5/X.711 (CMIP) indique que le protocole

CMIP résout toutes les syntaxes de type ANY DEFINED BY OID. Le § 7.5/X.711 s'énonce comme suit:

– la valeur de descripteur d'objet ASN.1 correspondante doit être: "CMIP-PCI";

– cette syntaxe abstraite est définie en vue d'inclure tous les types de données résolus par les productions ANY DEFINED BY X, dans lesquelles X est du type OBJECT IDENTIFIER.

I.4.2 Valeurs permises et requises

La relation des valeurs d'attributs entre les classes allomorphiques et les classes étendues est analogue à la relation entre superclasses et leurs sous-classes. Les valeurs requises de la classe allomorphique doivent être un sous-ensemble des valeurs requises de la classe étendue. A leur tour, les valeurs requises de la classe étendue doivent être un sous-ensemble des valeurs permises de la classe allomorphique. Finalement, les valeurs permises de la classe étendue doivent être un sous-ensemble des valeurs permises de la classe étendue. Ces relations sont illustrées dans la Figure I.1.

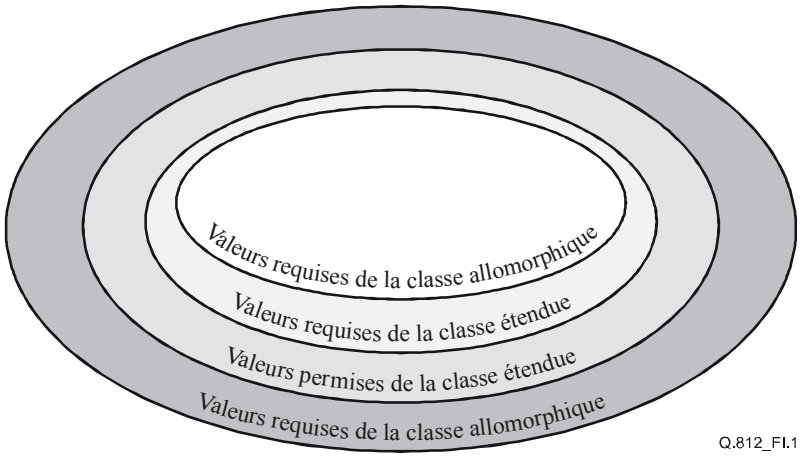

Figure I.1/Q.812 – Relation entre valeurs permises et requises

NOTE – Bien que les règles ci-dessus doivent être observées lors de la mise au point du modèle, il peut être difficile de les appliquer en pratique. Un exemple est la carte d'équipement multiport et la carte d'équipement définies dans la Rec. UIT-T M.3100. Les valeurs permises du statut de disponibilité étaient limitées à une seule valeur tandis que l'expérience pratique a montré que d'autres valeurs étaient requises. C'est pourquoi cette restriction a été supprimée dans la carte d'équipement multiport. La nouvelle version de la carte d'équipement ne pourra cependant pas être sous-classée à partir de la carte d'équipement car les valeurs permises ne peuvent pas être étendues et ne sont donc pas, au sens strict, allomorphiques. Bien que l'instance d'une classe étendue ait une valeur d'attribut extérieure à l'étendue permise pour la classe compatible, le système gérant peut assurer un certain niveau d'interopérabilité. Il doit être en mesure de coder la syntaxe ASN.1 de l'attribut.

I.4.3 Valeur initiale

Une spécification de classe d'objets gérés peut comporter des valeurs initiales pour zéro, un ou plusieurs attributs. Contrairement aux valeurs par défaut, les valeurs initiales créent une demande qui échoue si la valeur indiquée dans la demande est différente de la valeur initiale spécifiée. Lorsque la valeur est absente, l'agent fournit la valeur initiale spécifiée. Une classe étendue peut, pour un attribut donné, spécifier une valeur initiale qui est différente de celle qui correspond à la classe compatible. Lorsque l'agent crée l'objet géré, c'est la valeur initiale appropriée à la classe réelle qui sera utilisée. Ainsi, comme dans le cas des attributs à valeurs par défaut faisant l'objet du § I.2.1.2, le gestionnaire peut recevoir des valeurs d'attributs qui sont différentes des valeurs associées à la classe d'objets dans la demande. Il est recommandé, lors de la définition de valeurs initiales pour un attribut, que le gestionnaire ne fournisse pas la valeur dans la demande de création.

Cela évitera le rejet possible de la demande parce que la valeur initiale fournie n'est pas appropriée à la classe réelle.

I.4.4 Filtrage par objet unique

Lorsqu'une demande filtrée est émise, en supposant que l'agent l'a reconnue (selon les conditions indiquées plus haut), les cas suivants se présentent:

Cas 1: le filtre possède tous les attributs qu'il reconnaît et a été implémenté pour l'objet. Le fonctionnement du filtre n'est pas modifié.

Cas 2: le filtre possède des attributs qui ne sont pas implémentés par l'agent pour cet objet, soit parce que ces attributs sont conditionnels, soit parce qu'ils concernent la nouvelle version de l'objet. La condition qui est vérifiée pour chaque attribut est équivalente à: l'attribut existe et la valeur répond à la condition indiquée. Cette partie du filtre doit être évaluée comme vraie pour rendre les agents simples, quelle que soit la classe implémentée. Si l'attribut spécifié dans le filtre est "objectClass" et si la valeur à comparer est celle de la classe compatible, les objets de classe étendue ne répondront pas aux critères. Si le gestionnaire exige la sélection d'objets appartenant à la fois aux classes étendues et compatibles, le filtre doit avoir la fonction OR {equal{objectClass, x}, nonullIntersection {{x}, allomorphs}}.

I.4.5 Détection seulement

Le gestionnaire demande des opérations en fournissant un objet de base et un niveau de détection.

Cas 1: l'objet de base est la classe implémentée par l'agent:

– l'agent ne prend pas en charge l'allomorphisme et répond par la classe réelle pour les objets sélectionnés (sans tenir compte de la question de savoir s'il a implémenté la définition étendue qu'il reconnaît ou de savoir s'il n'a implémenté qu'une seule définition). Le gestionnaire peut recevoir des réponses pour des objets ayant des valeurs non reconnues pour le champ de classe (parce que le gestionnaire ne reconnaît pas le nouveau schéma). Le gestionnaire peut assurer une interopérabilité limitée, sur la base du nom et d'autres caractéristiques qu'il reconnaît;

– l'agent prend en charge l'allomorphisme et a implémenté des définitions étendues dans le domaine de visibilité sélectionné. Il effectue l'opération conformément aux classes réelles des objets contenus dans le domaine. La réponse utilise la classe réelle dans la classe d'objets gérés parce que l'agent peut ne pas être informé de la ou des valeurs contenues dans l'attribut "allomorphs", que le gestionnaire peut reconnaître ainsi que des détails relatifs à cette classe (attributs, résultat d'action, etc., comme indiqué ci-dessus). Même s'il prend en charge l'allomorphisme, il est plus simple de répondre dans ce cas en utilisant la classe réelle et les propriétés appropriées à cette classe. Le gestionnaire peut assurer l'interopérabilité s'il reconnaît aussi bien la version des définitions que l'interopérabilité limitée (une seule version est reconnue). (Si le gestionnaire prend en charge l'allomorphisme, il peut être utile que l'opération GET détectée demande que la valeur de l'attribut "allomorphs" soit renvoyée.)

Cas 2: l'objet de base est une classe différente de celle qui est contenue dans la demande mais le nom est reconnu (la classe est soit une définition plus récente que le contenu de la demande, soit une définition moins récente):

– l'agent ne prend pas en charge l'allomorphisme et implémente une définition moins récente. Il peut rejeter la demande parce que la classe n'est pas reconnue. Il peut également utiliser le nom et répondre par des objets contenus dans le domaine de visibilité. Si le gestionnaire reçoit le message "pas de classe d'objets de ce type" ou "conflit entre instances de classe", il peut le renvoyer avec la classe appropriée à l'objet de base. Ce n'est possible que si le gestionnaire assure l'interopérabilité et reconnaît la version prise en charge par l'agent. Il est possible que l'agent identifie l'objet de base d'après le nom (quelle que soit la classe), qu'il

sélectionne les objets dans le domaine et réponde au gestionnaire au moyen de la classe réelle. Le gestionnaire ne doit pas tenir compte des informations qu'il ne reconnaît pas s'il assure l'interopérabilité;

– l'agent prend en charge l'allomorphisme et détermine si la classe de l'objet de base est un allomorphe. Si c'est le cas, il effectue les opérations sur les objets sélectionnés (au moyen de la classe réelle) et répond au moyen de la classe réelle (interopérabilité assurée par le gestionnaire).

Dans les deux cas ci-dessus, si l'objet de base n'est pas identifié, une erreur est renvoyée.

Cas 3: bien que cela soit peu probable, il est possible que l'agent assure l'interopérabilité s'il possède la connaissance des versions prises en charge par le ou les gestionnaires. Dans ce cas, la réponse peut être personnalisée en fonction de la connaissance spécifique du gestionnaire.

I.4.6 Détection et filtrage

Lorsque la détection et le filtrage sont tous deux inclus dans la demande, un des trois cas traités ci-dessus doit être pris en considération. Les développements du § I.4.4 (Filtrage par objet unique) s'appliquent à chaque cas dont le résultat est la sélection des objets par application du domaine de visibilité. Aucun comportement additionnel n'est requis.

I.4.7 Nommage

Comme indiqué plus haut, la Rec. UIT-T X.720 | ISO/CEI 10165-1 définit l'allomorphisme comme une propriété de l'objet géré. En principe, il n'est pas nécessaire que deux classes (compatibles et étendues) soient associées par héritage afin de manifester un comportement allomorphique. Bien que cela ne soit pas spécifié dans la Rec. UIT-T X.720 | ISO/CEI 10165-1, il est nécessaire que la structure de nommage soit la même pour les deux classes. Même si le paramètre de classe d'objets gérés se rapporte à une classe allomorphique, il est nécessaire, afin que l'agent reconnaisse l'objet géré, que le champ d'objet géré utilise la même structure pour la classe réelle et pour la classe allomorphique. Une même structure implique que la séquence de construction des noms locaux et distinctifs soit la même (la classe supérieure et les attributs de nom distinctif relatif (RDN, *relative distinguished name*) sont les mêmes pour les classes étendues et allomorphiques). Cette condition est vérifiée dans la plupart des cas si les deux classes sont associées par héritage (le rattachement de noms peut inclure les mots AND SUBCLASSES).

L'exemple de la carte d'équipement à ports multiples est tel que les règles structurelles de nommage sont les mêmes que pour la carte d'équipement bien que le premier bloc ne puisse pas être déduit en tant que sous-classe (en raison de l'extension des valeurs permises). Du point de vue du nommage, il est donc possible de considérer une instance de carte d'équipement à ports multiples comme étant allomorphique par rapport à la classe des objets de type carte d'équipement.

I.5 Exemples d'utilisation de l'allomorphisme

Le présent paragraphe contient des exemples de scénarios dans lesquels les systèmes gérant et géré implémentent différentes versions d'un modèle d'information. Comme une réduction de tous les systèmes à la même version n'est pas possible, l'utilisation de l'allomorphisme prendra de l'importance pour assurer l'interopérabilité entre les systèmes.

Les figures de ces scénarios partent du principe que les systèmes agents et gestionnaires proviennent de plusieurs fournisseurs. Les numéros de version et la relation avec la version implémentée du modèle d'information ne sont donc pas en rattachement entre les fournisseurs.

La Figure I.2 décrit le scénario simple. Le schéma du modèle d'information (SMK, *schema for management information model*) correspond exactement aux mêmes définitions (qui proviennent toutes les deux de la même version du point de vue de l'interface). Des numéros différents servent à

illustrer la possibilité que, si différents vendeurs fournissent les systèmes, ils puissent utiliser différentes options de numérotation de version.

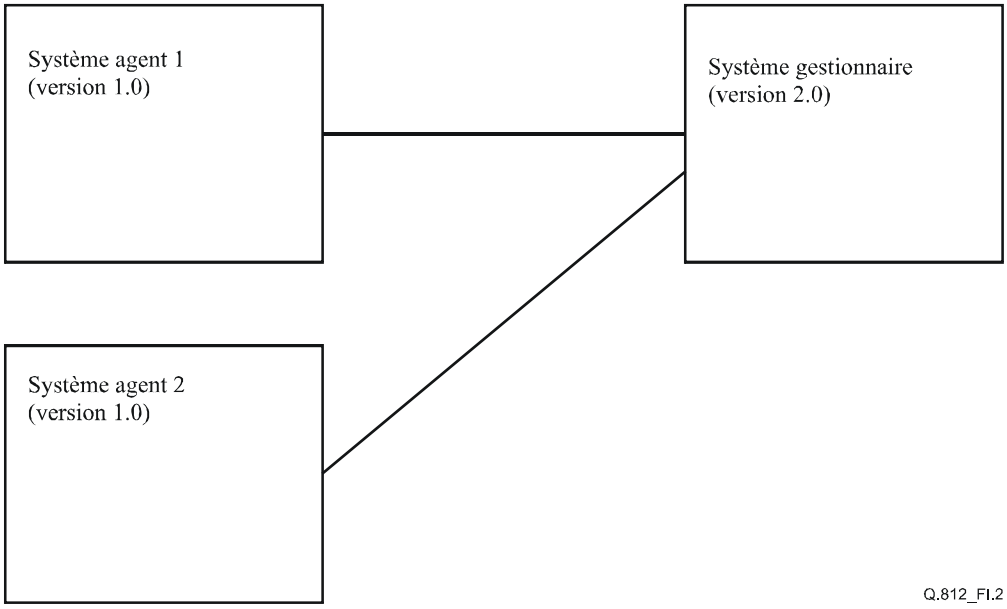

Figure I.2/Q.812 – Scénario 1

Dans ce cas, l'interopérabilité ne nécessite aucune prise en charge de l'allomorphisme. Aussi bien les systèmes agents que le système gestionnaire ne sont censés émettre ou recevoir des informations de gestion différentes de celles qui sont définies par le schéma.

La Figure I.3 décrit le scénario suivant. Le schéma du modèle d'informations de gestion (SMK) que le gestionnaire implémente possède plus de capacités que les système agents (version 1.0). La gestion-systèmes gère plusieurs systèmes agents (différents fournisseurs). Le système agent 2 (version 1.5) et le système gestionnaire (version 3.0) implémentent les mêmes éléments de service (le modèle SMK est le même du point de vue de l'interface). Le système agent 2 était également géré par le système gestionnaire 2, qui n'a pas évolué pour intégrer les nouveaux éléments de service.

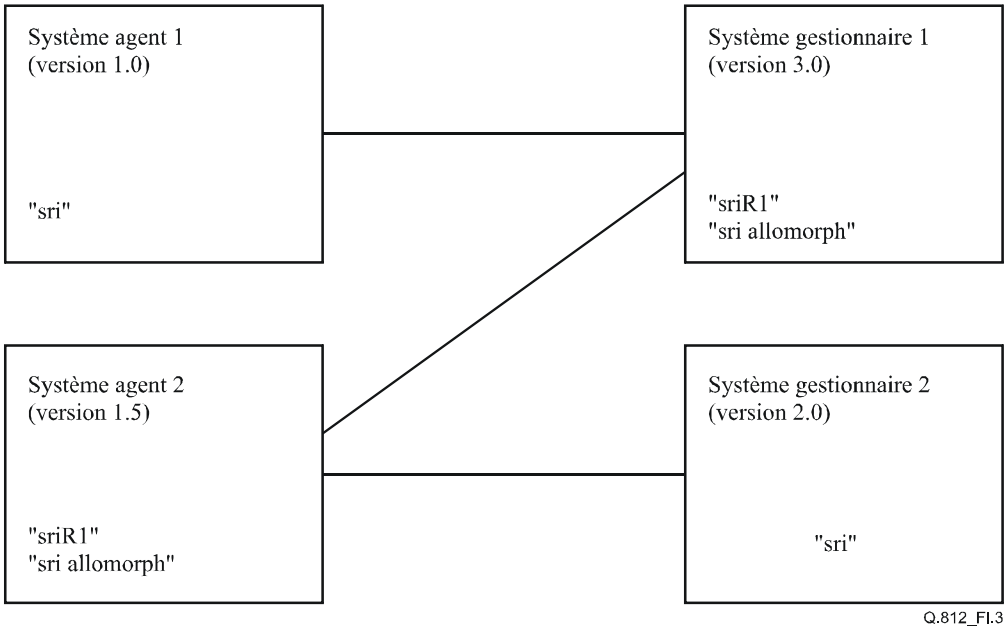

Figure I.3/Q.812 – Scénario 2

Cas 1: interopérabilité assurée par le gestionnaire: Pour plus de simplicité, considérons une classe d'objets gérés unique "sri" et une classe étendue "sriR1". Les solutions d'interopérabilité peuvent être expliquées au moyen de ce simple cas sans perte de généralisation (bien qu'un système puisse choisir de prendre en charge l'allomorphisme pour certaines classes et non pour d'autres). Supposons que le système gestionnaire de version 3.0 peut gérer des extensions qui ne sont pas offertes par le système agent 1 mais par le système agent 2.

Cas 2: la prise en charge de l'allomorphisme par le système agent 1 n'est pas applicable. Le système agent 2 prend en charge l'allomorphisme et a implémenté la classe "sriR1". L'attribut "allomorph" contient la valeur "sri". Les interactions entre le système gestionnaire 1 et les deux agents sont les mêmes que dans le cas 1. Le gestionnaire 2 ne reconnaît pas les capacités additionnelles de la classe "sri1" et, pour les notifications issues du système agent 2 (utilisant la classe étendue "sri1"), le comportement peut être différent du cas 1. Dans le cas de notifications définies seulement pour la classe sri1, le gestionnaire 2 ne saura pas comment les traiter. Il devra donc les ignorer pour ce qui est de l'activité de gestion. Comme le système agent 2 prend en charge l'allomorphisme, lorsque le gestionnaire demande une opération au moyen de la classe "sri", il effectue cette opération conformément aux spécifications pour la classe réelle "sriR1". L'agent peut informer le gestionnaire que la classe réelle est "sriR1" en l'insérant dans la réponse (ce qui n'est pas nécessaire si la demande est dirigée vers une instance spécifique). Sur la base de l'opération demandée, les informations fournies correspondront à celles de la classe réelle. Le gestionnaire 2 devra pouvoir ignorer les informations non reconnues sans interrompre l'association. Cela implique que le gestionnaire assure un niveau minimal d'interopérabilité.

Appendice II

Modifications des prescriptions de conformité ISP

Tableau II.1/Q.812 – Couche Transport

Norme de base (Rec. UIT-T X.224 | ISO/CEI 8073				ISP
Ident.	**Caractéristique**	**Paragraphe**	**Statut**	**Statut**
NAC2	Classe 2	6.5.4.h	NC2: Aucun 0,1,2	NC2: au moins 0
NAC4	Classe 4	6.5.4.h	NC4: None 0,1,2,3,4	NC4: au moins 0
NEF2	Classe 2	6.5.4.k	I2R2, T2F14:O	I2R2, T2F14:oo
NEF5	Classe 3	6.5.4.k	I3R2, T3F14:O	I0R2, T0F14:oo I2R2, T2F14:oo
NEF6	Classe 4	6.5.4.k	I4R2, T4F14:OO	I2R2, T2F14:oo I4R2, T4F14:oo
RC4	Avec quelles classes peut-on répondre si le CR propose seulement la Classe 4?	6.5.4.h Tableau 3	I4R2 or I2R2:4 or 2	I2R2:2, I4R2:4
RC4a	Avec quelles classes peut-on répondre si le CR propose la Classe 4 comme Classe préférée et que le paramètre d'une autre classe est présent?	6.5.4.h Tableau 3	I4R2:4, I2R2:2, I0R2:0 selon le codage de l'autre classe	I4R2:4, I2R2:2, I0R2:0 selon le codage de l'autre classe
S2	Acceptation de la fonction NCMS	Annexe B	O	oi
S3	Acceptation de la Classe 4 sur CLNS		O	oi
TED6	Classe 2	6.5.4.r	I2R2, T2F15:O	I2R2, T2F15:oo
TED8	Classe 4	6.5.4.r	I4R2, T4F15:O	I0R2, T0F15:ox
NUC1	"Non-utilisation de total de contrôle " proposé dans CR?	6.5.4.m	I4R1:mo	I4R1:mo
NUC2		6.5.4.m	I4R2:O	I4R2:mo

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, 2005