Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.500

(08/2005)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Annuaire

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services

Recommandation UIT-T X.500

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.379
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	**X.500–X.599**
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.889
Applications génériques de l'ASN.1	X.890–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	X.1000–

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

NORME INTERNATIONALE ISO/CEI 9594-1
RECOMMANDATION UIT-T X.500

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services

Résumé

La présente Recommandation | Norme internationale introduit les concepts d'annuaire et de base d'informations d'annuaire (DIB, *directory information base*). Elle donne un aperçu général des services et capacités qu'ils fournissent.

Source

La Recommandation UIT-T X.500 a été approuvée le 29 août 2005 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8. Un texte identique est publié comme Norme Internationale ISO/CEI 9594-1.

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

TABLE DES MATIÈRES

Page

1 Domaine d'application 1
2 Références normatives 1
2.1 Recommandations | Normes internationales identiques 1
3 Définitions 2
3.1 Définitions du modèle de communication 2
3.2 Définitions du modèle d'annuaire 2
3.3 Définitions concernant l'exploitation répartie 3
3.4 Définitions concernant la duplication 3
3.5 Définitions concernant l'annuaire de base 3
4 Abréviations 3
5 Conventions 4
6 Aperçu général de l'annuaire 4
7 Base d'informations d'annuaire (DIB) 6
8 Service d'annuaire 7
8.1 Introduction 7
8.2 Qualification de service 8
8.3 Interrogation de l'annuaire 8
8.4 Modification de l'annuaire 9
8.5 Autres résultats 9
9 Annuaire réparti 9
9.1 Modèle fonctionnel 10
9.2 Modèle organisationnel 10
9.3 Fonctionnement du modèle 10
10 Contrôle d'accès aux informations contenues dans l'annuaire 14
11 Administration du service 15
12 Duplication d'annuaire 15
12.1 Introduction 15
12.2 Formes de duplication d'annuaire 16
12.3 Duplication et cohérence des informations d'annuaire 17
12.4 Points de vue sur la duplication 17
12.5 Duplication et contrôle d'accès 18
13 Protocoles d'annuaire 18
14 Gestion-systèmes de l'annuaire 19
14.1 Introduction 19
14.2 Gestion du domaine de l'arbre DIT 19
14.3 Gestion des composantes de l'annuaire 19
Annexe A Application de l'annuaire 20
A.1 L'environnement de l'annuaire 20
A.2 Caractéristiques du service d'annuaire 20
A.3 Schémas d'utilisation de l'annuaire 20
A.4 Applications génériques 23
Annexe B Amendements et corrigenda 24

Introduction

La présente Recommandation | Norme internationale a été élaborée, ainsi que d'autres Recommandations | Normes internationales, pour faciliter l'interconnexion des systèmes de traitement de l'information et permettre ainsi d'assurer des services d'annuaire. L'ensemble de tous ces systèmes, avec les informations d'annuaire qu'ils contiennent, peut être considéré comme un tout intégré, appelé *annuaire*. Les informations de l'annuaire, appelées collectivement base d'informations d'annuaire (DIB), sont généralement utilisées pour faciliter la communication entre, avec ou à propos d'objets tels que des entités d'application, des personnes, des terminaux et des listes de distribution.

L'annuaire joue un rôle important dans l'interconnexion des systèmes ouverts, dont le but est de permettre, moyennant un minimum d'accords techniques en dehors des normes d'interconnexion proprement dites, l'interconnexion des systèmes de traitement de l'information:

- provenant de divers fabricants;
- gérés différemment;
- de niveaux de complexité différents;
- de générations différentes.

La présente Recommandation | Norme internationale présente et modélise les concepts de l'annuaire et de la base DIB. Elle donne un aperçu général des services et des possibilités qu'ils offrent. D'autres Recommandations | Normes internationales utilisent ces modèles pour définir le service abstrait fourni par l'annuaire et pour spécifier les protocoles permettant d'obtenir ou de diffuser ce service.

La présente Recommandation | Norme internationale fournit les cadres généraux de base permettant à d'autres organismes de normalisation et à des forums industriels de définir des profils d'industrie. L'utilisation d'un grand nombre des fonctionnalités définies comme facultatives dans ces cadres peut être rendue obligatoire dans certains environnements au moyen de profils. La présente cinquième édition révise et améliore d'un point de vue technique, mais ne remplace pas, la quatrième édition de la présente Recommandation | Norme internationale. Les implémentations peuvent encore revendiquer la conformité à la quatrième édition mais celle-ci finira par ne plus être prise en charge (c'est-à-dire que les erreurs signalées ne seront plus corrigées). Il est recommandé que les implémentations se conforment, dès que possible, à la présente cinquième édition.

Cette cinquième édition spécifie les versions 1 et 2 des protocoles d'annuaire.

Les première et deuxième éditions ne spécifiaient que la version 1. La plupart des services et protocoles spécifiés dans la présente édition sont conçus pour fonctionner selon la version 1. Certains services et protocoles améliorés, comme les erreurs signées, ne fonctionneront cependant pas avant que toutes les entités d'annuaire mises en jeu dans l'exploitation aient négocié la version 2. Quelle que soit la version négociée, on a traité les différences entre les services et entre les protocoles définis dans les cinq éditions, à l'exception de ceux qui sont spécifiquement définis dans la version 2 en utilisant les règles d'extensibilité définies dans l'édition actuelle de la Rec. UIT-T X.519 | ISO/CEI 9594-5.

L'Annexe A, qui fait partie intégrante de la présente Recommandation | Norme internationale, contient une description des types d'utilisation de l'annuaire.

L'Annexe B, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, donne la liste des amendements et des erreurs qui ont été signalées et dont on a tenu compte dans cette édition de la présente Recommandation | Norme internationale.

NORME INTERNATIONALE
RECOMMANDATION UIT

Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services

1 Domaine d'application

L'annuaire offre les possibilités d'annuaire requises par les applications OSI, les méthodes de gestion OSI, d'autres entités de couche OSI et les services de télécommunication. Parmi les possibilités qu'il offre, citons des "dénominations faciles à utiliser", c'est-à-dire des noms d'objets que les utilisateurs peuvent citer facilement (bien que tous les objets n'aient pas besoin d'avoir des noms faciles à utiliser); et le "mappage nom-adresse", grâce auquel il existe un lien dynamique entre les objets et leurs emplacements. Cette dernière capacité permet aux réseaux OSI, par exemple, d'être autonomes dans le sens où une adjonction, une suppression ou une modification des emplacements d'objet n'affecte pas le fonctionnement du réseau OSI.

L'annuaire n'est pas censé être un système de base de données général, bien qu'il puisse être fondé sur ce type de système. On suppose par exemple, comme cela est caractéristique des annuaires de communication, qu'il y a beaucoup plus "d'interrogations" que de mises à jour. La fréquence des mises à jour dépend normalement de la dynamique des personnes et des organisations et non, par exemple, de la dynamique des réseaux. L'application globale instantanée des mises à jour n'est pas non plus nécessaire: des conditions transitoires, dans lesquelles l'ancienne version et la nouvelle version de la même information coexistent, sont tout à fait acceptables.

Une caractéristique de l'annuaire est que les résultats des interrogations de l'annuaire ne dépendront ni de l'identité ni de l'emplacement du demandeur, sauf si cela découle de droits d'accès différents ou de mises à jour non diffusées. En raison de cette caractéristique, l'annuaire n'est pas approprié pour certaines applications de télécommunication, par exemple certains types d'acheminement. Dans les cas où les résultats dépendront de l'identité du demandeur, l'accès aux informations de l'annuaire et les mises à jour de l'annuaire pourront être refusés.

2 Références normatives

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

2.1 Recommandations | Normes internationales identiques

- 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.*
- Recommandation UIT-T X.501 (2005) | ISO/CEI 9594-2:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.*
- Recommandation UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*
- Recommandation UIT-T X.511 (2005) | ISO/CEI 9594-3:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition du service abstrait*.
- Recommandation UIT-T X.518 (2005) | ISO/CEI 9594-4:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: procédures pour le fonctionnement réparti.*
- Recommandation UIT-T X.519 (2005) | ISO/CEI 9594-5:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles.*

- Recommandation UIT-T X.520 (2005) | ISO/CEI 9594-6:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: types d'attributs sélectionnés*.
- Recommandation UIT-T X.521 (2005) | ISO/CEI 9594-7:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: classes d'objets sélectionnées.*
- Recommandation UIT-T X.525 (2005) | ISO/CEI 9594-9:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: duplication.*
- Recommandation UIT-T X.530 (2005) | ISO/CEI 9594-10:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: utilisation de la gestion-systèmes pour l'administration de l'annuaire.*

3 Définitions

Dans la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de communication

Les termes suivants sont définis dans la Rec. UIT-T X.519 | ISO/CEI 9594-5:

a) entité d'application;
b) couche Application;
c) processus d'application.

3.2 Définitions du modèle d'annuaire

Les termes suivants sont définis dans la Rec. UIT-T X.501 | ISO/CEI 9594-2:

a) contrôle d'accès;
b) domaine de gestion d'annuaire d'administration;
c) alias;
d) ascendant;
e) attribut;
f) type d'attribut;
g) valeur d'attribut;
h) authentification;
i) entrée composite;
j) contexte;
k) arbre d'information d'annuaire (DIT);
l) domaine de gestion d'annuaire (DMD);
m) agent de système d'annuaire (DSA);
n) agent utilisateur d'annuaire (DUA);
o) nom distinctif;
p) entrée;
q) famille (d'entrées);
r) groupe hiérarchique;
s) client LDAP;
t) demandeur LDAP;
u) répondeur LDAP;
v) serveur LDAP;
w) nom;
x) objet (d'intérêt);
y) domaine de gestion privé d'annuaire;
z) entrées liées;

aa) nom distinctif relatif;

bb) racine;

cc) schéma;

dd) politique de sécurité;

ee) objet subordonné;

ff) entrée supérieure;

gg) objet supérieur;

hh) arborescence.

3.3 Définitions concernant l'exploitation répartie

Les termes suivants sont définis dans la Rec. UIT-T X.518 | ISO/CEI 9594-4:

a) chaînage simple;

b) chaînage multiple;

c) renvoi.

3.4 Définitions concernant la duplication

Les termes suivants sont définis dans la Rec. UIT-T X.525 | ISO/CEI 9594-9:

a) copie cache (processus);

b) copie cache;

c) copie d'entrée;

d) DSA maître;

e) duplication;

f) consommateur d'informations miroirs;

g) fournisseur d'informations miroirs;

h) information miroir;

i) accord de duplication miroir.

3.5 Définitions concernant l'annuaire de base

Les termes suivants sont définis dans la présente Recommandation | Norme internationale:

3.5.1 **annuaire**: ensemble de systèmes ouverts coopérant à la fourniture de services d'annuaire.

3.5.2 **base d'informations d'annuaire (DIB, *directory information base*)**: ensemble d'informations géré par l'annuaire.

3.5.3 **utilisateur (d'annuaire)**: utilisateur final de l'annuaire, c'est-à-dire, l'entité ou la personne physique qui accède à l'annuaire.

4 Abréviations

Dans la présente Recommandation | Norme internationale, les abréviations suivantes sont utilisées:

ACI	Information de contrôle d'accès (*access control information*)
ADDMD	Domaine de gestion d'annuaire d'administration (*administration directory management domain*)
DAP	Protocole d'accès à l'annuaire (*directory access protocol*)
DIB	Base d'informations d'annuaire (*directory information base*)
DISP	Protocole de duplication miroir d'informations de l'annuaire (*directory information shadowing protocol*)
DIT	Arbre d'information d'annuaire (*directory information tree*)

DMD	Domaine de gestion d'annuaire (*directory management domain*)
DOP	Protocole de gestion des liens opérationnels d'annuaire (*directory operational binding management protocol*)
DSA	Agent de système d'annuaire (*directory system agent*)
DSP	Protocole du système d'annuaire (*directory system protocol*)
DUA	Agent d'utilisateur d'annuaire (*directory user agent*)
LDAP	Protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
OSI	Interconnexion des systèmes ouverts (*open systems interconnection*)
PRDMD	Domaine de gestion privé d'annuaire (*private directory management domain*)
RDN	Nom distinctif relatif (*relative distinguished name*)

5 Conventions

A quelques exceptions mineures près, la présente Spécification d'annuaire a été élaborée conformément aux "*Règles de présentation des textes communs UIT-T | ISO/CEI*" datant de novembre 2001.

L'expression "Spécification d'annuaire" (comme dans "la présente Spécification d'annuaire") désigne la Rec. UIT-T X.500 | ISO/CEI 9594-1. L'expression "Spécifications d'annuaire" désigne les Recommandations de la série X.500 et toutes les parties de l'ISO/CEI 9594.

La présente Spécification d'annuaire utilise l'expression "*systèmes de la première édition*" pour désigner les systèmes conformes à la première édition des Spécifications d'annuaire, c'est-à-dire à l'édition 1988 des Recommandations CCITT de la série X.500 et à l'ISO/CEI 9594:1990. La présente Spécification d'annuaire utilise l'expression "*systèmes de la deuxième édition*" pour désigner les systèmes conformes à la deuxième édition des Spécifications d'annuaire, c'est-à-dire à l'édition 1993 des Recommandations UIT-T de la série X.500 et à l'ISO/CEI 9594:1995. La présente Spécification d'annuaire utilise l'expression "*systèmes de la troisième édition*" pour désigner les systèmes conformes à la troisième édition des Spécifications d'annuaire, c'est-à-dire à l'édition 1997 des Recommandations UIT-T de la série X.500 et à l'ISO/CEI 9594:1998. La présente Spécification d'annuaire utilise l'expression "*systèmes de la quatrième édition*" pour désigner les systèmes conformes à la quatrième édition des Spécifications d'annuaire, c'est-à-dire à l'édition 2001 des Recommandations UIT-T X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.525 et X.530, à l'édition 2000 de la Rec. UIT-T X.509 et aux parties 1 à 10 de l'ISO/CEI 9594:2001.

La présente Spécification d'annuaire utilise l'expression "*systèmes de la cinquième édition*" pour désigner les systèmes conformes à la cinquième édition des Spécifications d'annuaire, c'est-à-dire à l'édition 2005 des Recommandations UIT-T X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525 et X.530 ainsi qu'aux parties 1 à 10 de l'ISO/CEI 9594:2005.

La présente Spécification d'annuaire présente la notation ASN.1 en caractères gras Helvetica. Lorsque des types et des valeurs ASN.1 sont cités dans le texte normal, ils en sont différenciés par leur présentation en caractères gras Helvetica. Les noms des procédures, généralement cités lorsque l'on spécifie la sémantique du traitement, sont différenciés du texte normal par une présentation en caractères gras Times. Les autorisations de contrôle d'accès sont présentées en caractères italiques Times.

6 Aperçu général de l'annuaire

L'*annuaire* est un ensemble de systèmes ouverts qui coopèrent pour établir une base de données logique contenant des informations sur un ensemble d'objets dans le monde réel. Les *utilisateurs* de l'annuaire, qu'il s'agisse de personnes ou de programmes d'ordinateurs, peuvent lire ou modifier les informations ou une partie de celles-ci, à condition qu'ils soient autorisés à le faire. Pour accéder à l'annuaire, chaque utilisateur est représenté par un agent d'utilisateur d'annuaire (DUA, *directory user agent*) ou par un client LDAP, tous deux considérés comme des processus d'application. Ces concepts sont illustrés sur la Figure 1.

NOTE – Les Spécifications d'annuaire s'appliquent à l'annuaire au singulier et traduisent l'intention de créer, par l'intermédiaire d'un espace de nom simple, unifié, un annuaire logique comprenant de nombreux systèmes et destiné à de nombreuses applications. La question de savoir si ces systèmes choisissent l'interfonctionnement dépendra des besoins des applications qu'ils assurent. Les applications traitant de mondes d'objets qui ne se croisent pas n'auront peut-être pas ce besoin. L'espace de nom unique facilite l'interfonctionnement ultérieur au cas où les besoins changeraient. Pour de multiples raisons, notamment de sécurité ou de connectivité, ou à cause de décisions commerciales, il est probable que certaines parties de l'annuaire ne seront pas atteignables à partir d'autres parties ayant des fonctionnements correspondant à la troisième édition. Il en résulte des représentations divergentes de l'annuaire, qui peuvent contenir des entrées liées au sujet d'un objet donné du monde réel. De telles entrées liées peuvent ou non avoir le même nom distinctif. Dans les systèmes de la quatrième édition ou d'une édition ultérieure, il est possible d'effectuer des opérations sur plusieurs représentations divergentes pour fournir à l'utilisateur une réponse intégrée.

- Les administrateurs de domaines DMD (voir le § 9.2) doivent parfois publier leur ou leurs propres représentations d'un objet concret donné. Un tel objet peut donc être modélisé par plusieurs entrées autonomes dans l'annuaire, et cela peut se produire indépendamment du fait qu'ils doivent ou ne doivent pas interfonctionner. L'interfonctionnement avec emploi du protocole DSP peut aussi ne pas être pris en charge.
- En dépit de la dernière phrase de la Note, il est aussi possible que des domaines DMD donnés préfèrent publier des informations sur les objets concrets dans leurs propres espaces de noms d'annuaire distincts (c'est-à-dire dans un ou plusieurs arbres DIT); dans ce cas, il se peut qu'un objet concret spécifique soit modélisé par des entrées dans le même espace de nom d'arbre DIT ou dans des espaces différents avec le même nom distinctif ou avec des noms différents dans chacun d'eux. On notera que certaines ressources d'annuaire (telles que l'acquisition de certificats et des fonctions associées basées sur les signatures numériques) ne peuvent pas être implémentées lorsque des objets distincts peuvent utiliser des noms distinctifs en partage.
- L'objectif des entrées associées est d'offrir un moyen par lequel les utilisateurs ont accès à de telles entrées, réunissant, si possible, l'information résultante. Cela pourrait s'appliquer à la situation décrite dans les deux alinéas précédents.

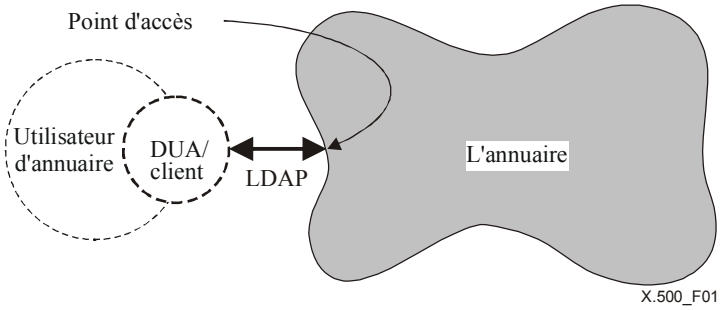

Figure 1 – Accès à l'annuaire

L'information contenue dans l'annuaire est appelée collectivement *base d'informations d'annuaire* (DIB, *directory information base*). Le paragraphe 7 donne un aperçu général de sa structure.

L'annuaire offre à ses utilisateurs un ensemble bien défini de capacités d'accès, appelé service abstrait de l'annuaire. Ce service, qui est décrit brièvement au § 8, offre une capacité simple de modification et d'extraction. Elle peut être établie avec des fonctions DUA locales pour offrir les capacités requises par les utilisateurs finals.

L'annuaire est réparti aux niveaux fonctionnel et organisationnel. Le paragraphe 9 donne un aperçu général des modèles correspondants de l'annuaire. Ils ont été élaborés afin de fournir un cadre pour que la coopération des divers éléments forme un tout intégré.

L'annuaire existe dès lors que les diverses autorités administratives contrôlent l'accès aux éléments d'information placés sous leur responsabilité. Le paragraphe 10 donne un aperçu général du contrôle d'accès.

En cas de répartition de l'annuaire, il peut être souhaitable de dupliquer des informations pour améliorer la performance et la disponibilité. Le paragraphe 11 donne un aperçu général du mécanisme de duplication de l'annuaire.

La mise à disposition et l'utilisation des services d'annuaire exigent que les utilisateurs (en réalité les agents DUA et/ou les clients LDAP) et les divers éléments fonctionnels de l'annuaire coopèrent les uns avec les autres. Très souvent, il sera nécessaire d'établir une coopération entre les processus d'application dans les différents systèmes ouverts, puis d'utiliser les protocoles d'application normalisés brièvement décrits au § 11, pour régir cette coopération.

L'annuaire a été conçu de façon à assurer des applications multiples, choisies parmi une vaste gamme de possibilités. La nature des applications assurées décide des objets qui sont énumérés dans l'annuaire, des utilisateurs qui accèdent à l'information et des types d'accès qui sont offerts. Les applications peuvent être très spécifiques (établissement de listes de distribution pour le courrier électronique) ou génériques (application d'annuaire de communications interpersonnelles). L'annuaire offre la possibilité d'exploiter des éléments communs aux différentes applications:

- un simple objet peut convenir pour plusieurs applications: il se peut encore qu'un même élément d'information, concernant un même objet puisse être approprié;
- pour cela, un certain nombre de classes d'objets et de types d'attribut sont définis; ils sont utiles pour toute une gamme d'applications. Ces définitions figurent dans la Rec. UIT-T X.520 | ISO/CEI 9594-6 et dans la Rec. UIT-T X.521 | ISO/CEI 9594-7;
- certains schémas d'utilisation de l'annuaire sont communs à une gamme d'applications: l'Annexe A en donne un aperçu général.

7 Base d'informations d'annuaire (DIB)

NOTE 1 – La base DIB et sa structure sont définies dans la Rec. UIT-T X.501 | ISO/CEI 9594-2.

La base DIB est un ensemble d'informations sur des objets. Elle est composée d'*entrées* (d'*annuaire*), chacune comprenant un ensemble d'informations sur un objet. Une entrée peut être un agrégat d'entrées de membre qui possèdent chacune des informations sur un aspect particulier d'un objet. Cette entrée est appelée entrée composite. Chaque entrée est composée d'*attributs*, chacun ayant un type et une ou plusieurs valeurs. Les types d'attribut qui sont présents dans une entrée donnée dépendent de la *classe* d'objets que l'entrée décrit. Chaque *valeur* d'un attribut peut être étiquetée avec un ou plusieurs *contextes* qui spécifient des informations sur la valeur, ces informations pouvant servir à déterminer l'applicabilité de la valeur.

Les entrées de la base DIB sont présentées sous forme arborescente: l'arbre d'information d'annuaire (DIT, *directory information tree*) dont les sommets représentent les entrées. Les entrées se trouvant près de la racine de l'arbre représenteront souvent des objets tels que des pays ou des organisations, alors que les entrées plus éloignées de la racine représenteront des personnes ou des processus d'application.

NOTE 2 – Les services définis dans les Spécifications d'annuaire ne fonctionnent que d'après une structure d'arbre (DIT). Les Spécifications d'annuaire n'excluent pas l'existence, à l'avenir, d'autres structures (selon les besoins).

Chaque entrée a un nom distinctif, qui l'identifie de façon unique et non ambiguë. Les caractéristiques du nom distinctif découlent de la structure d'arbre d'information. Le nom distinctif d'une entrée est composé du nom distinctif de son entrée supérieure, ainsi que des valeurs d'attribut spécialement désignées (les valeurs distinctives) de l'entrée.

Certaines entrées se trouvant au niveau des feuilles de l'arbre sont des entrées *alias* alors que toutes les autres entrées sont des entrées d'objets et des entrées composites. Les entrées alias désignent les entrées d'objet et constituent la base d'autres noms pour les objets correspondants.

Une entrée composite est une entrée représentant un objet unique; elle est une combinaison d'entrées de membres représentant chacune une partie des informations relatives à l'objet.

L'annuaire applique un ensemble de règles pour s'assurer que la base DIB reste bien formée face aux modifications qui interviennent dans le temps. Ces règles, appelées le *schéma de annuaire*, empêchent que les entrées aient des types d'attribut qui ne conviennent pas pour la classe d'objets, (les valeurs d'attribut ayant une forme incorrecte pour le type d'attribut) et même que les entrées aient des entrées subordonnées de la mauvaise classe.

La Figure 2 illustre les concepts ci-dessus d'arbre DIT et de ses éléments.

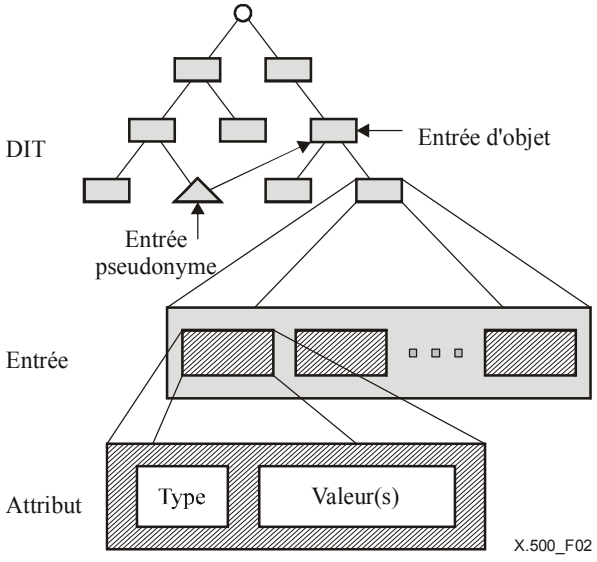

Figure 2 – Structure de l'arbre DIT et des entrées

La Figure 3 donne un exemple hypothétique d'arbre DIT. L'arbre donne des exemples de certaines des catégories types d'attributs utilisés pour identifier différents objets. Par exemple le nom:

{C=Royaume-Uni; L=Winslow, O=Services graphiques, CN=Imprimante laser}

identifie l'entité d'application "imprimante laser" qui a, dans son nom distinctif, l'attribut géographique de la localité.

Le résidant John Jones, dont le nom est {C=Royaume-Uni; L=Winslow, CN=John Jones} a le même attribut géographique dans son nom distinctif.

La croissance et la forme de l'arbre DIT, la définition du schéma d'annuaire et la sélection des noms distinctifs pour des entrées, à mesure qu'elles sont ajoutées, relèvent de la compétence des diverses autorités, dont la relation hiérarchique est reflétée par la forme de l'arbre. Les autorités doivent s'assurer, par exemple, que toutes les entrées dépendant de leur juridiction ont des noms distinctifs non ambigus, en gérant minutieusement les types d'attributs et les valeurs qui apparaissent dans ces noms. La responsabilité est transmise, comme le montre l'arbre, des autorités supérieures aux autorités subordonnées, le contrôle étant exercé au moyen du schéma.

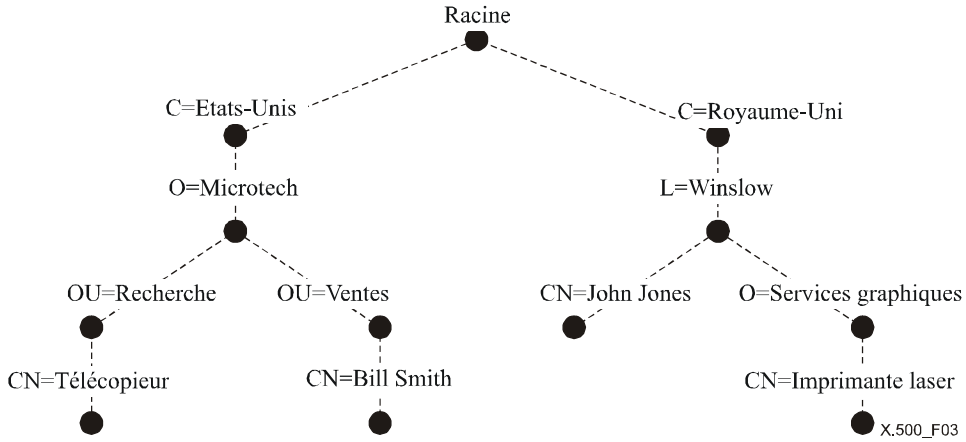

Figure 3 – Arbre hypothétique d'information de l'annuaire

La fonction de groupe hiérarchique permet de créer une autre relation hiérarchique entre les entrées, indépendamment de la relation hiérarchique reflétée par la structure de l'arbre DIT. L'opération de recherche dans l'annuaire (voir § 8.3.4.) peut restituer non seulement des informations provenant d'entrées mises en correspondance, mais aussi d'autres membres du groupe hiérarchique auquel peut appartenir l'entrée mise en correspondance. La fonction de groupe hiérarchique présente aussi l'avantage de pouvoir changer les relations hiérarchiques sans changer la structure de l'arbre DIT et donc les noms distinctifs des entrées.

8 Service d'annuaire

NOTE – La définition du service abstrait d'annuaire figure dans la Rec. UIT-T X.511 | ISO/CEI 9594-3.

8.1 Introduction

Le présent paragraphe donne un aperçu général du service qu'offre l'annuaire aux utilisateurs, représentés par leurs agents DUA et/ou leurs clients LDAP. Tous les services sont fournis par l'annuaire en réponse aux demandes provenant des agents DUA et/ou des clients LDAP. Il y a des demandes qui permettent l'interrogation de l'annuaire, comme décrit au § 8.3, et des demandes de modification comme décrit au § 8.4. De plus, les demandes de service peuvent être qualifiées, comme indiqué au § 8.2. L'annuaire indique toujours les résultats de chaque demande faite. La forme des résultats normaux est propre à chaque demande et est évidente d'après la description de la demande. La plupart des résultats anormaux sont communs à plusieurs réponses. Les possibilités sont décrites au § 8.5.

L'annuaire est conçu de façon que les modifications apportées à la base DIB, qu'elles soient le résultat d'une demande de service d'annuaire ou d'autres moyens (locaux), permettent à celle-ci de continuer à respecter les règles du schéma d'annuaire.

Un utilisateur et l'annuaire sont liés pendant un certain temps à un point d'accès à l'annuaire. Au moment où ils se lient, l'utilisateur et l'annuaire peuvent, en option, vérifier leur identité respective.

8.2 Qualification de service

8.2.1 Commandes de service

Diverses commandes peuvent être appliquées aux différentes demandes de service, avant tout pour permettre à l'utilisateur d'imposer à l'annuaire des limites à ne pas dépasser quant à l'utilisation des ressources, mais aussi pour contrôler la progression des opérations de l'annuaire. Des commandes sont notamment prévues concernant: la durée, l'ampleur des résultats, la portée de la recherche, les modes d'interaction et la priorité de la demande.

8.2.2 Paramètres de sécurité

Chaque demande peut être accompagnée d'informations fournies à l'appui des mécanismes de sécurité pour protéger l'information d'annuaire. Ces informations peuvent inclure: la demande de divers types de protection faite par l'utilisateur, une signature numérique de la demande ainsi que des informations pour aider l'entité concernée à vérifier la signature.

8.2.3 Filtres

Certaines demandes dont le résultat dépend d'informations provenant d'un certain nombre d'entrées ou les concernant, peuvent être accompagnées d'un ou de plusieurs filtres. Un filtre exprime une ou plusieurs conditions auxquelles une entrée ou une entrée composite doit satisfaire afin d'être retournée comme une partie du résultat. Cela permet de ne retourner que les entrées appropriées.

8.3 Interrogation de l'annuaire

8.3.1 Lecture

Une demande de lecture vise une entrée particulière ou une entrée composite et implique la restitution des valeurs de certains (ou de l'ensemble) des attributs de cette entrée. Dans le cas d'entrées composites, l'information des membres familiaux fait partie d'un ensemble (dont la syntaxe est analogue à celle d'un attribut) comprenant l'information de la famille sélectionnée. Lorsque seuls certains attributs doivent être retournés, l'agent DUA fournit la liste des types d'attributs en question dans le cadre de la demande. Un agent DUA peut aussi fournir un ou plusieurs contextes pour l'un au moins des types d'attributs en question, afin de sélectionner uniquement les valeurs qui s'appliquent dans les contextes spécifiés.

NOTE – Les clients LDAP ne prennent pas en charge l'opération de lecture.

8.3.2 Comparaison

Une demande de comparaison vise un attribut particulier d'une entrée donnée ou d'une entrée composite et oblige l'annuaire à vérifier si une valeur donnée correspond à une valeur de cet attribut. Un agent DUA peut aussi fournir un ou plusieurs contextes pour la valeur d'attribut en question afin d'imposer des contraintes à l'opération de comparaison.

NOTE – Par exemple, on peut l'utiliser pour vérifier un mot de passe dans le cas où ce dernier, qui figure dans l'annuaire, risque d'être inaccessible pour la lecture mais accessible pour la comparaison.

8.3.3 Listage

Une demande de listage oblige l'annuaire à restituer la liste des subordonnés immédiats d'une entrée désignée dans l'arbre DIT. Un agent DUA peut aussi fournir un ou plusieurs contextes en vue d'une sélection des contextes utilisés dans les noms RDN retournés.

NOTE – Les clients LDAP ne prennent pas en charge l'opération de listage.

8.3.4 Recherche

Une demande de recherche oblige l'annuaire à restituer les informations provenant de toutes les entrées ou de toutes les entrées composites dans une ou plusieurs parties de l'arbre DIT satisfaisant à certains filtres. Les informations provenant de chaque entrée comprennent une partie ou l'ensemble des attributs de cette entrée, comme pour la lecture. Les informations provenant d'entrées liées peuvent être combinées en fonction de certains critères d'association.

Il est possible d'imposer des restrictions aux types de recherches qui peuvent être effectuées en appliquant des règles de recherche. Il est aussi possible, comme le permettent ces règles, d'élargir ou de resserrer progressivement les recherches dans une seule opération de l'annuaire pour empêcher la restitution d'un nombre trop restreint ou au contraire trop important d'éléments d'information d'entrée.

8.3.5 Abandon

Une demande d'abandon, appliquée à une demande d'interrogation en instance informe l'annuaire que l'expéditeur de la demande ne désire plus qu'il soit donné suite à sa demande. L'annuaire peut, par exemple, arrêter le traitement de la demande et annuler les résultats déjà obtenus.

8.4 Modification de l'annuaire

8.4.1 Adjonction d'entrée

Une demande d'adjonction d'entrée entraîne l'adjonction à l'arbre DIT d'une nouvelle entrée feuille. Il est possible d'inclure des contextes avec les valeurs d'attribut associées à la nouvelle entrée.

8.4.2 Suppression d'entrée

Une demande de suppression d'entrée oblige à retirer l'entrée feuille de l'arbre DIT.

8.4.3 Modification d'entrée

Une demande de modification d'entrée oblige l'annuaire à apporter une série de modifications à une entrée ou à un membre familial donné. Il apporte soit toutes les modifications ou aucune modification et la base DIB reste toujours dans un état compatible avec le schéma. Les modifications autorisées comprennent l'adjonction, la suppression ou le remplacement d'attributs ou de valeurs d'attribut. Il est possible d'inclure des contextes avec les valeurs d'attribut qui sont ajoutées à l'entrée. Cette opération ne peut être utilisée que sur un seul membre familial, mais ne peut agir sur une entrée composite dans son ensemble.

Une opération de modification d'entrée peut, si nécessaire, fournir dans le résultat les informations contenues dans l'entrée simple ou composite après qu'une modification a été effectuée avec succès.

8.4.4 Modification du nom distinctif relatif

Une demande de modification du nom distinctif (DN, *distinguished name*) est utilisée pour modifier le nom distinctif relatif d'une entrée (entrée d'objet, entrée alias ou membre familial) ou pour déplacer une entrée vers une nouvelle entrée supérieure de l'arbre DIT. Si une entrée a des subordonnés, alors tous ceux-ci sont renommés ou déplacés de la même façon. Il est possible d'inclure des contextes dans le nouveau nom RDN de l'entrée. Dans le cas des membres familiaux, ceux-ci peuvent être déplacés de façon à avoir de nouveaux ascendants, à condition de rester dans la même entrée composite.

8.5 Autres résultats

8.5.1 Erreurs

Un service peut connaître une défaillance, par exemple en raison de problèmes posés par les paramètres fournis par l'utilisateur, auquel cas une erreur est signalée. L'information est retournée avec l'erreur, lorsque cela est possible, pour aider à résoudre le problème. Toutefois, seule la première erreur rencontrée par l'annuaire est en général signalée. En dehors de l'exemple mentionné ci-dessus concernant les problèmes que posent les paramètres fournis par l'utilisateur (en particulier les noms non valables pour les entrées ou les types d'attributs non valables), les erreurs peuvent provenir de violations des principes de sécurité, des règles de schéma et des contrôles de service.

8.5.2 Renvois

Un service peut échouer parce que le point d'accès auquel l'agent DUA ou le client LDAP est lié n'est pas celui qui convient le mieux pour exécuter la demande, par exemple du fait que l'information affectée par la demande est (d'un point de vue logique) très éloignée du point d'accès. En pareil cas, l'annuaire peut retourner un renvoi, qui suggère un point d'accès de remplacement auquel l'agent DUA ou le client LDAP peut faire sa demande.

NOTE – L'annuaire et l'agent DUA peuvent avoir chacun une préférence quant à l'utilisation des renvois ou au *chaînage* des demandes (voir § 9.3). L'agent DUA peut exprimer sa préférence au moyen de commandes de service. L'annuaire décide finalement de la solution à appliquer.

9 Annuaire réparti

NOTE – Les modèles d'annuaire sont définis dans la Rec. UIT-T X.501 | ISO/CEI 9594-2, alors que les procédures d'exploitation de l'annuaire réparti sont spécifiées dans la Rec. UIT-T X.518 | ISO/CEI 9594-4.

9.1 Modèle fonctionnel

Le modèle fonctionnel de l'annuaire est présenté à la Figure 4.

Un *agent de système d'annuaire (DSA)* est un processus d'application qui fait partie de l'annuaire et dont le rôle est d'assurer aux agents DUA, aux clients LDAP et/ou à d'autres agents DSA un accès à la base DIB. Un agent DSA peut utiliser les informations stockées dans sa base de données locale ou interagir avec d'autres agents DSA ou des serveurs LDAP pour exécuter des demandes. Par ailleurs, l'agent DSA peut diriger un demandeur vers un autre agent DSA qui peut aider à exécuter la demande. Un agent DSA capable d'émettre une demande LDAP et de comprendre la réponse LDAP associée est appelé demandeur LDAP. Un agent DSA capable de comprendre une demande LDAP et d'y répondre est appelé répondeur LDAP. Les bases de données locales dépendent entièrement de l'implémentation.

Un *serveur LDAP* est un processus d'application qui fait partie de l'annuaire, qui répond aux demandes en utilisant le protocole LDAP et dont le rôle est de fournir aux clients LDAP et/ou aux demandeurs LDAP un accès à la base DIB. Un serveur LDAP peut utiliser les informations stockées dans sa base de données locale ou peut diriger un demandeur vers un autre répondeur LDAP ou serveur LDAP qui peut aider à exécuter la demande. Comme dans le cas des agents DSA, les bases de données locales dépendent entièrement de l'implémentation.

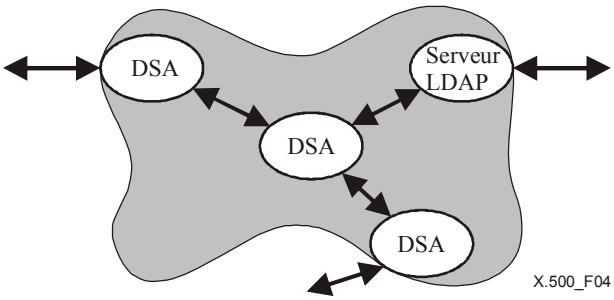

Figure 4 – Modèle fonctionnel de l'annuaire

9.2 Modèle organisationnel

Un ensemble comportant un ou plusieurs agents DSA et/ou serveurs LDAP et zéro, un ou plusieurs agents DUA et/ou clients LDAP gérés par une seule organisation peut former un domaine de gestion d'annuaire (DMD, *directory management domain*). L'organisation considérée peut choisir d'utiliser ou non les Spécifications d'annuaire pour régir les communications entre les éléments fonctionnels dans le domaine DMD.

Les autres Spécifications d'annuaire définissent certains aspects du comportement des agents DSA. A cet égard, un groupe d'agents DSA dans un domaine DMD peut, selon l'option de l'organisation qui dirige le domaine DMD, se comporter comme un agent DSA unique.

Un domaine DMD peut être un domaine de gestion d'annuaire d'administration (ADDMD) ou un domaine de gestion privé d'annuaire (PRDMD), selon qu'il est exploité ou non par une entreprise de télécommunication publique.

9.3 Fonctionnement du modèle

L'agent DUA ou le client LDAP interagit avec l'annuaire en communiquant avec un ou plusieurs agents DSA et/ou serveurs LDAP. Un agent DUA ou un client LDAP n'a pas besoin d'être lié à un agent DSA ou un serveur LDAP particulier. Il peut interagir directement avec divers agents DSA et/ou serveurs LDAP pour faire des demandes. Pour des raisons administratives, une interaction directe avec l'agent DSA ou le serveur LDAP qui a besoin d'exécuter la demande est parfois impossible, par exemple pour retourner des informations d'annuaire. Il se peut aussi que l'agent DUA ou le client LDAP accède à l'annuaire par le biais d'un agent DSA unique. A cette fin, une interaction entre agents DSA est nécessaire.

L'agent DSA est chargé d'exécuter les demandes des agents DUA et des clients LDAP et d'obtenir les informations nécessaires dont il ne dispose pas. Il peut prendre la responsabilité d'obtenir les informations en interagissant avec d'autres agents DSA et/ou serveurs LDAP pour le compte de l'agent DUA ou du client LDAP considéré.

Plusieurs cas de traitement de demandes ont été recensés et décrits ci-dessous (voir les Figures 5 à 7).

Sur la Figure 5a, l'agent DSA C reçoit un renvoi d'un agent DSA A et est chargé d'acheminer la demande directement à l'agent DSA B (désigné dans le renvoi de l'agent DSA A) ou d'acheminer le renvoi à l'agent DUA d'origine.

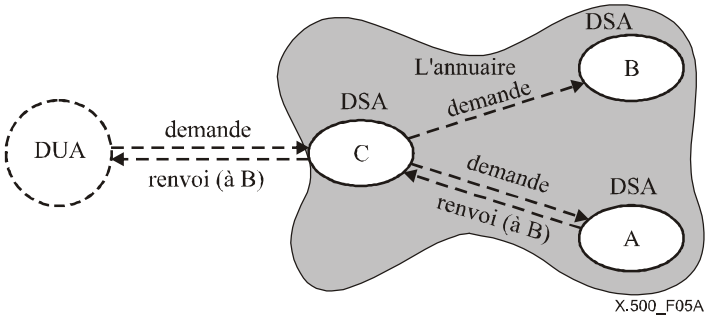

Figure 5a – Renvois

NOTE 1 – Si l'agent DSA C retourne le renvoi à l'agent DUA, la "demande (à B)" n'aura pas lieu. De même, si l'agent DSA C transmet la demande à l'agent DSA B, il ne retournera pas de renvoi à l'agent DUA.

Sur la Figure 5b, l'agent DSA C reçoit un renvoi de l'agent DSA A et est chargé d'acheminer la demande à l'agent DSA B (désigné dans le renvoi de l'agent DSA A) ou d'acheminer le renvoi au client LDAP d'origine.

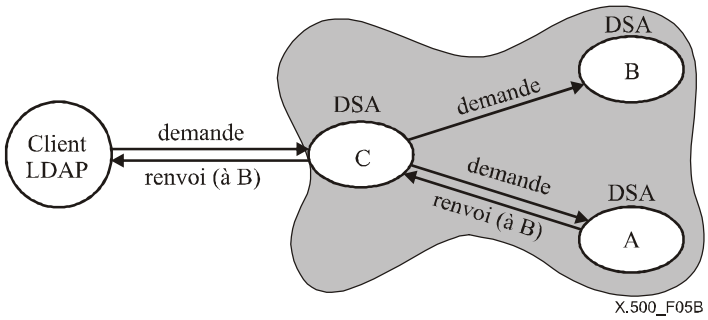

Figure 5b – Renvois

NOTE 2 – Outre sa capacité éventuelle à prendre en charge divers autres protocoles X.500, l'agent DSA C de la Figure 5b doit également être un répondeur LDAP.

NOTE 3 – Si l'agent DSA C retourne le renvoi au client LDAP, la "demande (à B)" n'aura pas lieu. De même, si l'agent DSA C achemine la demande à l'agent DSA B, il ne retournera pas de renvoi au client LDAP.

NOTE 4 – Si l'agent DSA C retourne le renvoi au client LDAP, ce renvoi doit avoir la forme d'un renvoi LDAP. Si le renvoi retourné par l'agent DSA A a la forme d'un renvoi LDAP, l'agent DSA C peut le retourner directement au client LDAP; dans le cas contraire, l'agent DSA C doit acheminer la demande à l'agent DSA B ou convertir le renvoi en un renvoi LDAP. Si l'agent DSA C retourne le renvoi au client LDAP, celui-ci se connectera directement à l'agent DSA B, qui doit également être un répondeur LDAP. L'agent DSA B devra également être un répondeur LDAP si l'agent DSA A retourne un renvoi LDAP et que l'agent DSA C achemine la demande directement à l'agent DSA B.

Sur la Figure 5c, l'agent DUA reçoit le renvoi de l'agent DSA C et est chargé de réémettre la demande directement à l'agent DSA A (désigné dans le renvoi de l'agent DSA C).

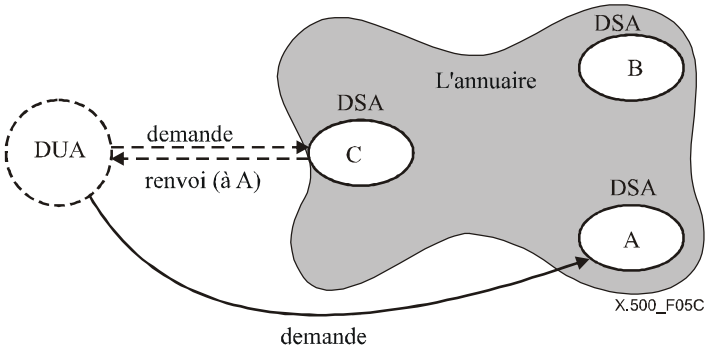

Figure 5c – Renvois

Sur la Figure 5d, le client LDAP reçoit le renvoi de l'agent DSA C et est chargé de réémettre la demande directement à l'agent DSA A (désigné dans le renvoi de l'agent DSA C).

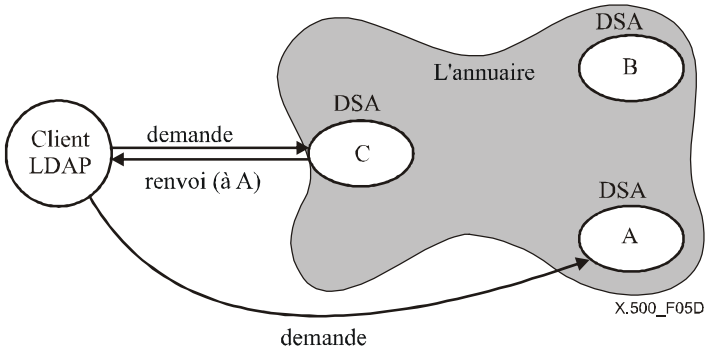

Figure 5d – Renvois

NOTE 5 – Les agents DSA A et DSA C de la Figure 5d doivent être des répondeurs LDAP. L'un d'eux pourrait également être un serveur LDAP.

NOTE 6 – Le renvoi retourné au client LDAP doit avoir la forme d'un renvoi LDAP.

Les Figures 6a à 6c illustrent le mécanisme de chaînage simple d'agents DSA, qui permet à la demande de passer par plusieurs agents DSA avant que la réponse soit envoyée.

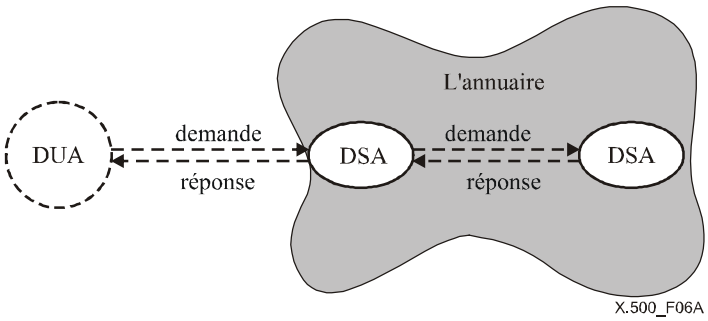

Figure 6a – Chaînage simple

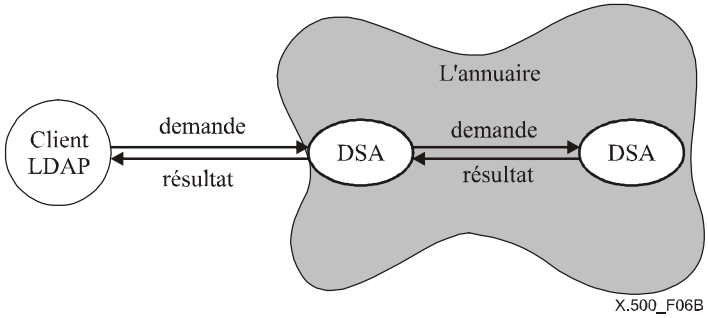

Figure 6b – Chaînage simple

NOTE 7 – Outre sa capacité éventuelle à prendre en charge divers autres protocoles X.500, l'agent DSA de gauche sur la Figure 6b doit également être un répondeur LDAP.

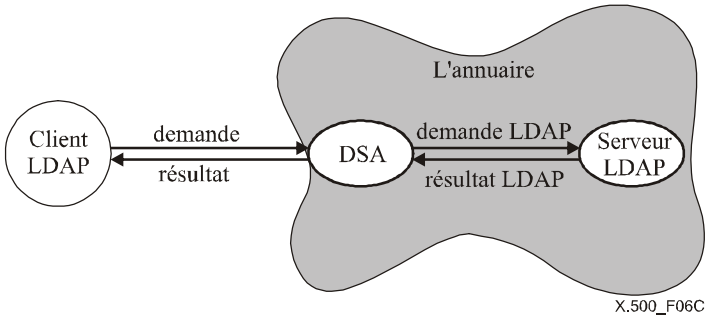

Figure 6c – Chaînage simple

NOTE 8 – Outre sa capacité éventuelle à prendre en charge divers autres protocoles X.500, l'agent DSA de la Figure 6c doit également être un répondeur LDAP et un demandeur LDAP.

Les Figures 7a à 7c illustrent le mécanisme de chaînage multiple, dans lequel l'agent DSA associé à l'agent DUA ou au client LDAP exécute la demande en la transmettant à au moins deux autres agents DSA et/ou serveurs LDAP, les demandes adressées à chaque agent DSA ou serveur LDAP étant identiques.

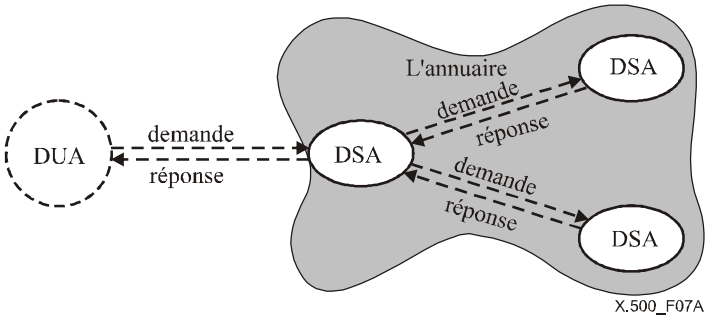

Figure 7a – Chaînage multiple

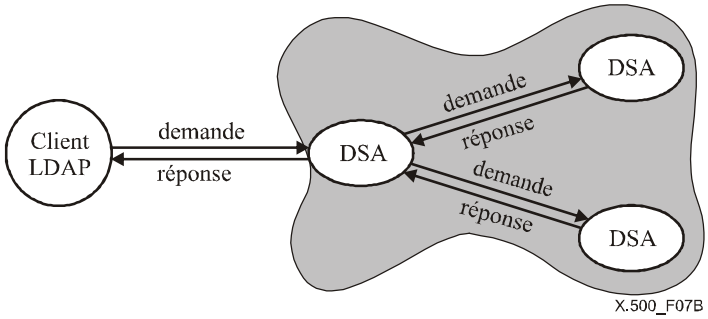

Figure 7b – Chaînage multiple

NOTE 9 – Outre sa capacité éventuelle à prendre en charge divers autres protocoles X.500, l'agent DSA de gauche sur la Figure 7b doit également être un répondeur LDAP.

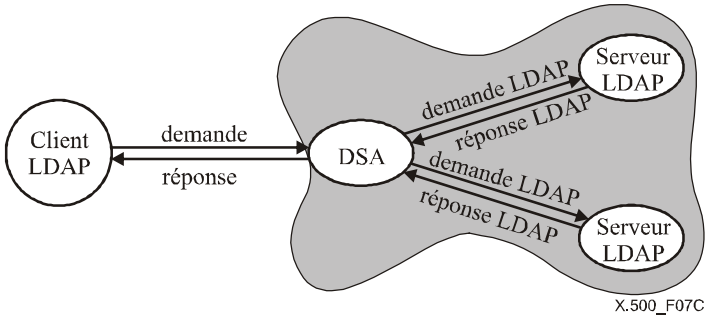

Figure 7c – Chaînage multiple

NOTE 10 – Outre sa capacité éventuelle à prendre en charge divers autres protocoles X.500, l'agent DSA de gauche sur la Figure 7c doit également être un répondeur LDAP et un demandeur LDAP.

Toutes les solutions ont leurs avantages. Par exemple, les mécanismes décrits sur les Figures 5b et 5d peuvent être utilisés lorsqu'il est souhaitable d'alléger la charge de l'agent DSA local. Dans d'autres cas, une solution hybride combinant un ensemble plus complexe d'interactions fonctionnelles peut être nécessaire pour satisfaire la demande de l'expéditeur, comme l'illustrent les Figures 8a et 8b.

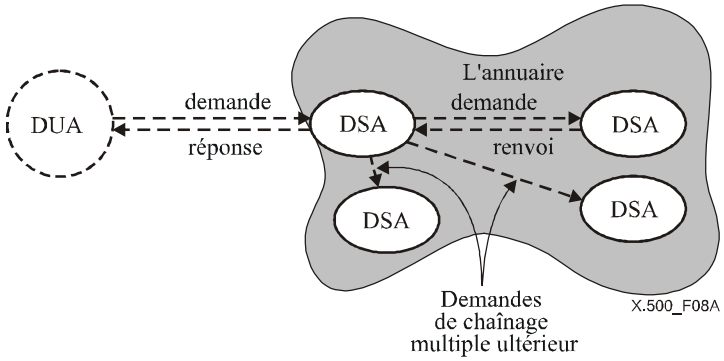

Figure 8a – Solutions hybrides à mode mixte

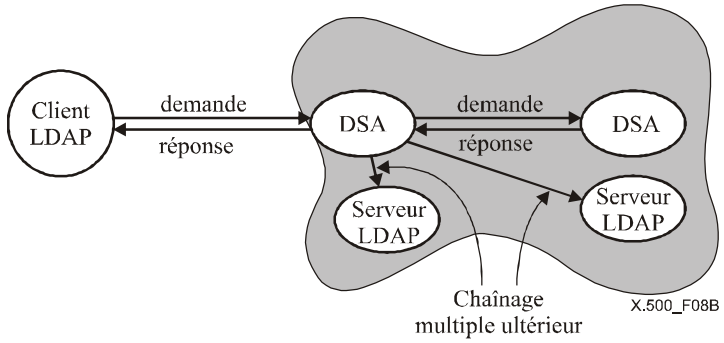

Figure 8b – Solutions hybrides à mode mixte

10 Contrôle d'accès aux informations contenues dans l'annuaire

NOTE – Le modèle de contrôle d'accès aux informations contenues dans l'annuaire est défini dans la Rec. UIT-T X.501 | ISO/CEI 9594-2.

L'accès aux informations contenues dans l'annuaire dépend de la politique de sécurité dont l'application est confiée aux autorités administratives. Cette politique comporte deux aspects qui influencent l'accès à l'annuaire, les procédures d'authentification et le système de contrôle d'accès.

Les procédures et les mécanismes d'authentification associés à l'annuaire intègrent des méthodes permettant de vérifier et de communiquer, le cas échéant, l'identité des agents DSA, l'identité des utilisateurs d'annuaire et l'origine des informations reçues en un point d'accès. Les procédures générales d'authentification sont définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

La définition du système de contrôle d'accès associé à l'annuaire intègre les méthodes de spécification de l'information de contrôle d'accès, l'exercice des droits d'accès définis par les informations de contrôle d'accès et de mise à jour de ces informations. L'exercice des droits d'accès englobe le contrôle d'accès aux informations contenues dans l'annuaire relatives à la structure de l'arbre DIT, des informations relatives aux utilisateurs de l'annuaire et des informations d'annuaire facultatives et notamment des informations de contrôle d'accès.

La Rec. UIT-T X.501 | ISO/CEI 9594-2 définit un modèle de contrôle d'accès particulier (parmi de nombreux autres possibles) appelé "contrôle d'accès de base" pour l'annuaire. Les autorités administratives peuvent utiliser tout ou partie de ce modèle pour appliquer leurs politiques de sécurité, elles peuvent aussi définir librement leurs propres systèmes. Ce modèle permet de contrôler l'accès aux informations contenues dans l'annuaire dans la base d'informations d'annuaire (DIB) (qui peut contenir des informations de structure et d'accès). Le contrôle d'accès aux informations permet d'éviter la détection, la révélation ou la modification de ces informations par des entités non autorisées.

Le contrôle d'accès aux informations permet d'éviter la détection, la divulgation ou la modification de ces informations par des entités non autorisées. La Rec. UIT-T X.501 | ISO/CEI 9594-2 définit trois modèles de contrôle d'accès particuliers pour l'annuaire, appelés "contrôle d'accès de base", "contrôle d'accès simplifié" et "contrôle d'accès fondé sur des règles". Les autorités administratives peuvent utiliser tout ou partie de ces modèles pour appliquer leurs politiques de sécurité, elles peuvent aussi définir librement leurs propres systèmes. Le modèle du contrôle d'accès de base permet de contrôler l'accès aux informations d'annuaire figurant dans la base d'informations d'annuaire (DIB) (qui peut contenir des informations de structure et d'accès). Le modèle du contrôle d'accès simplifié intègre un

sous-ensemble des fonctionnalités du modèle du contrôle d'accès de base. Le modèle du contrôle d'accès fondé sur des règles intègre des moyens supplémentaires permettant de contrôler l'accès aux informations d'annuaire figurant dans la base DIB (qui peut contenir des informations de structure et d'accès), ce modèle utilise des habilitations et des étiquettes. Ce modèle peut soit être utilisé seul, soit être utilisé conjointement avec l'un des autres modèles (de contrôle d'accès simplifié et de contrôle d'accès de base).

Le modèle d'accès de base à l'annuaire définit, pour chaque opération, un ou plusieurs points où des décisions peuvent être prises concernant le contrôle d'accès. Chaque décision fait intervenir :

- la composante dans l'annuaire à laquelle on accède, éventuellement une entrée composite complète;
- l'utilisateur demandeur de l'opération;
- un droit spécifique nécessaire à l'exécution d'une partie de l'opération;
- la politique de sécurité qui régit l'accès à l'élément en question.

Le modèle d'accès à l'annuaire fondé sur des règles définit, pour chaque opération, un ou plusieurs points où des décisions peuvent être prises concernant le contrôle d'accès. Chaque décision fait intervenir:

- une habilitation associée à l'utilisateur demandant un accès;
- une ou plusieurs étiquettes de sécurité associées aux informations auxquelles on accède;
- les règles de politique de sécurité qui régissent cet accès et qui permettent de déterminer si l'accès doit être refusé, sur la base d'une relation entre l'habilitation et l'étiquette de sécurité.

11 Administration du service

Le service abstrait d'annuaire, tel qu'il est défini dans la Rec. UIT-T X.501 | ISO/CEI 9594-2, fournit à l'utilisateur des moyens puissants et efficaces de navigation et de lecture concernant les informations d'annuaire.

Les présentes spécifications concernant l'annuaire offrent de nombreuses capacités d'administration du service qui permettent à des autorités administratives de dispenser et de limiter le service destiné à un utilisateur. L'autorité administrative peut avoir plusieurs raisons de limiter et d'adapter le service fourni à un utilisateur:

- l'autorité administrative connaît la qualité des informations qu'elle détient. Pour améliorer le taux de recherches fructueuses dans l'annuaire et s'assurer que seules les informations de qualité sont restituées, l'autorité administrative peut limiter les types d'attribut qui sont autorisés dans un filtre de recherche et les informations qui peuvent être restituées;
- pour protéger les ressources investies dans les informations vérifiées et corrigées, l'autorité administrative peut imposer des restrictions assez strictes sur les informations qui peuvent être restituées car elles sont adaptées au type d'utilisateur et au type particulier de service fourni;
- l'autorité administrative peut vouloir empêcher un mauvais usage de l'information, par exemple à des fins de commercialisation de masse (en sélectionnant toutes les personnes vivant dans une rue donnée ou toutes les personnes ayant une profession donnée, etc.);
- l'autorité administrative peut vouloir protéger les données personnelles au-delà de ce qui est possible avec le contrôle d'accès. Il peut s'agir notamment de renvoyer les adresses postales erronées, de ne pas autoriser les recherches effectuées à partir de chaînes de caractères très courtes, de ne pas autoriser les recherches utilisant certaines combinaisons d'attribut ou nécessitant certaines combinaisons, etc.;
- le type de restriction ou d'adaptation qui devrait être apporté au service fourni peut dépendre du groupe d'utilisateurs.

12 Duplication d'annuaire

NOTE – La duplication d'annuaire est définie dans la Rec. UIT-T X.525 | ISO/CEI 9594-9.

12.1 Introduction

Par duplication d'annuaire, on entend des copies d'informations d'entrée d'annuaire et des informations d'exploitation détenues par des agents DSA autres que l'agent DSA responsable de la création et de la mise à jour des informations. L'agent DSA qui contient les informations d'origine est appelé l'agent DSA maître.

Il est possible d'établir des systèmes d'annuaire qui n'utilisent pas d'informations dupliquées.

La duplication d'informations d'annuaire sert à répondre à deux types généraux de besoins: l'un concerne la qualité générale du service offert par l'annuaire et l'autre la gestion-systèmes d'annuaire.

L'utilisation de copies supplémentaires d'informations d'entrée d'annuaire peut permettre d'améliorer le service offert par l'annuaire:

a) elle peut améliorer la performance des systèmes d'annuaire en "rapprochant" les informations d'annuaire des différents utilisateurs d'annuaire;

b) elle peut améliorer la disponibilité du service d'annuaire en introduisant des informations d'annuaire et des composantes d'annuaire redondantes de façon que la défaillance d'une composante n'empêche aucun accès à l'information dans une partie de l'arbre DIT.

L'utilisation de copies supplémentaires d'informations d'entrée d'annuaire peut être utile dans la gestion-systèmes d'annuaire:

a) elle facilite la distribution de certaines informations d'exploitation (par exemple connaissances);

b) elle offre une possibilité de rétablissement à la suite de pannes sérieuses du système; en effet, elle permet de reconstituer les informations qui doivent figurer dans une composante de l'annuaire à partir d'une copie de ces informations, consignée dans une autre composante de l'annuaire.

12.2 Formes de duplication d'annuaire

Trois formes d'informations d'entrée dupliquées peuvent être détenues par les composantes de l'annuaire: les copies caches, les informations miroirs et les implémentations de plusieurs maîtres.

Les copies caches sont des copies d'informations d'entrée qu'une composante de l'annuaire obtient et utilise d'une façon qui n'est pas définie dans les Spécifications d'annuaire.

Les copies miroirs sont des copies d'informations d'annuaire qu'une composante de l'annuaire obtient et utilise d'une façon définie dans la Rec. UIT-T X.525 | ISO/CEI 9594-9.

Les implémentations de plusieurs maîtres conservent plusieurs instances inscriptibles de chaque entrée au sein d'un ensemble donné d'entrées d'annuaire. Chaque copie inscriptible d'une entrée d'annuaire est complète (elle comprend l'ensemble des attributs d'utilisateur et des attributs opérationnels partagés entre agents DSA). Exactement une de ces instances est identifiée de manière telle que l'annuaire puisse l'identifier comme étant l'instance principale et ce, afin de prendre en charge des scénarios de déploiement dans lesquels les mises à jour doivent être exécutées par rapport à un agent DSA unique (par exemple lorsqu'il s'agit d'incrémenter une valeur d'attribut utilisée en tant que compteur). La façon dont une composante d'annuaire obtient les copies inscriptibles d'une entrée et la cohérence entre copies inscriptibles est assurée après une modification ne relève pas de la présente spécification.

Les agents DSA ne peuvent conserver les informations obtenues d'un autre agent DUA que si cela est permis par la politique et les accords en vertu desquels les informations ont été initialement fournies. L'agent DSA détenteur de ces informations ne peut les fournir à des agents DUA et/ou à des clients LDAP que s'ils respectent la politique de contrôle d'accès à ces informations. Si l'on sait qu'il n'existe pas de contrôle d'accès en lecture à ces informations, celles-ci peuvent être fournies comme si l'autorisation de lecture avait été accordée.

Un agent DSA qui détient des informations caches ou miroirs transmet à l'agent DSA maître qui détient les informations toutes les demandes susceptibles de modifier les informations copiées. Un agent DSA qui détient des informations copiées transmet à l'agent DSA maître qui détient les informations toutes les demandes indiquant que ces informations copiées ne doivent pas être utilisées.

Lorsqu'il répond à une interrogation à l'aide d'informations copiées caches ou miroirs, l'agent DSA qui détient ces informations indique qu'une copie a été utilisée pour répondre à la demande.

Les autorités administratives responsables de deux agents DSA peuvent établir un accord de duplication d'informations miroirs en vertu duquel un agent DSA fournisseur d'informations miroirs s'engage à fournir à un autre agent DSA, consommateur d'informations miroirs, des informations miroirs d'une partie convenue de l'arbre DIT. Si l'accord de duplication d'informations miroirs utilisé pour l'obtention des informations miroirs l'y autorise, le consommateur d'informations miroirs peut conclure des accords avec d'autres agents DSA pour être fournisseur de copies pour les informations en question.

Outre les mises à jour de copies d'informations d'entrée détenues par le consommateur d'informations miroirs, des informations d'exploitation (par exemple des connaissances) peuvent aussi être fournies au consommateur d'information miroir par le fournisseur d'informations miroirs.

Quel que soit l'accord de duplication d'informations miroirs, les informations à dupliquer comprendront généralement trois éléments:

- les informations d'entrée dupliquées provenant d'un sous-arbre de l'arbre DIT;
- les informations opérationnelles associées dont celles relatives au contrôle d'accès, nécessaires pour assurer un accès total en lecture des informations dupliquées;
- à titre facultatif, des informations de connaissance subordonnées.

Les informations dupliquées peuvent former un sous-ensemble des informations complètes contenues dans le sous-arbre pour les raisons suivantes:

- on peut sélectionner les entrées en spécifiant seulement celles qui répondent à certains critères concernant leurs classes d'objets;
- dans chaque entrée, on peut sélectionner les attributs conformément à une spécification d'attributs;
- dans chaque attribut, on peut sélectionner les valeurs d'attribut sur la base de leurs contextes.

12.3 Duplication et cohérence des informations d'annuaire

Dans l'annuaire, la cohérence est assurée lorsque toutes les copies d'un attribut spécifique sont les mêmes. Parfois, pour assurer la cohérence, il peut être nécessaire d'avoir recours à des compromis car il peut y avoir dans l'annuaire des incohérences transitoires pour les informations miroirs et des incohérences permanentes pour des informations caches.

Les informations caches d'entrée peuvent devenir incohérentes et le rester par rapport aux informations actualisées par la composante de l'annuaire vers laquelle les mises à jour sont adressées. En revanche, les informations détenues par un consommateur d'informations miroirs sont rendues conformes avec les informations détenues par un fournisseur d'informations miroirs selon un programme inclus dans l'accord de duplication des informations miroirs.

Il est indispensable que les informations contenues dans une instance d'une entrée simple d'objet soient intrinsèquement cohérentes. Tout mécanisme de duplication sera accompagné de mécanismes destinés à garantir la cohérence interne des informations dupliquées et la fiabilité du service. L'annuaire définit les procédures de schémas permettant d'assurer la cohérence interne de chaque entrée.

Il est aussi indispensable que les informations de connaissance qui permettent à l'arbre DIT d'être réparti entre les agents DSA soient précises. Tout mécanisme de duplication doit être accompagné de mécanismes permettant de garantir l'exactitude des informations de connaissance et la fiabilité du service. L'annuaire définit des procédures prévoyant la manipulation des informations de connaissance minimales dont a besoin un agent DSA pour garantir la cohérence de chaque représentation de l'arbre DIT.

Lorsque les informations d'annuaire sont dupliquées, l'annuaire n'a pas de contraintes de temps précises pour parvenir à assurer la cohérence des informations. L'utilisateur d'informations miroirs aura confiance en ces informations pour les raisons suivantes:

- les informations miroirs sont intrinsèquement cohérentes;
- les connaissances qui les lient à sa représentation de l'arbre DIT sont précises;
- il y aura finalement cohérence entre l'entrée d'informations miroirs et l'entrée inscrite dans l'agent DSA maître.

12.4 Points de vue sur la duplication

Le présent paragraphe décrit les différentes façons dont se présente la duplication d'informations d'annuaire pour:

a) les utilisateurs de l'annuaire;

b) les utilisateurs administratifs;

c) les composantes d'exploitation de l'annuaire (agents DSA).

12.4.1 Point de vue de l'utilisateur de l'annuaire

Compte tenu de la nature de l'exploitation de l'annuaire, les informations dupliquées correspondront généralement aux informations détenues par l'agent DSA maître. En règle générale, les informations demandées, qui seront renvoyées à l'utilisateur final, seront donc acceptables et le fait qu'elles proviennent d'une copie ne sera pas important.

Il est toujours indiqué à l'utilisateur de l'annuaire s'il a été répondu à une demande par une information de copie d'entrée. Si l'utilisateur a besoin d'urgence d'informations, ou s'il peut détecter une incohérence, il a la possibilité de demander d'accéder aux informations détenues par l'agent DSA maître.

L'utilisateur de l'annuaire peut donc choisir entre recevoir parfois des informations qui ne sont pas à jour mais bénéficier d'une meilleure performance et d'une plus grande disponibilité ou de recevoir des informations très exactes mais ne disposer que d'une performance et d'une disponibilité parfois limitées.

12.4.2 Point de vue de l'utilisateur administratif

Un utilisateur administratif est chargé de gérer les informations détenues et le service offert par un agent DSA. Pour s'acquitter de cette fonction de gestion, il a besoin d'outils lui permettant de surveiller, de commander et d'optimiser le service de l'agent DSA.

La duplication, qui est une fonction normalisée (et locale) d'un agent DSA, est un des principaux outils mis à la disposition de l'utilisateur administratif pour optimiser le service fourni par un agent DSA.

12.4.3 Point de vue de l'agent DSA

Bien qu'un agent DSA puisse déceler la différence entre les informations dupliquées et les informations détenues par un maître, il utilise généralement ces deux types d'informations de la même façon, c'est-à-dire qu'il répond aux demandes de l'utilisateur par l'une ou l'autre de ces informations, selon ce qui convient le mieux.

Les informations maître et dupliquées sont équivalentes sauf dans deux cas: un agent DSA n'utilise que des informations d'entrée pour répondre à des demandes visant à modifier la base DIB et à des demandes d'interrogation qui signalent que les informations dupliquées ne sont pas acceptables.

De plus, étant donné que les informations détenues au niveau local peuvent être partielles (voir § 12.2), un agent DSA peut transmettre une demande à un autre agent DSA plus apte à fournir les informations demandées.

NOTE – Un agent DSA peut contenir des informations dupliquées depuis plusieurs sources, et ces informations peuvent faire double emploi. Si c'est le cas, l'agent DSA conservera séparément chacune de ces représentations de l'information telles qu'elles ont été dupliquées.

12.5 Duplication et contrôle d'accès

Le modèle de contrôle d'accès permet de spécifier les informations de contrôle d'accès pour un domaine de l'arbre DIT. Ce domaine peut dépasser les limites de l'agent DSA. Si plusieurs agents DSA interviennent, chacun détiendra les informations de contrôle d'accès appropriées.

Chaque fois que des entrées sont dupliquées pour un autre agent DSA, les informations de contrôle d'accès doivent aussi être dupliquées.

13 Protocoles d'annuaire

NOTE – Les protocoles d'annuaire définis pour permettre aux agents DUA et DSA de coopérer dans un système ouvert différent sont spécifiés dans la Rec. UIT-T X.519 | ISO/CEI 9594-5.

Il existe quatre protocoles d'annuaire:

- le protocole d'accès à l'annuaire (DAP, *directory access protocol*), qui définit l'échange de demandes et de réponses entre un agent DUA et un agent DSA;
- le protocole du système d'annuaire (DSP, *directory system protocol*), qui définit l'échange de demandes et de réponses entre deux agents DSA;
- le protocole de duplication miroir d'informations de l'annuaire (DISP, *directory information shadowing protocol*), qui définit l'échange des informations copiées entre deux agents DSA qui ont conclu des accords de duplication des informations miroirs;
- le protocole de gestion des liens opérationnels d'annuaire (DOP, *directory operational binding management protocol*), qui définit l'échange des informations administratives entre deux agents DSA permettant de gérer les liens opérationnels entre eux.

Chaque protocole est défini comme un ensemble d'éléments de protocole. Par exemple, le protocole DAP contient des éléments de protocole associés à l'interrogation et à la modification de l'annuaire.

14 Gestion-systèmes de l'annuaire

NOTE – La gestion-systèmes de l'annuaire est définie dans la Rec. UIT-T X.530 | ISO/CEI 9594-10.

14.1 Introduction

Le but de la gestion de l'annuaire est d'assurer que les informations contenues dans l'annuaire précises et nécessaires soient mises à disposition des utilisateurs dans les délais de réponse prévus et avec l'intégrité, la sécurité et le niveau de cohérence attendus. De plus, la gestion-systèmes doit être réalisée avec une incidence minimale sur le temps de traitement et la mémoire au niveau des plates-formes et du système de communication.

La gestion de l'annuaire est divisée en quatre segments principaux:

a) la gestion du domaine de l'arbre DIT: gestion des informations contenues dans l'annuaire;

b) la gestion de l'opération d'un seul agent DSA;

c) la gestion d'un seul agent DUA;

d) la gestion du domaine DMD: gestion intégrée des composantes fonctionnelles de l'annuaire.

La spécification sur la gestion-systèmes traite des trois premiers segments. La gestion du domaine de gestion d'annuaire (DMD) appelle un complément d'étude.

14.2 Gestion du domaine de l'arbre DIT

Les attributs d'utilisateur figurant dans l'annuaire sont gérés par le protocole d'accès à l'annuaire (DAP). Les attributs opérationnels peuvent aussi être gérés par ce protocole. Ces attributs comprennent les attributs associés aux informations, les attributs de sous-schéma, les attributs de contrôle d'accès et les attributs associés à l'arbre d'information de l'agent DSA, y compris les connaissances. Les connaissances peuvent aussi être gérées au moyen du protocole de gestion des liens opérationnels d'annuaire, du protocole de duplication miroir des informations de l'annuaire et du protocole du système d'annuaire.

14.3 Gestion des composantes de l'annuaire

La spécification sur la gestion-systèmes contient la définition des objets gérés de la gestion-systèmes OSI, objets servant à la gestion des composantes de l'annuaire (agents DUA et DSA) dans un domaine de l'annuaire. La gestion de ces composantes de l'annuaire peut être réalisée au moyen du protocole et des services communs d'informations de gestion.

Certaines prescriptions relatives à la gestion ne sont respectées ni par l'annuaire ni par les services de gestion mais sont respectées par des services définis localement.

Annexe A

Application de l'annuaire

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

A.1 L'environnement de l'annuaire

NOTE – Dans le présent paragraphe, le terme *réseau* est utilisé dans un sens général pour indiquer l'ensemble des systèmes reliés et des processus concernant tout service de télécommunication et non un seul système ou processus lié à la couche Réseau OSI.

L'environnement dans lequel l'annuaire offre des services est le suivant:

a) de nombreux réseaux de télécommunication seront établis à grande échelle et subiront constamment des changements:

   1) des objets de divers types entreront, seuls ou en groupe, dans le réseau et le quitteront, sans avertissement;

   2) la connectivité des objets (en particulier des nœuds de réseau) changera, en raison de l'adjonction ou de la suppression de trajets entre ces objets;

   3) les diverses caractéristiques des objets, telles que leurs adresses, leur disponibilité et leurs emplacements physiques, peuvent changer à tout moment;

b) bien que les changements soient fréquents, la durée de vie utile d'un objet donné n'est pas courte. Un objet interviendra beaucoup plus souvent dans les communications qu'il ne changera d'adresse, de disponibilité, d'emplacement physique, etc.;

c) les objets qui interviennent dans les services de télécommunication actuels sont généralement identifiés par des numéros ou d'autres chaînes de symboles, choisis pour leur facilité d'attribution ou de traitement mais pas pour leur facilité d'utilisation par des personnes.

A.2 Caractéristiques du service d'annuaire

Les capacités d'annuaire sont nécessaires pour les raisons suivantes:

a) le désir d'isoler (autant que possible) l'utilisateur du réseau des changements fréquents apportés à ce dernier. Pour ce faire, on peut prévoir une "zone de flou" entre les utilisateurs et les objets avec lesquels ils traitent. Cela signifie que les utilisateurs se réfèrent aux objets par leur nom et non, par exemple, par l'adresse. L'annuaire assure le service de mappage nécessaire;

b) le désir de donner l'image d'un réseau plus facile à utiliser. Par exemple, l'utilisation d'alias, la mise à disposition des *pages jaunes* (voir § A.3.5), etc., facilitent la recherche et l'utilisation d'informations de réseau.

L'annuaire permet aux utilisateurs d'obtenir diverses informations sur le réseau et prévoit la maintenance, la distribution et la sécurité de cette information.

A.3 Schémas d'utilisation de l'annuaire

NOTE – Le présent paragraphe concerne uniquement la recherche dans l'annuaire: on suppose que les services de modification d'annuaire ne servent qu'à maintenir la base DIB dans la forme nécessaire à l'application dans le temps.

A.3.1 Introduction

Le service d'annuaire est défini dans les Spécifications d'annuaire en termes de demandes particulières qu'un agent DUA peut formuler et de paramètres correspondants. Toutefois, un concepteur d'application pensera vraisemblablement en termes plus orientés vers des objectifs, lorsqu'il étudiera les besoins de recherche d'informations pour l'utilisation de l'annuaire dans cette application. En conséquence, le présent paragraphe décrit un certain nombre de schémas de haut niveau d'utilisation du service d'annuaire, qui sont susceptibles de convenir pour de nombreuses applications.

A.3.2 Recherche

La recherche directe dans l'annuaire fait intervenir l'agent DUA qui fournit le nom distinctif d'un objet, ainsi qu'un type d'attribut. L'annuaire renverra une ou plusieurs valeurs correspondant à ce type d'attribut. Il s'agit d'une généralisation de la fonction d'annuaire classique, que l'on obtient lorsque le type d'attribut demandé correspond à un type particulier d'adresse. Les types d'attributs pour divers types d'adresses sont normalisés, y compris l'adresse OSI du point PSAP (point d'accès au service de couche Présentation) l'adresse O/R de traitement de message et les numéros de téléphone et télex.

La recherche est assurée par le service de lecture, qui fournit aussi les autres généralisations suivantes:

- la recherche peut être fondée sur des noms autres que le nom distinctif de l'objet, par exemple des alias;
- les valeurs provenant d'un nombre de types d'attributs peuvent être obtenues par une simple demande: le cas extrême étant qu'il faille retourner les valeurs de tous les attributs dans l'entrée;
- des valeurs particulières d'un attribut peuvent être demandées sur la base d'un contexte (par exemple la valeur en français d'un nom d'organisation).

A.3.3 Dénomination facile à utiliser

On peut donner aux objets des noms que les utilisateurs puissent trouver (ou mémoriser) facilement. Les noms de ce type seront composés généralement d'attributs qui sont en quelque sorte inhérents à l'objet et non fabriqués à cette fin. Le nom d'un objet sera commun à toutes les applications qui s'y rapportent.

A.3.4 Navigation

Dans de nombreuses utilisations de annuaire conçues pour les individus, il se peut que l'utilisateur (ou l'agent DUA) ne puisse pas citer directement un nom, facile à utiliser ou non, concernant l'objet sur lequel il recherche des informations. Toutefois, l'utilisateur le reconnaîtra peut-être lorsqu'il le verra. La navigation permettra à l'utilisateur de parcourir la base DIB pour rechercher les entrées appropriées.

La navigation est une combinaison des services de listage et de recherche, assurée éventuellement en conjonction avec la lecture (bien que le service de recherche offre la capacité de lecture).

A.3.5 Pages jaunes

Il y a différentes façons d'assurer une capacité de type *pages jaunes*. La plus simple est fondée sur le filtrage et utilise des assertions sur des attributs particuliers dont les valeurs sont les catégories (par exemple le type d'attribut "catégorie affaires" défini dans la Rec. UIT-T X.520 | ISO/CEI 9594-6). Cette méthode ne nécessite pas l'établissement dans l'arbre DIT des informations spéciales, sauf pour s'assurer que les attributs requis sont présents. Toutefois, il peut en général être onéreux de faire des recherches s'il y a une vaste population car le filtrage nécessite la création de l'ensemble universel qui doit être filtré.

Une autre méthode est possible; elle est fondée sur l'établissement de sous-arbres spéciaux, dont les structures de dénomination sont conçues spécialement pour la recherche de type *pages jaunes*. La Figure A.1 donne un exemple de sous-arbre *pages jaunes* peuplé d'entrées alias uniquement. En réalité, les entrées dans les sous-arbres *pages jaunes* peuvent être un mélange d'entrées d'objet et d'entrées d'alias, du moment qu'il n'existe qu'une entrée d'objet pour chaque objet enregistré dans l'annuaire.

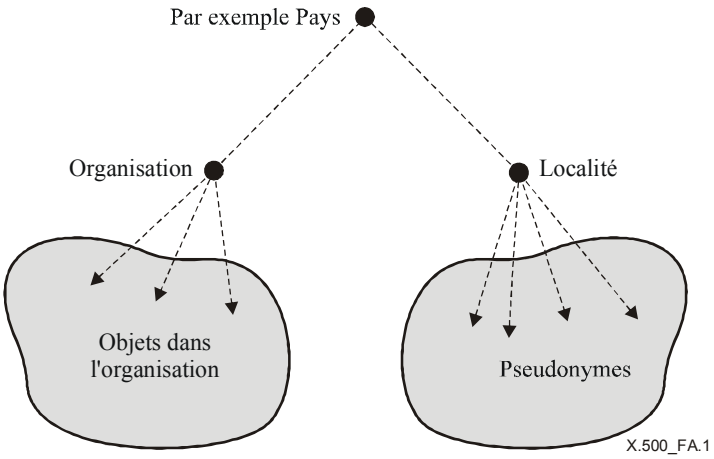

Figure A.1 – Méthode concernant les pages jaunes

A.3.6 Mesures visant à resserrer et à élargir les recherches

Dans de nombreuses consultations, après une première tentative de recherche, il arrive que l'on obtienne trop peu ou beaucoup trop d'informations. L'annuaire contient des dispositions permettant "d'élargir" la recherche de manière à offrir de meilleures chances de réussite (par exemple, lancement automatique d'une deuxième série de recherches établissant une correspondance phonétique plutôt qu'une correspondance stricte des chaînes de caractères) ou de la "resserrer", de façon à réduire le nombre d'occurrences. L'annuaire permet aussi de remplacer la règle de correspondance type qui s'applique généralement par une règle de correspondance plus appropriée applicable au niveau local.

Par exemple, au lieu d'une règle de correspondance des chaînes de caractères, on peut utiliser une règle de correspondance géographique pour faire correspondre une localité avec une autre localité enregistrée dans l'annuaire. Il est possible de combiner les deux règles: si la correspondance géographique stricte ne permet pas d'obtenir de résultats (il n'y a pas de correspondance entre "Warfield" et "Bracknell"), l'application d'une correspondance élargie pourrait réussir (il pourrait maintenant y avoir correspondance "Warfield" et "Bracknell" si la recherche élargie englobe Bracknell et les villages des environs immédiats, dont Warfield).

On peut aussi appliquer de telles mesures pour élargir les recherches dans les *Pages jaunes*: ainsi, une catégorie plus générique peut être remplacée par une catégorie plus spécifique. Ainsi, le mot "Restaurants" en tant que chaîne de caractères ne correspond pas en général à "Restaurants chinois" mais on peut obtenir ce résultat par substitution ou élargissement de la règle de correspondance.

A.3.7 Groupes

Un groupe est un ensemble dont les membres peuvent changer avec le temps par adjonction et suppression explicites de membres. Le groupe est un objet, tout comme ses membres. Il peut être demandé à l'annuaire:

- d'indiquer si un objet particulier est membre ou non d'un groupe;
- de donner la liste des membres d'un groupe.

Les groupes sont admis de la façon suivante: l'entrée contient un attribut "membre" à valeurs multiples (ce type d'attribut est défini dans la Rec. UIT-T X.520 | ISO/CEI 9594-6). Les deux capacités mentionnées peuvent être appliquées respectivement par comparaison et par lecture.

Un membre d'un groupe pourrait lui-même être un groupe si cela est important pour l'application. Toutefois, les services de vérification et d'expansion récurrents nécessaires devront être créés par l'agent DUA en dehors des versions non récurrentes fournies.

A.3.8 Authentification

Dans de nombreuses applications, il faut que les objets qui y participent donnent une preuve de leur identité avant d'être autorisés à effectuer une action. L'annuaire aide à assurer ce processus d'authentification. (Indépendamment de cela, l'annuaire demande à ses utilisateurs de s'authentifier eux-mêmes, de façon à assurer le contrôle d'accès.)

Dans la méthode d'authentification la plus directe, appelée "authentification simple", l'annuaire contient un attribut "mot de passe d'utilisateur" dans l'entrée pour tout utilisateur qui désire s'authentifier auprès d'un service. A la demande du service, l'annuaire confirmera ou niera qu'une valeur particulière fournie est (soit) réellement le mot de passe d'un utilisateur. Cela évite à celui-ci d'avoir besoin d'un mot de passe différent pour chaque service. Dans les cas où l'échange des mots de passe dans un contexte local qui repose sur une authentification simple est jugé non approprié, l'annuaire fournit en option des moyens de protéger ces mots de passe contre une réutilisation ou une utilisation erronée, par une fonction à sens unique.

La méthode la plus complexe, appelée "authentification renforcée" est fondée sur une cryptographie à clé publique, dans laquelle l'annuaire agit comme un dépôt des clés de chiffrement publiques des utilisateurs, convenablement protégées contre la fraude. Les étapes que les utilisateurs peuvent suivre pour obtenir les clés publiques des uns et des autres à partir de l'annuaire, puis authentifier ceux qui les utilisent, sont décrites en détail dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

A.3.9 Localisation fondée sur des attributs

Dans de nombreuses applications, il faut pouvoir déterminer rapidement s'il existe des entrées contenant une valeur d'attribut donnée et, dans l'affirmative, il faut pouvoir les trouver et les extraire rapidement. Ceci peut se faire de manière simple dans le cas d'un annuaire ne contenant qu'un seul agent DSA. En revanche, dans le cas d'un annuaire réparti, une recherche fondée sur des attributs peut être problématique dans le sens où la valeur limite supérieure du temps de recherche peut être difficile à contrôler.

Il existe une solution relativement simple à ce problème dans le cas d'un environnement dont l'ensemble des agents DSA est connu et géré en mode coopératif. Pour qu'une recherche rapide fondée sur des attributs données soit possible, un agent DSA unique (ou un ensemble d'agents DSA) peut être configuré de façon à comprendre une zone dupliquée filtrée contenant les attributs souhaités. La procédure de recherche peut ainsi être limitée à un seul agent DSA, capable de fournir rapidement une réponse positive ou négative et d'indiquer, lorsque l'entrée existe effectivement, l'agent DSA maître de cette dernière. Le mécanisme de duplication est étudié en détail dans la Rec. UIT-T X.525 | ISO/CEI 9594-9.

A.4 Applications génériques

A.4.1 Introduction

On peut imaginer qu'un certain nombre d'applications génériques sont assurées implicitement par annuaire: les applications qui ne sont pas propres à un service de télécommunication particulier. Deux de ces applications sont décrites ci-dessous: l'annuaire de communications interpersonnelles et l'annuaire de communications intersystèmes (pour OSI).

NOTE – L'authentification, décrite au § A.3.8 comme un schéma d'accès pourrait aussi être considérée comme une application d'annuaire générique.

A.4.2 Communications interpersonnelles

Le but de cette application est d'offrir aux individus (ou à leurs agents) des informations sur la façon de communiquer avec d'autres individus ou d'autres groupes.

Les classes d'objets suivantes sont certainement utilisées: personne, rôle organisationnel, groupe. De nombreuses autres classes interviennent aussi peut-être de façon moins directe, à savoir: pays, organisation, unité organisationnelle.

Les types d'attribut concernés, autres que ceux qui sont utilisés dans la dénomination, sont généralement les attributs d'adressage. Généralement, l'entrée pour une personne particulière aura les adresses correspondant à chacune des méthodes de communication par lesquelles cette personne peut être atteinte; ces dernières sont choisies parmi une liste non exhaustive comprenant au moins: la téléphonie, le courrier électronique, le télex, le RNIS, la remise physique (par exemple le système postal), la télécopie. Dans certains cas, comme pour le courrier électronique, l'entrée aura des informations supplémentaires telles que les types d'information que l'équipement d'utilisateur peut traiter. Si l'authentification doit être assurée, le mot de passe et/ou les pouvoirs de l'utilisateur seront nécessaires.

Les schémas de dénomination utilisés pour les diverses catégories d'objet devraient être faciles à utiliser, avec des alias établis le cas échéant pour donner d'autres noms et assurer la continuité après une modification de nom, etc.

Les schémas d'accès suivants seront présents dans cette application: recherche, dénomination facile à utiliser, navigation, *pages jaunes* et groupes, à divers degrés, l'authentification sera aussi utilisée.

A.4.3 Communications intersystèmes (pour OSI)

Conformément au modèle de référence OSI, deux fonctions d'annuaire sont nécessaires: l'une dans la couche Application qui mappe les titres d'entité d'application avec les adresses de présentation et l'autre dans la couche Réseau qui mappe les adresses de point d'accès aux services de couche Réseau (NSAP, *network service access point*) et les adresses de point de rattachement au sous-réseau (SNPA, *subnetwork point of attachment*).

NOTE – Dans le reste de ce paragraphe, seul le cas de la couche Application est traité.

Pour accomplir cette fonction, on consulte l'annuaire si l'information nécessaire pour assurer le mappage n'est pas disponible par d'autres moyens.

Les utilisateurs sont des entités d'application, et les classes d'objets présentant un intérêt sont aussi des entités d'applications ou des sous classes de celles-ci.

Le principal type d'attribut concerné, autre que ceux qui sont utilisés pour la dénomination, est l'adresse de présentation. D'autres types d'attribut, qui ne sont pas considérés comme nécessaires pour la fonction d'annuaire proprement dite, pourraient assurer la vérification ou la recherche du type d'entité d'application, ou des listes des contextes d'application, des syntaxes abstraites, etc. Les types d'attribut liés à l'authentification pourraient aussi être appropriés.

Annexe B

Amendements et corrigenda

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

Cette édition de la présente Spécification d'annuaire comprend le projet d'amendement suivant qui avait été voté et approuvé par l'ISO/CEI:

– Amendement 3 relatif à l'optimisation de l'alignement entre la Rec. UIT-T X.500 et le protocole LDAP.

Cette édition de la présente Spécification d'annuaire ne comprend aucun corrigendum technique étant donné qu'il n'y a pas eu de rapport d'erreurs concernant l'édition précédente de la présente Spécification d'annuaire.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006