

Remplacée par une version plus récente



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

X.500

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(11/93)

**RÉSEAUX DE COMMUNICATION DE DONNÉES ET
COMMUNICATIONS ENTRE SYSTÈMES OUVERTS
ANNUAIRE**

**TECHNOLOGIES DE L'INFORMATION –
INTERCONNEXION DES SYSTÈMES OUVERTS:
L'ANNUAIRE: VUE D'ENSEMBLE DES
CONCEPTS, MODÈLES ET SERVICES**

Recommandation UIT-T X.500
Remplacée par une version plus récente

(Antérieurement «Recommandation du CCITT»)

Remplacée par une version plus récente

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. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie 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. Le texte de la Recommandation X.500 de l'UIT-T a été approuvé le 16 novembre 1993. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 9594-1.

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.

© UIT 1995

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

Remplacée par une version plus récente

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX POUR DONNÉES ET INTERCONNEXION DES SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	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
Définition 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 de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Système mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

Remplacée par une version plus récente

TABLE DES MATIÈRES

	<i>Page</i>
Introduction.....	iii
1 Domaine d'application.....	1
2 Références normatives.....	1
3 Définitions.....	2
4 Abréviations.....	3
5 Conventions.....	4
6 Vue d'ensemble de l'Annuaire.....	4
7 Base d'informations Annuaire (DIB).....	5
8 Service d'Annuaire.....	7
9 Annuaire réparti.....	9
10 Contrôle d'accès aux informations contenues dans l'Annuaire.....	11
11 Copie d'Annuaire.....	12
12 Protocoles d'Annuaire.....	14
Annexe A – Application de l'Annuaire.....	16
Annexe B – Modifications et corrigendums.....	20

Remplacée par une version plus récente

Résumé

La présente Recommandation introduit les concepts d'Annuaire et de base d'information Annuaire (DIB) (*directory information base*). Elle donne une vue d'ensemble des services et capacités qu'ils fournissent.

Remplacée par une version plus récente

Introduction

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

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 de systèmes de traitement de l'information:

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

La présente Recommandation | Norme internationale donne une présentation et des modèles des concepts de l'Annuaire et de la DIB. Elle décrit les services et les possibilités qu'ils offrent. D'autres Recommandations | Normes internationales relatives à l'Annuaire 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.

Cette seconde édition révisé techniquement et améliore, mais ne remplace pas, la première édition de la présente Recommandation | Norme internationale. Les mises en œuvre peuvent encore prétendre à la conformité à la première édition.

Cette seconde édition spécifie la version 1 des protocoles et services de l'Annuaire. La première édition spécifie également la version 1. On a traité les différences entre les services et les protocoles définis dans les deux éditions en utilisant les règles d'extensibilité définies dans la présente version de la Rec. 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 modifications et des erreurs qui ont été signalées et dont on a tenu compte dans la présente version de la présente Recommandation | Norme internationale.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – L'ANNUAIRE: VUE D'ENSEMBLE 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 la «mise en correspondance nom-adresse», grâce à laquelle 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.

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | partie de Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute 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.501 (1993) | ISO/CEI 9594-2:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: modèles.*
- Recommandation UIT-T X.511 (1993) | ISO/CEI 9594-3:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: définition du service abstrait.*
- Recommandation UIT-T X.518 (1993) | ISO/CEI 9594-4:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: procédures d'exploitation répartie.*
- Recommandation UIT-T X.519 (1993) | ISO/CEI 9594-5:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: spécifications du protocole.*
- Recommandation UIT-T X.520 (1993) | ISO/CEI 9594-6:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: types d'attributs sélectionnés.*
- Recommandation UIT-T X.521 (1993) | ISO/CEI 9594-7:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: classes d'objets sélectionnées.*

- Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: cadre d'authentification.*
- Recommandation UIT-T X.525 (1993) | ISO/CEI 9594-9:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – L'Annuaire: copie.*
- Recommandation UIT-T X.880 (1994) | ISO/CEI 13712-1...¹⁾, *Technologie de l'information – Opérations à distance: concepts, modèle et notation.*

2.2 Paires de Recommandations | Normes internationales équivalents par leur contenu technique

- Recommandation UIT-T X.200 (1988), *Modèle de référence de base pour l'interconnexion des systèmes ouverts pour les publications du CCITT.*
- ISO 7498:1984, *Systèmes de traitement de l'information – Interconnexions des systèmes ouverts – Modèle de référence de base.*

3 Définitions

Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de référence OSI

Les termes suivants sont définis dans la Rec. X.200 et dans ISO 7498:

- a) *entité d'application;*
- b) *couche application;*
- c) *processus d'application;*
- d) *unité de données de protocole d'application;*
- e) *élément de service d'application;*
- f) *point d'accès au service réseau.*

3.2 Définitions du modèle d'Annuaire

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

- a) *commande d'accès;*
- b) *domaine de gestion d'Annuaire d'administration;*
- c) *alias;*
- d) *attribut;*
- e) *type d'attribut;*
- f) *valeur d'attribut;*
- g) *authentification;*
- h) *arbre d'informations de l'Annuaire (DIT);*
- i) *domaine de gestion d'Annuaire (DMD);*
- j) *agent de système d'Annuaire (DSA);*
- k) *agent d'utilisateur d'Annuaire (DUA);*
- l) *nom distinctif;*
- m) *entrée;*
- n) *nom;*
- o) *objet (d'intérêt);*

¹⁾ A publier.

- p) *domaine de gestion privé d'Annuaire*;
- q) *nom distinctif relatif*;
- r) *racine*;
- s) *schéma*;
- t) *politique de sécurité*
- u) *objet subordonné*;
- v) *entrée supérieure*;
- w) *objet supérieur*;
- x) *arbre*.

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*;
- b) *destination multiple*;
- c) *renvoi*.

3.4 Définitions concernant la copie

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) *copie*;
- f) *consommateur d'informations miroir*;
- g) *fournisseur d'informations miroir*;
- h) *informations 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 de données d'annuaire (DIB): 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

ACI	Information de contrôle d'accès (<i>access control information</i>)
ADDMD	Domaine de gestion d'Annuaire d'administration (<i>administration directory management domain</i>)
DAP	Protocole d'accès à l'Annuaire (<i>directory access protocol</i>)
DIB	Base d'informations Annuaire (<i>directory information base</i>)
DISP	Protocole de duplication miroir des informations de l'Annuaire (<i>directory information shadowing protocol</i>)
DIT	Arbre d'informations de l'Annuaire (<i>directory information tree</i>)
DMD	Domaine de gestion d'Annuaire (<i>directory management domain</i>)

DOP	Protocole de liens opérationnels d'Annuaire (<i>directory operational binding management protocol</i>)
DSA	Agent de système d'Annuaire (<i>directory system agent</i>)
DSP	Protocole du système d'Annuaire (<i>directory system protocol</i>)
DUA	Agent d'utilisateur d'Annuaire (<i>directory user agent</i>)
NSAP	Point d'accès du service réseau (<i>network service access point</i>)
OSI	Interconnexion des systèmes ouverts (<i>open systems interconnection</i>)
PRDMD	Domaine de gestion privé d'Annuaire (<i>private directory management domain</i>)
RDN	Nom distinctif relatif (<i>relative distinguished name</i>)

5 Conventions

A quelques exceptions mineures près, la présente Spécification d'Annuaire a été élaborée conformément aux directives concernant la «présentation des textes communs UIT-T | ISO/CEI», qui figurent dans le guide relatif à la coopération entre l'UIT-T et l'ISO/CEI JTC 1.

Le terme «Spécification d'Annuaire» (comme dans «la présente Spécification d'Annuaire») s'entend selon l'acception de la Rec. UIT-T X.500 | ISO/CEI 9594-1. Le terme «Spécifications d'Annuaire» s'entend selon l'acception des Recommandations de la série X.500 et de toutes les parties de l'ISO/CEI 9594.

Dans la présente Spécification d'Annuaire, le terme «systèmes de l'édition 1988» désigne les systèmes conformes à l'édition précédente (1988), c'est-à-dire à la version de 1988 des Recommandations de la série X.500 du CCITT et à la version de 1990 de l'ISO/CEI 9594. Pour les systèmes conformes aux Spécifications actuelles d'Annuaire on utilise le terme «systèmes de l'édition 1993».

6 Vue d'ensemble 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), qui est considéré comme un processus d'application. Ces concepts sont illustrés à 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.

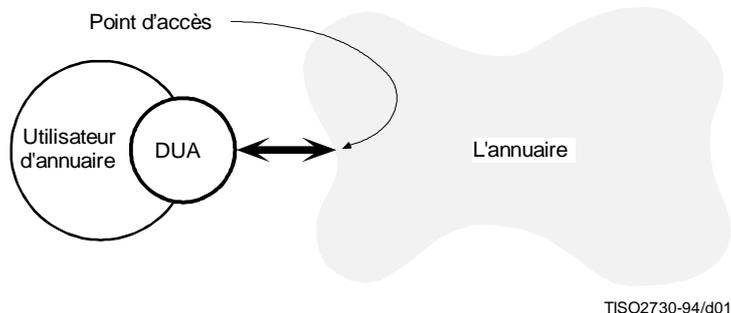


Figure 1 – Accès à l'Annuaire

L'information contenue dans l'Annuaire est appelée collectivement *base d'informations Annuaire* (DIB). L'article 7 donne une vue d'ensemble 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 de façon générale à l'article 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 sera probablement réparti, peut-être même très largement, aux niveaux fonctionnel et organisationnel. L'article 9 décrit les 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 contrôle d'accès est décrit à l'article 10.

En cas de répartition de l'Annuaire, il peut être souhaitable de copier des informations pour améliorer la performance et la disponibilité. Le mécanisme de copie de l'Annuaire est décrit à l'article 11.

La mise à disposition et l'utilisation des services d'annuaire exigent que les utilisateurs (en réalité les DUA) 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 décrits à l'article 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 décidera des objets qui seront énumérés dans l'Annuaire, des utilisateurs qui accéderont à l'information et des types d'accès qui seront 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 seront 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 seront communs à une gamme d'applications: ce sujet est étudié de façon plus approfondie à l'Annexe A.

7 Base d'informations Annuaire (DIB)

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

La 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. 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.

Les entrées de la DIB sont présentées sous forme arborescente: l'Arbre d'informations de l'Annuaire (DIT) 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 – Les services définis dans les présentes Spécifications d'Annuaire ne fonctionnent que d'après une structure d'arbre (DIT). Les présentes 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'informations. 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. Les entrées alias désignent les entrées d'objet et constituent la base d'autres noms pour les objets correspondants.

L'Annuaire applique un ensemble de règles pour s'assurer que la DIB reste bien formée face aux modifications qui interviennent dans le temps. Ces règles, appelées le *schéma de l'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 du DIT et de ses éléments.

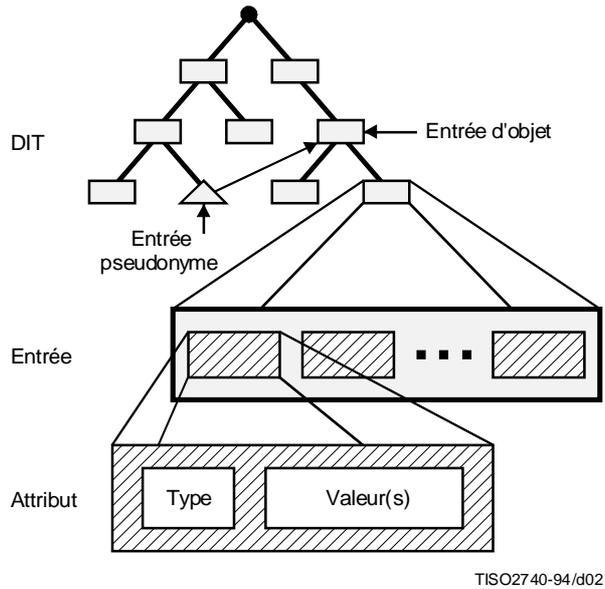


Figure 2 – Structure du DIT et des entrées

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

(C = Royaume-Uni; L = Winslow, O = Services graphiques, CN = Imprimante à laser)

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

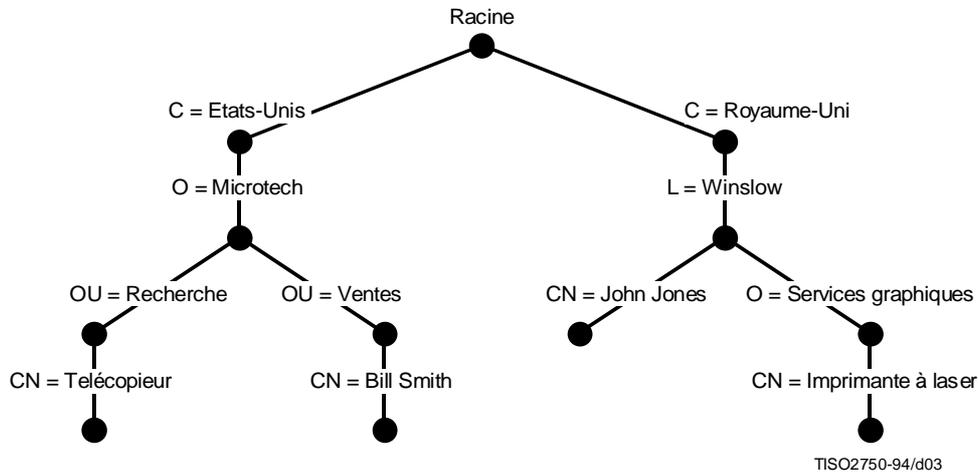


Figure 3 – Arbre hypothétique d'information de l'Annuaire

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 du 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.

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 article donne une vue d'ensemble du service qu'offre l'Annuaire aux utilisateurs, représentés par leurs DUA. Tous les services sont fournis par l'Annuaire en réponse aux demandes provenant des DUA. 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 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. 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 filtre. Un filtre exprime une ou plusieurs conditions auxquelles une entrée 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 et implique la restitution des valeurs de certains (ou de l'ensemble) des attributs de cette entrée. Lorsque seuls certains attributs doivent être retournés, le DUA fournit la liste des types d'attributs en question.

8.3.2 Comparaison

Une demande de comparaison vise un attribut particulier d'une entrée donnée et oblige l'Annuaire à vérifier si une valeur donnée correspond à une valeur de cet attribut.

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 Liste

Une demande de liste oblige l'Annuaire à restituer la liste des subordonnés immédiats d'une entrée désignée dans le DIT.

8.3.4 Recherche

Une demande de recherche oblige l'Annuaire à restituer les informations provenant de toutes les entrées dans une certaine partie du DIT satisfaisant à un filtre. Les informations provenant de chaque entrée comprennent une partie ou l'ensemble des attributs de cette entrée, comme pour la lecture.

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 au DIT d'une nouvelle entrée feuille (soit une entrée objet, soit une entrée alias).

8.4.2 Suppression d'entrée

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

NOTE – Comme pour l'adjonction d'entrée, ce service est utilisé actuellement pour les entrées «vraie feuille»; on l'améliorera dans l'avenir, en le généralisant.

8.4.3 Modification d'entrée

Une demande de modification d'entrée oblige l'Annuaire à apporter une série de modifications à une entrée donnée. Il apporte soit toutes les modifications ou aucune modification et le 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.

8.4.4 Modification du nom distinctif relatif

Une demande de modification du nom distinctif (DN) est utilisée pour modifier le nom distinctif relatif d'une entrée (entrée d'objet ou entrée alias) ou pour déplacer une entrée vers une nouvelle entrée supérieure du DIT. Si une entrée a des subordonnés, alors tous ceux-ci sont renommés ou déplacés de la même façon.

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 le DUA 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 (logiquement) très éloignée du point d'accès. En pareil cas, l'Annuaire peut retourner un renvoi, qui suggère un point d'accès de remplacement auquel le DUA peut faire sa demande.

NOTE – L'Annuaire et le DUA peuvent avoir chacun une préférence quant à l'utilisation des renvois ou au *chainage* des demandes (voir 8.3.3.2). Le 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.

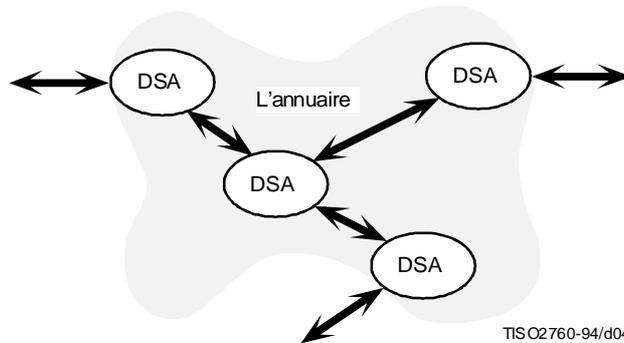


Figure 4 – Modèle fonctionnel de l'Annuaire

Un *agent de système d'Annuaire* (DSA) est un processus d'application OSI qui fait partie de l'Annuaire et dont le rôle est d'assurer un accès à la DIB, aux DUA et/ou à d'autres DSA. Un DSA peut utiliser l'information enregistrée dans sa base de données locale, ou interagir avec d'autres DSA pour effectuer des demandes. Par ailleurs, le DSA peut diriger un demandeur vers un autre DSA qui peut aider à effectuer la demande. Les bases de données locales dépendent entièrement de la mise en œuvre.

9.2 Modèle organisationnel

Un ensemble d'un ou de plusieurs DSA et d'aucun ou de plusieurs DUA gérés par une seule organisation peut former un domaine de gestion d'Annuaire (DMD). L'organisation en question peut choisir d'utiliser ou non les Spécifications d'Annuaire pour régir les communications entre les éléments fonctionnels dans le DMD.

Les autres Spécifications d'Annuaire spécifient certains aspects du comportement des DSA. A cet égard, un groupe de DSA dans un DMD peut, selon l'option de l'organisation qui dirige le DMD, se comporter comme un simple DSA.

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

NOTE – Il convient de reconnaître que l'appui fourni par les membres de l'UIT-T pour les systèmes d'annuaire privés entre dans le cadre des réglementations nationales. Ainsi, les possibilités techniques décrites peuvent être offertes ou non par une Administration qui assure des services d'annuaire. Le fonctionnement interne et la configuration des DMD privés n'entrent pas dans le cadre des Spécifications d'Annuaire envisagées.

9.3 Fonctionnement du modèle

Le DUA dialogue avec l'Annuaire en communiquant avec un ou plusieurs DSA. Un DUA n'a pas besoin d'être lié à un DSA particulier. Il peut entrer en interaction directe avec divers DSA pour faire des demandes. Pour des raisons administratives, une interaction directe avec le DSA qui a besoin d'exécuter la demande est parfois impossible, par exemple pour retourner des informations d'annuaire. Il peut aussi se faire que le DUA accède à l'Annuaire par un simple DSA. A cette fin, une interaction des DSA entre eux est nécessaire.

Le DSA est chargé d'exécuter les demandes des DUA 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 DSA pour le compte du DUA.

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

A la Figure 5a, le DSA C reçoit un renvoi d'un DSA A et il est chargé d'acheminer la demande directement au DSA B (désigné dans le renvoi du DSA A) ou d'acheminer le renvoi au DUA d'origine.

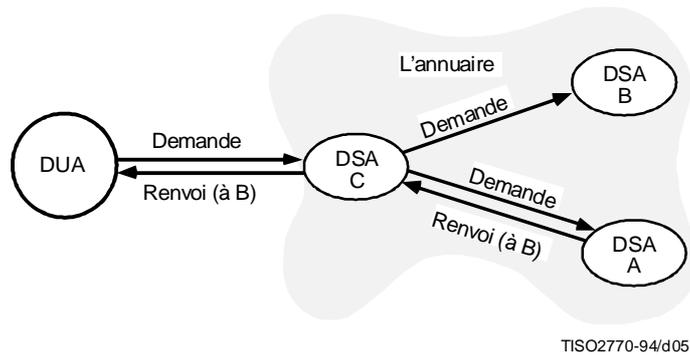


Figure 5a – Renvois

NOTE – Si le DSA C retourne le renvoi au DUA, la « demande (à B) » n'a pas lieu. De même, si le DSA C transmet la demande au DSA B, il ne retournera pas de renvoi au DUA.

Dans la Figure 5b, le DUA reçoit le renvoi du DSA C et il est chargé de réémettre la demande directement au DSA A (désigné dans le renvoi du DSA C).

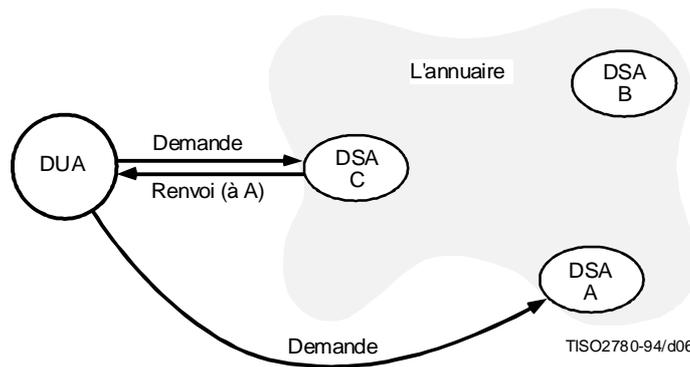


Figure 5b – Renvois

La Figure 6 montre le chaînage DSA unique, qui permet à la demande d'être transmise à travers plusieurs DSA avant que la réponse soit envoyée.

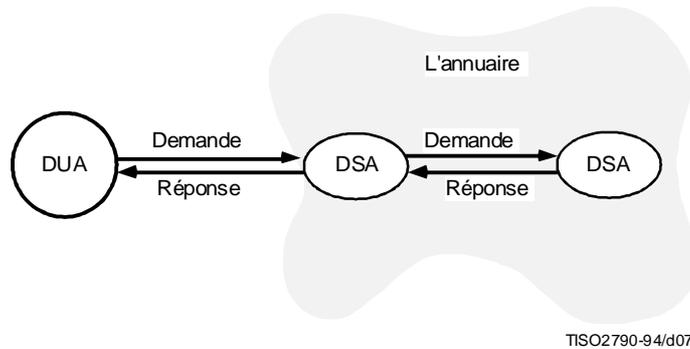


Figure 6 – Chaînage unique

La Figure 7 montre le chaînage multiple dans lequel le DSA associé au DUA exécute la demande en l'envoyant à deux autres DSA ou plus, la demande adressée à chaque DSA étant identique.

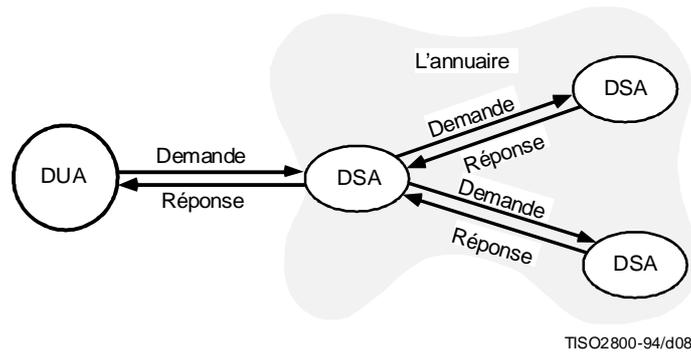


Figure 7 – Destination multiple

Toutes les solutions ont leurs avantages. Par exemple, la méthode décrite à la Figure 5 peut être utilisée lorsqu'il est souhaitable d'alléger la charge du 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 le montre la Figure 8.

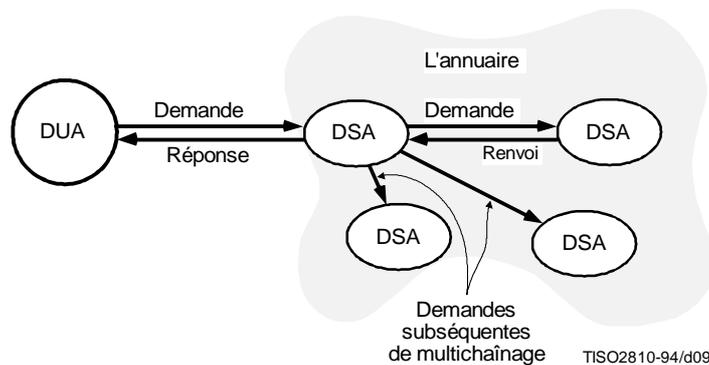


Figure 8 – Solutions hybrides des modes mixtes

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 9594-1.

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

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

11 Copie d'Annuaire

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

11.1 Introduction

Par copie 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. Le DSA qui contient les informations d'origine, est appelé le DSA maître.

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

La copie 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 des 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 du DIT.

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

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

11.2 Formes de copies d'annuaire

Deux formes d'informations d'entrée copiées peuvent être détenues par les composantes de l'Annuaire: les copies caches et les informations dupliquées.

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 spécifiée dans les Spécifications d'Annuaire.

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

L'agent DSA détenteur de ces informations ne peut les fournir aux autres agents DSA 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 ne peuvent être fournies que lorsque une autorisation de lecture a été accordée.

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

Lorsqu'il répond à une demande par une information copiée, le DSA qui détient l'information copiée doit indiquer 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 miroir en vertu duquel un DSA fournisseur d'informations miroir s'engage à fournir à un autre DSA, consommateur d'informations miroir, des informations miroir d'une partie convenue du DIT. Si l'accord de duplication d'informations miroir utilisé pour l'obtention des informations miroir l'y autorise, le consommateur d'informations miroir 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 miroir, des informations d'exploitation (par exemple des connaissances) peuvent aussi être fournies au consommateur d'information miroir par le fournisseur d'informations miroir.

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

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

Les informations copiées 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.

11.3 Copie 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 miroir et des incohérences permanentes pour des informations caches.

Les informations caches d'entrée peut 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 miroir sont rendues conformes avec les informations détenues par un fournisseur d'informations miroir selon un programme inclus dans l'accord de duplication des informations miroir.

Il est indispensable que les informations contenues dans une instance d'une entrée simple d'objet soient intrinsèquement cohérentes. Tout mécanisme de copie sera accompagné de mécanismes destinés à garantir la cohérence interne des informations copiées 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 au DIT d'être réparti entre les DSA soient précises. Tout mécanisme de copie 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 DSA pour garantir la cohérence de l'arbre DIT.

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

- les informations miroir sont intrinsèquement cohérentes; et
- les connaissances qui les lient au DIT sont précises; et
- il y aura finalement cohérence entre l'entrée d'informations miroir et l'entrée inscrite dans l'agent DSA maître.

11.4 Points de vue sur la copie

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

- a) les utilisateurs de l'Annuaire;
- b) les utilisateurs administratifs; et
- c) les composantes d'exploitation de l'Annuaire (DSA).

11.4.1 Point de vue de l'utilisateur de l'Annuaire

Compte tenu de la nature de l'exploitation de l'Annuaire, les informations copiées correspondront généralement aux informations détenues par le 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 le 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.

11.4.2 Point de vue de l'utilisateur administratif

Un utilisateur administratif est chargé de gérer les informations détenues et le service offert par un 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 du DSA.

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

11.4.3 Point de vue du DSA

Bien qu'un DSA puisse déceler la différence entre les informations copiées 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 copiées sont équivalentes sauf dans deux cas: un DSA n'utilise que des informations d'entrée pour répondre à des demandes visant à modifier la DIB et à des demandes d'interrogation qui signalent que les informations copiées ne sont pas acceptables.

De plus, étant donné que les informations détenues au niveau local peuvent être partielles (voir 11.2), un DSA peut transmettre une demande à un autre DSA plus apte à fournir les informations demandées.

11.5 Copie et contrôle d'accès

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

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

12 Protocoles d'Annuaire

NOTE – Les protocoles de la couche application OSI 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), qui définit l'échange de demandes et de réponses entre un agent DUA et un agent DSA;
- le protocole de système d'Annuaire (DSP), qui définit l'échange de demandes et de réponses entre deux DSA;

- le protocole de duplication miroir des informations de l'Annuaire (DISP), qui définit l'échange des informations copiées entre deux DSA qui ont conclu des accords de duplication des informations miroir.
- le protocole de liens opérationnels d'Annuaire (DOP), qui définit l'échange des informations administratives entre deux agents DSA permettent de gérer les liens opérationnels entre eux.

Chaque protocole est défini par un ou plusieurs contexte d'application, chacun contenant un ensemble d'éléments de protocole. Par exemple, le DAP contient des éléments de protocole associés à l'interrogation et à la modification de l'Annuaire.

Chaque contexte d'application se compose d'éléments de service d'application, lesquels sont définis pour l'utilisation du service d'opérations à distance (ROSE) de la Rec. UIT-T X.880 | ISO/CEI 13712-1 pour structurer et assurer leurs interactions. Ainsi, le DAP, le DSP, le DISP et le DOP sont-ils définis comme des ensembles d'opérations et d'erreurs à distance utilisant la notation ROS.

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 mise en correspondance 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 – Il ne s'agit ici que de la recherche dans l'Annuaire: on suppose que les services de modification d'Annuaire ne servent qu'à maintenir la 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 terme de demandes particulières qu'un 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 section 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 d'Annuaire, qui sera vraisemblablement le type d'interrogation le plus fréquent, fait intervenir le 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 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.

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 Recherche rapide

Dans de nombreuses utilisations de l'Annuaire conçues pour les individus, il se peut que l'utilisateur (ou 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 recherche rapide permettra à l'utilisateur de parcourir la DIB pour rechercher les entrées appropriées.

La recherche rapide 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 le 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.

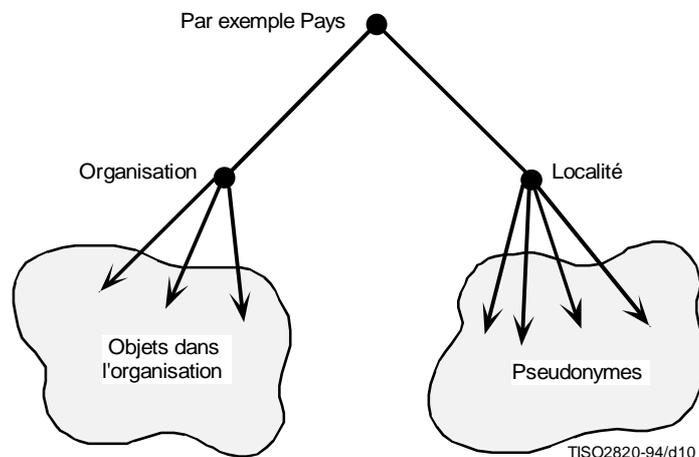


Figure A.1 – Méthode concernant les pages jaunes

A.3.6 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 le DUA en dehors des versions non récurrentes fournies.

A.3.7 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.4 Applications génériques

A.4.1 Introduction

On peut imaginer qu'un certain nombre d'applications génériques sont assurées implicitement par l'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 en A.3.7 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, recherche rapide, *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 met en correspondance les titres d'entité d'application avec les adresses de présentation et l'autre dans la couche réseau qui met en correspondance les adresses de NSAP (point d'accès à des services de couche réseau) et les adresses de SNPA (SNPA = Point de rattachement au sous-réseau).

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 la mise en correspondance 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.

Le principal schéma d'accès qui doit être présenté sera la recherche.

Annexe B

Modifications et corrigendums

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

Cette version de la présente Spécification d'Annuaire comprend les modifications suivantes:

- Modification 1 pour la copie, le schéma et le contrôle d'accès

Cette version de la présente Spécification d'Annuaire comprend les corrigendums techniques suivants, pour corriger les défauts signalés dans les relevés:

- il n'y a pas eu de relevés de défauts concernant l'édition précédente de la présente Spécification d'Annuaire.