
**Technologies de l'information —
Interconnexion de systèmes ouverts
(OSI) — L'annuaire: Définition du service
abstrait**

*Information technology — Open Systems Interconnection — The
Directory: Abstract service definition*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-3:2005](https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005)

<https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005>

PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-3:2005](https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005)

<https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005>

© ISO/CEI 2005

Droits de reproduction réservés. Sauf prescription différente, 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'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2006

Publié en Suisse

TABLE DES MATIÈRES

	<i>Page</i>	
1	Domaine d'application	1
2	Références normatives	1
2.1	Recommandations Normes internationales identiques	1
2.2	Autres références	2
3	Définitions	2
3.1	Définitions de base relatives à l'annuaire	2
3.2	Définitions relatives au modèle d'annuaire	2
3.3	Définitions relatives à la base d'informations d'annuaire	2
3.4	Définitions concernant les entrées d'annuaire	2
3.5	Définitions relatives aux noms	3
3.6	Définitions concernant les opérations réparties	3
3.7	Définitions concernant le service abstrait	3
4	Abréviations	4
5	Conventions	4
6	Aperçu général du service d'annuaire	4
7	Types d'information et procédures communes	5
7.1	Introduction	5
7.2	Types d'information définis ailleurs	5
7.3	Arguments communs (CommonArguments)	6
7.4	Résultats communs (CommonResults)	9
7.5	Commandes de service (ServiceControls)	10
7.6	Sélection d'information d'entrée (EntryInformationSelection)	12
7.7	Information d'entrée	16
7.8	Filtre (Filter)	18
7.9	Résultats paginés (pagedResults)	21
7.10	Paramètres de sécurité (SecurityParameters)	23
7.11	Eléments de procédure communs pour le contrôle d'accès de base (basic-access-control)	25
7.12	Gestion de l'arbre d'informations d'agent DSA	27
7.13	Procédures relatives aux familles d'entrées	27
8	Opérations de rattachement et de détachement	28
8.1	Rattachement à l'annuaire	28
8.2	Détachement de l'annuaire (DirectoryUnbind)	31
9	Opérations de lecture de l'annuaire	31
9.1	Lecture	31
9.2	Comparaison	34
9.3	Abandon	36
10	Opérations de recherche dans l'annuaire	37
10.1	Listage (List)	37
10.2	Recherche (Search)	40
11	Opérations de modification de l'annuaire	52
11.1	Adjonction d'entrée (addEntry)	52
11.2	Opération de suppression d'entrée (removeEntry)	54
11.3	Modification d'entrée (modifyEntry)	56
11.4	Modification du nom distinctif (modifyDN)	60
12	Erreurs	62
12.1	Priorité des erreurs	62
12.2	Abandoned	63
12.3	Abandon Failed	63
12.4	Attribute Error	63
12.5	Name Error	64
12.6	Referral (renvoi de référence)	65

	<i>Page</i>
12.7 Security Error.....	66
12.8 Service Error.....	66
12.9 Update Error.....	68
13 Analyse des arguments de l'opération de recherche.....	69
13.1 Vérification globale du filtre de recherche.....	70
13.2 Vérification des profils request-attribute-profiles.....	71
13.3 Vérification des commandes et de la sélection hiérarchique.....	72
13.4 Vérification de l'utilisation de la concordance.....	73
Annexe A – Service abstrait en ASN.1.....	75
Annexe B – Sémantique opérationnelle pour le contrôle d'accès de base.....	87
Annexe C – Exemples de la recherche de familles d'entrées.....	100
C.1 Exemple de famille unique.....	100
C.2 Exemple de plusieurs familles.....	101
Annexe D – Amendements et corrigenda.....	104

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-3:2005](https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005)

<https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005>

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 9594-3 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Rec. UIT-T X.511.

<https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005>

Cette cinquième édition constitue une révision technique de la quatrième édition (ISO/CEI 9594-3:2001), qui est provisoirement retenue afin de supporter les mises en application basées sur la quatrième édition.

L'ISO/CEI 9594 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire*:

- *Partie 1: Aperçu général des concepts, modèles et services*
- *Partie 2: Les modèles*
- *Partie 3: Définition du service abstrait*
- *Partie 4: Procédures pour le fonctionnement réparti*
- *Partie 5: Spécifications du protocole*
- *Partie 6: Types d'attributs sélectionnés*
- *Partie 7: Classes d'objets sélectionnées*
- *Partie 8: Cadre général des certificats de clé publique et d'attribut*
- *Partie 9: Duplication*
- *Partie 10: Utilisation de la gestion-systèmes pour l'administration de l'annuaire*

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, *directory information base*), 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 définit les capacités fournies par l'annuaire à ses utilisateurs.

La présente Recommandation | Norme internationale fournit les cadres de base permettant la définition de profils industriels par d'autres organismes de normalisation et par des forums industriels. L'utilisation d'un grand nombre des fonctionnalités optionnelles figurant dans ces cadres peut être rendue obligatoire dans certains environnements au moyen de profils. Cette cinquième édition révisé techniquement et améliore, 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 compte (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 de l'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, par exemple 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 définis dans la version 2, en utilisant les règles d'extensibilité définies dans la Rec. UIT-T X.519 | ISO/CEI 9594-5.

L'Annexe A, qui fait partie intégrante de la présente Recommandation | Norme internationale, présente le module ASN.1 pour le service abstrait d'annuaire.

L'Annexe B, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, présente des organigrammes qui décrivent la sémantique associée au contrôle d'accès de base dans la mesure où elle s'applique au traitement d'une opération d'annuaire.

L'Annexe C, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale donne des exemples de l'emploi des familles d'entrées.

L'Annexe D, qui ne fait pas partie intégrante de la présente Recommandation | Norme internationale, énumère les modifications et les relevés d'erreurs qui ont été incorporés pour former l'édition de la présente Recommandation | Norme internationale.

**NORME INTERNATIONALE
RECOMMANDATION UIT**

**Technologies de l'information – Interconnexion des systèmes ouverts –
L'annuaire: définition du service abstrait**

1 Domaine d'application

La présente Recommandation | Norme internationale définit de façon abstraite le service, visible de l'extérieur, que fournit l'annuaire.

La présente Recommandation | Norme internationale ne spécifie ni implémentations, ni produits individuels.

2 Références normatives

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

2.1 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.500 (2005) | ISO/CEI 9594-1:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services.*
- 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.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.*
- Recommandation UIT-T X.680 (2002) | ISO/CEI 8824-1:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*
- Recommandation UIT-T X.681 (2002) | ISO/CEI 8824-2:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*

ISO/CEI 9594-3:2005 (F)

- Recommandation UIT-T X.682 (2002) | ISO/CEI 8824-3:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*
- Recommandation UIT-T X.683 (2002) | ISO/CEI 8824-4:2002, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*

2.2 Autres références

- RFC 2025 (1996), *The Simple Public-Key GSS-API Mechanism (SPKM).*
- RFC 2222 (1997), *Simple Authentication and Security Layer (SASL).*

3 Définitions

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

3.1 Définitions de base relatives à l'annuaire

Les termes suivants sont définis dans la Rec. UIT-T X.500 | ISO/CEI 9594-1:

- annuaire;*
- base d'informations d'annuaire;*
- utilisateur (d'annuaire).*

3.2 Définitions relatives au modèle d'annuaire

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

- agent de système d'annuaire;*
- agent utilisateur d'annuaire.*

3.3 Définitions relatives à la base d'informations d'annuaire

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

- entrée pseudonyme (alias);*
- arbre d'informations d'annuaire;*
- entrée (d'annuaire);*
- supérieur immédiat;*
- entrée/objet immédiatement supérieur;*
- objet;*
- classe d'objets;*
- entrée d'objet;*
- subordonné;*
- supérieur;*
- ascendant;*
- famille (d'entrées);*
- entrée composée.*

3.4 Définitions concernant les entrées d'annuaire

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

- attribut;*
- type d'attribut;*
- valeur d'attribut;*
- assertion de valeur d'attribut;*
- contexte;*

- f) *type de contexte;*
- g) *valeur de contexte;*
- h) *attribut opérationnel;*
- i) *attribut utilisateur;*
- j) *règle de correspondance.*

3.5 Définitions relatives aux noms

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

- a) *pseudonyme;*
- b) *nom distinctif;*
- c) *nom (d'annuaire);*
- d) *nom allégué;*
- e) *nom distinctif relatif.*

3.6 Définitions concernant les opérations réparties

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

- a) *agent DSA rattaché;*
- b) *chaînage;*
- c) *exécuteur initial;*
- d) *renvoi de référence.*

3.7 Définitions concernant le service abstrait

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

3.7.1 recherche additionnelle: recherche à partir de l'objet **JoinBaseObject** tel que spécifié par l'expéditeur dans la demande **search**.

3.7.2 membre contributeur: membre de la famille dans une entrée composée qui a contribué à une opération de lecture, de recherche ou de modification d'entrée.

3.7.3 entrée explicitement non marquée: entrée ou membre de la famille qui est exclu du résultat de l'opération de recherche **SearchResult** en vertu d'une spécification donnée dans un attribut de commande référencé par la règle governing-search-rule.

3.7.4 groupement familial: ensemble de membres d'un attribut composé qui sont regroupés pour les besoins d'une évaluation des opérations.

3.7.5 filtre: assertion relative à la présence ou à la valeur de certains attributs d'une entrée et destinée à limiter le domaine d'application d'une recherche.

3.7.6 expéditeur: utilisateur qui est à l'origine d'une opération.

3.7.7 membre participant: membre de la famille qui est soit un membre contributeur soit un membre d'un groupement familial qui dans son ensemble concorde avec un filtre de recherche **search**.

3.7.8 recherche initiale: recherche qui débute à partir de l'objet de base **baseObject** comme l'a spécifié l'expéditeur dans la demande de recherche.

3.7.9 relaxation: modification progressive du comportement d'un filtre au cours d'une opération de recherche de manière à obtenir plus de résultats lorsque trop peu sont reçus, ou moins de résultats lorsque trop sont reçus.

3.7.10 commandes de service: paramètres transmis dans le cadre d'une opération qui limitent certains aspects de ses performances.

3.7.11 branche: groupement familial comprenant tous les membres dans un conduit, du membre de la famille feuille jusqu'à l'ascendant compris. Un membre de la famille résidera dans autant de branches qu'il y aura de membres de la famille feuilles sous lui (en tant que subordonnés immédiats ou non).

3.7.12 résultat multidiffusé: résultat d'une seule opération qui est inclus dans plusieurs réponses.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes sont utilisées:

AVA	Assertion de valeur d'attribut (<i>attribute value assertion</i>)
DIB	Base d'informations d'annuaire (<i>directory information base</i>)
DIT	Arbre d'information d'annuaire (<i>directory information tree</i>)
DMD	Domaine de gestion d'annuaire (<i>directory management domain</i>)
DSA	Agent de système d'annuaire (<i>directory system agent</i>)
DUA	Agent d'utilisateur d'annuaire (<i>directory user agent</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 *Règles de présentation des textes communs UIT-T* | ISO/CEI, novembre 2001.

Le terme "Spécification d'annuaire" (comme dans "la présente Spécification d'annuaire") s'entend comme désignant la Rec. UIT-T X.511 | ISO/CEI 9594-3. Le terme "Spécifications d'annuaire" s'entend comme désignant toutes les Recommandations de la série X.500 et toutes les parties de l'ISO/CEI 9594.

La présente Spécification d'annuaire utilise le terme *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 de la série X.500 du CCITT et de l'ISO/CEI 9594:1990. La présente Spécification d'annuaire utilise le terme *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 de l'ISO/CEI 9594:1995. La présente Spécification d'annuaire utilise le terme *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 de l'ISO/CEI 9594:1998. La présente Spécification d'annuaire utilise le terme *systèmes de la quatrième édition* pour désigner les systèmes conformes à la quatrième édition des Spécifications d'annuaire, c'est-à-dire aux éditions 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:édition 2001.

La présente Spécification d'annuaire utilise le terme *systèmes de la cinquième édition* pour désigner les systèmes conformes à la cinquième édition des Spécifications d'annuaire, c'est-à-dire aux éditions 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 et aux parties 1 à 10 de l'ISO/CEI 9594:édition 2005.

Cette Spécification d'annuaire présente la notation ASN.1 en caractères gras de la police 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, normalement cités lors de la spécification des sémantèmes de traitement, sont différenciés du texte normal par une présentation en caractères gras de la police Times. Les autorisations de contrôle d'accès sont présentées en caractères italiques de la police Times.

Si, dans une liste, les points sont numérotés (au lieu d'utiliser des tirets ou des lettres), ils sont considérés comme des étapes d'une procédure.

6 Aperçu général du service d'annuaire

Les services d'annuaire décrits dans la Rec. UIT-T X.501 | ISO/CEI 9594-2 sont fournis au moyen de points d'accès à des agents DUA, chaque agent DUA agissant au nom d'un utilisateur. La Figure 1 illustre ces concepts. L'annuaire offre des services à ses utilisateurs par l'intermédiaire d'un point d'accès, en exécutant un certain nombre d'opérations d'annuaire.

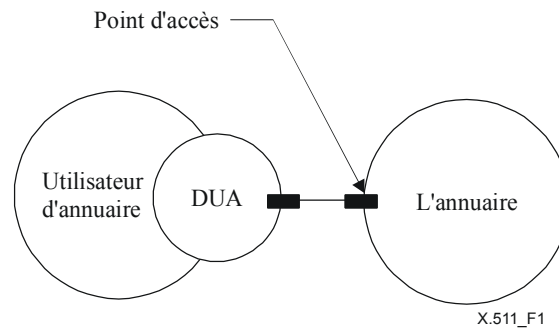


Figure 1 – Accès à l'annuaire

On distingue trois types d'opérations:

- les opérations de lecture de l'annuaire, qui consistent à interroger une seule entrée d'annuaire;
- les opérations de recherche dans l'annuaire, qui consistent à interroger éventuellement plusieurs entrées d'annuaire;
- les opérations de modification de l'annuaire.

Les opérations de lecture de l'annuaire, de recherche dans l'annuaire et de modification de l'annuaire sont spécifiées respectivement aux § 9, 10 et 11. La conformité avec les opérations d'annuaire est spécifiée dans la Rec. UIT-T X.519 | ISO/CEI 9594-5.

7 Types d'information et procédures communes

7.1 Introduction

Le présent paragraphe identifie et, dans certains cas, définit plusieurs types d'information qui seront par la suite utilisés pour définir des opérations d'annuaire. Ces types d'information désignent ceux qui sont communs à plusieurs opérations, ou qui le seront probablement dans l'avenir, ou ceux qui sont suffisamment complexes ou autonomes pour justifier une définition indépendante de l'opération qui les utilise.

Plusieurs types d'information utilisés dans la définition du service d'annuaire se trouvent en fait définis ailleurs. Ces types d'information sont identifiés au § 7.2 qui indique aussi la source de leur définition. Chacun des autres paragraphes (7.3 à 7.10) identifie et définit un type d'information.

Le présent paragraphe spécifie aussi certains éléments de procédure communs qui s'appliquent à la plupart ou à la totalité des opérations d'annuaire.

7.2 Types d'information définis ailleurs

Les types d'information suivants sont définis dans la Rec. UIT-T X.501 | ISO/CEI 9594-2:

- Attribute;**
- AttributeType;**
- AttributeValue;**
- AttributeValueAssertion;**
- Context;**
- ContextAssertion;**
- DistinguishedName;**
- Name;**
- OPTIONALLY-PROTECTED;**
- OPTIONALLY-PROTECTED-SEQ;**
- RelativeDistinguishedName.**

Le type d'information suivant est défini dans la Rec. UIT-T X.520 | ISO/CEI 9594-6:

- PresentationAddress.**

ISO/CEI 9594-3:2005 (F)

Les types d'information suivants sont définis dans la Rec. UIT-T X.509 | ISO/CEI 9594-8:

- a) **Certificate**;
- b) **SIGNED**;
- c) **CertificationPath**.

Le type d'information suivant est défini dans la Rec. UIT-T X.880 | ISO/CEI 13712-1:

- a) **Invokeld**.

Les types d'information suivants sont définis dans la Rec. UIT-T X.518 | ISO/CEI 9594-4:

- a) **OperationProgress**;
- b) **ContinuationReference**.

7.3 Arguments communs (CommonArguments)

L'information **CommonArguments** peut être présente pour accompagner l'invocation de chaque opération que l'annuaire peut accomplir.

CommonArguments ::= SET {

serviceControls	[30]	ServiceControls DEFAULT { },
securityParameters	[29]	SecurityParameters OPTIONAL,
requestor	[28]	DistinguishedName OPTIONAL,
operationProgress	[27]	OperationProgress
		DEFAULT { nameResolutionPhase notStarted },
aliasedRDNs	[26]	INTEGER OPTIONAL,
criticalExtensions	[25]	BIT STRING OPTIONAL,
referenceType	[24]	ReferenceType OPTIONAL,
entryOnly	[23]	BOOLEAN DEFAULT TRUE,
nameResolveOnMaster	[21]	BOOLEAN DEFAULT FALSE,
operationContexts	[20]	ContextSelection OPTIONAL,
familyGrouping	[19]	FamilyGrouping DEFAULT entryOnly }

Le composant **ServiceControls** est spécifié au § 7.5. Son absence est jugée équivalente à l'existence d'un ensemble de commandes vide.

Le composant **SecurityParameters** est spécifié au § 7.10. Si l'argument de l'opération doit être signé par le demandeur, le composant **SecurityParameters** doit être inclus dans cet argument. L'absence de ce composant est jugée équivalente à un ensemble vide.

Le nom distinctif **requestor** identifie le demandeur d'une opération donnée. Il contient le nom de l'utilisateur identifié au moment du rattachement à l'annuaire. Il peut être nécessaire lorsque la demande doit être signée (voir § 7.10) et il doit contenir le nom de l'utilisateur qui est à l'origine de la demande.

NOTE 1 – Lorsqu'un utilisateur possède des variantes nominatives distinctives qui sont différenciées par le contexte, le nom utilisé comme valeur du paramètre **requestor** doit être le nom distinctif primaire, si on le connaît. Sinon, l'authentification et le contrôle d'accès fondés sur la valeur du paramètre **requestor** peuvent ne pas fonctionner comme on le souhaite.

Les paramètres **operationProgress**, **referenceType**, **entryOnly**, **exclusions** et **nameResolveOnMaster** sont définis dans la Rec. UIT-T X.518 | ISO/CEI 9594-4. Ils sont fournis par un agent DUA:

- a) soit lors du traitement d'une référence de continuation retournée par un agent DSA en réponse à une opération antérieure et leurs valeurs sont copiées par l'agent DUA d'après la référence de continuation;
- b) soit lorsque l'agent DUA représente un utilisateur administratif qui gère l'arbre d'information de l'agent DSA et lorsque l'option **manageDSAIT** est activée dans les commandes de service.

Le paramètre **aliasedRDNs** indique à l'agent DSA que le paramètre **object** de l'opération a été créé par déréréférencement d'un alias lors d'une tentative d'opération précédente. La valeur d'entier indique le nombre de noms RDN contenus dans le nom provenant du déréréférencement de l'alias. (La valeur aura été fixée dans la réponse de renvoi de référence de l'opération précédente.)

NOTE 2 – Ce paramètre est fourni pour assurer la compatibilité avec les implémentations de l'annuaire selon la première édition. Les agents DUA (et DSA) implémentés selon des éditions postérieures des Spécifications d'annuaire ne mentionneront jamais ce paramètre dans l'information **CommonArguments** d'une demande ultérieure. Cela permettra à l'annuaire de ne pas signaler d'erreur lorsque des alias déréréférenceront d'autres alias.

Le paramètre **operationContexts** fournit un ensemble d'assertions contextuelles qui sont appliquées aux assertions de valeur d'attribut et une sélection d'informations d'entrée faite dans le cadre de cette opération. Cet ensemble ne contient par ailleurs aucune assertion contextuelle pour les mêmes types d'attribut et de contexte. Si le paramètre **operationContexts** n'est pas présent ou ne vise pas un type particulier d'attribut ou de contexte, les assertions

contextuelles par défaut doivent être appliquées par l'agent DSA comme décrit au § 7.6.1 et aux § 8.9.2.2 et 12.8 de la Rec. UIT-T X.501 | ISO/CEI 9594-2. Si le paramètre **allContexts** est choisi, tous les contextes sont applicables à tous les types d'attribut et les valeurs contextuelles par défaut qui pourraient avoir été fournies par l'agent DSA sont outrepassées. (Le composant **ContextSelection** est défini au § 7.6.)

Le paramètre **familyGrouping** sert à décrire quels membres de la famille doivent être sélectionnés pour le traitement d'une opération donnée. Il est décrit de manière plus complète dans le § 7.3.2.

7.3.1 Extensions critiques (criticalExtensions)

Le paramètre **criticalExtensions** fournit un mécanisme permettant d'énumérer un ensemble d'extensions qui sont critiques pour l'exécution d'une opération d'annuaire. Si le demandeur de l'opération étendue veut indiquer que l'opération doit être exécutée avec une ou plusieurs extensions (c'est-à-dire que l'exécution de l'opération sans ces extensions n'est pas acceptable), il positionne le ou les bits **criticalExtensions** qui correspondent à une ou plusieurs de ces extensions critiques. Si l'annuaire, ou une partie de l'annuaire, ne peut pas réaliser une extension critique, il renvoie une indication **unavailableCriticalExtension** (comme cause d'une erreur de type **ServiceError** ou comme valeur d'un qualificateur de type **PartialOutcomeQualifier**). Si l'annuaire ne peut pas effectuer une extension non critique, il ne tient pas compte de la présence de l'extension.

La présente spécification ne définit pas de règle relative à l'ordre suivant lequel un agent DSA d'exécution doit décoder et traiter les unités PDU qu'il reçoit. Un agent DSA qui reçoit une extension critique inconnue doit renvoyer une erreur de type **ServiceError** avec une cause de type **unavailableCriticalExtension** pour indiquer que l'opération a échoué.

Les présentes Spécifications d'annuaire définissent un certain nombre d'extensions. Ces extensions peuvent prendre la forme de bits supplémentaires numérotés dans une chaîne binaire de type BIT STRING ou de paramètres supplémentaires d'un type SET ou SEQUENCE. Elles ne sont pas prises en considération dans les systèmes conformes à la première édition. Chacune de ces extensions est accompagnée d'un entier identificateur correspondant au numéro du bit qui peut être sélectionné dans **criticalExtensions**. Si la criticité d'une extension est vérifiée, l'agent DUA doit sélectionner le bit correspondant dans le paramètre **criticalExtensions**. Si la criticité définie n'est pas vérifiée, l'agent DUA peut sélectionner ou ne pas sélectionner le bit correspondant dans le paramètre **criticalExtensions**.

Les extensions, leurs identificateurs, les opérations au cours desquelles elles sont permises, la criticité recommandée, les paragraphes où ils sont définis ainsi que les commandes LDAP correspondantes (éventuelles) sont indiqués dans le Tableau 1.

<https://standards.iteh.ai/catalog/standards/sist/35094f63-587f-452b-9691-017351e3587a/iso-iec-9594-3-2005>
Tableau 1 – Extensions

Extension	Identificateur	Opérations	Criticité	Définition (paragraphe)	Commande LDAP
subentries	1	Toutes	Non critique	7.5	1.3.6.1.4.1.4203.1.10.1
copyShallDo	2	Lecture, comparaison, listage, recherche	Non critique	7.5	
attribute size limit	3	Lecture, recherche	Non critique	7.5	
extraAttributes	4	Lecture, recherche	Non critique	7.6	
modifyRightsRequest	5	Lecture	Non critique	9.1	
pagedResultsRequest	6	Listage, recherche	Non critique	10.1	1.2.840.113556.1.4.319
matchedValuesOnly	7	Recherche	Non critique	10.2	1.2.826.0.1.3344810.2.3
extendedFilter	8	Recherche	Non critique	10.2	
targetSystem	9	Adjonction d'entrée	Critique	11.1	
useAliasOnUpdate	10	Adjonction d'entrée, suppression d'entrée, modification d'entrée	Critique	11.1	
newSuperior	11	Modification de nom distinctif	Critique	11.4	
manageDSAIT	12	Toutes	Critique	7.5, 7.13	2.16.840.1.113730.3.4.2
useContexts	13	Lecture, comparaison, listage, recherche, adjonction d'entrée, modification d'entrée, modification de nom distinctif	Non critique	7.6, 7.8	

Tableau 1 – Extensions

Extension	Identificateur	Opérations	Criticité	Définition (paragraphe)	Commande LDAP
partialNameResolution	14	Lecture, recherche	Non critique	7.5	
overspecFilter	15	Recherche	Non critique	10.1.3 f)	
selectionOnModify	16	Modification d'entrée	Non critique	11.3.2	
Paramètres de sécurité – Réponse	17	Toutes	Non critique	7.10	
Paramètres de sécurité – Code d'opération	18	Toutes	Non critique	7.10	
Paramètres de sécurité – Itinéraire de certification d'attribut	19	Toutes	Non critique	7.10	
Paramètres de sécurité – Protection d'erreur	20	Toutes	Non critique	7.10	
Justificatifs d'identité SPKM	21	Rattachement d'annuaire	(Note 3)	8.1.1	
Jeton de rattachement – Réponse	22	Rattachement d'annuaire	Non critique	8.1.1	
Jeton de rattachement – Algorithme int. de ratt., clé int. de ratt., algor. de conf. et inform. de clé de conf.	23	Rattachement d'annuaire	Non critique	8.1.1	
Jeton de rattachement – DIRQOP (obsolète)	24	Rattachement d'annuaire	Non critique	8.1.1	
Administration de service	25	Lecture, recherche, modification d'entrée	Critique	10.2.2, 13, § 16 de la Rec. UIT-T X.501 ISO/CEI 9594-2	
EntryCount	26	Recherche	Non critique	10.1.3	
hierarchySelection	27	Recherche	Non critique	7.5	
relaxation	28	Recherche	Non critique	7.8	
familyGrouping	29	Comparaison, recherche, suppression d'entrée	Non critique Non critique Critique	7.3.2, 7.8.3 et 9.2.2 10.2 11.2.2	
familyReturn	30	Lecture, recherche, modification d'entrée	Non critique Non critique Non critique	7.6.4, 7.7.1 et 9.1.3 10.2.3 11.3.3	
dnAttributes	31	Recherche	Non critique	10.2.2	
attributs conviviaux	32	Lecture, recherche	Non critique	7.6, 7.8.2	
Abandon de résultats paginés	33	Listage, recherche	Critique	7.9	
Résultats paginés sur le DSP	34	Listage, recherche	Non critique	7.9	
replaceValues	35	ModifyEntry	Critique	11.3.1, 11.3.2	

NOTE 1 – La première extension reçoit l'identificateur 1 et correspond au bit 1 de BIT STRING, dont le bit 0 n'est pas utilisé.

NOTE 2 – La version 2 ou plus du protocole est nécessaire pour effectuer une transformation de sécurité sur des données chiffrées ou signées et chiffrées, ou pour assurer une protection contre les erreurs ou résultats aux opérations Add Entry, Remove Entry, Modify Entry, Modify DN.

NOTE 3 – L'extension relative aux justificatifs d'identité du modèle SPKM doit être étiquetée comme étant critique, sauf si elle est utilisée dans des associations établies au moyen de la version 2 ou plus.

7.3.2 Groupement familial

Le groupement familial permet de regrouper une seule entrée, plusieurs entrées ou toutes les entrées d'une entrée composée afin de les examiner ensemble avant une évaluation des opérations. Cette sémantique peut ensuite être appliquée aux opérations suivantes (comme décrit ci-après): comparaison (afin de définir le domaine dans lequel l'attribut comparé pourrait être situé), recherche (afin de définir les groupements qui pourraient faire l'objet d'un filtrage), suppression d'entrée (afin de définir les groupements devant être supprimés). La notation ASN.1 suivante est employée pour sélectionner les membres d'une famille:

```
FamilyGrouping ::= ENUMERATED {
    entryOnly      (1),
    compoundEntry  (2),
    strands        (3),
    multiStrand    (4) }
```

entryOnly indique que le membre de la famille particulier qui a été sélectionné par l'opération doit être considéré comme appartenant au groupe. Ceci est la valeur par défaut qui assure la compatibilité avec les éditions précédentes des spécifications de l'annuaire.

compoundEntry indique que l'entrée composée complète qui a été sélectionnée par l'opération doit être considérée comme une unité en combinant tous les attributs. Pour les opérations de suppression d'entrée, ceci ne s'applique que lorsque le nom de l'objet spécifié est celui d'un ascendant d'une entrée composée, et entraîne la suppression de tous les membres de la famille par la même opération (soumise à la commande d'accès).

strands indique que toutes les branches associées au membre de la famille doivent être sélectionnées par l'opération. Cette option n'est pas valable pour les opérations de suppression d'entrée. Pour les opérations de recherche, les branches sont examinées individuellement aux fins de filtrage. Si l'ensemble combiné d'attributs d'une ou de plusieurs branches concorde avec le filtre, l'entrée composée est considérée comme concordant avec le filtre. Si l'objet de base est un membre enfant, il n'est tenu compte que des branches qui passent par cet objet de base. Pour les opérations de comparaison, l'ensemble des attributs de tous les membres de la famille dans toutes les branches auxquelles l'entrée appartient doit être utilisé pour comparaison.

multiStrand ne s'applique qu'aux opérations de recherche, et satisfait à la règle de concordance en matière de filtrage sur la base de l'information sur la famille. Il n'est pas tenu compte de cette option pour les autres opérations. Elle spécifie qu'une seule branche de chaque famille dans une entrée composée doit être examinée à la fois, mais dans toutes les combinaisons. **multiStrand** ne s'applique pas si l'objet de base est un membre de la famille enfant, auquel cas **multiStrand** ne doit pas être pris en compte et **entryOnly** doit lui être substitué.

7.4 Résultats communs (CommonResults)

L'information **CommonResults** ou **CommonResultsSeq** est présente pour qualifier le résultat de chaque opération de consultation que peut accomplir l'Annuaire. Elle est en outre présente dans chaque erreur qui est renvoyée.

CommonResults ::= SET {			
securityParameters	[30]	SecurityParameters	OPTIONAL,
performer	[29]	DistinguishedName	OPTIONAL,
aliasDereferenced	[28]	BOOLEAN	DEFAULT FALSE,
notification	[27]	SEQUENCE SIZE (1..MAX) OF Attribute	OPTIONAL }
CommonResultsSeq ::= SEQUENCE {			
securityParameters	[30]	SecurityParameters	OPTIONAL,
performer	[29]	DistinguishedName	OPTIONAL,
aliasDereferenced	[28]	BOOLEAN	DEFAULT FALSE,
notification	[27]	SEQUENCE SIZE (1..MAX) OF Attribute	OPTIONAL }

NOTE – Les composantes des informations **CommonResults** et **CommonResultsSeq** sont les mêmes. Les premières sont employées lorsqu'elles figurent parmi les types fixés par le type **COMPONENT OF**, tandis que les secondes sont utilisées de la même manière dans les types séquentiels.

Le composant **SecurityParameters** est spécifié au § 7.10. Si le résultat doit être signé par l'annuaire, le composant **SecurityParameters** doit être inclus dans le résultat. L'absence du composant **SecurityParameters** est considérée comme équivalente à un ensemble vide.

Le nom distinctif **performer** identifie l'exécutant d'une opération donnée. Il peut être nécessaire lorsque le résultat doit être signé (voir § 7.10) et il doit contenir le nom de l'agent DSA qui a signé le résultat.