



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.350

(08/2003)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET
MULTIMÉDIAS

Infrastructure des services audiovisuels – Systèmes et
équipements terminaux pour les services audiovisuels

**Architecture des services d'annuaire pour les
conférences multimédias**

Recommandation UIT-T H.350

RECOMMANDATIONS UIT-T DE LA SÉRIE H
SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
SYSTÈMES ET ÉQUIPEMENTS TERMINAUX POUR LES SERVICES AUDIOVISUELS	H.300–H.399
SERVICES COMPLÉMENTAIRES EN MULTIMÉDIA	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES À LARGE BANDE ET MULTIMÉDIAS TRI-SERVICES	
Services multimédias à large bande sur VDSL	H.610–H.619

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

Recommandation UIT-T H.350

Architecture des services d'annuaire pour les conférences multimédias

Résumé

La présente Recommandation décrit une architecture des services d'annuaire pour les conférences multimédias utilisant le protocole LDAP. Les services d'annuaire normalisés peuvent prendre en charge l'association de personnes à des extrémités, à des pages blanches consultables et à des hyperliens de numérotation. Les services d'annuaire peuvent également aider à la configuration des extrémités et à l'authentification par l'utilisateur sur la base de sources de données autorisées. La présente Recommandation décrit un schéma normalisé du protocole LDAP afin de représenter des extrémités dans le réseau et de les associer à des utilisateurs. Elle étudie les considérations relatives à la conception et à l'implémentation pour l'interdépendance d'annuaires publics, d'annuaires d'entreprise, de serveurs d'appels et d'extrémités spécifiquement vidéo et audio.

Source

La Recommandation H.350 de l'UIT-T a été approuvée par la Commission d'études 16 (2001-2004) de l'UIT-T le 6 août 2003 selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

H.235, H.320, H.323, LDAP, services d'annuaire, SIP.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

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

© UIT 2004

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

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
1.1	Objectifs de conception 2
1.2	Extension du schéma 3
2	Références..... 5
2.1	Références normatives..... 5
2.2	Références informatives 5
3	Définitions 5
4	Abréviations..... 6
5	Conventions 6
6	Définition de la classe commURIObject 6
6.1	commURIObject..... 6
6.2	commURI 7
7	Définition de la classe commObject..... 7
7.1	commObject 7
7.2	commUniqueId 8
7.3	commOwner 8
7.4	commPrivate..... 9
8	Fichiers commObject en format LDIF 9
8.1	Format LDIF pour fichier commURIObject 9
8.2	LDIF pour commObject 11
	Annexe A – Profil d'indexation..... 12
	Appendice I – Considérations relatives à l'implémentation..... 13
	I.1 Relation des annuaires d'entreprise avec les annuaires commObject..... 13
	Appendice II – Flux d'appels 14
	II.1 Scénarios de flux d'appel..... 14
	Appendice III – Annexes électroniques 17

Recommandation UIT-T H.350

Architecture des services d'annuaire pour les conférences multimédias

1 Domaine d'application

La présente Recommandation décrit une architecture des services d'annuaire pour les conférences multimédias utilisant le protocole LDAP. Les services d'annuaire normalisés peuvent prendre en charge l'association de personnes à des extrémités, à des pages blanches consultables et à des hyperliens de numérotation. Les services d'annuaire peuvent également aider à la configuration des extrémités et à l'authentification par l'utilisateur sur la base de sources de données autorisées. La présente Recommandation décrit un schéma normalisé du protocole LDAP afin de représenter les extrémités dans le réseau et de les associer à des utilisateurs. Elle étudie les considérations relatives à la conception et à l'implémentation pour l'interdépendance d'annuaires publics, d'annuaires d'entreprise, de serveurs d'appels et d'extrémités spécifiquement vidéo et audio.

L'utilisation d'une source commune de données autorisées pour les informations de serveur d'appels, d'extrémité, d'utilisateur, d'authentification et de pages blanches est un important aspect des environnements de conférences multimédias à grande échelle. Sans une source commune de données, les fournisseurs de services doivent créer des processus distincts afin de gérer chacune de ces fonctions. En normalisant le schéma de protocole LDAP utilisé afin de représenter les données sous-jacentes, les produits issus de différents vendeurs de système peuvent être déployés de concert afin de créer un environnement applicatif global. Par exemple, un moteur de recherche dans les pages blanches, mis au point par un fournisseur donné, pourrait fournir des informations d'annuaire à des téléphones IP produits par un second fournisseur, la signalisation étant gérée par un serveur d'appels produit à son tour par un troisième fournisseur. Chacun de ces systèmes disparates peut accéder à la même source de données sous-jacentes, ce qui réduit ou élimine la nécessité de coordonner les gestions particulières à chaque système. Un notable avantage pour l'utilisateur est que la gestion de ces données peut être incorporée dans les outils de gestion existants du client, ce qui permet une rapide et flexible amélioration des applications. En réalité, si de nombreux fournisseurs de solutions techniques ont déjà intégré le protocole LDAP dans leurs produits, ils y ont été forcés sans bénéficier d'un schéma normalisé. La présente Recommandation représente un effort visant à normaliser ces représentations et à améliorer l'interopérabilité et la qualité de fonctionnement.

Bien que les adresses URL soient déjà normalisées pour plusieurs protocoles de conférence, leur représentation dans un annuaire ne l'est pas. La présente Recommandation prend en charge une méthode normalisée d'exploration et de localisation des adresses URL. C'est là une étape nécessaire pour prendre en charge les 'hyperliens de numérotation'.

La gestion des configurations d'extrémité peut être améliorée si les réglages corrects sont mémorisés par le fournisseur de services à un emplacement qui est accessible aussi bien par le fournisseur de services que par l'extrémité. Le protocole LDAP fournit un emplacement de stockage pratique qui peut être consulté aussi bien par le serveur d'appels que par l'extrémité. Il est donc possible d'utiliser l'annuaire afin de prendre en charge la configuration d'extrémité, qui est importante pour simplifier le fonctionnement et prendre en charge la mobilité de l'utilisateur. Noter que d'autres techniques prennent également en charge la configuration d'extrémité, en particulier l'utilisation du protocole SNMP afin qu'une configuration complète et des enregistrements de serveur complets permettent d'obtenir les adresses du serveur d'inscriptions. Il convient donc de considérer la présente Recommandation, non pas comme une architecture de configuration d'extrémité autorisée, mais plutôt comme un outil pouvant aider à effectuer cette tâche. Noter que l'utilisation de la présente Recommandation implique une configuration d'extrémité fonctionnellement spécifique, de sorte qu'il est souhaitable que chaque extrémité ait une configuration unique.

Cette architecture utilise une classe d'objets génériques, appelée `commObject`, afin de représenter des attributs communs à tout protocole vidéo ou audio. Les classes auxiliaires représentent des protocoles spécifiques, tels que H.323, H.235, ou H.320, comme décrit dans la série des Recommandations H.350.x. De multiples classes H.350.x peuvent être combinées afin de représenter les extrémités qui prennent en charge plusieurs protocoles. Par exemple, les extrémités qui prennent en charge les protocoles H.323, H.235 et H.320 comporteront les protocoles H.350, H.350.1, H.350.2 et H.350.3 dans leurs représentations LDAP. Par ailleurs, chaque entrée devrait contenir la classe `commObject` en tant que classe d'objets structurelle de cette entrée.

Il y a deux composants de base dans l'architecture. L'objet `commURI` constitue une classe dont la seule fonction est d'associer une personne ou une ressource à une classe `commObject`. En plaçant un 'pointeur' `commURI` dans l'entrée d'annuaire d'un individu, celui-ci devient l'associé de l'objet `commObject` particulier qui a été visé. De même, l'objet `commObject` contient un pointeur, appelé `commOwner`, qui pointe sur l'individu ou la ressource associé(e) à l'objet `commObject`. C'est de cette façon que des personnes ou des ressources peuvent être associées à des extrémités. Le seul changement requis dans l'annuaire d'entreprise est l'adjonction de la simple classe d'objets `commURI`. Des données `commObject` peuvent être instanciées dans le même annuaire ou dans des annuaires totalement distincts, ce qui offre une flexibilité lors de l'implémentation.

1.1 Objectifs de conception

Des déploiements à grande échelle de services vidéo et audio par protocole IP ont démontré qu'un logiciel médiateur était nécessaire en complément des services d'annuaire. Les administrateurs de services ont besoin de serveurs d'appels compatibles avec les annuaires d'entreprise afin d'éviter la duplication des processus de gestion de compte. Les utilisateurs ont besoin des "pages blanches" afin de localiser d'autres utilisateurs avec lesquels ils souhaitent communiquer. Tous ces processus devraient extraire leurs informations de sources de données canoniques afin de réduire les processus administratifs redondants et de garantir l'exactitude des informations. Les critères de conception ci-après sont établis pour cette architecture, qui:

- 1) permet d'associer des informations d'extrémité à des personnes. En variante, cette architecture permet d'associer des informations d'extrémité à des ressources telles que des salles de conférence ou des salles de classe;
- 2) permet de consulter en ligne des "pages blanches" dans lesquelles les informations de numérotation (par exemple des adresses d'extrémité) peuvent être trouvées, de même que d'autres informations d'annuaire "traditionnelles" au sujet d'un utilisateur, telles que nom, adresse, téléphone, courriel, etc.;
- 3) permet de mémoriser toutes les informations d'extrémité dans une source de données canoniques (l'annuaire) plutôt que de les laisser dans le serveur d'appels local, de façon que les extrémités puissent être gérées par manipulation d'un annuaire d'entreprise plutôt que par entrée directe dans le serveur d'appels;
- 4) permet la création d'annuaires répartis à très grande échelle, qui contiennent des "portails" de consultation de pages blanches permettant de rechercher des utilisateurs dans de multiples annuaires institutionnels. Dans cette application, chaque annuaire d'entreprise s'inscrit auprès d'un annuaire d'annuaires (ou est fortuitement découvert par celui-ci). Cet annuaire d'annuaires est capable d'explorer de multiples annuaires en protocole LDAP;
- 5) permet de prendre en charge de multiples instances d'extrémité pour chaque utilisateur ou ressource;
- 6) représente les extrémités qui prennent en charge plusieurs protocoles, par exemple les extrémités qui sont à la fois H.320 et H.323;
- 7) mémorise assez d'informations au sujet de la configuration d'extrémité de façon que les réglages corrects de configuration puissent être décrits extrémité par extrémité aux

utilisateurs finals à titre d'utilitaire, ou puissent être chargés automatiquement dans l'extrémité;

- 8) est extensible dans la mesure nécessaire pour pouvoir y inclure des attributs propres à l'implémentation;
- 9) n'intervient pas dans l'annuaire d'entreprise, de façon que la prise en charge des conférences multimédias puisse être ajoutée de façon modulaire sans apporter de modifications notables à l'annuaire d'entreprise.

Le domaine d'application de la présente Recommandation ne contient pas d'extensions fonctionnelles des protocoles, définies à l'intérieur de ceux-ci. La présente Recommandation ne vise pas à ajouter des éléments de service, mais seulement à représenter des attributs de protocole existants. L'exception à ce cas se produit lorsque la fonctionnalité est impliquée par l'annuaire proprement dit, comme l'attribut `commPrivate`.

1.2 Extension du schéma

Les classes d'objets H.350 peuvent être étendues selon les nécessités pour des implémentations spécifiques. Par exemple, une classe peut être étendue de façon à prendre en charge des codes de référence de facturation. Les extensions du schéma ne sont pas considérées comme faisant partie de la norme et n'impliquent pas la conformité.

Dans certains cas, il peut être nécessaire d'étendre les schémas H.350 afin de représenter plus d'informations que les Recommandations ne peuvent en représenter. Cette possibilité peut être importante pour les développeurs qui implémentent une fonctionnalité d'extrémité non normalisée qu'il faut représenter par des attributs dans l'annuaire. Elle peut également être importante pour des applications commerciales. Par exemple, les attributs "modelNumber" et "accountNumber" sont des exemples d'attributs qui ne sont pas définis dans la norme mais qui peuvent être utiles s'il sont implémentés. L'adjonction d'attributs à cette architecture doit être effectuée de façon à ne pas compromettre la compatibilité avec la présente Recommandation.

Une analyse approfondie de la conception et de l'extension du schéma déborde du domaine d'application de la présente Recommandation. Voir le document IETF RFC 2252 pour les détails. Il existe deux méthodes fondamentales d'extension de schéma qui ne compromettent pas la compatibilité avec la présente Recommandation: l'extension par sous-classe et l'extension par classes auxiliaires.

1.2.1 Extension par sous-classe

Il est possible de créer une sous-classe d'une classe existante d'objets prédéfinis afin de lui ajouter de nouveaux attributs. Pour créer une sous-classe, une nouvelle classe d'objets doit être définie comme une sous-classe de celle qui existe par indication dans la définition de la nouvelle classe du fait que la classe existante est son supérieur. Une fois que la sous-classe est créée, de nouveaux attributs peuvent y être définis.

L'exemple suivant montre comment la classe `commObject` peut être sous-classée afin d'ajouter un attribut représentant un compte de facturation et un gestionnaire de facturation.

```
objectclass ( BillingInfo-OID
NAME 'BillingInfo'
DESC 'Billing Reference Information'
SUP commObject STRUCTURAL
MAY ( BillingAccount $ BillingManager $ )
)
```

Noter que l'identificateur `BillingInfo-OID` doit être remplacé par un identificateur OID réel. Noter également que, chaque fois qu'une classe structurelle est étendue, sa sous-classe doit également être structurelle.

L'entrée échantillon suivante montre les attributs nouvellement créés. Cet exemple utilise également le protocole de la Rec. UIT-T H.350.1 pour l'élément "h323Identity".

```
dn: commUniqueId=2000,ou=h323identity, dc=company, dc=com
objectclass: top
objectclass: commObject
objectclass: h323Identity
objectclass: BillingInfo
commUniqueId: 2000
BillingAccount: 0023456
BillingManager: John Smith
```

Noter que cet exemple et cette méthode démontrent l'extension de la classe d'objets générale commObject et non pas l'extension de classes H.350.x individuelles. Si l'on souhaite étendre une classe auxiliaire H.350.x, cette opération devrait être effectuée par la définition de classes auxiliaires supplémentaires prenant en charge les attributs recherchés, comme décrit au § 1.2.2.

1.2.2 Extension par utilisation de classes auxiliaires

Il est possible d'ajouter des attributs à une entrée LDAP en définissant une classe auxiliaire contenant les nouveaux attributs et en appliquant ces attributs à des valeurs instanciées dans l'annuaire. La classe auxiliaire ne sera pas sous-classée à partir d'une classe d'objets existante. Noter que cette classe auxiliaire devrait avoir comme supérieur la classe sommitale spéciale. L'exemple suivant crée les mêmes attributs de compte de facturation et de gestionnaire de facturation que dans l'exemple précédent, mais en les définissant dans leur propre classe auxiliaire.

```
objectclass ( BillingInfo-OID
NAME 'BillingInfo'
DESC 'Billing Reference Information'
SUP top AUXILIARY
MAY ( BillingAccount $ BillingManager $ )
)
```

Noter la façon dont le supérieur a passé de "commObject" à "top" et comment la classe d'objets est passée de structurelle à auxiliaire.

Il est recommandé que tous les attributs contenus dans la classe auxiliaire soient facultatifs plutôt qu'obligatoires. De cette façon, la classe auxiliaire d'objets elle-même peut être associée à une entrée, que des valeurs soient ou non présentes pour ses attributs.

L'exemple suivant montre une extrémité échantillon qui utilise la nouvelle classe auxiliaire et les nouveaux attributs. Cet exemple utilise également le protocole H.350.1 pour l'élément "h323Identity".

```
dn: commUniqueId=2000,ou=h323identity, dc=company, dc=com
objectclass: top
objectclass: commObject
objectclass: BillingInfo
commUniqueId: 2000
BillingAccount: 0023456
BillingManager: John Smith
```

1.2.3 Identificateurs d'objet

Un identificateur d'objet (OID, *object identifier*) pour un attribut est un unique identificateur numérique habituellement écrit sous la forme d'une séquence d'entiers séparés par des points. Par exemple, l'identificateur OID pour l'attribut commUniqueId est 0.0.8.350.1.1.2.1.1. Tous les attributs doivent avoir un identificateur OID. Les identificateurs OID peuvent être obtenus auprès de quiconque en possède déjà un et est disposé à en déléguer une partie sous forme d'arc, en

conservant un enregistrement de cet arc afin d'éviter les doubles emplois. Par ailleurs, l'Autorité chargée de l'assignation des numéros Internet (IANA, *Internet assigned numbers authority*) attribue des identificateurs OID à toute organisation qui le demande.

2 Références

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

2.1 Références normatives

- IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification*. (Protocole rapide d'accès à l'annuaire (version 3) – Spécification technique).

2.2 Références informatives

- Recommandation UIT-T H.225.0 (2003), *Protocoles de signalisation d'appel et paquets des flux monomédias pour les systèmes de communication multimédias en mode paquet*.
- Recommandation UIT-T H.235 (2003), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)*.
- Recommandation UIT-T H.320 (1999), *Systèmes et équipements terminaux visiophoniques à bande étroite*.
- Recommandation UIT-T H.323 (2003), *Systèmes de communication multimédia en mode paquet*.
- HOWES (Timothy A.), PhD, SMITH (Mark C.), GOOD (Gordon S.): *Understanding And Deploying LDAP Directory Services*, New Riders Publishing, 1999, ISBN: 1578700701. (Compréhension et déploiement des services d'annuaire en protocole LDAP)
- HOWES (Timothy A.), PhD, SMITH (Mark C.): *LDAP Programming Directory-Enabled Applications with Lightweight Directory Access Protocol*, New Riders Publishing, 1997, ISBN: 1578700000. (Applications de programmation LDAP activées par l'Annuaire en protocole rapide d'accès à l'Annuaire).

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 serveur d'appels: générateur de signalisation propre à un protocole qui route les appels vidéo ou audio dans le réseau. Dans la Rec. UIT-T H.323, cette entité est un portier. Dans le protocole SIP, cette entité est un serveur mandataire SIP. Noter que tous les protocoles de signalisation n'utilisent pas de serveur d'appels.

3.2 extrémité: entité logique qui fournit des fonctions de codage/décodage et de signalisation de média vidéo et/ou audio. Exemples:

- 1) un coffret commun de téléconférence qui est situé dans une salle de conférence;
- 2) un téléphone IP;

3) un logiciel qui reçoit des données vidéo et audio d'une caméra et d'un microphone, qui les code et qui applique une signalisation au moyen d'un ordinateur central.

3.3 annuaire d'entreprise: ensemble canonique d'informations relatives à des utilisateurs dans une organisation. Normalement, ces informations sont recueillies auprès de diverses unités organisationnelles afin de créer un ensemble. Par exemple, le département des ressources humaines peut fournir le nom et l'adresse, le service des télécommunications peut fournir le numéro de téléphone, le département informatique peut fournir l'adresse électronique, etc. Pour les fonctions de cette architecture, l'on part du principe qu'un annuaire d'entreprise est accessible par protocole LDAP.

3.4 pages blanches: application qui permet à des utilisateurs finals de rechercher l'adresse d'un autre utilisateur. Cette application peut être de type IP ou faire appel à une autre sorte d'interface avec l'utilisateur.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

CN nom commun (*common name*)

DN nom distinctif (nom propre) (*distinguished name*)

LDAP protocole rapide d'accès à l'annuaire (tel que défini dans la norme RFC 1777) (*lightweight directory access protocol*)

RDN nom distinctif relatif (*relative distinguished name*)

5 Conventions

Dans la présente Recommandation, les conventions suivantes s'appliquent:

l'auxiliaire "doit/doivent" indique une prescription obligatoire;

l'auxiliaire "devrait/devraient" (ou l'expression "il convient") indique une mesure suggérée mais facultative;

l'auxiliaire "peut/peuvent" indique une possibilité d'action plutôt qu'une recommandation de résultat.

Sauf spécification contraire expressément mentionnée, les références aux paragraphes, sous-paragraphes, annexes et appendices renvoient aux points correspondants de la présente Recommandation.

6 Définition de la classe commURIObject

Classe auxiliaire d'objets qui contient l'attribut commURI. Cet attribut est ajouté à un objet de personne ou de ressource afin d'associer à cet objet une ou plusieurs instances de la classe commObject. Ses valeurs sont des identificateurs URI du protocole LDAP qui pointent sur les objets communs associés, par exemple sur le pont de conférence H.323 et sur le téléphone à protocoles IP SIP d'un utilisateur. Noter que de multiples instances d'identificateurs commURI peuvent ne pas pointer sur le même annuaire d'objets commObject. En fait, chaque instance commURI peut pointer sur une extrémité gérée par un fournisseur de services différent.

6.1 commURIObject

OID: 0.0.8.350.1.1.1.2.1

objectclasses: (0.0.8.350.1.1.1.2.1

NAME 'commURIObject'

DESC 'object that contains the URI attribute type'

```
SUP top AUXILIARY
MAY ( commURI )
)
```

6.2 commURI

```
OID: 0.0.8.350.1.1.1.1.1
attributetypes: ( 0.0.8.350.1.1.1.1.1
NAME 'commURI'
DESC 'Labeled URI format to point to the distinguished name of the commUniqueId'
EQUALITY caseExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Classe de qualité d'application

normale

Nombre de valeurs

plusieurs

Définition

Identificateur URI étiqueté contenant une adresse URL du protocole LDAP identifiant l'annuaire contenant l'instance référencée commObject. Le filtre de recherche spécifié par cette adresse URL du LDAP doit spécifier une recherche d'égalité de l'attribut commUniqueId de la classe commObject.

Valeurs admissibles (si contrôlées)

Notes

Utilisé pour trouver l'extrémité de l'utilisateur en question. Le champ d'étiquette peut servir à représenter la fonction de l'extrémité, comme 'téléphone IP résidentiel' ou 'vidéotique' aux fins d'affichage sur l'interface avec l'utilisateur.

Noter que la partie étiquette du champ peut contenir des espaces comme dans l'exemple ci-dessous concernant la 'vidéotique'.

Sémantique

Exemple d'applications pour lesquelles cet attribut serait utile

Exemple (fragment de fichier LDIF)

```
commURI: ldap://directory.acme.com/dc=acme,dc=com??sub?(commUniqueId=bob)
desktop video
```

7 Définition de la classe commObject

Abstraction d'un appareil vidéo ou audio en protocole IP. La classe commObject permet de représenter une extrémité (extrémité H.323 ou agent utilisateur du protocole SIP ou autre extrémité de protocole) avec tous ses pseudonymes au moyen d'une seule entrée dans un annuaire. Noter que chaque entrée d'annuaire devrait contenir la classe commObject en tant que classe d'objets structurelle de cette entrée, laquelle peut également contenir des classes auxiliaires H.350.x.

7.1 commObject

```
OID: 0.0.8.350.1.1.2.2.1
objectclasses: (0.0.8.350.1.1.2.2.1
NAME 'commObject'
DESC 'object that contains the Communication attributes'
SUP top STRUCTURAL
MUST commUniqueId
MAY ( commOwner $ commPrivate )
)
```

7.2 commUniqueId

```
OID: 0.0.8.350.1.1.2.1.1
attributetypes: (0.0.8.350.1.1.2.1.1
NAME 'commUniqueId'
DESC 'To hold the endpoints unique Id'
EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Classe de qualité d'application

normale

Nombre de valeurs

plusieurs

Définition

Identificateur unique de l'extrémité.

Valeurs admissibles (si contrôlées)

Notes

Il s'agit du nom RDN de cet objet. En pratique, il y aura toujours un et un seul identificateur commUniqueId pour chaque extrémité. Cet attribut identifie de façon unique une extrémité dans l'annuaire d'objets commObject. Il doit être unique à l'intérieur de cet annuaire mais peut ne pas l'être à l'échelle mondiale. Cet attribut n'a pas de rapport avec l'annuaire d'entreprise.

Sémantique

Exemple d'applications pour lesquelles cet attribut serait utile

Exemple (fragment de fichier LDIF)

```
commUniqueId: bob
```

7.3 commOwner

```
OID: 0.0.8.350.1.1.2.1.2
attributetypes: 0.0.8.350.1.1.2.1.2
NAME 'commOwner'
DESC 'Labeled URI to point back to the original owner'
EQUALITY caseExactMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Classe de qualité d'application

normale

Nombre de valeurs

plusieurs

Définition

Format d'identificateur URI étiqueté de façon à repointer sur l'objet de personne ou de ressource associé à cette entrée.

Valeurs admissibles (si contrôlées)

Notes

Utilisé comme chercheur d'entrée inverse du ou des détenteurs. Cet attribut peut pointer sur des groupes. Noter que cet identificateur URI peut pointer sur un nom commun (cn), mais, dans les applications où l'on souhaite associer les informations d'authentification aussi bien

à l'annuaire commObject qu'à l'annuaire d'entreprise, il peut être souhaitable que l'attribut commOwner pointe sur un nom propre (dn) plutôt que sur un nom commun (cn), afin d'identifier ainsi de façon unique le détenteur de l'annuaire commObject.

Sémantique

Exemple d'applications pour lesquelles cet attribut serait utile

Exemple (fragment de fichier LDIF)

```
commOwner: ldap://directory.acme.com/dc=acme,dc=com??sub?(cn=bob%20smith)
commOwner: uid=bob,ou=people,dc=acme,dc=com
```

7.4 commPrivate

```
OID: 0.0.8.350.1.1.2.1.3
attributetypes: (0.0.8.350.1.1.2.1.3
NAME 'commPrivate'
DESC 'To decide whether the entry is visible to world or not'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Classe de qualité d'application

normale

Nombre de valeurs

plusieurs

Définition

A la disposition de l'utilisateur afin d'indiquer des options de confidentialité pour une extrémité, c'est-à-dire un numéro confidentiel.

Valeurs admissibles (si contrôlées)

Notes

Cet attribut est défini sous forme d'opérateur booléen. Une future version de la présente Recommandation pourra mettre au point un vocabulaire contrôlé pour cet attribut afin de tenir compte des multiples types de confidentialité.

Sémantique

Exemple d'applications pour lesquelles cet attribut serait utile

Exemple (fragment de fichier LDIF)

```
commPrivate: true
```

8 Fichiers commObject en format LDIF

Le présent paragraphe contient un fichier de configuration de schéma pour les classes commURIObject et commObject. Ce fichier pourra être utilisé afin de configurer un serveur LDAP de façon à prendre ces classes en charge.

8.1 Format LDIF pour fichier commURIObject

```
# Communication Object Schema
#
# Schema for Representing Communication Objects in an LDAP Directory
#
# Abstract
#
# This Recommendation defines the schema for representing Communication
# objects in an LDAP directory [LDAPv3]. It defines schema elements
# to represent a communication object URI [commURIObject].
```

```

#
#
#
#         .1 = Communication related work
#         .1.1 = commURIObject
#         .1.1.1 = attributes
#         .1.1.2 = objectclass
#         .1.1.3 = syntax
#
# Attribute Type Definitions
#
#     The following attribute types are defined in this Recommendation:
#
#         commURI
dn: cn=schema
changetype: modify
#
# if you need to change the definition of an attribute,
#         then first delete and re-add in one step
#
# if this is the first time you are adding the commObject
# objectclass using this LDIF file, then you should comment
# out the delete attributetypes modification since this will
# fail. Alternatively, if your ldapmodify has a switch to continue
# on errors, then just use that switch -- if you are careful
#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.1.1.1.1 NAME 'commURI' )
-
#
# re-add the attributes -- in case there is a change of definition
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.1.1.1.1
    NAME 'commURI'
    DESC 'Labeled URI format to point to the distinguished name of the
commUniqueId'
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
-
# Object Class Definitions
#
#     The following object classes are defined in this Recommendation:
#
#         commURIObject
#
# commURIObject
#
#     This auxiliary object class represents a URI attribute type
#
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.1.2.1 NAME 'commURIObject' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.1.2.1
    NAME 'commURIObject'
    DESC 'object that contains the URI attribute type'
    SUP top AUXILIARY
    MAY ( commURI )
    )
-
#

```

```
# end of LDIF
#
```

8.2 LDIF pour commObject

```
# Communication Object Schema
#
# Schema for Representing Communication Objects in an LDAP Directory
#
# Abstract
#
# This Recommendation defines the schema for representing Communication
# objects in an LDAP directory [LDAPv3]. It defines schema elements
# to represent a communication object [commObject].
#
#
#           .1 = Communication related work
#           .1.2 = commObject
#           .1.2.1 = attributes
#           .1.2.2 = objectclass
#           .1.2.3 = syntax
#
#
# Attribute Type Definitions
#
#   The following attribute types are defined in this Recommendation:
#
#       commUniqueId
#       commOwner
#       commPrivate
dn: cn=schema
changetype: modify
#
# if you need to change the definition of an attribute,
#       then first delete and re-add in one step
#
# if this is the first time you are adding the commObject
# objectclass using this LDIF file, then you should comment
# out the delete attributetypes modification since this will
# fail. Alternatively, if your ldapmodify has a switch to continue
# on errors, then just use that switch -- if you are careful
#
delete: attributetypes
attributetypes: (0.0.8.350.1.1.2.1.1 NAME 'commUniqueId' )
attributetypes: (0.0.8.350.1.1.2.1.2 NAME 'commOwner' )
attributetypes: (0.0.8.350.1.1.2.1.3 NAME 'commPrivate' )
-
#
# re-add the attributes -- in case there is a change of definition
#
#
add: attributetypes
attributetypes: (0.0.8.350.1.1.2.1.1
  NAME 'commUniqueId'
  DESC 'To hold the endpoints unique Id'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
attributetypes: (0.0.8.350.1.1.2.1.2
  NAME 'commOwner'
  DESC 'Labeled URI to point back to the original owner'
  EQUALITY caseExactMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

```

attributetypes: (0.0.8.350.1.1.2.1.3
  NAME 'commPrivate'
  DESC 'To decide whether the entry is visible to world or not'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
-
# Object Class Definitions
#
#   The following object classes are defined in this Recommendation:
#
#       commObject
#
# commObject
#
delete: objectclasses
objectclasses: (0.0.8.350.1.1.2.2.1 NAME 'commObject' )
-
add: objectclasses
objectclasses: (0.0.8.350.1.1.2.2.1
  NAME 'commObject'
  DESC 'object that contains the Communication attributes'
  SUP top STRUCTURAL
  MUST commUniqueId
  MAY ( commOwner $ commPrivate )
  )
-
#
# end of LDIF
#

```

Annexe A

Profil d'indexation

L'indexation d'attributs est une activité propre à l'implémentation, qui dépend de l'implémentation recherchée. Des attributs non indexés peuvent se traduire par des temps de recherche suffisamment longs pour rendre certaines applications inutilisables. L'exploration des utilisateurs et des pseudonymes devrait en particulier être rapide. Le profil d'indexation de la présente annexe décrit une configuration d'indexation pour annuaire commObject. Cette configuration sera optimisée à l'usage des applications d'annuaire d'annuaires. L'emploi de ce profil est facultatif.

commURI: aucune recommandation.

commUniqueId: égalité

commOwner: présence

commPrivate: présence

Appendice I

Considérations relatives à l'implémentation

I.1 Relation des annuaires d'entreprise avec les annuaires commObject

Les informations commObject ont un emplacement distinct des informations relatives aux personnes ou aux ressources. Leur emplacement peut être une sous-arborescence d'un très grand annuaire d'entreprise ou un serveur logique distinct. L'annuaire des personnes continuera à contenir les informations traditionnelles sur les individus ou sur les ressources, comme le nom, le numéro de téléphone, l'adresse, etc. Il contiendra également un lien commURI avec l'attribut commUniqueId contenu dans la classe commObject. Plutôt que d'étendre la classe des objets de personne dans l'annuaire d'entreprise, ce lien offre les avantages suivants:

- 1) les modifications à l'annuaire d'entreprise ne doivent pas être effectuées à la légère et ne sont souvent pas placées sous le contrôle administratif du fournisseur de services vidéo/audio sur IP;
- 2) les éléments associés aux communications vidéo et audio en protocole IP sont très dynamiques. La technique elle-même change rapidement en ce qui concerne l'annuaire d'entreprise. Par exemple, des modifications apportées à un protocole spécifique nécessiteront des modifications dans l'annuaire d'entreprise si la représentation de celui-ci a été héritée d'une classe d'objets contenant des personnes inscrites dans un annuaire d'entreprise et si cette représentation a été imbriquée dans cet annuaire d'entreprise;
- 3) un serveur d'appels peut avoir besoin d'accéder à des données de classe commObject d'une manière très différente de celle dont d'autres applications accèdent à l'annuaire d'entreprise. Un serveur distinct peut au besoin être configuré en fonction d'une politique de performance et d'accès afin de tenir compte de ces exigences d'implémentation. Par exemple, un serveur d'appels peut avoir besoin d'interroger le serveur commObject de nombreuses fois par seconde afin de gérer le traitement des appels en temps réel; il peut également lire et mettre en mémoire cache de nombreux attributs commObject à la fois.

Chaque utilisateur ou ressource possédant des capacités de conférences multimédias devrait avoir une instance de la classe commObject créée et associée à une entrée existante dans l'annuaire d'entreprise avec un identificateur commURI. Les serveurs d'appels peuvent fonctionner de deux façons. La méthode la plus simple consiste, pour le serveur d'appels, à lire périodiquement des instances de la classe commObject dans sa table interne d'extrémité. La méthode préférée et plus flexible consiste, pour le serveur d'appels, à interroger le serveur commObject chaque fois qu'il a besoin d'informations, comme lors de l'inscription d'une extrémité ou l'établissement d'un appel.

I.1.1 Personnes en fonction des ressources

Certaines implémentations de conférences multimédias sont très nettement orientées vers l'extrémité, alors que d'autres le sont vers l'utilisateur. Par exemple, il est courant de rencontrer une extrémité de téléconférence par vidéo de groupe dans une salle de conférence dont l'identité ne change jamais. Cette extrémité peut être appelée 'Salle de conférence 201'. Elle n'est associée à aucune personne en particulier mais elle est associée à la ressource "Salle de conférence 201" et est partagée par tous ceux qui ont besoin d'utiliser cette salle de conférence.

D'autre part, certaines extrémités sont spécifiques du contexte d'utilisateur et fondent leur identité sur leurs utilisateurs actuels. Par exemple, lors de sa connexion à un ordinateur sous l'identité "jdoe", une extrémité informatisée peut se configurer avec l'adresse de "jdoe" telle qu'elle est mémorisée dans le profil de cet utilisateur puis s'inscrire sous ce nom auprès d'un serveur d'appels. D'autres utilisateurs se connectant au même ordinateur peuvent avoir d'autres identités qui leur sont associées, de sorte que leurs messages d'inscription contiendront des informations d'identité différentes.

Cette différenciation des utilisateurs en fonction des ressources rend difficile l'association d'extrémités à des utilisateurs ou à des ressources. En fait, bien que des classes d'objets contenant des personnes soient facilement accessibles, il n'en est pas de même des classes d'objets contenant des ressources. Le fait d'associer un objet de communication à une personne au moyen d'un identificateur commURI généralise cette relation. Si un attribut commOwner pointe sur une classe d'objets contenant des personnes, cet objet de communication est associé à cette personne. Si un attribut commOwner pointe sur une classe d'objets contenant des ressources, cet objet de communication est associé à cette ressource. Inversement, des personnes ou des ressources peuvent avoir des pointeurs commURI qui les associent à des extrémités. Les annuaires d'entreprise qui ne prennent en charge que les personnes et non les ressources peuvent choisir de se contenter de traiter les ressources comme des personnes.

I.1.2 Sécurité et authentification

La plupart des domaines d'authentification sont orientés vers les personnes. Des ressources partagées telles que les systèmes de téléconférence en salle sont donc souvent moins sûres parce qu'elles ne sont pas associées à une identité d'authentification explicite. L'analyse des problèmes d'authentification est hors du domaine d'application de la présente Recommandation mais les réalisateurs sont instamment priés d'effectuer une exploration approfondie des aspects de sécurité correspondant à divers choix d'architecture.

L'accès à des listes de contrôle et les autres mécanismes de sécurité associés à l'annuaire sont hors du domaine d'application de la présente Recommandation. Les réalisateurs sont instamment priés d'examiner de près la confidentialité et la sécurité des données contenues dans l'annuaire.

Appendice II

Flux d'appels

II.1 Scénarios de flux d'appel

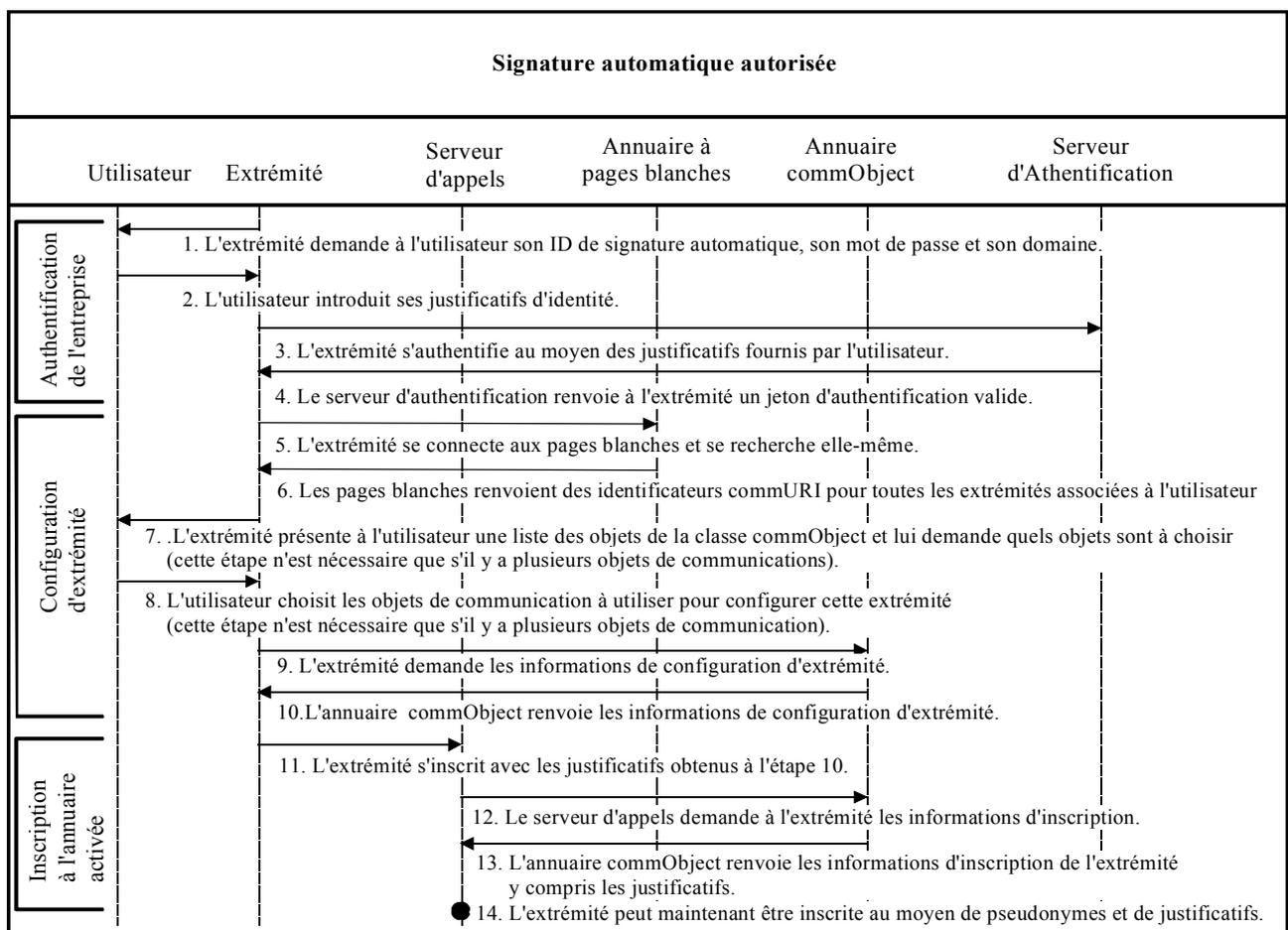
Les flux d'appel suivants représentent des scénarios applicatifs possibles qui montrent comment la Rec. UIT-T H.350 peut être utilisée. Ces flux d'appel n'ont valeur que d'illustration et ne sont pas normatifs. Plus précisément, la Rec. UIT-T H.350 définit la façon dont les éléments de données sont représentés dans les annuaires LDAP et non pas la façon dont ces éléments de données sont utilisés.

II.1.1 Exploration par l'utilisateur des pages blanches

La Figure II.1 montre comment une extrémité activée par protocole LDAP peut explorer un annuaire afin de trouver un utilisateur, obtenir les informations de classe commObject relatives à cet utilisateur, puis composer le numéro de l'extrémité de cet utilisateur. Dans ce scénario, l'extrémité pourrait être préconfigurée de façon à explorer un annuaire d'entreprise particulier ou à explorer un portail d'annuaires qui à son tour explore de nombreux annuaires. Ce scénario montre comment un appareil peut traiter l'exploration en présentant les choix et les résultats au moyen d'une interface avec l'utilisateur. Mais cette fonctionnalité peut également être implémentée au moyen d'une page Internet offrant une numérotation cliquable. Bien que cet exemple décrive une recherche directe par une extrémité en protocole LDAP, il convient de noter qu'il est également possible qu'un serveur d'appels effectue des explorations pour le compte de cette extrémité et qu'il transmette à celle-ci les informations par une voie de communication de remplacement en centralisant ainsi certains aspects de l'accès aux pages blanches.

II.1.3 Signature automatique sécurisée

La Figure II.3 montre comment on peut créer un environnement dans lequel un utilisateur fait appel à une identité existante d'authentification dans une entreprise pour accéder à une parmi plusieurs identités d'extrémité. Ce scénario comporte plusieurs caractéristiques fondamentales qui sont souhaitables dans des déploiements à grande échelle. L'extrémité est configurée automatiquement au moyen d'informations extraites de l'annuaire, ce qui élimine les erreurs d'utilisateur au cours du processus de configuration tout en simplifiant le déploiement. Par ailleurs, l'utilisateur est seulement tenu de mémoriser ses justificatifs de signature automatique, qui sont normalement son identifiant et son mot de passe d'utilisateur dans l'entreprise. Les extrémités peuvent (et devraient souvent) avoir différents justificatifs d'identité mais l'utilisateur n'a pas besoin de les connaître car ils sont chargés directement dans l'extrémité à partir de l'annuaire. Etant donné que les justificatifs d'extrémité sont chargés automatiquement, il est possible qu'ils soient fréquemment rafraîchis. Par exemple, un utilitaire de gestion pourrait produire des justificatifs aléatoires pour chaque extrémité et les mémoriser dans l'annuaire commObject au cours de chaque nuit, ce qui crée un environnement très sécurisé dans lequel les justificatifs peuvent être très robustes car ils peuvent être reconstitués rapidement même s'ils ont été découverts ou sont périmés. Ce scénario prend en charge l'utilisation d'identifiants/mots de passe ou de justificatifs d'extrémités fondés sur un certificat. Les certificats ont généralement été trouvés difficiles à mettre en œuvre car ils sont difficiles à gérer par les utilisateurs. Le présent scénario résout le problème de la gestion des certificats et ouvre la possibilité que ceux-ci soient gérés par un système central de gestion de certificats ou pour le compte de ce système, plutôt que pour le compte d'utilisateurs, ce qui épargne à ces derniers la complexité de l'infrastructure PKI tout en leur offrant ses avantages en matière de sécurité.



H.350_FA.3

Figure II.3/H.350 – Signature automatique sécurisée

Dans ce scénario, les étapes d'authentification représentent un utilisateur qui s'identifie auprès d'un serveur d'authentification existant, déjà déployé pour un système d'authentification par signature automatique à usage général (par exemple courriel, hypernavigation, partage de fichiers). Une fois authentifié, l'utilisateur peut se connecter directement au serveur LDAP et extraire toutes les informations de configuration relatives à l'extrémité sélectionnée, c'est-à-dire les données de configuration et les justificatifs d'authentification pour cette extrémité. Finalement, au moyen de ces justificatifs, l'extrémité peut s'authentifier auprès du serveur d'appels en utilisant tout mécanisme d'authentification installé (par exemple selon l'Annexe D ou E/H.235). Il convient d'utiliser la sécurité de couche Transport afin d'assurer la confidentialité de ces transactions.

Appendice III

Annexes électroniques¹

Le fichier `commURI.ldif.txt` ci-joint contient une version en texte seulement du fichier LDIF décrit au § 8.1.



`commURI.ldif.txt`

Le fichier `commObject.ldif.txt` ci-joint contient une version en texte seulement du fichier LDIF décrit au § 8.2.



`commObject.ldif.txt`

¹ Dans le but d'aider les utilisateurs de la version imprimée, le contenu de cet appendice est disponible gratuitement sur le site web des publications de l'UIT à l'adresse:

<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.350>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication