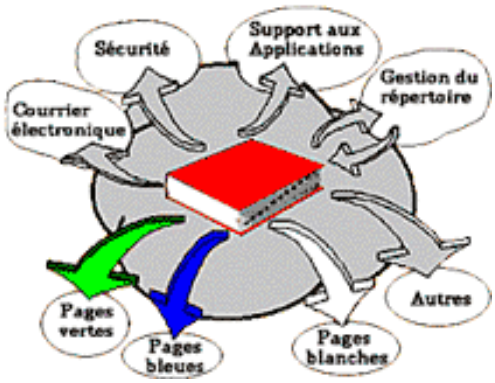
CONCEPTION DÉTAILLÉE

DU RÉPERTOIRE GOUVERNEMENTAL QUÉBÉCOIS



Document pour fins de consultation gouvernementale

1997-12-01

Sous-secrétariat à l'inforoute et aux ressources informationnelles
Secrétariat du Conseil du trésor

TABLE DES MATIÈRES

AVANT PROPOS

Les technologies de l'information et des communications posent des défis importants par leur évolution rapide et les possibilités exceptionnelles qu'elles offrent pour le renouvellement des services publics. Qu'il s'agisse d'améliorer la prestation des services en renforçant l'approche clientèle, de faciliter l'échange et l'exploitation de l'information, de rendre disponibles des services mieux adaptés ou d'en réduire les coûts, le recours aux technologies de l'information et l'adaptation à leur évolution sont incontournables. Par ailleurs, la diversité des éléments à prendre en compte et l'ampleur des investissements requis par la mise en place des nouvelles façons de faire exigent une vision globale ainsi qu'une collaboration entre tous les intervenants pour guider le changement et convenir des voies à suivre.

Une coordination gouvernementale dans le domaine des technologies de l'information est donc d'une importance stratégique pour assurer leur intégration et leur utilisation optimales dans l'Administration. Cette fonction, dévolue à la Sous-secrétariat à l'inforoute et aux ressources informationnelles (DCGTI) du Sous-secrétariat aux marchés publics et aux technologies de l'information du Secrétariat du Conseil du trésor, se concrétise par plusieurs actions dont l'élaboration d'orientations dans différents domaines, la proposition d'infrastructures et de services communs, le maintien d'un tableau de bord sur l'utilisation des technologies dans l'Administration, l'adaptation du cadre de gestion, etc..

Afin de réaliser cette fonction de coordination le plus efficacement possible, la DCGTI s'associe avec tous les ministères et les organismes et elle souhaite leur implication. Elle entend procéder à une large consultation sur les projets d'orientations, d'infrastructures et de services communs ainsi que de politiques avant que ces projets ne deviennent des positions gouvernementales officielles. La DCGTI entend également faire appel à la collaboration des ministères et des organismes dans la mise en place des mesures et des mécanismes de suivi de l'action gouvernementale en regard des technologies.

Le document qui suit s'inscrit dans cette foulée. La DCGTI soumet par la présente à la consultation gouvernementale une version préliminaire du document de conception détaillée du Répertoire gouvernemental. Ce document s'inspire de normes internationales de l'ISO (X.500) et de l'Internet (LDAP) qui marquent le développement de l'inforoute sur le plan mondial et mise sur l'expérience accumulée dans diverses Administrations. Il s'appuie sur une analyse circonstanciée de la question afin de proposer une solution concrète aux problèmes de l'Administration québécoise en termes de partage et d'exploitation des ressources informationnelles en réseau, et ce dans le respect des mesures de sécurité les plus strictes.

On peut soumettre toute question ou tout commentaire sur le document qui suit à :

M. René Lortie
Téléphone : (418) 528-6145
Télécopieur : (418) 646-3571
Courriel : rlortie@sct.gouv.qc.ca

M. Richard Parent
Téléphone : (418) 528-6147
Télécopieur : (418) 646-3571
Courriel : rparent@sct.gouv.qc.ca

Adresse Civique :
Secrétariat du Conseil du trésor
Direction de la coordination gouvernementale
en technologies de l'information
875, Grande Allée Est, 3e étage, section C
Québec (Québec) G1R 5R8

Note au lecteur : Il est possible que certaines erreurs linguistiques se soient glissées lors de la rédaction de ce document. La version officielle qui résultera de la consultation sera soumise à une révision linguistique plus poussée.

REMERCIEMENTS

Les auteurs tiennent à remercier particulièrement les personnes suivantes pour leur contribution au présent document :

- M. Jack L. Finley, du E-mail Program Management Office au Gouvernement fédéral américain, pour son assistance et son soutien, et notamment pour son encouragement à exploiter les documents produits par son équipe ;
- M^{me} Angèle Gosselin, des Services gouvernementaux de télécommunications et d'informatique des Travaux publics et Services gouvernementaux Canada, pour sa disponibilité à partager l'expérience acquise dans la mise en place des services de répertoire du gouvernement canadien ;
- M. Wallace Schwab, des Services Maurepas, traducteur et terminologue, pour sa contribution à l'élaboration d'une terminologie française appropriée et la traduction initiale de documents américains ;
- M^{me} Sophie Cormier, pour sa contribution à l'illustration du document et à son adaptation pour diffusion sur le Web ;
- M^{me} Johanne Tessier, pour sa contribution à la saisie, l'harmonisation et la mise en forme du texte ;
- M. Louis Lamothe, chef du Service de l'infrastructure et des services communs à la Sous-secrétariat à l'inforoute et aux ressources informationnelles, responsable à ce titre du dossier de la conception du Répertoire gouvernemental.

La participation ponctuelle de firmes spécialisées a également été sollicitée à un moment ou l'autre de la réalisation du document et de l'analyse qui a précédé. Il convient notamment de mentionner les firmes Gartner Group, Meta Group et Booz.Allen et Hamilton.

Les coauteurs,

René Lortie
Richard Parent

TABLE DES MATIÈRES GÉNÉRALES

CHAPITRE 1

1.0 Vue générale

La présente section a pour objet de situer le Répertoire gouvernemental dans le contexte du déploiement de l'inforoute et d'illustrer sommairement certaines de ses fonctionnalités, débouchant sur la nécessité de réaliser une conception détaillée du Répertoire, dont la teneur, annoncée en introduction, fera l'objet des chapitres suivants.

1.1 Contexte

Pour un ensemble de raisons aussi bien économiques que sociales et culturelles, dans un contexte de mondialisation des échanges, de tertiarisation de l'économie et d'implantation généralisée d'une véritable société de l'information, l'appareil d'État doit rehausser l'efficacité, l'efficience et la cohérence de son action. Ce constat et cette nécessité s'imposent à tout État moderne. Le Québec n'y fait pas exception. En réponse à ces exigences, diverses mesures ont déjà été prises allant dans le sens du renouvellement de l'Administration québécoise. La conception détaillée du Répertoire électronique gouvernemental, que livre le présent document, est de celles-là.

Le Répertoire gouvernemental s'inscrit ainsi dans le contexte général de la mise en place de l'inforoute gouvernementale. L'inforoute gouvernementale constitue une composante majeure de l'inforoute québécoise, elle-même partie intégrante de l'inforoute mondiale en voie d'établissement. La conception de l'inforoute gouvernementale procède d'une vision globale ralliant les intervenants du Secrétariat du Conseil du trésor et qui teinte chacun des projets qui en découlent, dont le Répertoire. Cette vision, illustrée à la Figure 1-1, s'harmonise tout à fait avec les intentions et les efforts de planification stratégique à l'échelle gouvernementale.

Essentiellement, la poursuite des objectifs de l'État inhérents à ses diverses missions doit être centrée sur le client, dans le plus grand souci de cohérence interne entre les ministères et les organismes.

« La poursuite de ces objectifs doit aller de pair avec une préoccupation de réduire les lourdeurs administratives et de prévoir de nouveaux modes de partenariat entre les ministères et les organismes, les autres administrations et l'entreprise privée. Elle doit également prévoir la régionalisation en tendant à rapprocher la gestion des services publics des clientèles qu'ils desservent. Les ministères et les organismes devront rechercher la simplification et la rationalisation des structures et programmes existants. L'organisation de l'ensemble des services de l'État devra être améliorée (des services plus accessibles, plus rapides, mieux adaptés), rationalisée (conforme aux possibilités de l'État) et simplifiée (services mieux intégrés et harmonisés).

Présence unie et forte, approche clientèle, guichets uniques, partage et échange de l'information, cohérence de l'action gouvernementale, initiatives structurantes, mise à profit d'infrastructures technologiques, allégement administratif, voilà autant de principes, de projets et d'exigences qui concourent à la mise en place d'une véritable inforoute gouvernementale, vecteur des efforts de l'ensemble des ministères et organismes vers l'atteinte des objectifs gouvernementaux de développement économique, culturel et social.

L'inforoute gouvernementale peut contribuer au passage de l'État couloirs, compartimenté, vers l'État réseau, au fonctionnement organique, favorisant l'échange continu avec ses clientèles et une compétitivité accrue de la société québécoise par un recours structuré, coordonné et concerté aux possibilités offertes par les technologies de l'information en réseau. »[1]

[1] L'inforoute gouvernementale : notre vision, DCGTI, Secrétariat du Conseil du trésor, 7 novembre 1997

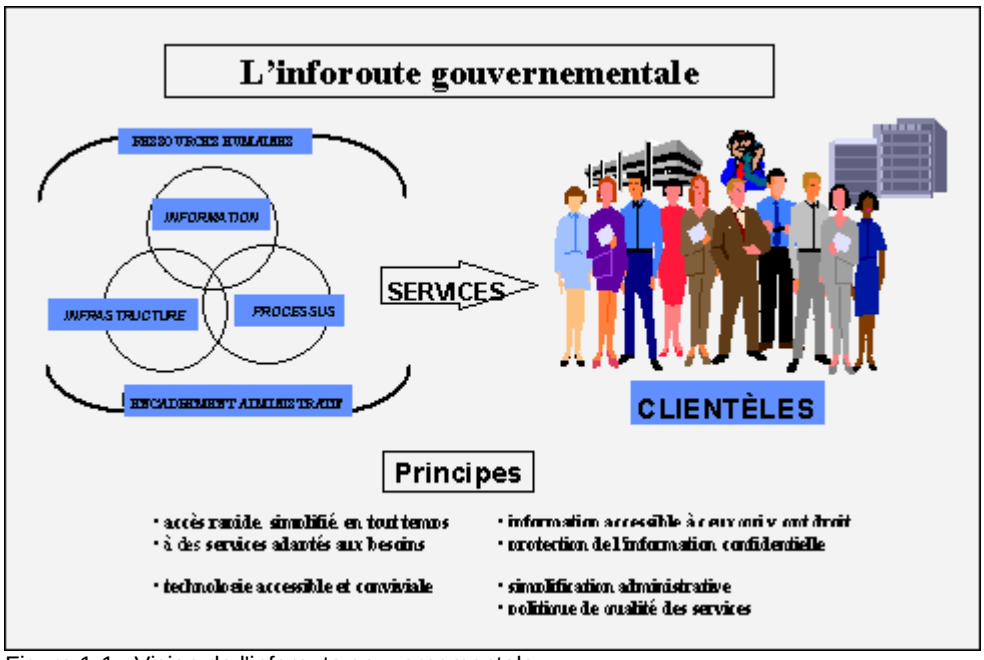


Figure 1-1 : Vision de l'inforoute gouvernementale

Conçue dans ces termes, l'inforoute gouvernementale assurera l'échange, le partage et le traitement de l'information à l'aide d'infrastructures communes dans le cadre de processus de travail visant à produire des services à l'intention des clientèles du gouvernement. Comptant parmi les infrastructures communes, le Répertoire aura, dans ce contexte, à jouer un rôle tout à fait essentiel.

1.2 Un aperçu du Répertoire gouvernemental

Infrastructure d'échange et de communication, l'inforoute permet de partager et de réutiliser un certain nombre d'« objets » d'intérêt commun. Encore faut-il pouvoir repérer ces objets. Dans un premier temps, il faut ne serait-ce que pouvoir repérer l'adresse électronique de ses interlocuteurs. Il faut localiser des sources d'information, repérer et partager l'information pertinente, des documents, des données de toutes sortes. Intégrer ces données dans des applications, de façon automatique ou non. Assurer l'accès, la rationalisation et la réutilisation, dans la recherche de l'efficience, de la cohérence et de l'efficacité des opérations gouvernementales. Il faut pouvoir assurer la sécurité de l'accès et des échanges : plus il y a partage possible, plus resserrées doivent être les mesures de sécurité. Le répertoire électronique gouvernemental est une pièce essentielle pour répondre à ces besoins, dans le contexte proprement gouvernemental comme dans celui de la société québécoise et mondiale.

La solution apportée par le Répertoire Gouvernemental repose sur une organisation de l'information qui en permet la désignation unique et sans ambiguïté, la gestion, le partage et la réutilisation. La mise en œuvre de cette solution suppose une technologie appropriée. Par ailleurs, la solution recherchée doit s'inscrire harmonieusement dans la philosophie administrative qui prévaut et qui est fondée sur la responsabilisation des ministères et organismes. Il existe un modèle de répertoire convenant à ces exigences. Il s'agit du répertoire X.500, issu des travaux d'organismes de normalisation internationale. Ce modèle de répertoire a été conçu à l'origine, soit il y a environ dix ans, pour répondre à des besoins précis dans le domaine des télécommunications. La richesse de sa conception a toutefois bientôt permis d'en élargir considérablement l'usage. Le modèle d'information du répertoire X.500 a été repris par

l'Internet et tous les grands producteurs informatiques s'inspirent à des degrés divers de ce modèle pour la conception de leur propre répertoire.. Si les protocoles développés à l'origine dans le monde Internet pour palier certaines lourdeurs de fonctionnement des répertoires X.500 sur les micro-ordinateurs de l'époque ont ouvert une voie complémentaire, et quelquefois parallèle, à la conception des répertoires, il demeure une volonté maintes fois affirmée de conserver le même modèle d'information et d'harmoniser le fonctionnement des répertoires totalement conformes à X.500 et d'inspiration Internet, de sorte qu'en définitive, l'essentiel du modèle de répertoire X.500 loge au cœur du développement de l'inforoute.

Pointant vers les ressources de tous ordres que l'on désire faire connaître aux personnes comme aux applications informatiques, le mécanisme de répertoire fournit l'accès aux « cartes routières » de l'inforoute, dont il constitue le centre nerveux et le centre d'aiguillage. Essentiellement, un répertoire X.500 est une base de données répartie optimisée pour fournir des références, soit un dispositif d'emmagasinage d'information sur des « objets » d'intérêt pour une communauté d'usagers (ex. : le gouvernement, un ministère, les responsables de la gestion du personnel, les clientèles du gouvernement, la population, etc.). La base est répartie sur plusieurs serveurs relevant chacun, selon le cas, d'une organisation toute entière ou d'une unité administrative donnée, qui gèrent chacun en propre l'information qui les concerne directement, selon un modèle général d'information partagé par l'ensemble, mais permettant également des particularités locales.

Les serveurs communiquent entre eux, selon des protocoles d'échange prédéfinis, pour rendre disponible l'information demandée par le requérant. Le caractère réparti de la base et de sa gestion permet de respecter les particularités et l'autonomie de gestion des M/O, tandis que la conformité à des normes internationales permet d'assurer l'interfonctionnalité de l'ensemble à l'échelle du gouvernement dans son entier, ce qui est un des buts premiers de l'inforoute gouvernementale. Il est à noter que l'accès aux données du répertoire est soumis à des procédures d'attribution de droits et d'identification, de rigueur variable, selon les données en cause, le statut du requérant, etc.

L'interfonctionnalité et les capacités d'échanges sont toutefois loin de se limiter à l'échelle de l'Administration. Dans l'esprit de la norme X.500, chaque répertoire s'inscrit dans une arborescence remontant, par organisations et par pays, jusqu'au niveau mondial, ce qui permet à la limite une interconnexion à l'échelle de la planète (moyennant ententes à cet effet), en même temps qu'une désignation distinctive de chacun des objets répertoriés dans quelque répertoire que ce soit. Le Répertoire jette ainsi les bases d'une infrastructure d'échange capable de supporter des applications non seulement à l'interne mais avec l'externe, aussi bien au niveau local que national ou même mondial. On peut penser ainsi aux échanges que le gouvernement doit entretenir avec ses réseaux (Santé, Éducation, monde municipal), ses clientèles de particuliers et d'entreprises de même que ses fournisseurs, sans oublier les grands réseaux internationaux établis par les institutions financières.

Par ailleurs, ce qui est très important pour les fins gouvernementales, la gestion de la base (et de la certification des utilisateurs par l'entremise d'une infrastructure de sécurité à clés publiques, qu'elle est conçue pour soutenir) est elle aussi répartie selon une structure hiérarchique qui est susceptible d'épouser la plupart du temps de façon intégrale les structures organisationnelles de l'appareil d'État. Par gestion de la base, on entend notamment les responsabilités quant au contenu et à la structure de la base, à la saisie, à l'entretien et au partage des données ainsi qu'à la mise en place et au respect des mesures de sécurité. Le répertoire X.500 allie la centralisation des principaux aspects technologiques à la responsabilisation et à l'engagement des intervenants locaux en matière de gestion du contenu informationnel, pour assurer l'efficacité du fonctionnement administratif.

1.3 Les services du Répertoire gouvernemental

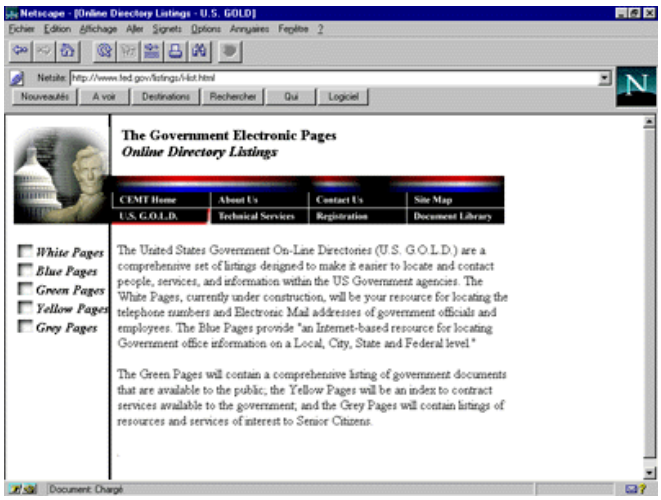
Bien que les normes soient strictes quant aux protocoles assurant le fonctionnement du répertoire X.500, elles laissent beaucoup de latitude quant au contenu de sa base de données. Certains usages sont cependant en train de s'imposer en raison de leur opportunité, sans pour cela fermer la voie à toute autre initiative, bien au contraire. Tous ces services[2] sont de plus en plus accessibles par l'entremise d'interfaces courantes et bon marché, telles que des interfaces Web sur Internet, et la tendance à la généralisation de ce phénomène est sans équivoque. Plusieurs gouvernements ont déjà opté pour la mise en place de répertoires à l'échelle de l'ensemble de l'Administration et un bon nombre de réalisations sont déjà évidentes (voir Annexe 5).

On peut regrouper les services du Répertoire selon les catégories suivantes[3], qui constituent autant de façons de meubler et d'exploiter la base de données.

1.3.1 Les services de consultation

À l'origine, le répertoire X.500 était l'analogue électronique de l'annuaire téléphonique ; la désignation des services de consultation conserve donc des traces de cette analogie. À noter que les Pages blanches, bleues et vertes n'épuisent pas la liste des possibilités et que d'autres couleurs de pages ou services de consultation pourraient venir s'ajouter sans affecter autrement le fonctionnement du Répertoire. À titre indicatif, notons que le répertoire du gouvernement fédéral américain, à l'avant-garde à bien des égards, offre une gamme étendue de services de consultation (voir Figure 1-2).

Figure 1-2 : Répertoire gouvernemental américain



1.3.1.1 Le service de Pages blanches

Les Pages blanches fournissent l'information permettant de rejoindre une personne (ex.: téléphone, télécopieur, adresse électronique, adresse physique, etc.) au sein d'une collectivité quelconque (notamment une organisation), habituellement à partir du nom de cette personne. Elles permettent de situer la personne dans l'organisation ou d'obtenir d'autres renseignements la concernant, comme par

---

2 On notera qu'à terme il s'agit de services répartis, assurés et gérés en très grande partie par les M/O participants eux-mêmes (modèle en réseau), par opposition à un service offert par un fournisseur unique et central à des consommateurs qui ne sont que passifs (modèle en étoile).

3 Telles que proposées par le gouvernement fédéral américain et en accord avec les usages observés et recommandés en la matière par les firmes spécialisées, dont Gartner Group.

exemple son certificat de clé publique (d'une importance centrale en matière de **sécurité**). Sur le même principe, on pourrait imaginer un service référant à des applications, des dispositifs, des appareils, etc. Plusieurs gouvernements offrent déjà un service de Pages blanches, dont le gouvernement fédéral canadien, où ce service connaît une très grande popularité.

1.3.1.2 Le service de Pages bleues

Les Pages bleues permettent de repérer, et possiblement de contacter, une organisation à partir de mots-clés décrivant les programmes et activités de cette organisation. Elles sont destinées à fournir des renseignements, à diriger le requérant vers la solution à son problème et à obtenir les documents, tels des formulaires, nécessaires à l'initiation de sa démarche. Elles servent aussi à présenter les structures organisationnelles et les mandats et ressources spécialisées des unités administratives. On notera que les fonctions remplies par les Pages bleues s'apparentent en bonne part au mandat d'information de Communication Québec, du ministère des Relations avec les citoyens et de l'Immigration (MRCI). Cette fonction de répertoire est en voie de s'implanter dans diverses administrations.

1.3.1.3 Le service de Pages vertes

Les Pages vertes fournissent l'information (ex. : titre, auteur, identifiant unique, description, version, hyperliens avec site FTP ou Web où trouver le document, autres liens connexes, etc.) permettant de repérer un document et d'y avoir accès, dans la mesure des restrictions qui peuvent s'appliquer de par la loi. Elles concernent tout type de documents (ex. : formulaires, dossiers, directives, règlements, normes, images, messages vocaux, données, dossiers multimédias, collections, sites Web, etc.). De très nombreux foyers de services de cet ordre existent déjà de par le monde, appuyés sur l'expertise des spécialistes en sciences de l'information.

1.3.2 Les services de soutien aux applications

Le Répertoire constitue le centre nerveux des services sur l'inforoute et il est au cœur des applications et services en réseau. Il est ainsi possible de programmer des applications pour accéder au Répertoire afin d'y déposer ou récupérer de l'information de façon tout à fait automatique, transparente à l'usager. La mise à disposition d'une telle panoplie de nouveaux services communs, alliée à une modélisation plus rationnelle de l'information dont dispose le gouvernement, est susceptible de bouleverser les conditions et processus du développement d'applications dans les ministères et organismes et d'ouvrir la voie à un changement majeur des pratiques. On peut notamment recourir au Répertoire pour soutenir les types d'applications qui suivent.

Messagerie électronique : le Répertoire permet de recueillir et de garder en mémoire les paramètres de télémessagerie (ex.: adresses, préférences, exigences, conditions) propres à une personne, à un groupe de travail ou à une organisation, ou encore à une liste de distribution, de façon à automatiser l'échange de courrier selon les modalités appropriées (ex.: conversion automatique de formats de documents, adressage automatique individualisé ou de groupe, automatisation d'applications de formulaire électronique, etc.).

Sécurité : il s'agit sans doute là d'une application du Répertoire gouvernemental parmi les plus fondamentales et qui aura les **effets structurels** les plus profonds, au plan économique et autres, sur le gouvernement et sur la société dans son entier.

Une des caractéristiques majeures offertes par un répertoire X.500 est la capacité de ce dernier d'héberger une infrastructure de sécurité à clés publiques (ICP) permettant, par la gestion des clés publiques, l'émission de certificats et la validation des transactions, d'assurer la sécurité des échanges en réseau (confidentialité, intégrité, authentification, certification, non-répudiation) et le recours à la signature numérique. Les procédures de sécurisation des échanges électroniques, dans le secteur privé comme dans le secteur public, avec les particuliers comme avec les entreprises, s'alignent sur X.509, qui est la norme spécifique de la famille X.500 qui régit la gestion des clés publiques et des certificats ; il s'agit là d'un phénomène mondial. Les certificats de clés publiques sont répertoriés dans les Pages blanches des personnes et des organisations. Les applications y accèdent directement. Les opérations sont transparentes à l'usager.

Applications spécifiques à une organisation : les organisations peuvent recourir au Répertoire pour conserver et rendre accessibles des données utilisées par des applications qui leur sont propres ; les capacités de référence d'un répertoire X.500 peuvent s'appliquer à tout objet qui présente un intérêt pour l'organisation. À titre d'exemple, il serait possible de recourir au Répertoire pour assurer la mise en mémoire de toutes données utiles à la gestion des ressources humaines, matérielles, financières ou informationnelles, et l'accès automatique ou non à ces données, dans un ministère ou organisme comme dans l'ensemble du gouvernement.

Autres : le répertoire peut soutenir tout le domaine des services assurés en matière de commerce électronique, les services Web et autres services Internet et intranet, ce qui, en fait, ouvre la voie à un ensemble illimité d'applications.

En somme, le Répertoire, de par ses fonctions, loge au cœur de l'inforoute gouvernementale, assurant la sécurité des accès et la confidentialité des échanges, autant à l'interne qu'avec l'externe, et pointant vers les ressources disponibles tout en permettant leur partage selon des processus de travail et des cheminements de l'information convenus.

1.4 Le Répertoire gouvernemental : du concept à la réalité

La voie est en bonne partie tracée pour le Répertoire gouvernemental québécois. Il reste maintenant à formaliser sa conception détaillée et organiser les efforts requis pour sa mise en place et son fonctionnement. Les sections qui suivent sont un pas de plus en ce sens. Nous aborderons dans un premier temps l'architecture du service de Répertoire (Chapitre 2), pour examiner ensuite de plus près les questions d'appellation et les caractéristiques de la structure arborescente du Répertoire (Chapitre 3), exposer les mécanismes de sécurité du Répertoire et leur architecture (Chapitre 4) et, finalement, détailler la pièce maîtresse que constitue le schéma du Répertoire (Chapitre 5). Des annexes viendront compléter ce document de conception détaillée en vue d'en enrichir le sens et la compréhension. Le mouvement étant lancé, tout progrès ultérieur devra maintenant compter sur la participation active et l'engagement déterminé des ministères et organismes en vue de faire passer le Répertoire gouvernemental du concept à la réalité.

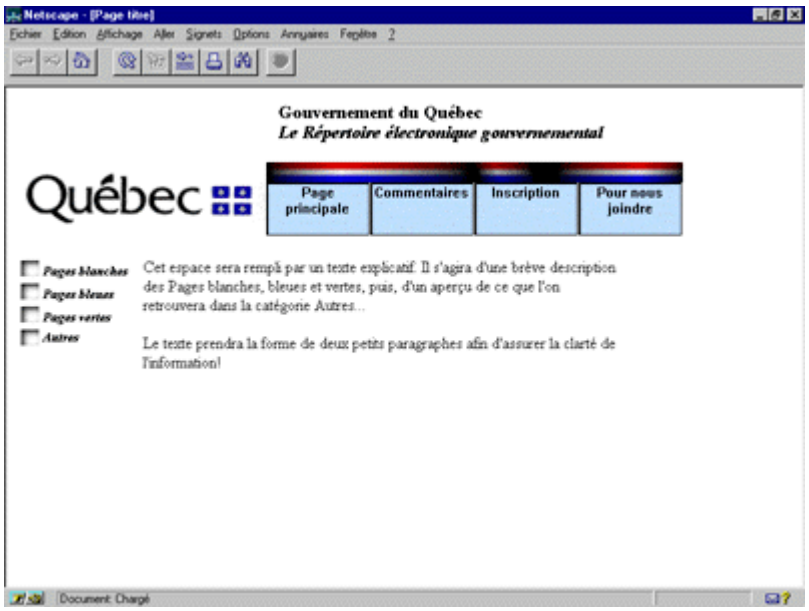


Figure 1-3 : Une maquette de page d'accueil du Répertoire gouvernemental

CHAPITRE 2

2.0 L'architecture du service de répertoire

Le présent chapitre fournit un aperçu de l'architecture générale du service de Répertoire gouvernemental. Cette architecture, établie à partir d'un certain nombre de principes généraux, regroupe un ensemble de composantes réunies autour d'un modèle général misant sur les particularités d'un répertoire X.500.

2.1 Principes architecturaux

Le Répertoire gouvernemental sera fondé sur des normes internationales émanant de l'Union internationale des télécommunications et de l'ISO ainsi que des organes de normalisation de l'Internet, soit principalement l'IETF (*Internet Engineering Task Force*). Son évolution continue, dans le respect des besoins de l'appareil gouvernemental et de la société québécoise dans son ensemble, s'ajustera aux conditions et tendances prévalant sur la scène mondiale en matière de technologie et d'usage des répertoires.

Dans l'optique générale d'améliorer l'efficacité et l'efficience de l'appareil gouvernemental et la qualité des services offerts aux clientèles gouvernementales, l'architecture du Répertoire gouvernemental tiendra principalement compte du développement et de l'évolution des normes précitées, des fonctionnalités qu'elles supportent, de leur complémentarité, de leur implantation dans des produits, de la disponibilité de ces derniers et de la facilité et de l'étendue de leur utilisation. Elle tiendra également compte de la situation actuelle dans les ministères et organismes en ce qui a trait aux répertoires de même que de l'implantation plus générale de l'inforoute gouvernementale et des technologies qui la supportent, notamment les intranets gouvernemental et ministériels.

2.2 Le modèle général

Le modèle général du Répertoire gouvernemental sera établi à partir du modèle de répertoire X.500, tel que repris à son compte par le monde de l'Internet et tel qu'implanté et commercialisé par les principaux fabricants. Essentiellement, un répertoire X.500 est constitué d'un ensemble de processus complexes, dont le fonctionnement est réparti pour assurer la prestation et l'administration de services de référence à des ressources en réseau.

La publication de la première édition des spécifications du répertoire X.500 remonte à 1988, alors qu'était produite pour la première fois la série de recommandations X.500 du Comité Consultatif International en Téléphonie et Télégraphie (CCITT), reprise en 1990 sous forme de la famille de normes 9594 de l'ISO/CEI (Organisation internationale de normalisation/Commission électrotechnique internationale). La deuxième édition des spécifications a été publiée en 1993 sous forme de la série de recommandations X.500 de l'UIT (Union internationale des télécommunications), qui a succédé au CCITT, également reprise en 1995 sous la norme internationale ISO/CEI 9594. À l'heure actuelle, les deux groupes en collaboration finalisent une troisième édition des spécifications de répertoire, laquelle comprendra notamment la gestion du système du répertoire et une amélioration des mesures de sécurité. Certaines des recommandations de l'UIT sont déjà finalisées dans leur version 1997. Par ailleurs, malgré qu'il subsiste de part et d'autre des tenants de positions extrémistes, appuyées sur diverses motivations, on observe de plus en plus une disposition à collaborer activement entre les instances de normalisation de l'UIT/ISO et de l'Internet en vue d'harmoniser l'évolution des répertoires et des normes qui les régissent. Ces dispositions se manifestent notamment par la présence active de représentants d'entreprises qui conçoivent,

produisent et offrent des produits conformes aux normes de l'UIT/ISO au sein des groupes produisant les RFC d'Internet relatives aux répertoires.

L'objectif principal à l'origine du service de répertoire X.500 fut de fournir la conversion en adresses de télémessagerie des noms de ressources désignant des utilisateurs ou des réseaux pour ainsi faciliter le transfert des données de divers ordres entre utilisateurs. La conception orientée objet, l'extensibilité et le caractère réparti du répertoire X.500 font en sorte qu'il est bien adapté pour jouer le rôle de répertoire global. L'architecture du répertoire X.500 propose une seule arborescence à l'échelle de la planète, dans laquelle divers pays possèdent différentes parties de l'arbre et où des entités subordonnées occupent des portions de l'arborescence nationale. Chaque partie de l'arborescence doit être en mesure de partager des informations avec les autres parties. L'accent s'étant ces dernières années déplacé vers la mise en place de réseaux privés d'entreprises et devant la vague déferlante de l'Internet autant dans les organisations que chez les particuliers, le principe unifiant de la famille de normes X.500 a de plus en plus été mis de l'avant pour intégrer des répertoires hétérogènes à une échelle moindre que celle du répertoire mondial initialement envisagé, bien que cet objectif n'ait jamais été abandonné comme tel. La gamme des possibilités offertes par le modèle général de répertoire X.500 permet ainsi d'envisager qu'une infrastructure mise sur pied pour les fins internes d'une organisation comme le gouvernement s'insère éventuellement de façon toute naturelle dans une infrastructure d'envergure mondiale, dont l'édification s'opère graduellement.

Dans le respect des ces principes et du modèle général retenu, on distinguera les trois principales composantes de l'architecture générale du service de Répertoire que sont l'information et son organisation, les serveurs et leur fonctionnement et les interfaces clients donnant accès aux services.

2.3 L'information

Le modèle général d'information qui sera retenu est celui qui est spécifié par les recommandations de la série X.500, également préconisé par le monde de l'Internet et recueillant l'adhésion, partielle ou intégrale, des principaux producteurs. L'adhésion étendue aux principes de construction de ce modèle général d'information constitue, en dernière analyse, le principal facteur commun permettant d'espérer atteindre un répertoire intégré à partir des protocoles et produits sur le marché ou actuellement envisageables.

2.3.1 Les données du répertoire

La base des entrées du répertoire (DIB, pour Directory Information Base) constitue la base de données, le recueil des informations auquel le répertoire donne accès. Elle renferme les informations collectives emmagasinées dans le répertoire. La base se compose d'entrées, lesquelles consistent en un recueil d'informations relatives à un objet, par ex. à une personne, à une organisation, à un ordinateur. Pour chaque objet, il existe une entrée dans le répertoire. Chaque entrée dans cette base possède un ensemble prédéfini d'attributs, par ex. le nom ainsi que les coordonnées physiques et électroniques.

Les informations contenues dans la base des entrées peuvent être réparties sur un grand nombre de serveurs de répertoire, chacun détenant une portion de l'information totale. De plus, chaque serveur du répertoire peut contenir des copies d'autres portions de la base des entrées du répertoire. La répartition de la base des entrées du répertoire sera transparente pour l'utilisateur, donnant l'impression que toute la base des entrées du répertoire se trouve hébergée sur un seul serveur. Pour soutenir cette transparence, il est nécessaire que chaque serveur du répertoire puisse accéder aux données associées à un

nom (nom distinctif ou alias) contenu dans la base des entrées. Si le serveur de répertoire ne contient pas d'entrée associée à un nom distinctif (ou de copie miroir de telle entrée), il devra en principe être en mesure d'interagir avec les autres serveurs de répertoire pour identifier le bon serveur qui contient les données à récupérer.

2.3.2 L'arborescence du répertoire (DIT, pour Directory Information Tree)

La base des entrées du répertoire se fonde sur une structure logique en arbre, appelée l'arborescence du répertoire, qui constitue l'élément central du modèle d'information. Chaque entrée de la base se situe dans un des embranchements de cette structure arborescente. La base des entrées du répertoire constitue la réalisation physique du répertoire X.500, alors que l'arborescence du répertoire définit la représentation logique de l'espace d'appellation, sa ramification. Cette hiérarchie logique fournit le contexte d'appellation au sein duquel on construit les noms distinctifs pour identifier de façon unique les entrées du répertoire.

On identifie chaque entrée dans l'arborescence du répertoire de manière unique au moyen de séquences ordonnées d'attributs que l'on appelle des noms distinctifs relatifs (RDNs) qui entrent dans la composition du nom distinctif (DN). La séquence des noms distinctifs relatifs à partir de la racine de l'arborescence du répertoire jusqu'à l'objet dénommé constitue le nom distinctif.

Il n'est pas nécessaire que les noms distinctifs relatifs qui composent un nom distinctif soient uniques au sein de l'espace d'appellation du répertoire. Il faut, cependant, qu'en agençant la séquence des noms relatifs, le nom distinctif qui en résulte soit unique. Dans le chapitre 3, on trouve des indications sur la façon de nommer les objets contenus dans le répertoire. À titre d'exemple, le nom distinctif pour l'entrée de répertoire de Marc-Antoine Savard, hypothétique employé de la Direction générale des télécommunications, pourrait, selon ce qui est proposé, être constitué de la séquence de noms distinctifs relatifs qui suit :
C=CAN ; O=gouv. du Québec ; OU=Secrétariat du Conseil du trésor ; OU=SSSG ; OU=DGT ; CN=Savard, Marc-Antoine[4]

2.3.3 Les contextes d'appellation

Un contexte d'appellation est une branche de l'arborescence du répertoire dont l'ensemble des entrées partage la même autorité administrative et se trouve hébergé dans le même serveur-maître (« master DSA »). Un contexte d'appellation prend son point d'origine dans la strate supérieure de la ramification et se prolonge dans les strates inférieures jusqu'aux feuilles. Ainsi, l'ensemble du Répertoire gouvernemental, situé dans une arborescence plus vaste (québécoise, canadienne, mondiale), définit le contour du domaine gouvernemental, sous l'autorité administrative du gouvernement et auquel correspond le contexte d'appellation propre au gouvernement. Une répartition analogue des responsabilités prévaut aux niveaux inférieurs, l'arborescence du Répertoire gouvernemental étant elle-même subdivisée en cascade en contextes d'appellation disjoints, chacun situé sous une autorité administrative particulière et hébergé dans un même serveur maître. Le « domaine gouvernemental » comprend essentiellement les ministères et les organismes, leur personnel, leurs publications, leurs services, etc. Les domaines individuels composant le Répertoire gouvernemental doivent développer et adapter sur une base consensuelle des directives, politiques, procédures et méthodes standardisées afin d'établir, de gérer et d'utiliser efficacement le Répertoire et ses services.

[4] Ces sigles seront expliqués plus loin dans le texte.

2.4 Les serveurs et leur fonctionnement

Les caractéristiques des serveurs et de leur fonctionnement sont principalement spécifiées par la famille de normes X.500. Des aménagements, des variantes et des innovations sont apportés par divers RFC publiés par l'IETF afin de simplifier et d'alléger le modèle ainsi spécifié et de l'aligner de plus près avec les caractéristiques de l'Internet.

Le serveur de répertoire (DSA, pour Directory System Agent, selon la terminologie de l'UIT/ISO) est la composante du répertoire qui emmagasine et entretient la base des entrées. Ce serveur est un processus d'application qui donne accès aux informations concernant les entrées du répertoire. De multiples serveurs de répertoire peuvent être associés à une base d'entrées, chaque serveur supportant une partie de la base. Bien que cela ne soit pas absolument obligatoire, le répertoire X.500 est conçu pour fonctionner de façon répartie. Les serveurs travaillent de concert en partageant les informations de sorte que l'utilisateur puisse visualiser et parcourir tous les serveurs comme s'il s'agissait d'un seul répertoire. Le serveur de répertoire offre aussi des fonctions permettant de rediriger les demandes d'information pour lesquelles il ne détient pas les données nécessaires, et ce grâce au recours à ses informations de référence internes. Les fonctions de chaînage (« chaining ») et de réacheminement (« referral ») permettent aux serveurs de répertoire de traiter et de diriger les requêtes d'information vers le serveur qui, dans ce modèle réparti, contient les données sollicitées.

La topologie du répertoire sera généralement à l'image de celle de l'organisation qui se dote d'un tel service. On peut donc prévoir qu'à terme chaque ministère ou organisme se dotera d'un ou de plusieurs serveurs de répertoire. Les exigences particulières de chaque M/O détermineront le nombre de serveurs à mettre en œuvre. Les interrelations entre ces serveurs dans le cadre de l'arborescence du répertoire gouvernemental seront examinées et discutées ci-après.

2.4.1 Les facteurs de conception de la topologie du Répertoire gouvernemental

La conception de la topologie du Répertoire gouvernemental sera déterminée par plusieurs facteurs, notamment :

- la taille du ministère ou de l'organisme ;
- la taille des unités administratives au sein du ministère ou de l'organisme ;
- la fiabilité du réseau de télécommunications qui sera emprunté ;
- la distance qui sépare les données du répertoire de l'auteur des requêtes ;
- le volume de communications entre les ministères et les services ;
- les exigences de performance ;
- le type de liaison en réseau entre les ministères et les services ;
- la préoccupation des ministères et des services à l'égard de la sécurité.

Le volume de communications entre le personnel de deux ministères exerce une influence directe sur les méthodes retenues pour le transfert des informations entre serveurs. Si, par exemple, les champs d'action de deux ministères sont intimement interreliés et que les communications entre leurs personnels respectifs sont considérables, les échanges d'information entre leurs serveurs de répertoire devraient normalement recourir à la duplication des données ou au miroitage. Dans le cas, par contre, où les personnels de deux ministères entretiennent peu d'échanges entre eux, le chaînage devrait probablement être la méthode retenue pour assurer le partage des données du répertoire.

La possibilité d'utiliser le Répertoire gouvernemental pour obtenir les adresses de courrier électronique sur les réseaux locaux constitue une préoccupation importante. Étant donné

la prolifération de réseaux de communication au sein du gouvernement, il arrive très fréquemment que l'on veuille connaître l'adresse électronique d'une organisation ou d'un employé donnés. La possibilité pour l'utilisateur de prendre connaissance de l'adresse électronique en direct reposera sur la capacité ou non de la topologie des serveurs à supporter le fonctionnement du répertoire sur l'étendue des réseaux locaux en question.

2.4.2 La topologie de base du Répertoire gouvernemental

Dans chaque domaine individuel composant le domaine gouvernemental, un serveur joue le rôle de point d'accès reconnu (« Well Known Entry Point ») dans l'arborescence du répertoire. On prévoit que chaque M/O sera chargé de faire fonctionner au moins un serveur jouant le rôle de point d'accès reconnu.

Les points d'accès reconnus contiennent suffisamment d'information de référence pour naviguer dans l'arborescence par le truchement des mécanismes de références supérieure, inférieure et croisée. Le niveau supérieur de l'arborescence sera réparti parmi les serveurs jouant le rôle de points d'accès reconnus. Il faut retenir qu'il s'agit d'abord d'une topologie de l'information et non d'une topologie de composantes comme telles. Il pourra ainsi arriver qu'il y ait plus d'un serveur-point d'accès reconnu par domaine, dépendant de la configuration des réseaux, du profil d'utilisation et des critères de sécurité retenus. Les accords de miroitage et de duplication pourront aussi affecter la topologie des composantes.

Les serveurs-points d'accès reconnus de la racine du Répertoire gouvernemental contiendront suffisamment d'information de référence pour faire office d'agents de chaînage et de réacheminement pour les domaines nationaux collatéraux (ex. : des domaines dans le secteur privé québécois, le domaine de gestion du gouvernement fédéral, etc.) et de point d'accès pour d'autres serveurs de répertoire au niveau international. Les serveurs des ministères et organismes seront répartis au niveau supérieur de l'arborescence du répertoire. L'information de référence sur la topologie des serveurs et la répartition de l'arborescence parmi les serveurs au sein des M/O seront déterminées à l'interne de chaque ministère ou organisme. De plus, le chaînage, le réacheminement et la duplication des données seront déterminés par chaque M/O à partir de critères de fonctionnement locaux.

2.4.3 Les protocoles qui régissent le fonctionnement du Répertoire gouvernemental

Pour communiquer entre eux, les interfaces client et les serveurs du répertoire ont besoin de protocoles. On associe cinq protocoles de base[5] au répertoire X.500. Un certain nombre d'autres protocoles devront à tout le moins faire l'objet d'un suivi afin de planifier l'évolution du Répertoire gouvernemental.

2.4.3.1 Le protocole d'accès au répertoire (DAP, pour Directory Access Protocol)

Les interfaces client communiquent avec les serveurs au moyen d'un protocole d'accès au répertoire, qui définit l'échange des requêtes adressées aux serveurs et des résultats fournis par ces derniers. On accède au répertoire par une série de ports de service définie dans la série de recommandations X.500. Chaque port fournit un ensemble spécifique de services. Les services définissent les opérations du répertoire, soit par exemple la liaison au répertoire, la lecture, la recherche et les modification des entrées. De plus, le protocole d'accès au répertoire retourne les codes de résultat et d'erreur.

[5] Quatre si on considère que LDAP n'est qu'un sous-ensemble de DAP.

2.4.3.2 Le protocole allégé d'accès au répertoire (LDAP, pour Lightweight Directory Access Protocol)

Le protocole allégé est généralement utilisé pour l'accès aux répertoires X.500 par les réseaux TCP/IP. Il est également utilisé pour accéder aux répertoires dits LDAP, soit ceux qui, sans être accessibles par DAP, le sont par LDAP. Ce protocole, disposant d'une interface de programmation d'applications (API) simple et facile d'utilisation, est maintenant le plus utilisé pour accéder aux répertoires X.500. Il donne à l'utilisateur accès au répertoire X.500 d'une manière grandement simplifiée tout en affichant les fonctionnalités les plus utiles et courantes du protocole d'accès au répertoire.

Essentiellement, LDAP, activement soutenu par Netscape et recueillant l'appui d'une quarantaine de fournisseurs parmi les plus influents (dont Microsoft), offre aux clients fonctionnant sur TCP/IP un mécanisme simplifié pour interroger et gérer une base de données constituée d'objets organisés de façon hiérarchique et caractérisés par des attributs auxquels sont affectées des valeurs. Ce faisant, il se situe nettement dans la lignée de X.500 dont il emprunte la structure hiérarchique d'organisation des données et la spécification de classes d'objets et d'attributs.

Le protocole LDAP possède un pouvoir d'intégration indéniable. Les clients LDAP peuvent accéder à de l'information détenue sur une variété de serveurs : d'une part, ils peuvent accéder directement à des serveurs LDAP contenant l'information recherchée, ou encore à des serveurs propriétaires qui interprètent des requêtes LDAP ; d'autre part, ils peuvent accéder à des serveurs de répertoire X.500 comme tels. Dans ce dernier cas, ils peuvent procéder de trois façons différentes, en fonction des installations en place : ils peuvent soit adresser une requête à un serveur X.500 qui interprète LDAP, ou à un processus LDAP fonctionnant en parallèle sur un serveur X.500, soit encore passer par un serveur LDAP dit « X.500 enabled » pour s'adresser directement à la base de données maintenue sur un serveur X.500. Il faut noter que lorsqu'un client LDAP se branche à un serveur de répertoire exécutant des fonctions LDAP en parallèle, ce client a essentiellement un accès total aux données du répertoire emmagasinées dans les autres serveurs du répertoire. Cet accès total s'opère par l'entremise du protocole du système de répertoire X.500, qui permet à un serveur d'obtenir des données des autres serveurs du répertoire et de les acheminer vers le client d'origine qui les a demandées. Les protocoles LDAP et X.500 se révèlent ainsi complémentaires l'un de l'autre.

Des efforts importants sont consacrés à l'évolution de LDAP. La version 3 de ce protocole, sur le point d'être adoptée, promet d'étendre considérablement la gamme des fonctionnalités offertes pour inclure notamment des capacités accrues de modification, de réacheminement des requêtes, de duplication des entrées et de sécurité des transmissions, tout en ajoutant des capacités d'extensions.

Le Répertoire gouvernemental supportera le protocole allégé d'accès au répertoire dans ses versions actuelles et futures. Bien que plusieurs questions de conception et de développement demeurent ouvertes dans le marché des répertoires, force est de noter que la tendance dominante actuelle et prévisible va vers le regroupement fonctionnel par LDAP de répertoires hétérogènes conformes soit à LDAP, soit à X.500.

2.4.3.3 Le protocole du système de répertoire (DSP, pour Directory System Protocol)

On utilise ce protocole entre les serveurs du répertoire pour répondre à des requêtes d'utilisateurs qui exigent d'aller chercher des informations réparties sur plusieurs serveurs du répertoire via des ports de service désignés. Le chaînage permet d'acheminer les requêtes d'information adressées au répertoire, via une multiplicité de serveurs, jusqu'au serveur particulier qui contient les informations recherchées. Le serveur approprié ayant été déterminé, l'opération désignée peut s'exécuter sur ce même serveur par le recours au protocole d'accès au répertoire avec les arguments et résultats de chaînage en cause. Le chaînage est invisible à l'utilisateur et s'exécute en redirigeant progressivement la requête à travers un certain nombre de serveurs qui, à chaque étape, recueillent et évaluent les résultats de la requête jusqu'à ce que les données recherchées soient récupérées et retournées par l'entremise de la « chaîne » de serveurs ainsi constituée.

2.4.3.4 Le protocole de liaison opérationnelle du répertoire (DOP, pour Directory Operational Binding Protocol)

Le protocole de liaison opérationnelle du répertoire régit les relations entre deux serveurs de répertoire qui conviennent d'une entente d'association, en vue soit d'effectuer des copies miroir d'information (« shadowing »), soit de mettre à jour des pointeurs référentiels (« knowledge reference pointers ») pour le réacheminement des requêtes. Le protocole de liaison opérationnelle du répertoire permet la négociation d'ententes entre serveurs et la définition des paramètres qui régiront leur association.

2.4.3.5 Le protocole de miroitage (DISP, pour Directory Information Shadowing Protocol)

Le protocole de miroitage est utilisé pour régir le transfert d'information entre serveurs du répertoire en vue de constituer ou de mettre à jour des copies miroir d'information. Les serveurs doivent avoir convenu d'une entente d'association selon les termes du protocole de liaison opérationnelle du répertoire avant de recourir au protocole de miroitage pour reproduire sur place l'information détenue sur un autre serveur ou pour en faire la mise à jour.

La série de recommandations X.500 de 1988 incorporait le protocole d'accès au répertoire et le protocole du système de répertoire, alors que les extensions de 1993 ont étendu la suite de protocoles pour inclure le protocole de miroitage et celui de liaison opérationnelle du répertoire, afin de prendre en charge la duplication des entrées.

2.4.3.6 Autres protocoles en émergence

Compte tenu du rôle moteur de l'Internet et des intranets, il conviendra de suivre attentivement l'évolution de certaines autres normes de l'Internet relatives aux répertoires et notamment celles qui, comme le Common Indexing Protocol (CIP) et Whois++, préconisent une échange généralisé d'index entre serveurs de répertoire. Par ailleurs, l'accès aux données de répertoire par l'entremise d'interfaces Java pourrait amener une façon nouvelle de concevoir les répertoires et d'y accéder.

2.4.4 Fonctionnement des services du Répertoire

Deux mécanismes principaux assurent le fonctionnement des services du Répertoire, soit la copie de données et les mécanismes de référence.

2.4.4.1 La copie de données entre serveurs de répertoire

Un répertoire X.500 permet de reproduire dans plusieurs serveurs de répertoire des données contenues dans un seul des serveurs. Cette architecture répartie améliore la disponibilité des données et la performance d'accès. Le répertoire X.500 recourt à un modèle de duplication qui décrit deux types de reproduction : la mise en mémoire cache (« caching »), qui n'est pas spécifiée comme telle dans la norme, et la production de copies miroir, ou miroitage (« shadowing »).

2.4.4.1.1 La mise en mémoire cache

La forme la plus simple de reproduction est la mise en mémoire cache où une copie statique des données est maintenue dans le serveur de répertoire. Ce procédé de reproduction ne comporte cependant aucun mécanisme de mise à jour pour assurer l'actualisation des données gardées en mémoire cache et, plus important encore, les mécanismes des contrôles d'accès ne s'appliquent pas nécessairement aux données en mémoire cache. La mise en mémoire cache n'est pas régie par les recommandations de la famille X.500 comme telles.

2.4.4.1.2 Le miroitage

Le miroitage est une forme de reproduction possédant des mécanismes inhérents de mise à jour. Un serveur de répertoire contiendra une partie de l'arborescence du répertoire dans laquelle il sera possible d'effectuer des changements directement et pour laquelle il sera désigné comme étant le serveur-maître. D'autres serveurs de répertoire pourront contenir des copies de ces mêmes données et on les appellera serveurs-miroirs. Un serveur donné peut être maître pour certaines données et miroir pour certaines autres. La reproduction des données obéira aux spécifications du protocole de miroitage déjà mentionné et pourra s'effectuer selon diverses modalités.

2.4.4.1.2.1 Le miroitage primaire et secondaire

Le miroitage primaire est une disposition en vertu de laquelle les consommateurs-miroirs se procurent leurs données directement du serveur-maître de répertoire. Le miroitage secondaire est une extension du miroitage primaire en ce qu'un consommateur initial des données du serveur-maître agit à titre de fournisseur-miroir aux autres consommateurs. Le principal avantage du miroitage secondaire provient du fait que le serveur-maître de répertoire n'a pas besoin de fournir des copies-miroirs à tous les consommateurs. Le répertoire électronique du gouvernement procédera au miroitage primaire et secondaire.

2.4.4.1.2.2 Les accords de miroitage

Un accord de miroitage est un devis formel, écrit, des types de données ou d'informations de référence (« knowledge information ») qui seront reproduits dans l'arborescence du répertoire ainsi que la fréquence de leurs mises à jour. L'accord précise les unités de duplication et les zones, les attributs et les informations de référence qui feront l'objet d'une duplication. L'accord désigne aussi le serveur-maître de répertoire pour

chaque élément à reproduire. L'emploi d'un devis formel permet la révision et l'analyse de la redondance de la structure de l'arborescence, des données référentielles et des entrées, afin de prévenir tout mauvais fonctionnement. Puisque les accords de miroitage mettent en cause de multiples serveurs de répertoire, la modification d'un accord de miroitage devra se faire en coordination avec les autres administrateurs de serveurs du Répertoire.

2.4.4.2 Les mécanismes de référence

L'architecture répartie du Répertoire gouvernemental doit demeurer transparente pour les utilisateurs, qui doivent pouvoir circuler dans la base des entrées avec la même facilité que si cette dernière résidait entièrement dans chacun des serveurs du répertoire. Pour satisfaire cette exigence, tout serveur doit être en mesure d'accéder aux données contenues dans la base des entrées du répertoire relativement à n'importe quel nom (c.-à-d. tout nom distinctif ou alias d'un objet). Si le serveur n'héberge pas lui-même d'entrée d'objet ou de copie d'entrée d'objet correspondant au nom en question, il devra alors pouvoir récupérer cette entrée ailleurs dans la base des entrées du répertoire en échangeant de façon directe ou indirecte avec les autres serveurs.

Les mécanismes de référence inhérents au fonctionnement des services du Répertoire s'appuient sur l'information de référence. Ces mécanismes de référence donnent lieu à divers types et modes d'interaction entre les composantes du système client-serveur qui sous-tend les services de répertoire.

2.4.4.2.1 L'information de référence (« knowledge information ») du Répertoire gouvernemental

L'information de référence est constituée des données opérationnelles détenues par un serveur de répertoire et représentant une description partielle de la base des entrées de même que des copies d'entrées gardées par d'autres serveurs de répertoire. Elle est utilisée par les serveurs pour déterminer avec quel autre serveur communiquer lorsque les requêtes en provenance des interface client ou des autres serveurs du répertoire ne peuvent être satisfaites par les données hébergées localement. L'information de référence permet d'associer, directement ou indirectement, le nom d'une entrée de répertoire avec le serveur qui contient l'entrée ou une copie de celle-ci.

2.4.4.2.2 Les types de références

Les méta-données sur la répartition de la base d'entrées entre les serveurs du Répertoire gouvernemental seront emmagasinées et entretenues dans chacun des serveurs qui font partie du répertoire réparti. Elles donneront lieu à divers types de référence :

Référence supérieure. Référence contenant de l'information relative à un serveur de répertoire situé plus haut dans l'arborescence et que l'on considère capable de trouver une entrée partout dans l'arborescence du répertoire. Ce type de référence est constitué de l'adresse réseau (URL en général) d'un serveur du répertoire.

Référence inférieure. Référence contenant de l'information relative à un serveur de répertoire situé plus bas dans l'arborescence et qui détient une ou plusieurs entrée(s) ou copie(s) d'entrée(s). Ce type de référence se compose de l'adresse réseau du serveur de répertoire qui héberge les entrées, ou copies des entrées, d'un ou de plusieurs contextes d'appellation directement inférieurs.

Référence immédiatement supérieure. Référence contenant de l'information relative à un serveur de répertoire situé dans la strate immédiatement supérieure et qui détient une entrée ou copie d'entrée spécifique. Ce type de référence se compose de l'indicatif de contexte (« context prefix ») du contexte d'appellation qui est directement supérieur à celui hébergé par le serveur qui contient l'information de référence ainsi que de l'adresse réseau du serveur hébergeant ce contexte d'appellation.

Référence immédiatement inférieure. Référence contenant de l'information relative à un serveur de répertoire situé dans la strate immédiatement inférieure de l'arborescence et qui détient une entrée ou copie d'entrée spécifique. Ce type de référence se compose de l'indicatif de contexte d'un contexte d'appellation qui est directement inférieur à celui hébergé par le serveur qui contient la référence ainsi que de l'adresse réseau du serveur hébergeant ce contexte d'appellation.

Référence croisée. Référence contenant de l'information relative à tout serveur de répertoire qui détient une entrée ou copie d'entrée. Elle sert à des fins d'optimisation. Comme il s'agit d'un raccourci ad hoc, il n'est pas nécessaire de suivre les embranchements vers le haut ou vers le bas comme avec les autres références.

2.4.4.2.3 Les modes d'interaction entre l'interface client et le serveur de répertoire en matière de référence

Le Répertoire gouvernemental supportera trois modes d'interaction entre les interfaces client et les serveurs de répertoire dans l'exécution de ses opérations. On pourra empêcher l'accès à ces opérations lorsque les politiques et les applications spécifiques l'exigeront. On distingue ainsi le chaînage (« chaining », la transmission ciblée (« multiple chaining ») et le réacheminement (« referral »).

Au cours des opérations de chaînage, les serveurs de répertoire interagissent directement les uns avec les autres par l'entremise du protocole du système de répertoire. Les requêtes d'information sont acheminées d'un serveur de répertoire à un autre. Les requêtes transitent progressivement d'un serveur à un autre sans que l'utilisateur en soit informé jusqu'à ce qu'elles atteignent celui qui contient l'information sollicitée.

La transmission ciblée constitue un cas particulier de chaînage par lequel une requête est acheminée en même temps à plusieurs serveurs de répertoire dans l'espoir qu'un ou plusieurs d'entre eux seront en mesure de satisfaire la requête.

Le réacheminement, pour sa part, amène l'interface client ou le serveur de répertoire à contacter progressivement chaque serveur de répertoire afin d'obtenir en retour l'information sollicitée. Chaque serveur de répertoire sollicité retourne toute l'information dont il dispose en réponse à la requête ainsi qu'un pointeur vers un autre serveur de répertoire qui héberge l'information recherchée ou du moins une partie de celle-ci. Informés de ce pointeur, l'interface client ou le serveur du répertoire doivent ensuite entrer en communication avec le serveur de répertoire suivant afin de poursuivre l'opération.

2.5 Les interfaces clients

Nous proposerons une typologie des interfaces clients pour en présenter ensuite une description sommaire.

2.5.1 Typologie des interfaces clients

Les services du Répertoire étant accessibles autant aux utilisateurs humains qu'aux applications informatiques, nous distinguerons d'abord les interfaces d'utilisateur et les applications-clients. Parmi les interfaces d'utilisateur, nous distinguerons les interfaces d'information publique (interfaces d'accès par Internet, bornes interactives) et les interfaces gouvernementales (employés, administrateurs du Répertoire).

- Interfaces d'utilisateurs
- interfaces d'information publique
- interfaces d'accès par Internet
  - bornes interactives
- interfaces gouvernementales
  - employés
  - administrateurs du Répertoire applications clients

2.5.2 Description sommaire des interfaces clients

L'interface client du répertoire (DUA, pour Directory User Agent) est la composante du service de Répertoire qui communique avec le serveur et fournit les moyens pour accéder aux informations contenues dans la base des entrées. La structure sous-jacente de l'information du répertoire n'est pas visible aux utilisateurs. L'interface client permet à l'utilisateur de recourir à diverses fonctions telles que feuilleter les listes du répertoire (« browse »), faire des recherches sur des mots-clés (« search »), et autres fonctions telles que visualiser (« read »), ajouter, modifier et supprimer des entrées au répertoire. L'interface client peut être utilisée par une personne (interface d'utilisateur) ou un processus d'application (application client). De plus, l'interface client peut adopter différentes modalités et se présenter par exemple sous forme d'interface graphique, d'écran tactile ou de dispositif à commande vocale ou de commandes produites par le système. Tous les services fournis par le répertoire le sont en réponse à des requêtes. Les mécanismes de sécurité peuvent servir à limiter la capacité des utilisateurs à visualiser, à modifier ou à supprimer des informations à partir des mesures de contrôle d'accès aux informations contenues dans le répertoire.

2.5.2.1 Interfaces d'utilisateur

Les interfaces d'utilisateur sont celles qui fournissent aux utilisateurs humains des interfaces graphiques afin de lire ou de modifier les informations emmagasinées dans les services du répertoire et les autres services connexes.

Les interfaces d'utilisateurs seront des interfaces client polyvalentes qui supporteront une gamme de protocoles nécessaire pour accéder au Répertoire du gouvernement et aux recueils d'information connexes. Ces protocoles peuvent comprendre l'un ou l'autre ou l'ensemble des protocoles suivants :

- le protocole d'accès au répertoire (DAP) - la norme UIT/ISO pour accéder aux répertoires X.500 par les réseaux OSI ;
- le protocole allégé d'accès au répertoire (LDAP) - la norme de facto pour accéder aux répertoires X.500 par les réseaux TCP/IP ;
- Hyper-Text Transfer Protocol (HTTP), ou Protocole de transport hypertexte - norme Internet de facto pour communiquer avec les serveurs Web ;
- Hyper-Text Markup Language (HTML), ou Langage de balisage hypertexte - norme Internet de facto pour établir des liens entre objets par HTTP sur le Web ;
- Z39.50 Wide Area Information Service (WAIS) - service réparti d'emmagasinage et de récupération de documents fonctionnant sur Internet, défini par l'ANSI/NISO et dont l'usage se répand au niveau international.

Les protocoles ci-dessus sont supportés de façon à présenter à l'utilisateur une gamme étendue d'informations à partir d'une même interface. La présente section décrira la topologie d'interface d'information recommandée (types d'interfaces requis, emplacement approximatif), qu'il s'agisse d'interfaces d'information publique ou d'interfaces utilisées par le personnel à l'emploi du gouvernement.

2.5.2.1.1 Interfaces d'information publiques

Les interfaces d'information publiques peuvent prendre à la fois la forme de dispositifs intégrés placés dans des lieux publics ou d'interfaces d'accès pour les citoyens, les entreprises rendus disponibles sur les sites Web des ministères et organismes.

2.5.2.1.1.1 Les bornes interactives, ou guichets électroniques

Les bornes interactives se définissent comme étant des interfaces d'utilisateur matérielles et logicielles situées dans un emplacement accessible au public pour permettre aux gens d'accéder aux informations concernant le gouvernement, tels que les personnes contact dans les M/O, les services gouvernementaux, les formulaires, etc. Elles se présentent comme des interfaces d'information de portée générale et facilement accessibles au public.

Ce type d'interface fonctionnera en mode hypertexte pour permettre d'accéder aux informations emmagasinées dans les serveurs WEB du gouvernement via les protocoles HTML et HTTP. De plus, les bornes interactives supporteront la norme Z39.50 pour assurer l'accès intégré aux recueils de documents gouvernementaux disponibles en direct.

Les bornes interactives seront installées dans des lieux publics tels les bibliothèques, les centres commerciaux et autres emplacements semblables. Les interfaces de bornes interactives seront assez polyvalentes pour permettre au public de se procurer des informations de type Pages blanches, bleues et vertes relatives aux personnes et aux organisations, aux programmes et aux services de même qu'aux documents du gouvernement. Des bornes interactives pourront aussi offrir la capacité d'imprimer les informations récupérées, telles les formules de déclarations d'impôt, les listes de services gouvernementaux et autres renseignements semblables.

Les bornes interactives seront configurées pour utiliser le protocole allégé d'accès au répertoire pour se relier au serveur le plus proche en mode asynchrone par TCP/IP. Les serveurs en question seront configurés pour se procurer et conserver une copie de l'arborescence des M/O les plus éloignés, ou encore ils pourront, par chaînage, acheminer une requête vers le serveur approprié.

Par exemple, un particulier pourrait se servir d'une borne située à Chicoutimi pour demander un formulaire de déclaration d'impôt auprès du ministère du Revenu. La borne interactive accéderait au serveur local de répertoire pour chercher où se trouve le formulaire d'impôt. Le serveur local réacheminerait la requête en direction du serveur de répertoire du ministère du Revenu, lequel à son tour récupérerait le document parmi les documents du ministère accessibles en direct, possiblement emmagasinés sur un serveur Z39.50/WAIS à Québec. Le formulaire serait ensuite imprimé par la borne interactive à la demande de l'utilisateur.

2.5.2.1.1.2 Les interfaces d'accès à partir des sites Web du gouvernement

Il s'agit d'interfaces pour utilisateurs accessibles au public (ex. : entreprises ou particuliers, associations) qui veut obtenir accès au Répertoire gouvernemental et aux services connexes par l'entremise de micro-ordinateurs branchés au réseau Internet. Le niveau d'accès aux informations du répertoire qui sera accordé dépendra des contrôles d'accès au Répertoire qui auront été définis pour l'utilisateur en question (voir le chapitre 4.0, Les mécanismes de sécurité et leur architecture).

Ces interfaces partagent les caractéristiques suivantes avec celles qui sont utilisées par les bornes interactives :

- utilisation du protocole allégé d'accès au répertoire ;
- support de Z39.50 pour les services de recherche et de récupération de documents assurés par le gouvernement ;
- support des protocoles HTML et HTTP pour se relier aux serveurs WEB du gouvernement ;

- interface polyvalente permettant de consulter les services de Pages blanches, bleues, jaunes et vertes ;
- possibilité d'imprimer localement les informations ainsi récupérées, moyennant l'équipement de chacun.

2.5.2.1.2 Interfaces gouvernementales (employés, administrateurs)

On distingue deux variantes de l'interface à la disposition du personnel du gouvernement, soit, d'une part, l'interface à l'intention des employés du gouvernement qui doivent consulter le Répertoire, ou encore modifier les données qui les concernent, et, d'autre part, l'interface utilisée par les administrateurs du Répertoire pour exécuter un ensemble de tâches de gestion du Répertoire. Il peut s'agir de la même interface physique, la différence essentielle étant l'étendue des droits d'accès accordés à l'utilisateur dans l'un et l'autre cas.

2.5.2.1.2.1 Les interfaces des employés du gouvernement

Les employés du gouvernement de façon générale et les administrateurs de serveur en particulier pourront accéder au Répertoire du gouvernement par des interfaces de répertoire plus spécialisées ou offrant plus de fonctionnalités que celles qui seront offertes au public, étant entendu que les employés gouvernementaux ont besoin d'une gamme plus étendue ou complexe d'informations nécessaires à l'exercice de leurs fonctions. L'interface à l'usage des employés du gouvernement fera appel aux mêmes protocoles que les interfaces à l'usage du public (ex. : support des protocoles LDAP, HTML, HTTP, Z39.50). Parce qu'elle donnera accès à une gamme étendue d'informations dont certaines seront à diffusion restreinte, l'interface gouvernementale fera directement appel aux mesures d'authentification et de contrôle d'accès définies par le schéma du Répertoire gouvernemental. L'interface d'information des employés du gouvernement demandera à l'employé un mot de passe ou une identification par clé privée de chiffrement afin d'authentifier l'utilisateur et d'accorder l'accès approprié à l'information contenue dans le Répertoire du gouvernement.

Ce type d'interface pourra être personnalisé pour supporter les exigences particulières spécifiées par les M/O. Il fournira des mécanismes avancés pour effectuer la recherche et la récupération des types d'information requis par les employés du gouvernement dans l'exécution de leurs tâches quotidiennes. Ces informations proviendront notamment de consultations effectuées dans le répertoire général des employés du gouvernement afin de retrouver les numéros de téléphones ou de télécopieurs, les adresses de courrier électronique et autres informations nécessaires pour assurer les communications à l'échelle gouvernementale ou le fonctionnement de l'appareil administratif de façon générale.

On recommande que chaque employé du gouvernement qui a besoin d'accéder au répertoire et aux services connexes sur une

base régulière puisse disposer sur son micro-ordinateur d'une interface affichant les caractéristiques suivantes :

- utilisation du protocole allégé d'accès au répertoire pour se brancher sur le serveur local de répertoire au moyen d'une connexion TCP/IP sur réseau local ;
- disponibilité de versions appropriées aux diverses plates-formes (Windows, Macintosh, UNIX, autres) ;
- support des protocoles HTML, HTTP et Z39.50.

Cette topologie de l'interface client du répertoire serait déployée dans tous les M/O de façon semblable afin de permettre aux employés du gouvernement l'accès au Répertoire.

2.5.2.1.2.2 Les interfaces d'administration du Répertoire gouvernemental

Ce type d'interface spécialisé de par ses fonctions est conçu pour que les administrateurs du Répertoire puissent gérer pleinement le Répertoire et ses services. La gestion du Répertoire porte sur l'ajout, la modification et la suppression des entrées relatives aux employés ou à l'organisation, les mécanismes et ententes de duplication des entrées de répertoire et autres types d'opérations administratives analogues.

L'interface d'administration du répertoire permettra aux administrateurs du répertoire X.500 de gérer le service du répertoire. L'interface d'administration permettra aux administrateurs d'accomplir les tâches suivantes :

- l'ajout, la suppression, la modification des entrées dans le serveur de répertoire X.500 ;
- la configuration de l'information de référence ;
- la configuration des mots de passe et des procédures d'authentification ;
- la configuration des informations de contrôle d'accès ;
- la configuration des procédures de mise à jour des copies miroir ;
- la surveillance des activités et des registres du serveur de répertoire.

Chaque site gouvernemental qui maintient un serveur de répertoire devra disposer d'une interface d'administration localement ou par accès à distance. Un serveur du répertoire ne peut être administré sans qu'une interface d'administration ne lui soit rattachée. Les interfaces d'administration doivent utiliser le protocole complet d'accès au répertoire plutôt que le protocole allégé afin de soutenir toutes les fonctionnalités requises.

2.5.2.2 Applications clients

Les applications clients sont celles qui utilisent les services du Répertoire pour répondre à des requêtes adressées par des programmes ou applications

informatiques plutôt que par des humains. À titre d'exemple, pour les applications de commerce électronique et autres échanges et transactions sécurisés, il pourra s'agir de récupérer des certificats de clés publiques, ou de vérifier des listes de révocation de ces clés, le cas échéant. Pour les applications de messagerie, il pourra s'agir de repérer l'adresse électronique d'une personne, ou de tous les membres d'une liste de distribution. Pour les applications client-serveur de façon générale, il pourra s'agir de localiser les adresses de réseau et autres informations analogues sur les serveurs. Les applications client ont besoin de l'adresse réseau des applications serveurs avec lesquels elles veulent communiquer. En utilisant le répertoire X.500 à cet effet, la partie serveur des applications peut être déployée sur des serveurs en réseau sans que l'adresse du serveur soit « figée » dans l'application client. Ce principe fondamental de l'informatique répartie permet à la partie serveur des applications de se déplacer d'ordinateur en ordinateur sans affecter le grand nombre d'applications client déjà déployées.

Les applications seront inscrites en tant qu'entrées du Répertoire gouvernemental dans la classe d'objets « processus d'application ». L'un des attributs obligatoires à chaque processus d'application est son adresse de réseau, y compris les adresses de port et de prise TCP/IP. Les applications client auront besoin d'être développées ou restructurées afin d'utiliser les protocoles LDAP, DAP ou les appels de l'interface de programmation appropriée afin d'interagir avec le répertoire. De plus, les applications pourraient avoir besoin de supporter les protocoles HTML, HTTP et/ou Z39.50 pour accéder à des services connexes.

2.6 Modèle général d'architecture du Répertoire gouvernemental

À partir de ce qui précède, nous proposerons les grands traits de l'architecture générale cible du répertoire gouvernemental et de la stratégie de transition pour y parvenir.

2.6.1 Le méta-répertoire

Par-delà la considération des bienfaits inhérents aux grandes structures homogènes et généralisées reposant sans exceptions sur des normes uniformes de bout en bout, la logique qui préside à l'équipement en répertoires des M/O, comme des organisations du secteur privé, est en grande partie commerciale et fonction de la disponibilité de produits sur le marché. Cette logique conduit à l'acquisition de produits différents et peu ou pas compatibles, tendance alimentée par la liberté accrue laissée aux M/O dans la gestion de leur budget informatique. Des répertoires locaux et non reliés les uns aux autres sont ainsi en train de s'implanter dans les organisations par l'entremise surtout des réseaux locaux, des systèmes d'exploitation, des systèmes de courrier et des intranets. Soutenue par le faible coût de ces produits, leur facilité d'implantation et la poussée irrésistible de l'informatique en réseau, cette tendance à l'implantation de répertoires hétérogènes, comme autant d'îlots isolés, irait en s'intensifiant.

Bien que la très grande majorité des répertoires offerts soient compatibles LDAP, ces derniers ne forment pas pour autant un tout intégré : chaque serveur donnant accès à un répertoire LDAP possède sa propre adresse réseau ; chacun a ses propres mécanismes et politiques de contrôle d'accès, sa base de données d'usagers et de mots de passe, et son propre schéma. On fait ainsi face à une collection, un archipel, de services de répertoire sans communication entre eux, mais tous, ou presque tous, accessibles par LDAP.

Face à cela, la solution préconisée consiste à mettre en place un méta-répertoire à ossature de base X.500 et avec accès frontal LDAP, associant des répertoires hétérogènes compatibles X.500 ou LDAP au fonctionnement du répertoire réparti spécifié par X.500.

Le méta-répertoire permet la mise en place d'une confédération de serveurs hétérogènes réunis en un tout fonctionnel unifié, les avantages et les caractéristiques de X.500 étant mis à contribution pour créer un ensemble de services de répertoire accessibles par LDAP. Le méta-répertoire joue sur les deux tableaux en misant à la fois sur les avantages de X.500 et de LDAP, soit un service de répertoire X.500 étendu pour utiliser LDAP comme protocole d'accès aux multiples répertoires qui, sans être compatibles X.500, sont cependant compatibles LDAP.

Le méta-répertoire offre ainsi une vision et un fonctionnement intégré des diverses composantes de répertoire de l'organisation et il favorise la coexistence des serveurs X.500 et LDAP. Ses principales caractéristiques sont : un schéma commun, un ensemble unifié d'informations à partir du contenu des divers répertoires de l'organisation ; une seule adresse réseau ; un seul mécanisme d'accès ; un point unique pour l'administration des divers répertoires individuels ; les fonctionnalités de X.500, dont la réplication des données ; l'interface LDAP ; l'intermédiaire de connexion avec d'autres serveurs compatibles LDAP. Un tel service de répertoire peut s'édifier à partir d'extensions à un serveur X.500.

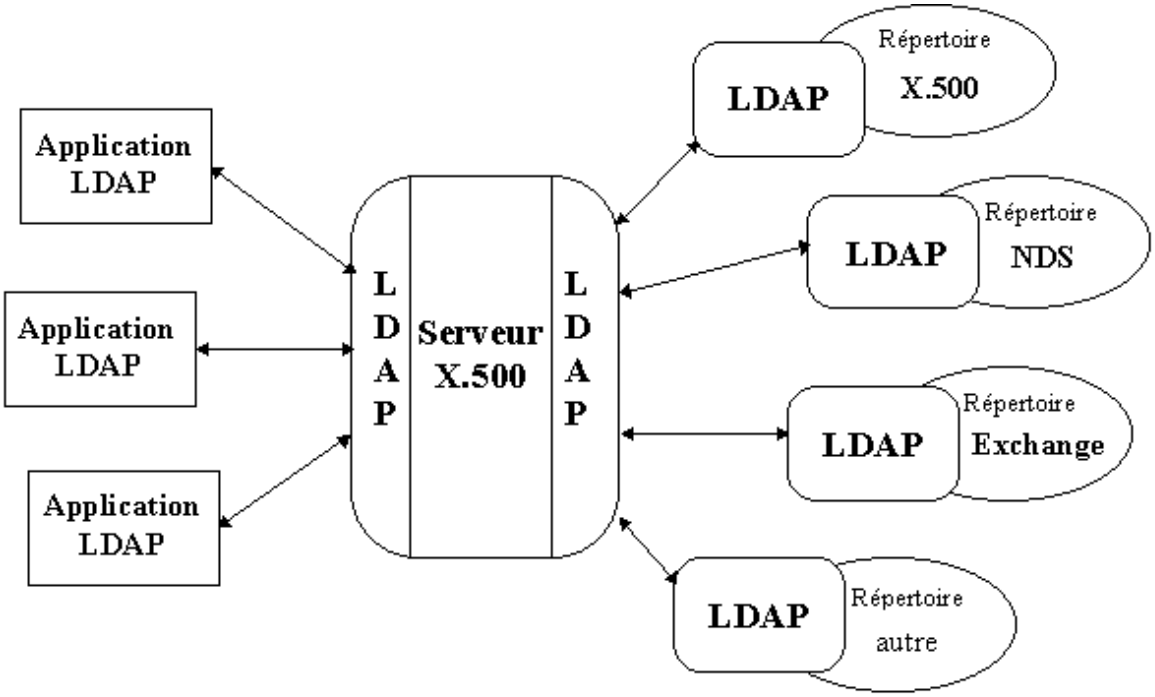


Figure 2-1 : Méta-répertoire avec dorsale X.500 et accès LDAP

Vu de cette façon, le méta-répertoire est analogue aux entrepôts de données qui intègrent l'information d'affaires provenant de diverses bases de données transactionnelles. Vu dans l'axe de l'évolution des systèmes, le méta-répertoire constitue une composante

importante de la migration des répertoires propriétaires vers des répertoires à base de normes ouvertes. Dans sa plus simple expression, il s'assimile à une centrale de synchronisation à base X.500.

2.6.2 La synchronisation du répertoire comme mesure transitoire

Le Répertoire gouvernemental supportera la synchronisation des répertoires à titre de mesure transitoire vers l'interfonctionnalité permise par X.500. La topologie recommandée pour la synchronisation des répertoires consiste à utiliser la base des entrées du répertoire X.500 comme dépôt pour les informations de type Pages blanches sur les employés du gouvernement, notamment les adresses électroniques. Le serveur principal du répertoire assurera le fil conducteur pour tenir ensemble la base des entrées du répertoire à travers les multiples implantations de synchronisation du répertoire. Les M/O seront chargés de synchroniser les répertoires de leurs systèmes de courrier électronique existants avec le Répertoire gouvernemental. Cette stratégie de transition pour les données existantes s'accompagnera en même temps de l'intégration et de l'implantation, par prototypage successif, de services nouveaux (ex. : services Pages bleues, Pages vertes, sécurisation des échanges électroniques) dont les données seront hébergées dans les serveurs répartis du Répertoire.

Il existera plusieurs façons pour les utilisateurs d'accéder aux données de répertoires qui feront l'objet de synchronisation. Toutes les procédures suivantes seront disponibles :

- fureteurs Web, tels que Navigator ou Explorateur ;
- accès aux répertoires de courrier électronique sur réseaux locaux (les adresses s'affichent selon le format propre au système de courrier électronique sur réseau local) ;
- interfaces client qui utilisent le protocole allégé d'accès au répertoire ;
- bottins de format propriétaire présentant des données de répertoire X.500 maintenues sur réseau local.

CHAPITRE 3

3.0 Appellation et structure de l'arborescence du répertoire

La présente section propose des conventions d'appellation et des règles et modalités d'inscription pour l'espace d'appellation du Répertoire gouvernemental, soit, dans le grand schème du répertoire mondial auquel conduisent les recommandations X.500 de l'UIT, la ramification de l'arborescence mondiale qui se situe directement sous la responsabilité administrative du gouvernement du Québec. Des indications spécifiques seront données sur les conventions d'appellation et les règles et modalités d'inscription des unités organisationnelles de premier niveau sous l'autorité du Registraire gouvernemental. La délégation d'autorité en faveur des unités organisationnelles de premier niveau sera esquissée. Des directives générales seront ensuite formulées relativement aux questions d'appellation et de structure de l'arborescence qui sont particulièrement pertinentes aux niveaux inférieurs (unités organisationnelles de niveau 2 et plus) de l'espace d'appellation du gouvernement.

3.1 Unités organisationnelles de premier niveau

Le gouvernement du Québec est inscrit dans l'arborescence mondiale, sous la province de Québec[6], à titre d'organisation[7]. Les ministères et les organismes sont inscrits à titre d'unités organisationnelles[8], immédiatement sous le gouvernement[9]. Les M/O constituent ainsi des unités organisationnelles de premier niveau. La figure 3-1 illustre le concept de premier niveau de l'arborescence du Répertoire gouvernemental.

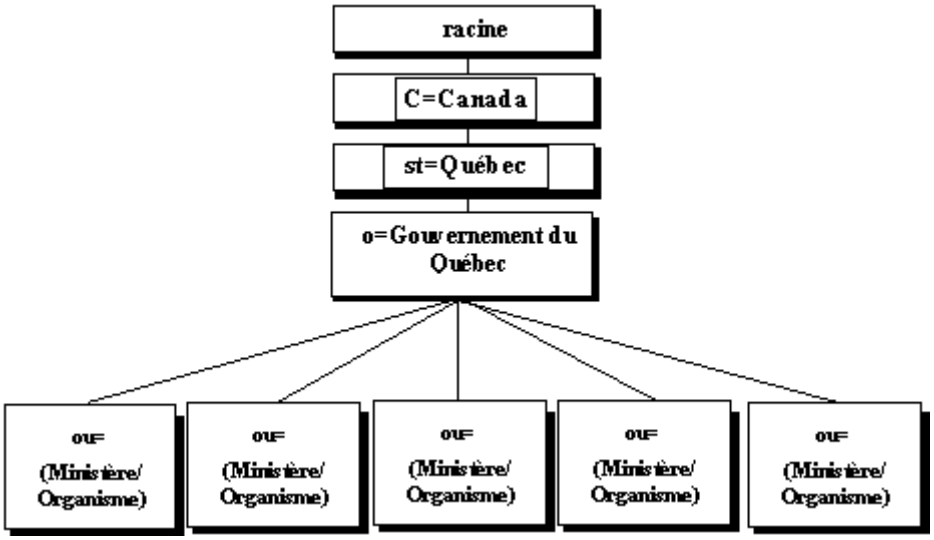


Figure 3-1 : Premier niveau de l'arborescence du Répertoire gouvernemental

La constitution du premier niveau d'unités organisationnelles du Répertoire gouvernemental est soumise à des règles d'inscription et d'appellation spécifiques.

3.1.1 Règles et modalités d'inscription

Les règles et les modalités d'inscription comportent des procédures usuelles et des mesures d'exception.

---

[6] StateOrProvince, st=
[7] organization, O=
[8] organizationalUnit, OU=
[9] O=GQ

3.1.1.1 Procédures usuelles

La liste de référence pour fin d'inscription au Répertoire des unités organisationnelles de premier niveau est celle qui est établie par les autorités du Conseil exécutif. Par définition, les unités organisationnelles de premier niveau sont celles, dans la hiérarchie, qui ne sont incluses dans aucune autre. L'inscription de tout ministère ou organisme au répertoire gouvernemental se fera par l'entremise du Registraire gouvernemental. De plus, le Registraire acceptera l'inscription à titre d'unité organisationnelle de premier niveau de toute autre entité organisationnelle désignée expressément à ce titre par les autorités du Conseil exécutif. Après entente à cet effet avec les secteurs et réseaux concernés, et avec l'accord des autorités appropriées du Conseil exécutif, le Registraire pourra également inscrire à titre d'unité organisationnelle de premier niveau toute unité organisationnelle de niveau approprié des secteurs législatif et judiciaire ainsi que des réseaux de la santé, de l'éducation et du monde municipal.

Lorsque l'unité organisationnelle qui demande à s'inscrire au premier niveau peut être incluse dans une des unités organisationnelles de premier niveau, le Registraire informera à la fois l'organisme « parent » et l'organisme demandeur de l'existence d'un conflit. Le Registraire agira ensuite comme médiateur entre les parties pour régler le différend. Dans tous les cas, l'organisme demandeur pourra figurer comme alias parmi les unités organisationnelles de premier niveau alors que les données à son égard seront subordonnées à l'unité organisationnelle dûment inscrite à ce titre en vertu des dispositions susmentionnées.

3.1.1.2 Exceptions

Toute unité organisationnelle de premier niveau telle que désignée par les autorités compétentes du Conseil exécutif peut prendre sur elle de désigner d'autres unités organisationnelles de premier niveau comme lui étant subordonnées aux fins des processus d'appellation et d'inscription au Répertoire gouvernemental. À titre d'exemple, le ministère de la Culture et des Communications pourrait, par hypothèse, vouloir situer sous son égide, pour des fins d'appellation et d'inscription, les organismes que sont la Commission de toponymie du Québec, la Commission des biens culturels ou le Centre de conservation du Québec. Un tel arrangement serait acceptable aux conditions suivantes :

- Que les parties en cause soumettent au Registraire gouvernemental un mémoire d'entente signifiant leur commun accord.
- Que les organismes ainsi inclus dans le MCCQ conviennent de retirer leur inscription à titre d'unité organisationnelle de premier niveau.

À l'inverse, toute unité organisationnelle de premier niveau telle que désignée par les autorités compétentes du Conseil exécutif peut prendre sur elle de désigner toute unité organisationnelle de niveau inférieur située sous elle à titre d'unité organisationnelle de premier niveau aux fins d'appellation et d'inscription au Répertoire gouvernemental. À titre d'exemple, le ministère de la Culture et des Communications pourrait, par hypothèse, décider de désigner le Secrétariat à la politique linguistique à titre d'unité organisationnelle de premier niveau, même si une telle décision différait de la liste établie par les autorités compétentes du Conseil exécutif. Un tel arrangement serait acceptable aux conditions suivantes :

- Que les parties en cause soumettent au Registraire gouvernemental un mémoire d'entente signifiant leur commun accord.

- Que l'unité organisationnelle qui accède ainsi au premier niveau d'unité organisationnelle convienne de désigner un Registraire interne, chargé des processus d'appellation et d'inscription au Répertoire pour la ramification du domaine gouvernemental qui la concerne.
- Que ladite unité organisationnelle convienne de soumettre son inscription à titre d'unité organisationnelle de premier niveau et de se conformer aux politiques et procédures d'appellation et d'inscription à ce même niveau.

3.1.2 Conventions d'appellation

Le nom désignant l'entité inscrite est celui qui figure dans la liste établie par les autorités du Conseil exécutif et que l'on retrouve à l'Annexe A. La syntaxe de ce nom peut prendre la forme suivante :

- Ministère de ..., du ..., des ...
- Conseil de ..., du ..., des ...
- Société ..., Régie ..., etc. de ..., du ..., des ...

À l'inscription, on pourra attribuer un ou plusieurs autres noms pour désigner l'unité organisationnelle en question. À titre d'exemple, le ministère des Transports pourrait demander qu'on le désigne également par les autres noms suivants :

- Transports
- MTQ

Afin de faciliter les recherches dans le Répertoire, on pourra désigner un nombre illimité de noms pour représenter l'entité inscrite. Toutefois, un seul de ces noms (dans le cas présent, Ministère des Transport) pourra faire office de nom distinctif relatif (RDN, pour « Relative Distinguished Name »). Le nom distinctif relatif est celui sous lequel sera désignée l'unité organisationnelle en réponse à une recherche effectuée dans le Répertoire.

Par exemple, toute requête qui utiliserait une partie ou l'ensemble des noms « Ministère des Transports », « Transport » ou « MTQ », attribués au ministère s'occupant des transports, ferait apparaître l'entrée du répertoire pour le « Ministère des Transports », le nom distinctif relatif attribué pour désigner de façon exclusive ce ministère parmi l'ensemble des M/O du gouvernement du Québec.

3.2 Délégation d'autorité

En vertu de l'autorité qui lui est déléguée en matière d'appellation et d'inscription par les instances supérieures ayant juridiction sur le territoire québécois, le Registraire gouvernemental déléguera une part de cette même autorité aux organisations qui s'inscrivent à titre d'unités organisationnelles de premier niveau. En plus d'assumer la part de responsabilités qui lui revient en ce qui a trait à la gestion des systèmes du Répertoire[10], chaque unité

[10] Soit, essentiellement, prendre en charge :

- La configuration du système - assurer la modularité des composantes logicielles et matérielles pour en faciliter la modification tout en suscitant un minimum d'impact sur les opérations du répertoire.
- Le contrôle des anomalies de fonctionnement - le répertoire utilisera un mécanisme de vérification permettant d'identifier les problèmes opérationnels, de détecter les atteintes à la sécurité et de produire des diagnostics qui contribuent à restaurer les services du Répertoire.
- La performance - le répertoire sera configuré de manière à en optimiser la performance, laquelle sera calculée à partir du temps de réponse aux requêtes des utilisateurs.

organisationnelle de premier niveau se verra aussi déléguer des responsabilités en matière de gestion de l'information du Répertoire.

Chaque unité organisationnelle de premier niveau devra ainsi assurer l'établissement d'un Registraire interne, chargé d'appliquer les politiques d'appellation et d'inscription au sein du M/O, ou de façon générale, de l'unité organisationnelle de premier niveau en cause. Les registraires internes des M/O sont responsables de l'inscription des unités organisationnelles situées sous les unités organisationnelles de premier niveau (soit les unités organisationnelles de niveau 2 et plus) et, de façon générale, ils assurent le respect du schéma du Répertoire. Le registraire interne peut déléguer une part de responsabilité à des paliers inférieurs.

Le registraire doit notamment maintenir à jour un registre des noms distinctifs relatifs au sein de l'unité organisationnelle afin de conserver le caractère unique des noms. Le registraire interne doit ainsi s'assurer que chaque objet dans la ramification située sous l'unité organisationnelle de premier niveau possède un nom distinct et qui ne présente pas d'ambiguïté. De plus, le registraire interne doit assurer la qualité, et notamment l'exactitude, des données contenues dans la base des entrées du répertoire pour l'unité organisationnelle de premier niveau qui le concerne.

Le registraire interne, par l'entremise de l'unité organisationnelle de premier niveau où il se situe, peut désigner un mandataire pour s'acquitter des tâches qui lui sont déléguées. À titre d'exemple, il se pourrait que le Conseil des Arts et des Lettres du Québec désire, par hypothèse, figurer au Répertoire gouvernemental, sans pour autant devenir un gestionnaire de domaine du Répertoire gouvernemental. Dans ce cas, le Conseil pourrait, par exemple, désigner le MCCQ comme mandataire.

3.3 Unités organisationnelles de deuxième niveau et plus

Chaque unité organisationnelle de premier niveau bénéficie d'une délégation d'autorité de la part du Registraire gouvernemental en matière d'appellation et d'inscription au Répertoire. Chaque unité organisationnelle de premier niveau sera de plus responsable de mettre en place et d'entretenir la structure, et notamment la cascade d'unités organisationnelles de niveau 2 et plus, qui lui conviendra le mieux tout en respectant les directives et recommandations générales exposées ci-après.

3.3.1 Les noms distinctifs

Un nom distinctif de répertoire (DN, pour « Distinguished Name ») est assigné à chaque entrée du Répertoire afin d'établir un lien entre un nom d'usage courant et des valeurs contenues dans une entrée du Répertoire. Les entrées dans un répertoire de type X.500 sont reliées les unes aux autres par la structure hiérarchisée que représente l'arborescence du répertoire.

Qu'il s'agisse de personnes de l'organisation, de documents, d'appareils, de processus d'application, de rôle dans l'organisation, etc., chaque entrée dans l'arborescence du répertoire est identifiée de manière unique par son nom distinctif. Le nom distinctif d'un objet donné se définit comme étant la séquence de noms distinctifs relatifs de cette entrée

---

- La sécurité - le répertoire fournira des mécanismes de contrôle d'accès pour protéger les informations au niveau des attributs.
- La comptabilité - le répertoire sera un service auto-financé et facturé à l'usage de façon à récupérer les coûts d'exploitation

qui représente l'objet en question et toutes les entrées qui lui sont supérieures, et ce en ordre décroissant. Chaque entrée possède un nom distinctif relatif qui lui est unique et qui constitue une valeur d'attribut formant le nom distinctif de cette entrée. Les entités (personnes, documents, appareils ou autres) qui font l'objet d'une entrée sont listées sous la ramification correspondante du ministère ou à l'organisme en cause.

3.3.2 Les alias

On peut utiliser un alias pour toute entrée du Répertoire afin de faciliter la recherche d'un objet répertorié en lui procurant une identité/emplacement d'emprunt qui ne fait que référer à sa véritable identité/emplacement dans l'arborescence. On peut placer un alias à tout niveau de l'arborescence. Une entrée d'alias ne contient qu'un nom distinctif relatif et le nom distinctif de l'entrée d'objet à laquelle elle réfère. Une entrée d'alias n'a pas de subordonnées et elle est par conséquent toujours située à l'extrémité d'une branche de l'arborescence. L'entrée d'objet pointée par l'entrée d'alias est celle qui contient véritablement les données sollicitées. On appellera « résolution » (« dereferencing ») la conversion d'un nom d'alias en nom d'objet. La figure suivante offre un exemple d'alias d'unité organisationnelle pour le Secrétariat de l'autoroute de l'information, qui serait effectivement une unité organisationnelle de premier niveau bien définie comme telle, soit essentiellement une unité organisationnelle relevant directement d'un ministre, mais qu'il pourrait par ailleurs être utile de retrouver lorsque l'on cherche sous « Ministère de la Culture et des Communications ».

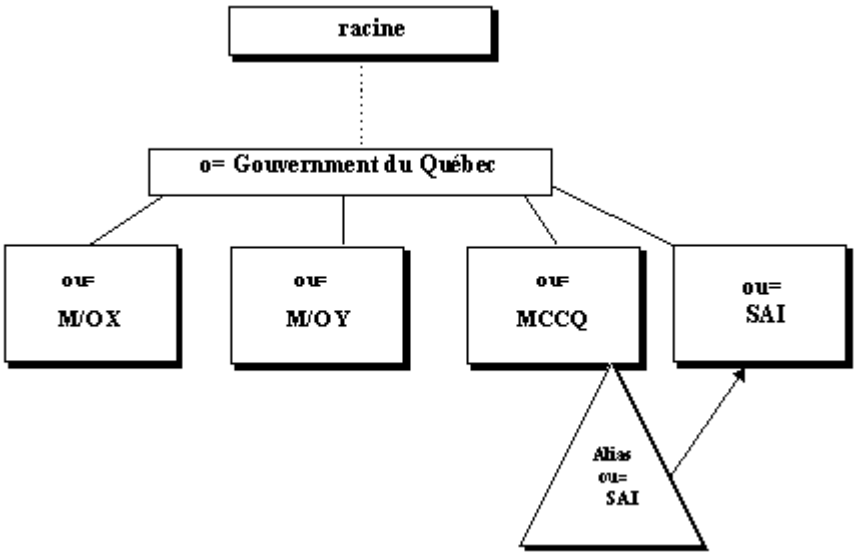


Figure 3-2 : Exemple d'alias d'unité organisationnelle

3.3.3 La conception de l'arborescence

La conception de l'arborescence du répertoire devra résulter d'un compromis entre le nombre de niveaux de l'arborescence et l'étalement de cette dernière, tout en maintenant la désignation unique des objets répertoriés[11]. Il n'est généralement pas nécessaire de documenter toute la structure administrative d'un M/O pour assurer la désignation unique des objets répertoriés. Il est recommandé que l'arborescence ne comporte pas plus de huit niveaux. La conception de l'arborescence devra refléter l'organisation de l'information

[11] À titre d'exemple, si l'arborescence du Répertoire gouvernemental québécois ne comportait qu'un seul niveau, il faudrait composer avec pas moins de 12 Pierre Tremblay et 15 Pierre Morin, alors que quelques niveaux supplémentaires suffiraient à éviter une telle éventualité.

qui se révélera la plus efficace pour les fins de l'utilisation du Répertoire.

À partir du deuxième niveau de l'arborescence, les M/O auront la possibilité de recourir à des entrées d'unité organisationnelle ou de localité. Une localité peut tenir lieu d'une unité organisationnelle à partir du niveau 2 si l'unité organisationnelle de niveau supérieur est dispersée géographiquement. On pourra utiliser une classe d'objet soit de localité, soit d'unité organisationnelle pour indiquer le lieu en cause, tout dépendant de la capacité de l'interface client du répertoire à effectuer la recherche indifféremment sur l'une ou l'autre classe d'objet. La désignation par l'entremise de la localité ajouterait un niveau à l'arborescence du répertoire pour une unité organisationnelle qui est dispersée géographiquement, mais elle se traduirait probablement par contre par un temps de recherche plus court.

3.3.4 La convention d'appellation d'une unité organisationnelle

L'appellation des unités organisationnelles des M/O doit s'inspirer du Plan d'organisation administrative supérieure (POAS) respectif de chacun des ministères ou organismes. Le nom doit être convivial et aussi bref que possible, tout en demeurant reconnaissable.

3.3.5 La convention d'appellation d'une localité

L'appellation des localités doit s'inspirer des désignations usuelles ou officielles d'origine administrative (ex. : Est du Québec, Chaudière-Appalaches) ou proprement géographique (ex. : Rimouski).

3.3.6 La convention d'appellation d'une personne de l'organisation

Le nom courant d'une personne de l'organisation sera désigné par la combinaison « nom de famille, prénom ». Chaque nom courant devra être unique au sein d'un même contexte d'appellation. Les noms courants seront formés à partir des entrées contenues dans les dossiers du personnel de l'organisation. Les noms pourront être composés directement à partir des informations emmagasinées dans le système du personnel (ex. : SAGIP). Chaque organisme devra résoudre les doublons en recourant aux règles d'écriture usuelles, si ce n'est déjà fait dans les dossiers du personnel. L'inscription de plusieurs valeurs possibles pour le nom courant, y compris les surnoms, permettra de faciliter la recherche. Il est prévu que la recherche sur les noms courants s'effectuera sur les champs de « nom de famille » et de « prénom » et selon ce qui est spécifié par la norme canadienne de classement.

3.4 Les arborescences non-opérationnelles

Si besoin est de noms distinctifs relatifs pour fins d'expériences, on recommande l'ajout d'un (p) pour « provisoire » à la suite du nom distinctif relatif. On agit de la sorte pour indiquer que l'arborescence du répertoire qui suit est un banc d'essai, plutôt qu'une unité opérationnelle

3.5 Les fournisseurs du gouvernement

Les fournisseurs de biens et services à l'intention du gouvernement qui n'apparaissent pas ailleurs dans le répertoire pourront bénéficier d'une entrée au répertoire. L'entrée du fournisseur peut apparaître à titre d'unité organisationnelle de niveau 2 ou plus à tout endroit approprié de l'arborescence gouvernementale. Par exemple, si la partie contractant avec le ministère des Ressources naturelles (MRN) s'appelle SNC-Lavalin, le nom distinctif relatif dans l'arborescence du MRN serait :
OU = SNC-Lavalin

Les fournisseurs, comme tout autre objet du Répertoire, peuvent également être désignés par des entrées d'alias à tout niveau du Répertoire.

4.0 Les mécanismes de sécurité et leur architecture

Le Répertoire gouvernemental doit absolument être doté de mécanismes de sécurité afin de protéger et de sauvegarder l'information qu'il contient. Il faut aussi contrôler l'accès par les utilisateurs et les applications, ainsi que les échanges avec eux. Il est appelé à contenir de plus en plus d'information précieuse ; cette information ne doit pas être vulnérable. Sa structure répartie est utile dans la segmentation de l'information et facilite la gestion du contrôle d'accès en fonction d'autorisations définies formellement et avec précision. Un agencement élaboré de concepts, de logiciels, de procédures administratives et d'arrangement des composantes physiques permet de garantir un degré élevé de sécurité répondant aux plus hautes exigences.

Les normes de services X.500 définissent deux mécanismes visant la sécurité des informations contenues dans un répertoire :

- le cadre d'authentification : il s'agit d'identifier avec certitude l'utilisateur ou l'application qui demande l'accès au répertoire.
- le cadre de contrôle d'accès : il s'agit de permettre aux détenteurs de l'information contenue dans la base des entrées de limiter l'accès et de restreindre les opérations effectuées sur les entrées.

Dans le contexte du répertoire du gouvernement, la question de la sécurité revêt une importance capitale pour les références internes. Comme il a déjà été expliqué, les données dans la base d'entrées résident dans un ou plusieurs serveurs du répertoire. Lorsqu'une interface client sollicite des informations pour un utilisateur ou une application, le serveur donnera une réponse en utilisant la méthode que l'on a conçue et implantée dans la topologie du répertoire. Les données du répertoire seront retournées soit au moyen d'un réacheminement via des serveurs interconnectés ou par une lecture directe au serveur à partir d'une copie des informations en question. Dans un cas comme dans l'autre, il est possible que des personnes non autorisées tentent d'accéder aux éléments de données ou aux applications. Pour empêcher la destruction ou la mauvaise utilisation des informations aux mains d'intrus, certains mécanismes de sécurité ont été intégrés au répertoire X.500.

Le présent chapitre comporte les trois sections suivantes :

1. besoins de sécurité en réseau,
2. arrangements administratifs pour un fonctionnement en sécurité du Répertoire,
3. arrangements techniques du Répertoire pour assurer la sécurité des utilisations.

4.1 Besoins de sécurité en réseau

Au cours des trois dernières années, l'Internet est venu bouleverser le paradigme de base dans la façon d'envisager les risques et les solutions. Les militaires, les banques et les grandes entreprises s'adonnent depuis longtemps aux échanges électroniques en misant sur des réseaux protégés, d'usage exclusif, pour augmenter la sécurité des transactions entre partenaires peu nombreux et se connaissant bien. Cette situation est en voie de se transformer très rapidement. Les échanges s'ouvrent, se multiplient et se complexifient. Cette multiplication des échanges oblige à en repenser la sécurisation.

Dans cette veine, le nouveau paradigme de sécurité est basé sur l'idée que les réseaux ouverts sont difficiles à protéger, en fait qu'il vaut mieux les considérer comme un milieu hostile. La solution consiste par conséquent à renforcer le blindage des messages. Cette vue s'est imposée en raison, d'une part, des conditions d'usage de réseaux publics non protégés et vulnérables qui caractérisent l'Internet, et, d'autre part, de la multiplication projetée d'échanges devant faire l'objet d'une authentification multilatérale et ouverte entre un nombre de partenaires

des milliers de fois plus nombreux qu'auparavant. Dans cette situation nouvelle, aux mécanismes de sécurité préexistants, qui seront conservés (sauf peut-être le maintien coûteux de réseaux protégés), viendront s'ajouter des mécanismes nouveaux fondés sur une application de mathématiques complexes des grands nombres premiers permettant d'ajouter plusieurs fonctions cruciales de sécurité, en particulier la sécurité de transmission en réseau public.

La présente section vise à expliquer comment sont reliés les concepts et les mécanismes de sécurité en réseau et quelles sont les grandes mesures de sécurité jugées nécessaires au fonctionnement du Répertoire.

4.1.1 Concepts de sécurité en réseau

Une panoplie d'approches et de standards existent en vue de garantir la sécurité des ressources et échanges en réseau. Une liste de cinq concepts (ISO 7498-2, 1989) se révèle utile pour embrasser l'ensemble des questions de sécurité dans un fonctionnement en réseau :

- Contrôle d'accès : sert à déterminer quelles données ou applications un utilisateur authentifié est autorisé à consulter, modifier, etc.
- Identification et authentification : sert à déterminer qui se connecte à un serveur donné et son identité véritable (au moyen d'un identifiant d'utilisateur, mot de passe, clé de chiffrement certifiée).
- Confidentialité des données : sert à garantir la confidentialité d'une information (habituellement par chiffrement), sa non-accessibilité lors de sa transmission ou dans les recueils et archives.
- Intégrité des données : sert à garantir que les données n'ont pas été modifiées lors de leur transmission ou depuis la dernière mise à jour officielle (vérification par régénération de données ayant été chiffrées).
- Non-désaveu ou non-répudiation : sert à empêcher le destinataire de pouvoir nier avoir reçu un message ou l'émetteur de pouvoir nier l'avoir transmis (pour transfert de fonds, commande, obligation contractuelle).

4.1.2 Mécanismes de sécurité en réseau

L'évolution des réseaux locaux ou étendus vers la nécessaire interdépendance avec l'inforoute sous-tendent un besoin accru de contrôle d'accès. Si l'information à partager doit s'accroître, il faut aussi une sophistication plus grande du contrôle d'accès. Il s'agit d'un domaine où le Répertoire fournira un apport crucial.

Il y a longtemps que les messages transmis sont encryptés ou chiffrés pour les rendre inintelligibles en cas d'interception. La transmission du code nécessaire au déchiffrement a été résolue soit en conservant le même code longtemps, soit en ayant convenu d'une liste de codes possibles à l'avance, soit encore en transmettant ce code par un canal différent de transmission. Il faut qu'il y ait eu partage d'un secret sur une période de temps. Ce code, sous sa forme électronique la plus répandue aujourd'hui, s'appelle une *clé symétrique* pour signifier que c'est le même code qui est utilisé au moment de chiffrer et de déchiffrer.

L'invention d'une procédure plus récente, l'encryptage par *clés asymétriques*, introduit une nouveauté par laquelle la clé de déchiffrement n'est plus la même que la clé de chiffrement. Ce que cette innovation change vraiment, c'est qu'il n'y a plus obligation de partager un secret valable plus d'une fois entre l'émetteur et le destinataire. Les clés asymétriques existent en paires indissociables obtenues mathématiquement. Une paire de

clés asymétriques est appelée *biclé*. Une biclé est composée d'une clé privée, que le détenteur ne divulgue à personne, et d'une clé publique, c'est-à-dire associée à un *nom distinctif* dans un répertoire accessible publiquement. Les caractéristiques particulières des biclés ont servi de base à des mécanismes nouveaux importants comme la signature numérique, la certification et l'enveloppe numérique.

La figure 4-1 présente une vue schématique de l'échange d'un document électronique : des éléments, des étapes et des concepts de sécurité marquent le parcours d'un document répondant aux exigences de sécurité entre un émetteur et un destinataire. Le haut de la figure illustre ce que l'émetteur du document fait pour le signer puis le rendre illisible afin de le transmettre, puis ce que le destinataire fait pour pouvoir lire le document et en vérifier la signature.

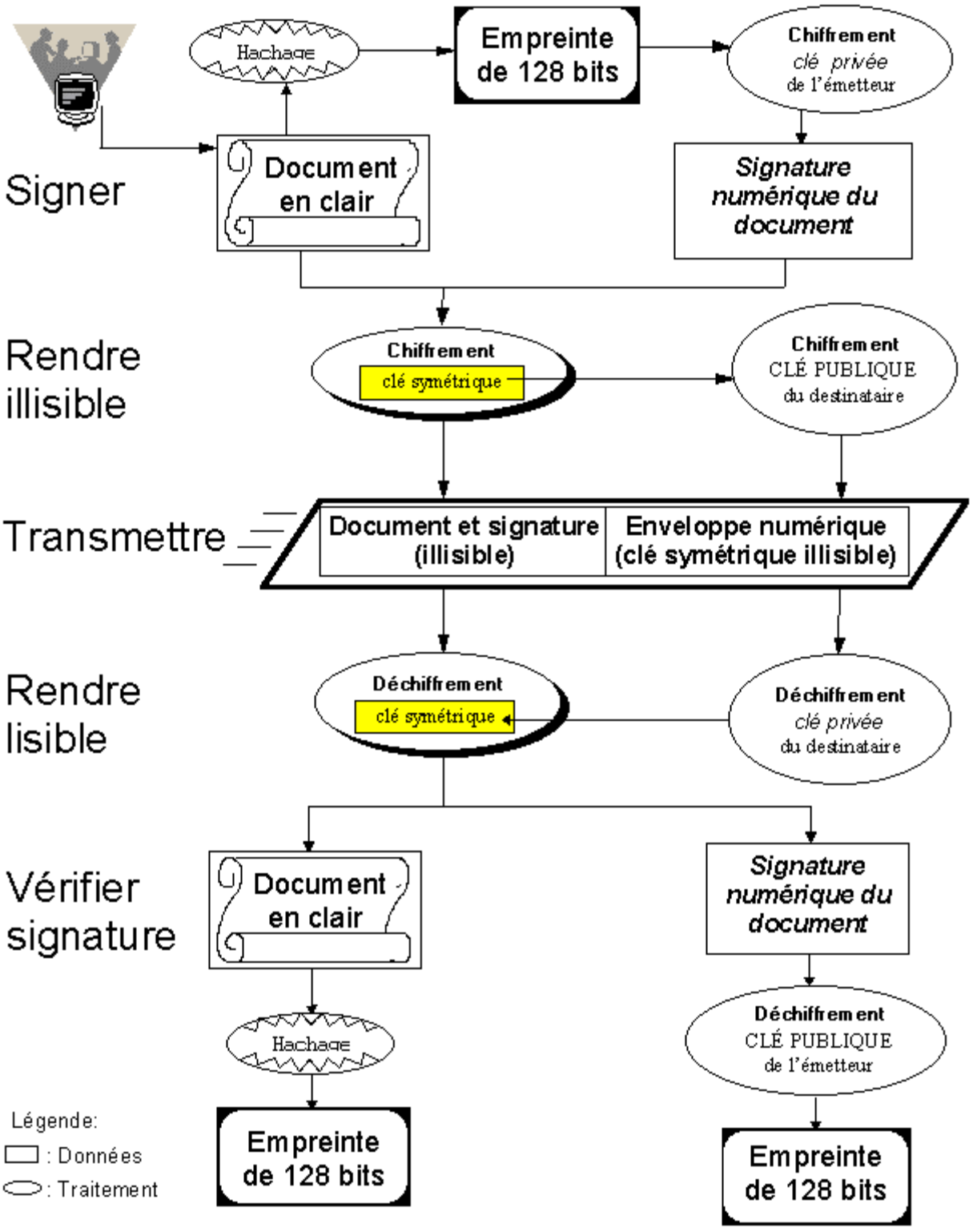


Figure 4-1
Vue schématique de l'échange d'un document

Signer le document assure de deux choses :

- que le document n'a pas été modifié d'un iota tant que l'empreinte résultant de l'algorithme de hachage reste égale : intégrité ;
- que le document a été signé par la seule personne à connaître le secret de sa clé privée puisque le déchiffrement avec la clé publique correspondante doit parvenir à la même valeur d'empreinte : authentification de l'identité de l'émetteur, non-répudiation.

Le document lui-même est rendu illisible en le chiffrant avec une clé symétrique. Cette clé symétrique est transmise au destinataire en la rendant à son tour illisible à toute autre personne que le destinataire grâce au chiffrement effectué avec la clé publique du destinataire. La clé symétrique rendue illisible est appelée l'enveloppe numérique, au sens qu'elle sert à cacher le contenu lors de la transmission : confidentialité, authentification de l'identité du destinataire.

Chez le destinataire, rendre lisible le document consiste à d'abord ouvrir l'enveloppe pour récupérer la clé symétrique, puis déchiffrer le reste du message, c'est-à-dire le document et la signature attachée. Le destinataire peut alors vérifier l'intégrité du document et l'authentification de l'émetteur, s'assurant ainsi de la non-répudiation ultérieure du document. La vérification de l'intégrité du document et de l'identité de l'émetteur sera réussie si les deux empreintes obtenues par des chemins différents sont identiques

4.1.3 Trois grandes mesures de sécurité

Les mesures de sécurité se trouvent étroitement entrelacées. Il y a beaucoup d'ingéniosité dans la réutilisation de quelques éléments de base pour effectuer des transformations et vérifications au bénéfice de diverses finalités de sécurité. Ainsi en est-il du contrôle de l'accès, de l'identification des utilisateurs et de la sécurité de transmission. Ces grandes mesures de sécurité seront présentées en détail dans la troisième section du chapitre. Leur étroite interdépendance sera mise en relief.

4.2 Arrangements administratifs pour le fonctionnement en sécurité du Répertoire

Si les aspects techniques comportent certaines difficultés de mise en application, les arrangements administratifs sont probablement un défi plus grand encore. Avant même que le système technique du Répertoire puisse être déployé, il faut que des définitions de procédures et des attributions de responsabilité aient auparavant été adoptées.

Dans cette section, quatre volets sont présentés comme essentiels à l'encadrement administratif pour la production du Répertoire, son fonctionnement et la réalisation de ses services afin d'assurer la sécurité de cette ressource commune.

4.2.1 Gestion des ressources humaines

Les unités administratives actuellement chargées de la gestion des ressources humaines ont un rôle important à jouer dans le chargement du Répertoire et sa mise à jour selon les mouvements du personnel. Les données sur le personnel sont présentement hébergées dans le système SAGIP, dont la nouvelle conception en cours tiendra compte du nouvel environnement informationnel gouvernemental caractérisé notamment par le Répertoire. La responsabilité des unités administratives chargées de la gestion des ressources humaines quant à l'alimentation et la mise à jour du Répertoire devrait notamment porter sur les renseignements associant les personnes à des rôles dans l'organisation et aux autorisations rattachées à ces rôles. La responsabilité critique de gestion des ressources humaines est de certifier qu'une personne travaille présentement à tel endroit d'une

structure organisationnelle et qu'elle peut être contactée pour lui remettre un token d'identification de la main à la main.

4.2.2 Administration financière

Les unités administratives actuellement chargées de gestion financière disposent de l'expertise sur les procédures de délégation de signature ainsi que des règles et procédures relatives aux autorisations rattachées à des rôles dans l'organisation. Les règles d'administration relatives à la délégation d'autorité requises dans le schéma du Répertoire ainsi que les règles de validation des transactions devraient être produites avec une contribution importante de cette source. Leur responsabilité couvre également la gestion documentaire essentielle à la conservation des documents électroniques signés numériquement et qui ont une valeur probante.

4.2.3 Gestion des ressources informationnelles

Les unités administratives actuellement chargées de la gestion des ressources informationnelles sont responsables :

- du support aux outils de création, d'exploitation et d'utilisation du Répertoire ;
- du recours à des formats et processus prédéfinis ;
- du déploiement d'un objet logique (biclé) en liaison avec les services communs de répertoire et de cryptographie de l'infrastructure gouvernementale. La responsabilité de gestion des ressources informationnelles est de certifier que tel utilisateur qui détient un token physique contenant un objet logique (la biclé) utilise telle valeur de clé publique (garantie dans un certification de clé publique).

4.2.4 Infrastructure juridique de la signature numérique

Les travaux du ministère de la Justice sont très avancés pour ce qui est d'offrir une infrastructure juridique à la signature numérique, notamment quant aux conditions requises pour qu'un document électronique ait une valeur probante, aux exigences générales relatives à la certification des personnes au sein d'une organisation pour l'authentification d'identité et la signature numérique, aux exigences pour une infrastructure à clé publique, aux exigences relatives à la conservation, etc. Ces considérations particulières sont abordées dans les chantiers de sécurité et d'ingénierie documentaire, qui profitent de l'expertise en ces matières du ministère de la Justice. Le dossier juridique de réglementation doit progresser pour habiliter prestement l'administration publique à mener des activités sûres basées sur l'électronique là où le support papier est encore aujourd'hui essentiel.

4.3 Arrangements techniques du Répertoire pour assurer la sécurité des utilisations

Les arrangements techniques doivent couvrir trois volets : le contrôle d'accès, l'authentification et certification, la sécurité de transmission.

4.3.1 Contrôle d'accès

Les informations de contrôle d'accès sont utilisées de concert avec les informations d'authentification afin d'accéder à l'information emmagasinée dans la base des entrées. Il existe deux niveaux d'information de contrôle d'accès décrits dans la série de recommandations du répertoire X.500 (1993) :

1. Le contrôle d'accès simplifié
2. Le contrôle d'accès de base

Le contrôle d'accès *simplifié* se résume à interdire ou autoriser l'accès à l'ensemble d'une sous-arborescence, sans permettre d'y singulariser des éléments ou des entrées que l'on aurait voulu protéger. Il ne permet qu'une partie de la fonctionnalité souhaitable : si l'effet est positif en réduisant considérablement la charge de traitement que l'on associe à l'évaluation des droits d'accès d'un utilisateur, c'est une limitation trop inhibante pour la richesse de contenu voulue dans les entrées du Répertoire gouvernemental.

Le contrôle d'accès *de base* est un axe très fort des mesures de sécurité. Le plan du contrôle d'accès de base permet aux administrateurs du répertoire de définir les politiques de contrôle d'accès sous la forme de listes de contrôle d'accès. Ces listes précisent les informations sous protection (que l'on appelle les éléments protégés) et les catégories d'utilisateurs contre lesquelles on les protège. De plus, une liste indique les actions permises à l'endroit des éléments protégés sous la forme de permissions explicites. À titre d'exemple, un utilisateur du répertoire pourrait être identifié comme membre d'une catégorie particulière d'utilisateurs n'ayant qu'une autorisation d'accès *Lecture seulement* pour une entrée ou un attribut qualifié d'élément protégé. Dans la norme X.500 (1993), on trouve un algorithme appelé la « Access Control Decision Function » (ACDF) qui sert à déterminer, à partir du niveau d'authentification reçu, quelle fonction gérant les listes de contrôle d'accès s'applique à une requête combinée utilisateur/opération en particulier. En l'occurrence, le cadre ACDF pourrait déterminer qu'un utilisateur qui ouvre une session dans le répertoire en utilisant un simple mot de passe ne bénéficierait que d'un accès en Lecture seulement pour un attribut donné, alors qu'un accès en Modification nécessiterait que l'utilisateur ait ouvert la session en utilisant une authentification serrée. C'est ainsi que l'interface client est en mesure de supporter un contrôle sélectif au répertoire d'abord par l'authentification de l'utilisateur et, ensuite, en permettant un découpage raffiné du contenu pour prescrire les droits d'entrée selon le niveau d'authentification produit.

Le contrôle d'accès de base suppose que l'identité du demandeur soit bien établie à partir d'une authentification simple ou serrée (définie en 4.3.2). Le modèle ACDF intègre plusieurs paramètres possibles à partir desquels on peut définir et contrôler l'accès au Répertoire. Ces paramètres sont :

- les éléments de données qui peuvent devenir accessibles ;
- la portée de l'accès à un élément de données ;
- les autorisations d'opérations sur des entrées ;
- les autorisations d'opérations sur les attributs et leur(s) valeur(s) ;
- l'appartenance des utilisateurs à des catégories.

<u>Les éléments de données qui peuvent devenir accessibles</u>

Le modèle de contrôle d'accès de base définit les types de données auxquelles il sera possible ou non d'avoir accès, sous réserve de conditions à déterminer. Il admet pour les autorisations d'utilisateur une définition unique, reliée à la *catégorie d'utilisateur* chez le demandeur, pour chacun des éléments qui suivent :

- entrée,
- tous les types d'attribut d'utilisateur,
- type d'attribut,
- toutes les valeurs d'attribut,
- tous les types et toutes les valeurs d'attribut d'utilisateur,
- valeur d'attribut,
- *valeur-sur-soi* : quand un utilisateur accède à l'entrée le concernant lui-même, il a certains droits personnels, ou concernant son propre rôle, ou encore son statut de membre d'un groupe de noms.

La portée de l'accès à un élément de données

De par sa nature, un élément de données peut-être d'emblée accessible à tous ou restreint à l'accès de certains. Le contrôle d'accès de base définit les catégories d'utilisateurs auxquelles s'appliquent les autorisations de traiter des informations, y compris :

- *tous-les-utilisateurs* : tous les utilisateurs du répertoire (accompagnés de coordonnées facultatives pour le niveau d'authentification requis).
- *entrée-sur-soi* : l'utilisateur qui a le même nom-distinctif que cette entrée.
- *nom* : l'utilisateur qui a le nom-distinctif précisé dans la requête (avec un identificateur-unique facultatif).
- *groupe-d'utilisateurs* : l'ensemble des utilisateurs qui sont membres d'une entrée groupe-de-noms-uniques identifié par un nom-distinctif. Les membres d'un groupe-de-noms-uniques doivent prendre des noms d'objet individuel et ne peuvent demeurer des noms d'autres groupes-de-noms-uniques.
- *sous-arborescence* : l'ensemble des utilisateurs dont le nom-distinctif entre dans la définition de cette sous-arborescence.

Les autorisations d'opérations sur des entrées

Les catégories d'autorisation pour des opérations sur les entrées de répertoire que l'on peut accorder aux utilisateurs sur la base du résultat de leur authentification auprès du serveur sont :

- *Lire* : afficher l'information pour l'entrée nommée dans la requête.
- *Consulter* : afficher les entrées en réponse à des requêtes dont la forme n'oblige pas à expliciter les noms, par exemple une liste.
- *Ajouter* : permet la création d'une entrée dans l'arborescence ; la nouvelle entrée créée est assujettie aux contrôles de tous les attributs et toutes les valeurs d'attribut qu'elle contient.
- *Supprimer* : permet la suppression d'une entrée de l'arborescence sans tenir compte des contrôles des attributs ou des valeurs d'attributs qu'elle contient.
- *Modifier* : permet la modification de l'information contenue dans une entrée.
- *Renommer* : opération essentielle pour doter une entrée d'un nouveau nom-distinctif-relatif et qui répercute les changements dans les noms-distinctifs des entrées subordonnées.
- *Révéler en cas d'erreur :* permet la divulgation d'un nom d'entrée lors d'un résultat erroné (ou vide).
- *Exporter* : permet l'exportation d'une entrée et des subordonnées, c'est-à-dire leur retrait du site actuel et leur enregistrement dans un autre site, le tout sous réserve de l'octroi des autorisations d'usage au point d'arrivée. Il se peut que le nom-distinctif-relatif ait à être *renommé*.
- *Importer :* permet l'importation d'une entrée et de ses subordonnées, c'est-à-dire leur retrait d'un autre site pour les enregistrer dans un site permissible, sous réserve de l'octroi des autorisations au site de départ.
- *Révéler le nom distinctif :* la valeur du nom-distinctif de l'entrée peut être divulguée dans le résultat d'une opération.

Les autorisations d'opérations sur les attributs et leur(s) valeur(s)

Les catégories d'autorisation pour les attributs et les valeurs d'attribut de répertoire, sur la base du résultat de l'authentification auprès du serveur, sont :

- *Comparer* : permet l'utilisation des attributs et des valeurs dans une opération de comparaison.

- *Lire* : permet d'afficher les attributs et les valeurs contenus dans les entrées en réponse aux opérations Lire et Consulter.
- *Filtre de repérage* : permet l'évaluation d'un filtre à l'intérieur d'une opération de repérage (Consulter).
- *Ajouter* : s'il est octroyé pour un attribut, il permet l'addition d'un attribut en autant que toutes les valeurs d'attribut puissent aussi l'être. S'il est octroyé pour une valeur d'attribut, il permet l'addition d'une valeur à un attribut existant.
- *Supprimer* : s'il est octroyé pour un attribut, il permet la suppression complète d'un attribut et de toutes ses valeurs. S'il est octroyé pour une valeur d'attribut, il permet la suppression de cette valeur d'un attribut existant.
- *Révéler en cas d'erreur* : s'il est octroyé pour un attribut, il autorise la divulgation de cet attribut s'il subit une erreur d'attribut ou une erreur de sécurité. S'il est octroyé pour une valeur d'attribut, il autorise la divulgation de cette valeur d'attribut affectée par une erreur d'attribut ou une erreur de sécurité.

L'appartenance des utilisateurs à des catégories

L'établissement du contrôle d'accès au Répertoire est une condition de départ. Ce contrôle d'accès doit être fondé sur une authentification de l'identité de chaque utilisateur qui sollicite un accès. Cette identité du demandeur devrait être associée à une catégorie particulière d'utilisateurs afin de faciliter la création et la mise à jour des autorisations de tous les utilisateurs. Un certain nombre de catégories générales ont été définies dont les trois premières ont un caractère spécial :

- *Anonyme* : cette première catégorie vise à permettre un accès à la portion publique du Répertoire à tout demandeur sans qu'il ait à s'identifier.
- *Anonyme-authentifié* : on se servira de cette catégorie pour des attributions temporaires de droits d'accès pour accommoder des utilisateurs devant mener des opérations spéciales (sur les données d'acquisition par exemple) et qui ont été dûment identifiés et autorisés au préalable.
- *Soi* : certaines permissions sont accordées en recourant à cette catégorie pour établir dynamiquement, via les noms-distinctifs, qu'un utilisateur peut effectuer des opérations sur les données qui portent sur lui-même.
- *Utilisateur-du-gouvernement* : personnes dont l'identité est établie par le gouvernement en leur qualité d'employés ou l'équivalent. Un minimum de permissions générales existent à l'échelle gouvernementale.
- *Membre-d'unité-organisationnelle :* tout membre-d'unité-organisationnelle est aussi utilisateur-du-gouvernement, mais il jouit en plus de permissions venant par le fait de travailler dans tel ministère, telle direction particulière ou tout autre niveau d'unité-organisationnelle dans l'arborescence. C'est selon ce que chaque unité organisationnelle décide pour sa gestion d'ensemble de données et documents et des opérations s'y appliquant.
- *Gestionnaire-de-serveur-de-répertoire :* ce poste de contrôle requiert un accès généralement poussé en termes d'entrées, d'attributs et de valeurs d'attribut, ainsi que dans les opérations. Il peut y avoir autant de gestionnaires de ce type que voulu aussi longtemps que les sous-arbres et les classes d'objet du répertoire sont l'objet de responsabilités uniques claires.
- *Gestionnaire-de-certification* : ce poste de contrôle requiert un accès spécialisé aux attributs de certification pour les entrées utilisateur-du-gouvernement aux fins de l'authentification serrée et de l'authentification simple, ainsi que l'accès aux algorithmes de cryptographie associés.
- *Gestionnaire-de-contenu* : l'importance de l'actif informationnel qui en viendra à tirer

profit des services de répertoire dans les communications par réseau fera augmenter corrélativement le nombre de personnes qui ont des responsabilité de création et révision du contenu au niveau d'entrées, d'attributs et de valeurs d'attributs dans le Répertoire. Ils auront des autorisations taillées sur mesure dans leurs accès et leurs opérations associées pour assumer leurs responsabilités.

Ces trois dernières catégories peuvent sans doute donner lieu à diverses formes d'hybridation des responsabilités, et conséquemment des autorisations.

La norme X.500 fournit également un modèle administratif pour la mise en oeuvre des contrôles d'accès. En effet les sous-arborescences cloisonnent en domaines disjoints le contrôle d'accès à des zones administratives spécifiquement protégées. Des ajustements sont possibles dans la répartition de l'administration de la sécurité entre les services communs du gouvernement et ceux qui sont offerts à des niveaux hiérarchiques inférieurs des unités-organisationnelles. Chaque sous-domaine de contrôle d'accès constitue une « aire administrative close »; les emboîtements de ces aires closes peuvent faire en sorte qu'à tout niveau de la hiérarchie il reste possible d'assumer la responsabilité de sa propre politique de sécurité.

4.3.2 Authentification et certification

L'authentification de l'identité des utilisateurs est soit :

- simple : basée sur un mot de passe ajouté à un nom distinctif.
- serrée : basée sur la détention par l'utilisateur d'une clé privée liée à un certificat de clé publique, de façon à rendre vérifiable l'identité réclamée.

En fait il y a une troisième catégorie qui est l'absence d'authentification afin de pouvoir rendre accessible la partie publique du Répertoire à des utilisateurs anonymes

4.3.2.1 Authentification simple

L'authentification simple fonctionne sur la base d'une combinaison de nom-distinctif et de mot-de-passe fournis par une entité (soit une application ou un utilisateur) pour établir son identité auprès d'un serveur du répertoire. Ensemble, le nom-distinctif et le mot-de-passe constituent une identité ; sauf peut-être sur un réseau protégé, la transmission du mot de passe devrait être chiffrée lors de sa transition du client au serveur, ce qu'on appelle une authentification simple protégée. Le serveur vérifie la correspondance avec le mot-de-passe inscrit dans l'entrée du répertoire correspondant au nom-distinctif.

4.3.2.2 Authentification serrée

L'authentification serrée est fondée sur des techniques de chiffrement par des clés asymétriques, ou biclés. Les échanges entre composantes recourent à la signature numérique, ce qui suppose l'emploi des clés privées : la détention de ce secret (la clé privée) est considérée comme preuve d'identité fiable dans le cyberespace grâce à son inclusion dans des schèmes mathématiques sophistiqués. L'utilisateur détient son secret (clé privée) sur le disque rigide d'un poste de travail qu'il contrôle, ou sur une disquette, ou sur une carte à microprocesseur. C'est dans le Répertoire qu'est enregistré un certificat de clé publique dans l'entrée de cet utilisateur. Il est rendu disponible aux utilisateurs, pour vérifier les identités, de la même manière que d'autres informations dans le Répertoire sont retournées suite à une requête. L'authentification serrée est nécessaire pour la sécurité de l'application qu'est le Répertoire ; en retour le Répertoire véhicule un élément clé de la sécurisation de toutes les autres applications.

Les certificats de clé publique enregistrés dans le Répertoire doivent avoir le format défini par la norme X.509. Le certificat d'une entité représente son moyen d'identification numérique, une sorte de permis de conduire pour l'inforoute. C'est ainsi qu'un utilisateur se trouve capable de s'identifier en interaction avec les protocoles utilisés dans l'Internet ou ailleurs. Le certificat contient le nom du détenteur, sa clé publique, une date d'expiration, le nom de l'autorité de certification émettrice du certificat, un numéro de série, et la signature numérique de ce certificat par son émetteur.

Une autorité de certification, en émettant un certificat, garantit qu'une clé publique est associée à une identité. Une fonction de validation de signature doit faire appel à ces certificats qui doivent être publiquement accessibles sur l'inforoute ou un intranet local selon les cas. Un certificat perdu, volé, annulé doit être rendu public par l'autorité de certification au moyen d'une liste de révocation. Pour les communications internes au domaine gouvernemental, l'autorité de certification des utilisateurs est unique et la vérification est faite en un seul point logique.

La gestion des certificats comporte plusieurs volets pouvant être assumés par un seul ou quelques acteurs :

- l'authentification d'une personne
- la distribution de tokens comme une carte à puce
- l'annonce de révocation
- la génération des clés
- l'archivage des biclés.

Divers arrangements institutionnels et opérationnels sont envisageables. Une forme d'arrangement recommandée serait que chaque utilisateur authentifié dispose de deux clés privés : l'une pour générer sa signature qui resterait strictement privée, l'autre pour le chiffrement (avec son mot de passe associé) et dont une copie serait enregistrée par un service central pour protéger l'organisation contre la perte d'information en cas de décès par exemple d'une personne.

Pour les communications avec des entités externes, d'autres autorités de certification sont impliquées. Des ententes de reconnaissance réciproque entre autorités de certification sont nécessaires. Une entente amène deux autorités à émettre chacune pour l'autre un certificat de clé publique qu'elles enregistrent dans un attribut spécial de l'entrée de cette autorité dans leur répertoire, la paire de certification réciproque. Mises bout à bout, ces paires de certification permettent de tracer des chemins de certification, permettant par exemple au ministère de l'Environnement de communiquer en sécurité avec une entreprise de l'Ontario ou du Maine. Les services et institutions concernant les autorités de certification et des services spéciaux de notarisation, sauvegarde de secrets, archivage sécurisé sont en émergence de sources multiples. La Chambre des Notaires du Québec est à l'avant-garde dans ces essais de définition et de services inforoutiers. Il est dans l'intérêt du gouvernement de pouvoir faire appel à un tiers, fiable, sérieux, bien organisé, et ayant une bonne compréhension des volets juridiques et technologiques des communications et transactions d'affaire sur l'inforoute.

Bien que le répertoire permet également de desservir en sécurité des utilisateurs ne s'authentifiant que par la connaissance d'un mot de passe et que l'authentification simple peut être efficace dans de nombreux contextes, l'évolution autour de l'Internet a vite facilité l'accès généralisé et convivial à des technologies d'authentification serrée de l'identité des utilisateurs. Sans nul doute, l'identité numérique est devenue nécessaire et se généralisera en 1998 et 1999. La signature numérique devenant rapidement monnaie courante, l'identité numérique qui sous-tend cette signature sera bientôt appelée à devenir la base de l'identification des utilisateurs gouvernementaux.

4.3.3 Sécurité de transmission

Le Répertoire joue un rôle important dans la sécurité de transmission. En effet, parce qu'il emmagasine les certificats de clé publique dans les entrées des personnes, il est sollicité à chaque envoi d'un document signé afin de constituer l'enveloppe numérique qui protégera la transmission de la clé symétrique, elle-même nécessaire au déchiffrement du document par le destinataire. C'est la plus belle astuce de cette approche, telle qu'illustrée à la figure 4A, qui chiffre la clé symétrique avec la clé publique du destinataire et que lui seul peut ouvrir grâce à sa clé privée. C'était en quelque sorte le chaînon manquant des solutions antérieures qui devaient prendre des chemins plus tortueux pour partager le secret de la clé symétrique servant à la fois à chiffrer et à déchiffrer. Maintenant, grâce à ce moyen, des clés ne durant qu'une session plutôt qu'un mois ou un jour sont devenues la pratique la plus courante des échanges encryptés dans l'inforoute.

Les protocoles et mécanismes disponibles pour la sécurité des transmissions sur un réseau non protégé sont déjà abondants et couvrent des contextes variés (du général au spécifique) :

- Secure MIME, pour la télémessagerie,
- SSL 3.0, qui permet d'établir des « tunnels » pour la transmission,
- SASL (Simple Authentification and Security Layer), qui fournit une couche de chiffrement pour les protocoles avec connexion,
- les extensions LDAP pour un Transport Security Layer (TLS), quand les utilisateurs et applications n'ont pas une identité authentifiée, ainsi que les extensions LDAP à SASL, quand les mécanismes d'authentification sont présents.

4.4 Une politique de sécurité

Le Répertoire sera couvert par la politique de sécurité en vue de garantir la plus grande intégrité des informations. Cette politique reposera sur les trois éléments suivants :

1. l'administration de la sécurité
2. une vérification de la sécurité
3. la sécurité physique

4.4.1 Les éléments d'administration de la sécurité

L'administration de la sécurité dans le répertoire comprend les éléments suivants :

- Les administrateurs des systèmes du Répertoire utiliseront des procédures d'authentification simple ou serrée afin d'assurer le contrôle d'accès au répertoire. Le recours à l'authentification simple ou élaborée sera déterminé par chaque organisme. On recommande, cependant, l'authentification serrée pour les administrateurs des systèmes qui devront modifier les entrées du répertoire.

- Chaque interface client devra restreindre l'accès à ses données de configuration.
- On exigera une documentation de la sécurité requise et en vigueur pour la révision et l'approbation de chaque serveur du Répertoire.
- La mémoire du serveur et de la base des entrées sera protégée afin de la doter de la plus haute confidentialité.
- Le serveur fournira des moyens pour prévenir les actes accidentels, non autorisés ou malicieux qui pourraient entraîner une altération des mécanismes de sécurité ou des niveaux d'accès.
- Le serveur fournira des services d'intégrité des données et des moyens pour prévenir les actes accidentels, non autorisés ou malicieux qui pourraient entraîner une altération des informations du Répertoire.
- Aucun mauvais fonctionnement ne provenant que d'une seule erreur du matériel, du logiciel ou d'un individu ne devrait suffire à contourner les contrôles de sécurité obligatoires. Il faudrait ainsi à tout le moins deux erreurs simultanées d'origine indépendante pour que la défense de la sécurité puise être affectée.

4.4.2 Les éléments de vérification de la sécurité

Le Répertoire sera doté de mécanismes de vérification afin de journaliser et faire l'historique de l'utilisation du Répertoire. Afin d'assurer le plus haut niveau de sécurité nécessaire dans chaque organisme, le Répertoire comprendra les éléments de vérification suivants :

- Le Répertoire sera en mesure de pourvoir à l'imputabilité par la journalisation de toutes les requêtes et aussi de supporter une analyse à la fois de la surveillance de sécurité et des actes ayant un impact sur celle-ci (c.-à-d. des tentatives réussies ou non de pénétrer le système, des atteintes aux procédures ou aux politiques de sécurité).
- Une journalisation des informations pour supporter la surveillance de la performance sera fournie par le Répertoire.
- Une journalisation des informations pour supporter la détection et l'identification des erreurs sera fournie par le Répertoire.
- Le Répertoire produira et gardera une journalisation de toutes les atteintes à la sécurité pendant 30 jours.
- L'interface client aura la capacité de produire une journalisation des activités de l'interface.
- L'interface client sera dotée de moyens pour empêcher des tentatives de fermer ou de contourner les capacités de journalisation du logiciel.

4.4.3 Les éléments de sécurité physique

Le Répertoire recourra à des moyens appropriés pour assurer l'intégrité physique des composantes qui entrent dans sa composition (par exemple, les interfaces et les serveurs). Pour fournir ce niveau d'intégrité physique, le Répertoire sera protégé contre des menaces physiques telles les intrus, le feu et l'inondation, ainsi que contre des défaillances électroniques et techniques.

4.4.4 Les serveurs pare-feu ou garde-barrière

Certains M/O pourront mettre en place des serveurs pare-feu pour s'assurer que seuls les utilisateurs autorisés pourront accéder à des endroits spécifiques ou choisis de la base des entrées. On anticipe que ces serveurs seront implantés pour l'accès du grand public et pour les organismes ayant besoin de communiquer des informations avec des entités à l'extérieur du domaine du répertoire gouvernemental et de celui de leur propre organisme.

L'importance des serveurs pare-feu doit cependant être limitée en raison de ses processus d'identification basés sur les adresses IP, les noms de domaine et les combinaisons de nom d'utilisateur et mot de passe, qui sont tous des moyens vulnérables. La généralisation du recours aux signatures numériques accroîtra l'importance du rôle joué par le Répertoire dans le contrôle d'accès. Cette tendance est soutenue par le risque d'étranglement de la transmission qu'occasionne un pare-feu par opposition à un monde où tous les serveurs et tous les clients génèrent et vérifient à tout bout de champ des signatures numériques.

CHAPITRE 5

5.0 Le Schéma du Répertoire gouvernemental

Toute entrée du Répertoire doit être conforme à une classe d'objet particulière. La classe d'objet à laquelle une entrée appartient est forcément identifiée dans un attribut de chaque entrée. Chaque classe d'objet porte un nom et comporte un modèle de contenu sous forme d'attributs obligatoires et d'attributs facultatifs servant à décrire les entrées de cette classe. Une classe d'objet offre donc un cadre générique pour la description des entrées appartenant à cette classe. Une classe peut être divisée en sous-classes qui héritent de ses attributs et qui se distinguent entre elles par l'ajout d'attributs propres à chaque sous-classe.

Le Schéma du Répertoire comprend une certaine variété de classes prédéfinies pour satisfaire aux besoins les plus courants et typiques des usages prévus dans l'organisation gouvernementale. Ce chapitre présente d'abord la définition de ces classes d'objet, de leurs attributs, des règles sur la façon de nommer les entrées, et des règles sur la structuration de l'ensemble des classes d'objet. Une deuxième section du chapitre définit les attributs servant à la description des entrées. Dans une troisième section, les trois services de consultation décrits au premier chapitre (Pages blanches, bleues, vertes) sont repris en leur associant des classes d'objet et en expliquant certains aspects particuliers.

5.1 Les classes d'objet

Dans la présente section, une liste des classes d'objet est présentée. Ensemble, ces classes se veulent le plus inclusives possibles par rapport aux besoins du partage de l'information gouvernementale. Diverses contraintes s'appliquant à ces classes d'objet seront présentées :

- les attributs obligatoires et facultatifs s'appliquant à la description des objets,
- les règles d'appellation, ou quel est l'attribut qui sert à former le nom donné à l'objet dans l'entrée du répertoire,
- les règles de structure qui définissent les relations hiérarchiques permises entre une classe d'objet et les autres classes.

Il existe aussi des règles de contenu qui permettent de spécifier la définition d'une classe pour, par exemple, l'adapter aux besoins du gouvernement.

5.1.1 Classes d'objet structurelles

Un ensemble de classes d'objet génériques est présenté ci-après. Pour chaque classe d'objet, un texte descriptif est fourni avec quelques indications sur son utilisation possible. En annexe 3, ces classes sont reprises avec en plus les règles de structure et d'appellation de même que les attributs obligatoires et facultatifs qui s'appliquent.

Les classes d'objet incluses ci-après remontent pour la plupart à la recommandation X.521 (1993) de l'UIT ; les choix effectués par le gouvernement américain ont été pris en compte ; enfin quelques nouveautés ont été ajoutées à partir de la version 3 de LDAP (1997) et de RFC antérieurs de l'Internet (en particulier 1274). Ces classes sont améliorables, mais elles devraient constituer une première base suffisante pour une utilisation généralisée dans la description des objets. La création des entrées selon les formats prescrits permettra l'obtention des bénéfices attendus d'un service de répertoire.

Les classes d'objet sont présentées dans un ordre destiné à en faciliter la compréhension. Nous présentons vingt-six classes qui illustrent bien la diversité d'objets les plus fréquemment utilisés dans la création des entrées. Les noms des classes s'écrivent avec

une majuscule initiale et avec trait d'union s'ils sont formés de plus d'un mot. Le lecteur est prié de référer à l'annexe 4 pour obtenir l'appellation correspondante en anglais. Voici la liste des classes définies :

Organisation Unité-organisationnelle Rôle-dans-l'organisation Personne-de-l'organisation Groupe-de-noms Processus-d'application Entité d'application Serveur-de-répertoire Collection Document Équipment Localité Alias	Pays Personne Personne-à-domicile Groupe-de-noms-uniques Source-de-contrôle-des-certificats-révoqués Sous-entrée Domaine Personne-branchée Local Compte Objet-rattaché-à-un-domaine Objet-simple-de-sécurité Référer

N.B. : Dans le cas des cinq classes d'objet spécifiées dans la troisième section du chapitre, leur définition générale, suggérée soit dans les normes ISO, les RFC de l'Internet ou le répertoire du gouvernement américain, est quant même fournie ici parmi les autres à titre indicatif.

ORGANISATION

Il n'y a qu'une entrée pour cette classe : le gouvernement du Québec dans son ensemble.

UNITÉ-ORGANISATIONNELLE

Les entrées *Unité-organisationnelle* représentent des subdivisions d'une entrée Organisation. Dans le Répertoire, les ministères et organismes gouvernementaux sont de la classe *Unité-organisationnelle*, de même que les directions et services qui les constituent. Pour des fins administratives, nous distinguerons des unités organisationnelles de niveaux différents.

Exemples : - Ministère de l'Éducation
- Régie d'assurance-maladie du Québec

RÔLE-DANS-L'ORGANISATION

Les entrées Rôle-dans-l'organisation représentent les postes ou les rôles au sein d'une *Organisation* et contiennent généralement le nom-distinctif complet de la personne qui occupe ce poste ou exerce ce rôle. Cette valeur peut être mise à jour régulièrement, afin de refléter les changements qui surviennent dans le personnel. Ces entrées peuvent servir, par exemple, dans la description d'un plan d'organisation administrative.

PERSONNE-DE-L'ORGANISATION

Les entrées *Personne-de-l'organisation* représentent les individus qui sont à l'emploi d'une Organisation ou associés à celle-ci. Au gouvernement du Québec, outre les employés de tous niveaux et les contractuels, il y a aussi les personnes élues députés, les personnes désignées ou nommées (par exemple sur des Commissions). La classe d'objet *Personne-de-l'organisation* est une sous-classe de *Personne*.

GROUPE-DE-NOMS
La classe d'objet *Groupe-de-noms* fournit un mécanisme pour l'emmagasinage d'un ensemble non ordonné de noms-distinctifs complets d'entrées au répertoire. Ces noms distinctifs peuvent désigner des personnes-de-l'organisation ou d'autres groupes-de-noms. Cette classe sert à supporter des groupes d'intérêt, des regroupements d'individus provenant d'une ou de plusieurs branches de l'arborescence, qui ont à communiquer entre eux : groupes de direction, groupes de travail, comités, listes de distribution. Le recours à cette classe permet de faire prendre en charge par le Répertoire les tâches de contrôle d'accès et de distribution d'information inhérentes à de multiples situations courantes de communications administratives et d'affaires (ex. : envois à toutes les directions des ressources humaines).

PROCESSUS-D'APPLICATION
La classe d'objet *Processus-d'application* fournit un mécanisme pour documenter une composante fonctionnelle utilisable dans diverses applications ; par exemple, la production de documents, leur gestion, leur distribution pourraient constituer un processus d'application.

ENTITÉ-D'APPLICATION
La classe d'objet *Entité-d'application* est une sous-composante fonctionnelle d'un *Processus-d'application* ; par exemple le routage des messages est une partie récurrente des tâches dans beaucoup de situations.

COLLECTION
La classe d'objet *Collection* fournit un mécanisme qui permet de désigner des rassemblements d'entrées de la classe *Document*. Il s'agit donc d'un regroupement de métadonnées sur, par exemple, les Lois refondues du Québec, des manuels de gestion, le contenu d'un site Web.

DOCUMENT
La classe d'objet *Document* fournit un mécanisme qui permet de décrire et repérer de l'information grâce aux renseignements bibliographiques ou références de documents (métadonnées).

SERVEUR-DE-RÉPERTOIRE
Cette classe d'objet, *Serveur-de-répertoire*, permet de désigner les entrées qui représentent les serveurs dans l'arborescence du Répertoire. Il s'agit d'une sous-classe de *Entité-d'application* ainsi que du serveur racine.

ÉQUIPEMENT
La classe d'objet *Équipement* sert à documenter le matériel tel les imprimantes, les ordinateurs ainsi que d'autres périphériques ou matériel de réseau, à des fins d'inventaire, d'adressage ou autres.

LOCALITÉ
Les entrées *Localité* peuvent représenter des entités géographiques comme une province ou un État, une ville, un édifice, etc. Elles peuvent par exemple servir à représenter les bureaux locaux ou régionaux d'un ministère ou d'un organisme.

ALIAS
L'*Alias* sert de base à la constitution des classes d'objet spéciales qui ne comportent qu'un pseudonyme et effectuent le renvoi à un nom-courant d'une entrée de la classe d'objet identifiée, par exemple : *Localité, Personne-de-l'organisation*, ou *Unité-organisationnelle*. *Alias* ne s'emploie pas seul mais en association avec une classe d'objet existante. Le recours à l'*Alias*

pour attribuer une autre forme repérable à un objet permet d'obtenir un deuxième nom-distinctif pour un objet, tandis que plusieurs formes de nom-courant n'ont pas cet effet. Les *Alias* servent à des fins de gestion, par exemple le réacheminement de courrier après un déplacement de personnel, ou pour camoufler l'identité d'entrées spécialement sensibles (par ex. : services d'enquête).

PAYS
Une entrée de *Pays* n'est créée qu'une fois pour un pays par l'autorité administrative concernée.

PERSONNE
La classe générique de *Personne* sert à la description des individus humains.

PERSONNE-À-DOMICILE
Les entrées de la classe *Personne-à-domicile* servent à décrire des personnes dans le contexte de leur résidence personnelle ou de leur domicile. Cette classe pourrait éventuellement accueillir la clientèle gouvernementale des personnes vivant au Québec.

GROUPE-DE-NOMS-UNIQUES
La classe *Groupe-de-noms-uniques* sert à définir des entrées qui contiennent une liste non ordonnée de noms d'objets ou d'autres groupes de noms dont l'intégrité est garantie. Cette liste est stable et n'est modifiée que par une action administrative intentionnelle. Le fait d'être membre d'un groupe constitue un laissez-passer dans un contrôle d'accès (ex. : groupe des sous-ministres).

SOURCE-DE-CONTRÔLE-DES-CERTIFICATS-RÉVOQUÉS
Cette classe sert à identifier le serveur devant être interrogé pour vérifier la liste de révocation des certificats d'utilisateurs afin de pouvoir valider une transaction.

SOUS-ENTRÉE
La classe *Sous-entrée* sert à décrire les sous-arbres pour l'administration des services x.500.

DOMAINE
Un *Domaine* consiste en une branche d'un répertoire, spécifiée par une *Sous-entrée* et son *Sous-schéma*, sous le contrôle d'une autorité administrative.

PERSONNE-BRANCHÉE
Sous-classe de *Personne-de-l'organisation* pour les exigences courantes dans le déploiement de répertoires Internet et intranet (en ajoutant quelques attributs couramment requis à ceux de X.521 sur *Personne-de-l'organisation*).

Note : Dans la troisième section, cette classe se trouve entièrement intégrée au modèle de *Personne-de-l'organisation*.

LOCAL
Cette classe d'objet sert à désigner un local par son nom ou son numéro et à en permettre une description.

COMPTE
Cette classe d'objet sert à représenter une *Personne* ou une *Unité-organisationnelle*. en tant que sujet de dettes, débits ou crédits.

OBJET-RATTACHÉ-À-UN-DOMAINE
Cette classe d'objet sert à représenter le rattachement d'un objet à un *Domaine* du Répertoire.

OBJET-SIMPLE-DE-SÉCURITÉ
Cette classe d'objet sert à identifier un objet lié à un contrôle d'accès du niveau d'authentification simple (ex. : mot de passe).

RÉFÉRER
Cette classe d'objet sert à décrire l'information de référence dans l'environnement des répertoires.

Cette classe d'objet, *Référer*, sert à représenter de l'information de référence générique dans les répertoires LDAP et peut, via les URI, pointer vers d'autres répertoires, qu'ils soient LDAP ou autre. L'information de référence en cause est relative à l'environnement de serveurs et de services dans l'inforoute. Cette classe d'objet est à l'usage des serveurs et n'est généralement pas visible pour les utilisateurs.

La figure 5-1 offre une représentation assez conventionnelle des relations de structure (supérieure, subordonnée) entre les principales classes d'objet qui viennent d'être listées. On peut observer divers phénomènes :

- l'*Unité-organisationnelle* est la classe d'objet à laquelle se trouve subordonnées le plus grand nombre de classes d'objet ;
- deux classes d'objet se subdivisent à volonté pour la création de nouvelles classes subordonnées : *Unité-organisationnelle* et *Localité*.

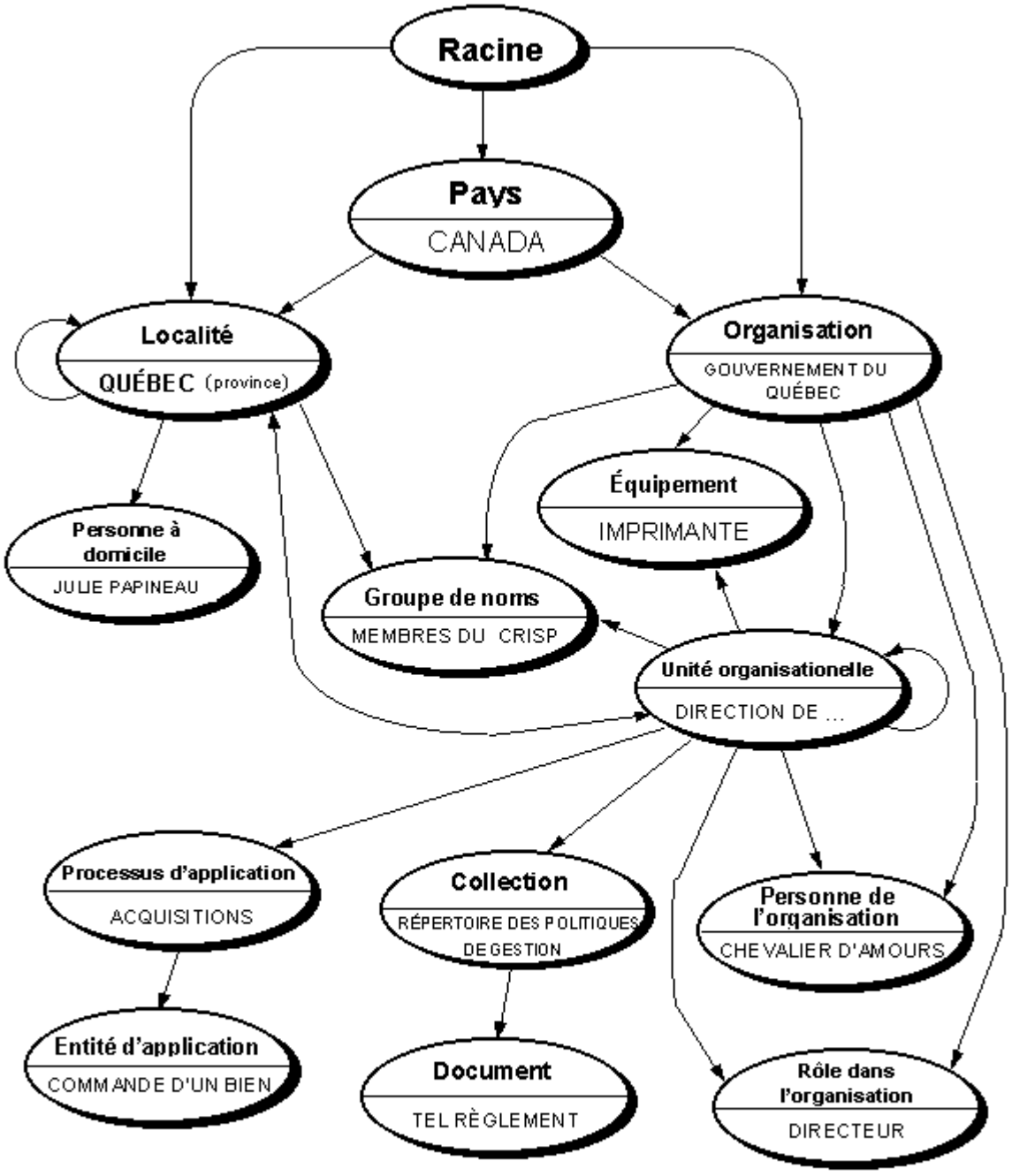


Figure 5-1
Structure suggérée pour l'arborescence d'information du Répertoire enrichie d'un exemple (X.521 1993)
(Classe d'objets supérieure → subordonnée)

5.1.2 Classes d'objet auxiliaires

Le type structurel n'est que l'un des trois types de classes qu'on trouve dans un répertoire. Un des types est dit abstrait et ne compte que deux classes dont l'une est l'*Alias* et l'autre la racine logique au sommet de l'arborescence de l'information. Ces classes ont peu de

contenu : nous avons vu au chapitre deux que la racine logique est vide et occupe une position strictement technique de sommet, tandis que l'*Alias* ne fait que référer à une autre entrée.

L'autre type de classes, dites auxiliaires, a une grande importance pratique. En effet, si un ministère par exemple veut définir des attributs correspondant à ses besoins spécifiques, les classes auxiliaires permettent de les ajouter à une ou plusieurs classes de type structurel en permettant qu'un héritage multiple de propriétés viennent supporter la définition des attributs disponibles pour la création d'entrées.

Huit classes auxiliaires doivent être disponibles dans les serveurs du Répertoire :

- Sous-entrée-d'attribut-collectif
- Sous-schéma
- Contrôle-d'accès-de-sous-entrée
- Information-de-sécurité-d'utilisateur
- Utilisateur-étroitement-identifié
- Autorité-de-certification
- Autorité-de-certification-V2
- Objet-URI-étiqueté

SOUS-ENTRÉE-D'ATTRIBUT-COLLECTIF

Cette classe d'objet est importante dans l'administration des serveurs X.500. Elle contient un ou des attributs dits collectifs, c'est-à-dire qu'ils sont reproduits dans chacune des entrées de cette branche du Répertoire qu'une sous-entrée concerne. En d'autres mots, les attributs collectifs sont partagés par un ensemble d'entrées et contribuent à un emmagasinage plus économique.

Les attributs de télécommunications, postaux, de localisation, d'organisation sont souvent l'objet d'un modèle en cascade des éléments d'information partagés grâce au mécanisme des attributs collectifs à placer à la racine d'un domaine sous une autorité administrative du répertoire.

SOUS-SCHÉMA

Cette classe d'objet est importante pour enregistrer des sous-schémas dans les serveurs X.500. Le *Sous-schéma* spécifie le modèle d'information utilisé dans un domaine du répertoire. Il contient les types-d'attributs, les classes d'objet, les règles de structure, les syntaxes et les règles-d'appariement. Le Schéma du Répertoire est constitué de Sous-schémas disjoints, sans recouvrement.

CONTRÔLE-D'ACCÈS-DE-SOUS-ENTRÉE

Cette classe d'objet est importante dans l'administration de serveurs X.500. Elle s'utilise en conjonction avec la classe *Sous-entrée*. Elle contient de l'information prescriptive du contrôle d'accès à exercer dans cette branche du répertoire que la Sous-entrée concerne. Les opérations se catégorisent en repérer, lire, modifier, tandis que l'information se catégorise en public, protégé (groupe), confidentiel.

INFORMATION-DE-SÉCURITÉ-D'UTILISATEUR

Listes de groupes dont l'utilisateur est membre, et liste des autorisations de l'utilisateur.

UTILISATEUR-ÉTROITEMENT-IDENTIFIÉ

La classe *Utilisateur-étroitement-identifié* sert à définir les entrées pour des objets qui peuvent être étroitement identifiés grâce à l'authentification d'identité permise par les certificats de clé publique.

AUTORITÉ-DE-CERTIFICATION
La classe *Autorité-de-certification* sert à définir les entrées pour les objets qui agissent comme source de distribution des certificats. Les autorités de certification sont définies dans ISO/IEC 9594-8.

AUTORITÉ-DE-CERTIFICATION-V2

OBJET-URI-ÉTIQUETÉ
L'utilité de cette classe d'objet est de pouvoir être ajoutée aisément à des objets existants du répertoire en vue de permettre l'inclusion normalisée de valeurs d'URI dans une entrée. Cela n'empêche d'ailleurs pas l'inclusion directe du type d'attribut URI-étiqueté dans d'autres classes d'objets. Défini dans RFC 2079 (janvier 1997). L'étiquette doit avoir valeur indicative pour l'utilisateur.

Afin de jeter un regard plus global sur les trente-quatre classes d'objet présentées dans cette section, la figure 5-2 liste les principales classes d'objet en fonction des trois services de consultation du répertoire. Deux classes d'objet, *Alias* et *Personne*, n'y figurent pas directement. On peut observer que ce sont les Pages bleues qui regroupent le plus grand nombre de classes d'objet, ce qui traduit en somme que les répertoires sont des créations destinées à servir principalement aux organisations. Cependant, les expériences antérieures montrent que ce sont les Pages blanches qui sont le plus sollicitées de façon directe.

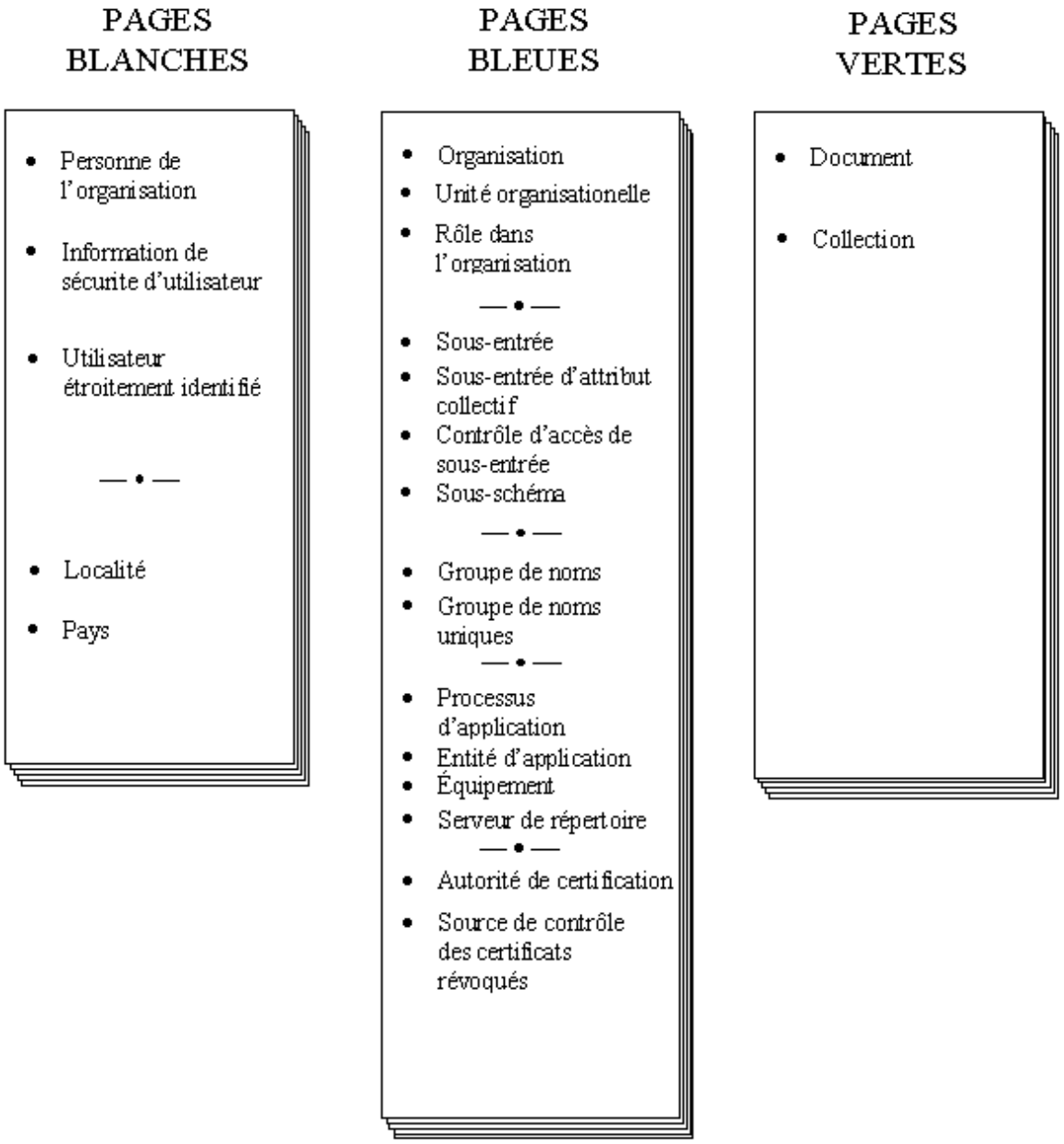


Figure 5-2
Répartition des principales classes d'objet entre les trois services de consultation du Répertoire

La liste des classes d'objet que nous avons présentée a une bonne valeur indicative, mais il n'y a pas de véritable consensus d'établi dans tous les détails. Il y a en particulier des tensions entre X.500 et LDAP que l'on ne peut pas éviter de régler en pratique grâce à une collaboration internationale déjà bien engagée. Toutes ces classes d'objet n'ont pas à être utilisées. Et, évidemment, il est possible d'en créer de nouvelles pour mieux répondre aux besoins d'une organisation.

5.2 Les attributs

On appelle attributs les éléments d'information jugés utiles pour décrire des objets. Chacun des ces éléments d'information particuliers constitue un type d'attribut et possède un nom qui lui est propre (ex. : numéro-de-télécopieur). Le type d'attribut détermine si ce dernier peut prendre une ou plusieurs valeurs, leur syntaxe, les règles d'appariement associées, etc. Par exemple, le type d'attribut nom-de-famille pourra contenir une seule valeur, être composé de caractères alphabétiques et se prêter à des recherches à l'aide de filtres déterminés. Chaque classe d'objet se trouve décrite par un sous-ensemble des attributs utilisés par le Répertoire. Certains attributs se retrouvent dans chacune des entrées, quelle qu'en soit la classe. D'autres attributs ne se retrouvent que dans une seule classe d'objet.

La présente section est constituée d'une présentation de la plupart des attributs usuels en puisant aux mêmes sources que précédemment (ISO, Internet, répertoire gouvernemental américain). D'autres attributs propres au gouvernement du Québec viendront s'ajouter dans la troisième section du chapitre. On notera que les noms d'attributs commencent par une minuscule pour aider à les distinguer des noms de classe d'objet qui commencent par une majuscule. Pour rendre plus claire cette présentation, les attributs sont regroupés en fonction de certains aspects (dont la valeur est surtout pédagogique) :

- télécommunications
- poste
- localisation géographique
- organisation
- sécurité
- noms
- noms de personnes
- autres attributs d'une personne
- subdivisions du répertoire
- attributs opérationnels X.500
- attributs opérationnels LDAP

5.2.1 Ensemble d'attributs télécommunications :

regroupe les attributs généralement utilisés pour les communications d'affaires.

- numéro-de-téléphone : la valeur est exprimée en une chaîne de caractères composé selon la forme internationale reconnue (voir X.500) par exemple : +1 418 651 8976.
- numéro-de-télécopieur :la valeur du numéro de téléphone est suivie des paramètres de télécopie comme ceux du format d'impression :
- numéro-de-télex : selon la forme internationale reconnue.
- identifiant-de-terminal-télétex : selon la forme internationale reconnue.
- adresse-X121 : selon la forme internationale reconnue.
- adresse-de-présentation : cet attribut contient une adresse de présentation OSI en accord avec le RFC 1278.
- mode-de-livraison-préféré : cet attribut indique le type de système de télémessagerie dont se sert un utilisateur dans un cadre d'opération X.400.
- information-de-protocole : cet attribut est utilisé en conjonction avec l'attribut adresse-de-présentation pour fournir des informations au service de réseau OSI.
- numéro-RNIS-international : cet attribut désigne un numéro selon la convention RNIS (Réseau numérique à intégration de services).

- adresse-de-télémessagerie : cet attribut spécifie un attribut d'adresse de télémessagerie (casier postal électronique) selon la convention Internet (RFC 822).
- ordinateur-hôte : cet attribut spécifie le nom de domaine d'un ordinateur-hôte.
- téléphone-à-domicile : cet attribut contient le numéro de téléphone associé au domicile d'une personne selon le format international.
- adresse-d'autre-télémessagerie : cet attribut contient les valeurs désignant d'autres formes d'adresse de télémessagerie que les adresses Internet (RFC 822).
- cellulaire : cet attribut contient le numéro de téléphone cellulaire associé à une personne selon le format international.
- pagette : cet attribut contient le numéro de téléphone de pagette (téléavertisseur) pour une personne selon le format international.
- option-préférée-de-messagerie : cet attribut permet à un utilisateur d'indiquer s'il préfère recevoir des documents par la poste (''physical'') ou par télémessagerie (''electronic''). L'absence de l'attribut est interprétée comme signifiant que la personne ne souhaite pas être incluse dans une liste de distribution.
- URI-étiqueté : cet attribut spécifie un URI (Uniform Resource Identifier : identifiant uniforme de ressource) et une information descriptive qui est facultative. Défini dans RFC 2079 (janvier 1997). L'URI se limite actuellement à un seul type, l'URL (Uniform Resource Locator : référence uniforme de ressource). L'utilité de cet attribut est qu'il normalise l'inclusion d'un URL dans une entrée.
- cellulaire-personnel : cet attribut spécifie le numéro de téléphone du cellulaire personnel (non pour affaires) de quelqu'un.
- télécopieur-personnel : cet attribut spécifie le numéro de téléphone du télécopieur personnel (non pour affaires) de quelqu'un.
- pagette-personnelle : cet attribut spécifie le numéro de téléphone de la pagette personnelle (non pour affaires) de quelqu'un.
- langue-préférée : cet attribut spécifie la langue à utiliser de préférence pour communiquer avec une personne ; au gouvernement du Québec, cet attribut est normalement FR pour français, qui est la langue de l'administration.

5.2.2 Ensemble d'attributs postal :

regroupe les attributs utilisés pour définir ceux qui sont directement associés à la livraison postale

- adresse-postale : format familier, spécifié dans un guide de la Société canadienne des postes.
- code-postal : selon les formats prescrits dans les pays de destination.
- casier-postal : service postal au niveau local attribuant un numéro à une boîte de dépôt du courier.
- nom-de-bureau-pour-livraison-physique : désignation d'un endroit où s'effectue la réception de biens ou de courrier livrés.
- adresse-enregistrée : cet attribut contient une adresse postale appropriée pour la réception de do-cuments afin de pouvoir enregistrer la livraison grâce à une signature autorisée.
- adresse-domiciliaire : cet attribut spécifie l'adresse du domicile d'une personne (limite de 6 lignes de 30 caractères).

5.2.3 Ensemble d'attributs localisation :

regroupe les attributs utilisés afin de situer et re-trouver la position d'un objet physique dans l'espace géographique.

- nom-de-pays : cet attribut contient un code de deux lettres servant à désigner les pays selon la norme ISO 3166
- nom-de-localité : cet attribut contient un nom de lieu géographique comme une ville, une région.
- nom-de-province-ou-État : cet attribut contient le nom complet d'une province ou d'un État d'une fédération.
- numéro-de-porte : cet attribut contient l'adresse physique de l'objet désigné dans une entrée, par exemple, une adresse de livraison.
- identifiant-d'édifice : cet attribut sert à identifier un édifice en un lieu.
- emplacement : cet attribut contient des coordonnées de lieu comme un nom ou un numéro de salle. Il se combine généralement à un nom d'édifice, ou à un numéro-de-porte, localité, etc.
- numéro-de-local : cet attribut indique la localisation d'un objet, substituable à l'attribut emplacement.
- indicateur-de-destination : cet attribut indique un lieu pour le service de livraison de télégramme.

5.2.4 Ensemble d'attributs organisation :

regroupe les attributs typiques d'une organisation ou d'une unité organisationnelle.

- nom-de-l'organisation : cet attribut contient le nom d'une organisation.
- nom-de-l'unité-organisationnelle : cet attribut contient le nom d'une unité organisationnelle.
- organigramme : présentation arborescente de la structure d'une organisation ou d'une unité organisationnelle avec indication des noms de subdivisions.
- description : cet attribut contient une description lisible (texte) de l'objet nommé dans une entrée.
- catégorie-d'affaires :cet attribut décrit la sorte d'affaires réalisées par une organisation.
- mots-clés : cet attribut contient généralement plusieurs valeurs qui représentent des catégories symboliques ou concepts servant à qualifier le contenu selon les termes convenus ou descripteurs. Ceux-ci sont préférablement arrangés dans un thésaurus ou dans un plan de classification. Il serait souhaitable d'établir le vocabulaire des programmes et services gouvernementaux.
- renvoi : cet attribut contient les noms-distinctifs d'objets pouvant être associés à une entrée.
- point-de-contact : attribut qui sert à désigner les moyens d'entrer en communication avec un service gouvernemental, que le moyen soit téléphonique, en personne ou sur le Web.
- heures-d'ouverture : attribut qui sert à désigner les heures où il est possible d'entrer en communication avec un service gouvernemental, que le moyen soit téléphonique ou en personne.
- formulaire-de-requête : attribut désignant une adresse URL pour l'obtention d'une interface Web apte à supporter la formulation d'une demande d'information.
- titre-personnel : cet attribut contient un titre particulier d'une personne dans son contexte social (ex. : M., Mme, maire, Révérend), professionnel (avocat, ingénieur, technicien), ou académique.

- tenant-de-rôle : cet attribut contient le nom d'une personne-de-l'organisation pour un rôle-dans-l'organisation.
- agenda : cet attribut contient, directement ou par référence, les données temporelles (libre-occupé) d'un objet d'information (personne-de-l'organisation, dispositif, emplacement) pour une période indéterminée à venir.
- numéro-d'unité-organisationnelle : identifiant numérique attribué à une unité administrative dans une organisation.
- numéro-d'employé : identifiant numérique attribué à un employé dans une organisation.
- type-d'employé : cet attribut indique le type d'emploi ou de poste qu'occupe une personne.
- logo : cet attribut contient une petite image du logo de l'organisation à laquelle un objet appartient ou est rattaché (en format JPEG).
- catégorie-d'utilisateur : cet attribut sert à contenir un nom descriptif de catégorie dont l'utilisateur est membre.
- gestionnaire : cet attribut spécifie le gestionnaire de l'objet réel qui est représenté dans une entrée.
- secrétaire : cet attribut spécifie le nom distinctif d'une personne dans l'entrée d'une autre personne pour qui elle agit comme secrétaire.
- nom-du-rôle : cet attribut contient le nom d'un rôle (position ou fonction comme sous-ministre, directeur, analyste) pour une personne-de-l'organisation.

5.2.5 Ensemble d'attributs sécurité :

regroupe les attributs typiques relatifs à la sécurité, au contrôle d'accès et à l'authentification de l'identité.

- identifiant-d'utilisateur : cet attribut spécifie un nom d'accès (login) à un système.
- mot-de-passe : cet attribut contient une chaîne de caractères propre à un utilisateur et qui sous-tend l'assurance de son identification. Utilisé dans le contrôle d'accès.
- membre : cet attribut contient le nom d'une personne-de-l'organisation ou d'un groupe-de-noms et constitue un laissez-passer pour un contrôle d'accès.
- autorisations : indications de contrôle d'accès (4.3.1) : quelle information du Répertoire est accessi-ble et quelles opérations (lire, créer, modifier) peuvent y être effectuées.
- nom-de-domaine-du-répertoire : cet attribut désigne un domaine de gestion du répertoire, soit l'autorité qui opère le serveur de répertoire.
- algorithmes-disponibles : cet attribut contient les noms des algorithmes de cryptographie utilisés dans un serveur ou dans un client. Il peut s'agir d'algorithmes de hachage (MD2, MD5), de chiffrement par clé symétrique (DES, RC2, RC4, CAST, IDEA) et par clés asymétri-ques(RSA).
- certificat-d'utilisateur : la valeur de cet attribut est un certificat X.509, communément appelé certificat de clé publique. En raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.
- membre-unique : cet attribut contient le nom-courant d'un groupe-de-noms-uniques dont fait partie une personne-de-l'organisation ou un groupe-de-noms-uniques.
- détenteur : cet attribut contient le nom d'une personne-de-l'organisation qui est propriétaire, res-ponsable de la création et de la modification d'un objet d'information.
- certificat-d'autorité-de-certification : cet attribut contient un message signé numériquement par une autorité de certification et attestant que la clé publique qui s'y trouve est reliée à la clé privée détenue par un utilisateur. En raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.

- liste-de-révocation-de-certificat : cet attribut contient des certificats de clés publiques devenues invalides parce que le secret de la clé privée a été compromis ou que son détenteur n'est plus autorisé à l'utiliser. En raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.
- liste-delta-de-révocation : cet attribut contient les ajouts à une liste de révocation depuis la plus récente mise à jour. En raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.
- liste-de-révocation-d'autorité : cet attribut contient les noms des autorités de certification qui n'ont pas ou n'ont plus la confiance requise, et dont les certificats signés ne sont pas ou ne sont plus reconnus valides. En raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.
- paire-de-certification-réciproque : en raison des variantes du certificat X.509 (1988, 1993), l'emmagasinage et la transmission s'effectuent en code binaire.
- certificat-d'utilisateur-S/MIME : cet attribut spécifie un certificat d'utilisateur particulier à utiliser avec le protocole S/MIME (RFC 1847).

5.2.6 Attributs généraux de noms :

regroupe les attributs qui concernent les appellations données aux objets dans les entrées.

- nom-d'objet-d'alias : cet attribut est propre aux sous-classes d'objet associées à alias et sa valeur indique le nom-courant d'un objet de la classe désignée avec alias.
- numéro-de-série : cet attribut contient un numéro unique rattaché à un objet (souvent un dispositif).
- nom : ce supertype d'attribut sert dans la formation des types d'attribut formés d'une chaîne de caractères composant une appellation pour un objet, le nom qu'on lui donne.
- identifiant-unique-X.500 : cet attribut sert à distinguer entre les objets quand un nom-distinctif doit être utilisé plus d'une fois en fonction des règles d'appellation prévalantes. L'ajout de cet attribut fait en sorte de préserver le caractère unique de chaque nom-distinctif.
- nom-distinctif : cet attribut n'est pas utilisé pour le nom de l'objet, mais c'est un type de base dont héritent certains attributs dont la syntaxe requiert le nom-distinctif d'un objet.
- identifiant-d'objet : cet attribut est composé d'un nom descriptif et d'un identifiant numérique pour désigner uniquement un objet d'information.
- identifiant-unique : cet attribut spécifie un identifiant unique pour un objet représenté dans une entrée du répertoire. Il s'agit le plus souvent de numéros générés localement dans un domaine donné.

5.2.7 Attributs pour le nom-courant d'une personne :

regroupe des attributs supplémentaires s'appliquant au nom-courant d'une personne

- nom-courant : cet attribut contient un nom pour un objet, par exemple le nom au complet d'une personne. La valeur est répétable, ce qui permet d'enregistrer plusieurs formes du nom, par exemple Madeleine Nadeau et Mado Nadeau. Une seule forme sert cependant à la composition du nom-distinctif.
- nom-de-famille : cet attribut ne concerne que la classe personne et ses sous-classes ; il contient une partie du nom-courant, le patronyme ou nom de famille.

- prénom-usuel : cet attribut contient le prénom usuel d'une personne, excluant toute initiale qui précède le nom-de-famille.
- initiales : cet attribut contient les initiales du prénom et toute autre initiale, mais en excluant le nom-de-famille.
- suffixe-de-nom : cet attribut contient la partie du nom d'une personne qui indique la génération (par ex. : junior).

5.2.8 Autres attributs d'une personne :

regroupe des attributs hétérogènes s'appliquant à une personne.

- passe-temps : cet attribut est d'un type à part pour indiquer une zone où la personne désignée dans une entrée peut mettre une information de son propre choix (à prendre comme équivalent à l'attribut "drink").
- immatriculation-d'automobile : numéro de plaque d'immatriculation qui est attachée à un véhicule automobile que conduit quelqu'un.
- photo : cet attribut spécifie une photo encodée en JPEG (Joint Photographic Encoding Group) et qui représente l'objet décrit par une entrée ou quelque chose qui est associé à cet objet.
- langues : cet attribut spécifie la ou les langue(s) connue(s) par une personne ou un objet et qui peut (peuvent) être utilisée(s) pour communiquer avec cette personne ou cet objet. L'indication de la langue est faite selon le code RFC 1766. L'ordre dans lequel les langues sont listées va de la mieux connue jusqu'à celle qui serait moins maîtrisée mais valant d'être mentionnée, surtout pour les langues moins répandues en contexte québécois.
- audio : cet attribut permet de stocker des éléments sonores dans le Répertoire.

5.2.9 Attributs des subdivisions du Répertoire :

Regroupe divers attributs reliés aux sub-divisions du répertoire en un sens général, allant de l'abstrait au concret.

- aide-au-repérage : cet attribut sert à certaines interfaces client (X.500) à construire des filtres de repérage.
- aide-au-repérage-amélioré : cet attribut sert à certaines interfaces client (X.500) à construire des filtres de repérage dans les requêtes.
- classe-d'objet : les valeurs décrivent la sorte d'objet qu'une entrée représente. Cet attribut est présent dans toutes les entrées avec au moins deux valeurs dont l'une est soit racine ou alias
- information-de-référence : cet attribut a trait aux informations détenues par chaque serveur sur les autres serveurs de répertoire dans un environnement X.500.
- contexte-d'application-disponible : cet attribut contient les identifiants des contextes d'applications OSI.
- qualificatif-de-domaine : dans le cas de fusion de sources qui pourraient mettre en péril le caractère unique des noms-distinctifs, un qualificatif de domaine est ajouté à l'ensemble des noms-distinctifs.
- classe-d'objet-extensible : lorsqu'elle est présente dans une entrée, la classe-d'objet-extensible permet à cette entrée de contenir tout attribut facultatif.
- partie-d'un-domaine : cet attribut sert à spécifier une composante d'un domaine (par ex. : « com », « edu »).
- fiche-de-domaine : cet attribut spécifie les ressources d'un domaine qui sont associées à un objet.

- domaine-associé : cet attribut spécifie un domaine de DNS qui est associé à un objet dans l'arborescence du répertoire.
- ref : cet attribut sert à enregistrer dans un serveur LDAP l'information de référence sur l'environnement des serveurs de répertoire. Il permet de référer-par-nom, de référer-à-supérieur, et de référer-sans-nom de façon analogue à X.500 respectivement pour l'information de référence de type « subordonné », « supérieur » et « subordonné non spécifique ».

5.2.10 Attributs opérationnels X.500 :

ces attributs sont définis dans X.501 (1993) comme devant être supportés par tous les serveurs X.500, et ils sont repris dans les proposi-tions actuelles sur LDAP. On notera que les quatre premiers attributs assurent la base opérationnelle pour les attributs de l'administration des entrées elles-mêmes.

- création-horodatée : cet attribut apparaît dans les entrées créées avec l'opération Ajouter (Add) à la base des entrées. Indication en « Temps généralisé » (X.208) et spécifiant la zone du fuseau horaire. Par exemple : 1997122510302.
- modification-horodatée : cet attribut apparaît dans les entrées modifiées avec l'opération de Modifier (Modify) la base des entrées.
- nom-du-créateur : cet attribut contient le nom du (des) créateur(s) de l'entrée, soit le nom-courant de l'utilisateur qui a effectué l'opération d'ajout.
- nom-du-modificateur : cet attribut contient le nom du (des) modificateur(s) de l'entrée, soit le nom-courant de l'utilisateur qui a effectué l'opération de modification.
- entrée-de-sous-schéma : la valeur de cet attribut est le nom d'une entrée de sous-schéma (ou d'une sous-entrée si le serveur est basé sur X.500). Ce sous-schéma présente les attributs que ce serveur utilise.
- types-d'attribut : cet attribut se retrouve généralement dans l'entrée de sous-schéma.
- règles-d'appariement : cet attribut définit les cas d'égalité pour qu'il y ait correspondance entre une requête et une entrée dans le repérage et la comparaison des valeurs d'attributs.
- usage-de-règles-d'appariement : cet attribut contient les noms des attributs qui sont appropriés pour les règles d'appariement extensibles.

5.2.11 Attributs opérationnels LDAP :

ces attributs opérationnels s'ajoutent aux précédents sur les serveurs LDAP, où ils doivent être présents dans le serveur racine du répertoire.

- contexte-d'appellation : les valeurs de cet attribut correspondent aux contextes d'appellation dont ce serveur est maître ou qu'il miroite. Si un serveur n'est maître d'aucune information, cet attribut est absent. Cet attribut permet à un client de choisir les bases d'objet pertinentes pour le repérage.
- autres-serveurs : les valeurs de cet attribut sont des URL d'autres serveurs qui peuvent être contactés quant ce serveur n'est pas disponible.
- extensions-disponibles : les valeurs de cet attribut sont des identifiants-d'objet indiquant quelles opérations extensionnées sont disponibles sur ce serveur.
- contrôles-disponibles : les valeurs de cet attribut sont des identifiants-d'objet indiquant quels contrôles sont disponibles sur ce serveur.
- mécanismes-SASL-disponibles : les valeurs de cet attribut sont les noms des mécanismes SASL qui sont disponibles sur ce serveur (SASL : Simple Authentification and Security Layer).

- versions-LDAP-disponibles : les valeurs de cet attribut sont les versions du protocole LDAP disponibles sur ce serveur.
- syntaxes-LDAP-disponibles : cet attribut facultatif des serveurs sert à fournir la liste des syntaxes disponibles, chaque valeur désignant une syntaxe. Ces valeurs sont des identifiants-d'objet des syntaxes.

La figure 5-3 présente une vue synthétique des attributs. Les onze regroupements d'attributs y sont placés dans une forme circulaire, selon le modèle d'une roue cerclée d'un pneu. Le cercle noir représente un pneu au sens de point de contact entre la partie logique (interne) de la roue et la piste d'atterrissage du fonctionnement réel : c'est l'aspect de l'implantation des serveurs, des logiciels, des protocoles et de l'administration technique des entrées. Les neuf autres groupes d'attributs sont situés dans la roue elle-même, la partie logique. Des attributs formels de noms et de subdivisions y sont reliés respectivement à des attributs de noms de personnes et d'organisations. On y voit ces quatre groupes d'attributs pointer vers un rectangle arrondi listant quatre autres groupes d'attributs : télécommunications, postal, localisation, sécurité. Le contenu du rectangle arrondi concentre le principal effet utile attendu du répertoire, qui est de fournir des pointeurs permettant d'atteindre les divers types d'objets enregistrés au répertoire, quel que soit le moyen de communication utilisé.

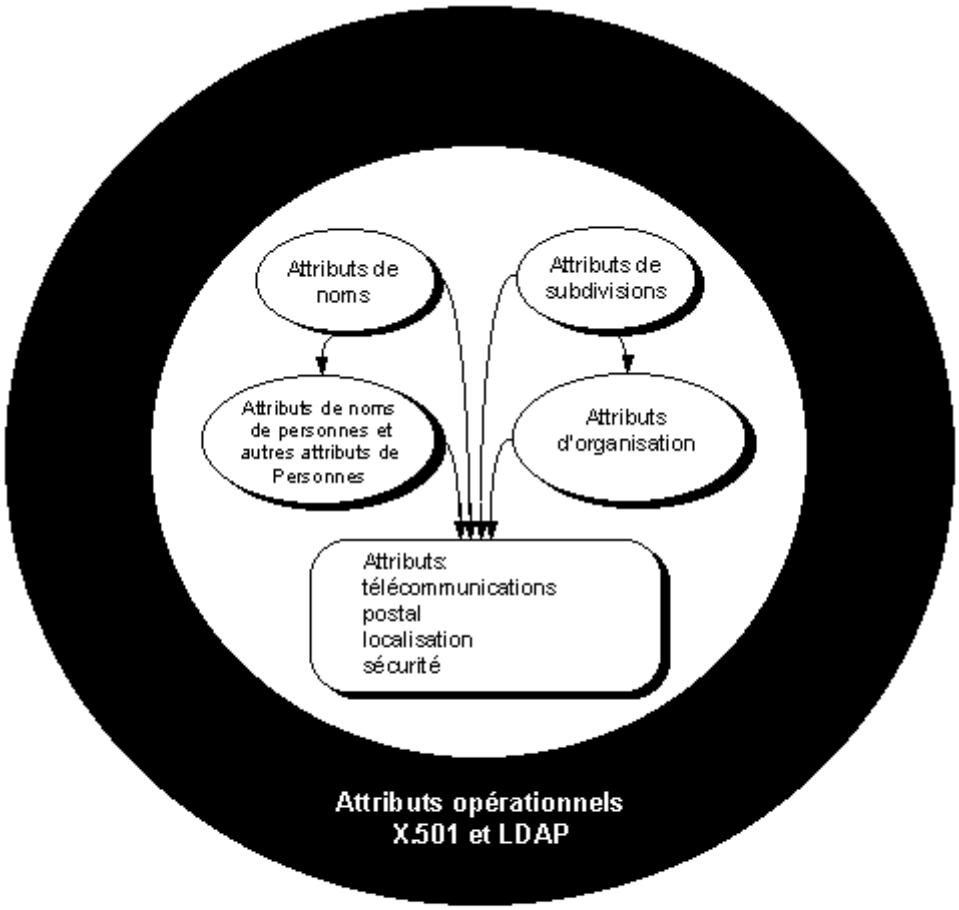


Figure 5-3
Vue synthétique des attributs du Répertoire

La liste des attributs que nous avons présentée a une bonne valeur indicative, mais il n'y a pas de véritable consensus d'établi dans tous les détails. En partie parce que la situation reste mouvante, quelques attributs présentés sont menacés de désuétude et pourraient ne pas être utilisés. La prochaine section définira d'ailleurs quelques attributs supplémentaires dans la définition de classes d'objets de façon adaptée aux besoins du gouvernement du Québec.

5.3 Définition des premières classes d'objet

Tel que mentionné en introduction du chapitre, un nombre réduit de classes d'objets ont été l'objet d'une attention particulière de définition pour répondre aux besoins du gouvernement. La priorité qui leur a été accordée résulte du fait que ces classes d'objet présentent un caractère plus urgent d'inventaire et permettent d'entrevoir des bénéfices plus importants par rapport aux autres classes d'objet. Un autre facteur qui a influencé leur choix a été la prise d'initiative d'intervenants gouvernementaux désireux de contribuer à leur définition.

Les classes d'objet choisies se retrouvent dans les trois services suivants de consultation du Répertoire :

- Pages blanches : la classe Personne-de-l'organisation ;
- Pages bleues : les classes Organisation et Unité-organisationnelle ;
- Pages vertes : la classe Document.

Les classes d'objet et les attributs qui ont été présentés dans les deux premières sections de ce chapitre constituent un éventail d'objets prédéfinis, convenus internationalement, parmi lesquels les développeurs du Répertoire gouvernemental du Québec regarderont d'abord pour choisir ce dont ils ont besoin pour les objets qu'ils auront décidé de répertorier. Une correspondance maximale avec cette offre publique est une garantie d'interopérabilité dans la galaxie des répertoires, l'une des plus structurantes du cyberespace.

La présente section effectue donc des choix parmi les classes d'objet et les attributs conventionnels, et spécifie les attributs de quelques classes d'objet en ajustant et en ajoutant des attributs en fonction des besoins privilégiés dans ce premier échantillon de portée la plus générale possible. À noter que le terme « Facultatif » dans les tableaux qui suivent signifie qu'on est libre d'utiliser ou non cet attribut, ce qui est distinct du mot « optionnel » qui, lui, signifie qu'un choix obligatoire doive être fait entre deux ou plusieurs possibilités.

5.3.1 Personne-de-l'organisation

Personne-de-l'organisation est une sous-classe de *Personne* qui sous-tend la description des en-trées du Répertoire pour les employés, les mandataires, des élus ou autres personnes aussi étroi-tement associées à l'appareil gouvernemental. L'entrée sert à identifier chaque employé, ses adresses, ses autorisations et d'autres renseignements de sécurité. En outre, comme pour toute entrée du Répertoire, quelques attributs supplémentaires servent à l'administration des entrées dans la base de données du Répertoire. Les attributs de la classe *Personne-branchée* ont été intégrés dans le format présenté ci-après. Une norme de carte d'affaires électronique a été proposée pour l'Internet sous le nom de VCard 2.0. Tous ses attributs se trouvent inclus dans la présente proposition.

Liste des attributs d'une entrée Personne-de-l'organisation

Attributs	O : obligatoire F : facultatif	R : répétable U : valeur unique
classe-d'objet : Personne-de-l'organisation	O	U
nom-courant : cet attribut contient un nom pour un objet, par exemple le nom au complet d'une personne. La valeur est répétable, ce qui permet d'enregistrer plusieurs formes du nom, par exemple Madeleine et Mado. Une seule forme sert cependant à la composition du nom-distinctif.	O	R
nom-de-famille : cet attribut ne concerne que la classe Personne et ses sous-classes ; il contient une partie du nom-courant, le patronyme ou nom de famille.	O	U
prénom-usuel : cet attribut contient le prénom usuel d'une personne, excluant toute initiale qui précède le nom-de-famille.	O	
initiales : cet attribut contient les initiales du prénom et de toute autre initiale, mais en excluant le nom-de-famille.	F	U

identifiant-unique-X.500 : cet attribut sert à distinguer entre les objets quand un nom-distinctif doit être utilisé plus d'une fois en fonction des règles d'appellation prévalantes. L'ajout de cet attribut fait en sorte de préserver le caractère unique de chaque nom-distinctif.	F	U
langues : cet attribut spécifie (la) les langues connues par un objet et qui peuvent être utilisées pour communiquer avec cette personne ou cet objet. L'indication de la langue est faite selon le code RFC 1766. L'ordre dans lequel les langues sont listées va de la mieux connue jusqu'à celle qui serait moins maîtrisée mais valant d'être mentionnée, surtout pour les langues moins répandues en contexte québécois.	F	R
langue-préférée : cet attribut spécifie la langue à utiliser de préférence pour communiquer avec une personne ; au gouvernement du Québec, cet attribut est normalement FR pour français, qui est la langue de l'administration.	F	R
titre-personnel : cet attribut contient un titre particulier d'une personne dans son contexte social (ex. : M., Mme, maire, Révérend), professionnel (avocat, ingénieur, technicien), ou académique.	F	R
photo : cet attribut spécifie une photo encodée en JPEG (Joint Photographic Encoding Group) et qui représente l'objet décrit par une entrée ou quelque chose qui est associé à cet objet.	F	U
audio : cet attribut permet de stocker des éléments sonores dans le Répertoire.	F	U
passe-temps : cet attribut est d'un type à part pour indiquer une zone où la personne désignée dans une entrée peut mettre une information de son propre choix (à prendre comme équivalent à l'attribut ''drink'').	F	U
nom-distinctif : cet attribut n'est pas utilisé pour le nom de l'objet, mais c'est un type de base dont héritent certains attributs dont la syntaxe requiert le nom-distinctif d'un objet.	O	U
numéro-d'employé : identifiant numérique attribué à un employé dans une organisation.	F	U
nom-de-l'unité-organisationnelle : cet attribut contient le nom d'une unité organisationnelle.	O	U
nom-du-rôle : cet attribut contient le nom d'un rôle (position ou fonction comme sous-ministre, directeur, analyste) pour une personne-de-l'organisation.	F	U
Mots-clés : le recours à des mots-clés permet d'associer des dossiers, expertises, langues connues, etc., à la personne, selon ce qui est jugé utile en contexte.	F	R
catégorie-d'utilisateur : cet attribut sert à contenir un nom descriptif de catégorie dont l'utilisateur est membre.	F	U
type-d'employé : cet attribut indique le type d'emploi ou de poste qu'occupe une personne.	F	U
numéro-de-téléphone : la valeur est exprimée en une chaîne de caractères composé selon la forme interna-tionale reconnue (voir X.500) par exemple : +1 418 651 8976.	O	U
numéro-de-télécopieur : la valeur du numéro de téléphone est suivie des paramètres de télécopie comme ceux du format d'impression :	F	U
adresse-de-télémessagerie : cet attribut spécifie un attribut d'adresse de télémessagerie (casier postal électronique) selon la convention Internet (RFC 822).	F	U

adresse-d'autre-télémessagerie : cet attribut contient les valeurs désignant d'autres formes d'adresse de télémessagerie que les adresses Internet (RFC 822).	F	U
cellulaire : cet attribut contient le numéro de téléphone cellulaire associé à une personne selon le format international.	F	U
adresse-postale : format familier, spécifié dans un guide de la Société canadienne des postes.	O	U
identifiant-d'édifice : cet attribut sert à identifier un édifice en un lieu.	F	U
numéro-de-local : cet attribut indique la localisation d'un objet, substituable à l'attribut emplacement.	F	U
téléphone-à-domicile : cet attribut contient le numéro de téléphone associé au domicile d'une personne selon le format international.	F	U
cellulaire-personnel : cet attribut spécifie le numéro de téléphone du cellulaire personnel (pas pour affaires) de quelqu'un.	F	U
adresse-domiciliaire : cet attribut spécifie l'adresse du domicile d'une personne (limite de 6 lignes de 30 caractères).	F	U
immatriculation-d'automobile : numéro de plaque d'immatriculation qui est attachée à un véhicule automobile que conduit quelqu'un.	F	U
identifiant-d'utilisateur : cet attribut spécifie un nom d'accès (login) à un système.	F	U
mot-de-passe : cet attribut contient une chaîne de caractères propre à un utilisateur et qui sous-tend l'assurance de son identification. Utilisé dans le contrôle d'accès.	F	U
membre : cet attribut contient le nom d'une personne-de-l'organisation ou d'un groupe-de-noms et constitue un laissez-passer pour un contrôle d'accès.	F	R
membre-unique : cet attribut contient le nom-courant d'un groupe-de-noms-uniques dont fait partie une personne-de-l'organisation ou un groupe-de-noms-uniques	F	R
certificat-d'utilisateur : la valeur de cet attribut est un certi-ficat X.509, communément appelé certificat de clé publique.	F	R
certificat-d'utilisateur-S/MIME : cet attribut spécifie un certificat d'utilisateur particulier à utiliser avec le protocole S/MIME (RFC 1847)	F	R
autorisations : indications de contrôle d'accès (4.3.1) : quelle information du Répertoire est accessible et quelles opérations (lire, créer, modifier) peuvent y être effectuées.	F	R
création-horodatée : cet attribut apparaît dans les entrées créées avec l'opération Ajouter (Add) à la base des entrées. Indication en « Temps généralisé » (X.208) et spécifiant la zone du fuseau horaire. Par exemple : 1997122510302.	O	U
modification-horodatée : cet attribut apparaît dans les entrées modifiées avec l'opération de Modifier (Modify) la base des entrées.	O	U
nom-du-créateur : cet attribut contient le nom du (des) créateur(s) de l'entrée, soit le nom-courant de l'utilisateur qui a effectué l'opération d'ajouter (Add) une entrée.	O	R
nom-du-modificateur : cet attribut contient le nom du (des) modificateur(s) de l'entrée, soit le nom-courant de l'utilisateur qui a effectué l'opération de modification.	O	R
langue-de-l'entrée : abréviation de la langue dans laquelle est rédigée l'entrée.	O	U
identifiant-séquentiel-d'entrée : chaque entrée reçoit un numéro matricule à la suite de l'abréviation du nom d'une unité-organisationnelle.	O	U

5.3.2 Organisation

La classe d'objet Organisation contient une seule entrée, soit celle du Gouvernement du Québec. Il s'agit d'une classe particulière qui joue le rôle de racine du Répertoire et fait ainsi appel à de nombreuses considérations d'ordre organisationnel. Par convention, le gouvernement du Québec est l'organisation qui exerce le contrôle sur le Répertoire gouvernemental. L'objet du présent chapitre offre des éléments de conception du schéma du répertoire gouvernemental qui esquisse un espace de possibilités et fournit un premier cadre de définition : classes d'objet, types d'attributs, règles de structures entre classes d'objet, règles d'appellation, règles de contenu, règles d'appariement. Le gouvernement exerce plusieurs responsabilités : il contrôle la racine du répertoire, il est au sommet de la hiérarchie de certification, il peut offrir des services communs de garde-barrière et de contrôle des transactions, il peut aussi héberger divers recueils, listes d'autorité, thésaurus de descripteurs et mots-clés des activités gouvernementales, banque de terminologie, etc. Une variété de services communs de l'infrastructure de l'inforoute gouvernementale dépendent de ce sommet hiérarchique.

La conception de ce premier niveau déborde largement des questions techniques. Pour être complète, cette conception doit être accompagnée d'arrangements institutionnels dans l'appareil administratif. Les règles devant être définies pour la spécification du schéma du domaine Gouvernement du Québec dépendent en partie de la participation de nombreuses instances administratives à l'élaboration, à la mise à l'essai et au déploiement de nouvelles procédures prenant appui sur le Répertoire gouvernemental. Parmi les démarches entreprises à l'automne 1997, notons-en cinq qui ont une portée horizontale :

- les démarches de conception technique du Répertoire menées par la direction générale des Télécommunications ;
- la contribution particulière des unités de gestion des ressources humaines quant à la création et à la mise à jour des entrées de personne-de-l'organisation pour les données d'identification et d'adresses ;
- la contribution particulière des unités de gestion financière pour adapter les règles et procédures en délégation du pouvoir de signature aux conditions de déploiement d'une infrastructure à clé publique implantée en se servant du Répertoire gouvernemental ;
- la contribution particulière du MRCI grâce à son réseau de collaboration coordonné autour de Communication-Québec et de la direction de l'Inforoute et de l'information documentaire dans l'élaboration de conventions et d'un guide pour la production du contenu des entrées de Pages bleues du Répertoire ;
- les démarches d'étude et de concertation sur la sécurité inforoutière, ainsi que le projet-pilote relatif à l'infrastructure à clés publiques menées par le SCT, le SAI et d'autres intervenants gouvernementaux.

5.3.3 Unité-organisationnelle

La classe *Unité-organisationnelle* comprend les ministères et organismes et leurs subdivisions jusqu'au plus bas niveau voulu des unités administratives. Les unités organisationnelles de premier niveau, c'est-à-dire les ministères et les organismes, vont assumer la responsabilité d'éléments communs d'information, tel un organigramme. Les *Unités-organisationnelles* se définissent principalement avec les attributs caractéristiques des Pages bleues, soit la structure hiérarchique et la description des programmes et services.

Liste des attributs d'une entrée Unité-organisationnelle

Attributs	O : obligatoire F : facultatif	R : répétable U : valeur unique
classe-d'objet : Unité-organisationnelle	O	U
nom-courant de l'Unité-organisationnelle, soit le nom officiel au long ; le sigle ou l'acronyme peut apparaître comme nom-courant à la suite, de même que des appellations anciennes par exemple, puisque cet attribut est répétable et que l'organisme pourra être ainsi repéré plus facilement.	O	R
alias-d'unité-organisationnelle : l'emploi de cet attribut a un effet semblable à la répétition du nom-courant de l'Unité-organisationnelle, mais permet d'accroître la visibilité de cette autre appellation de l'Unité-organisationnelle. La chose est utile quand une Unité-organisationnelle, dans une position hiérarchique modeste, est très connue du public et susceptible d'être fréquemment sollicitée.	F	U
organigramme : l'organigramme sert à situer une Unité-organisationnelle dans une portion de la structure administrative. Alors que l'organigramme du gouvernement fourni par l'entrée Organisation permet de situer les ministères et organismes dans les grandes missions gouvernementales, chacune de ces Unités-organisationnelles de premier niveau doit créer et tenir à jour un organigramme des subdivisions administratives sous son contrôle. Les Unités-organisationnelles de deuxième niveau et plus recourent à cet outil commun pour informer les utilisateurs de leur position. La délégation est possible selon les politiques de chaque ministère ou organisme dans les limites du schéma de la classe supérieure (organisation).	O	U
mandat : énoncé du mandat et des principaux objectifs de l'Unité-organisationnelle.	O	U
catégorie-d'affaires : classe générale d'activité à laquelle l'Unité-organisationnelle se rattache principalement (à partir d'une liste établie par Communication-Québec).	O	U
mots-clés de l'Unité organisationnelle : liste de sujets spécifiques dont s'occupe principalement une unité-organisationnelle et qui la différencient des autres subdivisions.liste des principaux Rôles-dans-l'organisation qui font partie d'une Unité-organisationnelle.	O	R
point-de-contact : cet attribut sert à indiquer un ou des points de contact avec l'Unité-organisationnelle, qu'il s'agisse d'un numéro de téléphone pour renseigne-ments généraux, d'un site Web, ou d'un comptoir. Les attributs appropriés sont choisis dans les trois en-sembles d'attributs d'adresses (télécommunications, postal, localisation). Les renseignements peuvent provenir des entrées Personnes-de-l'organisation via des références croisées avec des tenants-de-rôle qui y sont identifiés : on obtient une relation entre des en-trées de Pages bleues qui font appel à des entrées de Pages blanches pour en offrir une perception intégrée à l'utilisateur.	O	R
heures-d'ouverture : indications relatives aux heures d'ouverture ou de disponibilité des services du(des) point-de-contact.	O	R
programme-service : nom-courant d'un programme ou d'un service qui dépend de l'Unité-organisationnelle. La description se décompose en une série d'attributs :	O	R

- clientèle : désignation de la clientèle visée.
  F R
- description : texte explicatif de l'objet et des modalités générales d'un programme ou service.

O U

- définitions : définition de termes particuliers utilisés dans le cadre d'un programme ou service.
  F R
- point-de-contact : noms-courants du(des) répondant(s) que les clients du programme ou service peuvent contacter ; il peut s'agir du nom-courant d'une personne-de-l'organisation (Pages blanches) ou du nom-courant d'un rôle-dans-l'organisation (Pages bleues).
  O R
- formulaires : liste des noms-courants de formulaires nécessaires et utiles au fonctionnement d'un programme ou service.
  F R
- publications : désignation sommaire de publications papier ou électroniques pertinentes au programme ou service et pointeur vers leurs entrées correspondantes dans les Pages vertes.
  F R
- cadre-légal : lois, règlements, dispositions générale déterminant l'accès à un programme ou service ou sa réalisation.
  F R
- dates-début-fin : période de mise en vigueur, prochaine échéance, date-limite s'appliquant à un programme ou service.
  F R
- démarches : explication des démarches devant être entreprises par le client du programme ou service
  F R
- coûts-mode-de-paiement : tout montant à payer et toute modalité de paiement pour le client du programme ou service.
  F R
- délai-de-traitement : délai moyen ou courant dans le traitement d'un cas ou d'un dossier soumis dans le cadre du programme ou du service.
  F R
- Q-R : texte explicatif arrangé en liste de questions-réponses à propos du programme ou service.
  F R

F R

F	R	
création-horodatée	O	U
modification-horodatée	O	R
nom-du-créateur	O	U
nom-du-modificateur	O	R
langue de l'entrée	O	U
nom-du-responsable-dans-l'unité-organisationnelle	O	R

nom-du-responsable-à-Communication-Québec	F	R
notes : explication, remarque, interprétation à propos de l'entrée	F	R
identifiant-séquentiel-d'entrée : numéro unique identi-fiant une entrée qui se compose du sigle de l'organisation qui produit l'entrée, suivi d'un numéro matricule ou de contrôle.	O	U

Ces entrées Unité-organisationnelle peuvent être interrogées avec les requêtes usuelles adressées au Répertoire, c'est-à-dire en sélectionnant parmi les classes d'objet et en fournissant des valeurs d'attributs, ou encore en cherchant au moyen de toute chaîne de caractères. Cependant, la réalisation du mandat du MRCI dans l'inforoute gouvernementale va permettre la création de pages de navigation sur le Web pour faciliter l'exploitation par le public et les entreprises de cette base d'information descriptive de l'ensemble de l'activité gouvernementale. Cette valeur ajoutée comprendra notamment des cheminements dans les Pages bleues centrés sur des événements sociaux fréquents (naissance, décès, mariage, déménagement, entrée à l'école, perte d'emploi, obtention d'emploi, maladie, accident), des aperçus généraux et dossiers-synthèses, des arbres de décision pour assister certains choix, diverses listes. Cela comprend aussi divers renseignements généraux et des listes pour aider citoyens et entreprises à effectuer des transactions de tous types avec l'administration publique. La liste des catégories-d'affaires pourrait relever de ce service central, de même qu'un thésaurus de descripteurs et mots-clés pour la catégorisation des activités gouvernementales.

5.3.4 Document

La classe Document est relativement familière puisque cette entrée n'est qu'une version améliorée de la traditionnelle fiche de bibliothèque contenant une référence bibliographique. L'entrée offre une structure pour identifier le document, pour le localiser dans le monde papier ou dans le cyberespace, et pour obtenir l'accès au document. Une première version des attributs de cette classe avait été préparée en juin 1996 par le Groupe des responsables de la gestion documentaire (GRGD). Elle vient d'être révisée dans le cadre du Chantier en ingénierie documentaire coordonné par le Conseil du trésor. Sa révision a tenu compte d'évaluations menées au Canada et aux États-Unis sur le format GILS (Government Information Locator Service), modèle qui avait été adapté par le GRGD en 1996. Voici la liste courante (octobre 1997), encore en cours de révision sur des points mineurs.

Liste des attributs d'une entrée Document

Attributs	O : obligatoire F : facultatif	R : répétable U : valeur unique
Classe-d'objet : Document	O	U
Titre : cet élément contient le titre complet du document y compris les sous-titres. Un titre est d'autant plus utile s'il aide à établir rapidement sa pertinence en condensant son apport particulier en rapport avec un sujet général.	O	U
Organisation-source : cet élément identifie l'organisation d'où origine le document. Il contient « Québec (Gouv.) » et le nom d'une organisation gouvernementale suivi possiblement du ou des noms d'une branche de cette organisation.	O	U
Auteur : les noms des individus ou collectivités responsables du contenu intellectuel du document référencé.	F	R

Langue-du-document : langue du contenu du document référencé, selon le code international de langues (RFC 1766).	O	R
Date-de-publication du document référencé, sous la forme AAAAMMJJ.	F	R
Mots-clés-de-source-connue : cet élément identifie des thésaurus ou index connus et énumère pour chacun des mots-clés ou descripteurs normalisés qui en sont tirés pour décrire le contenu du document.	F	R
Mots-clés-de-source-locale : cet élément sert à énumérer des termes définis localement, qu'ils soient normalisés ou non.	F	R
Résumé : cet élément est constitué d'un texte court qui décrit le contenu d'une ressource informationnelle.	F	R
Référence-géographique-par-coordonnées : latitudes extrêmes nord et sud et longitudes extrêmes est-ouest, Référence-géographique-par-nom-de-lieu, qui peut soit se trouver dans un thésaurus ou index connu, soit être un terme local (Répertoire des toponymes du Québec).	F F	U
Période couverte par le contenu du document ; l'indication peut être selon une forme prescrite, soit décrite textuellement.	F	R
Source-des-données : cet élément sert à identifier la source de production des données qui alimente un système d'information. Il peut s'agir d'une organisa-tion gouvernementale ou autre.	F	R
Méthodologie : Cet élément identifie tout outil spécialisé, ou toute technique ou méthode utilisée pour pro-duire cette ressource informationnelle. La validité, le degré de fiabilité et toute possibilité d'erreur devrait aussi être décrite.	F	U
Autres-agents-de-production : cet élément sert à identi-fier les agents de production du document autres que l'organisation source, l'auteur et le distributeur, et qui ont joué un rôle dans la création du document. Les noms de rôle peuvent être variés dont : directeur de publication, traducteur, illustrateur, compilateur, éditeur (pas un simple distributeur) ou toute autre contribution intellectuelle significative au contenu.	F	R
Information-supplémentaire : tout autre renseignement utile qu'un regroupement ou une organisation souhaite ajouter concernant un document ou une information.	F	R
Codification : identifiant universel (ISBN, ISSN), ou identifiant utilisé en classification des documents, en gestion documentaire, en gestion des bibliothèques ou en archivistique ; les sources connues (Dewey, Library of Congress) et les sources locales (plan de classification d'un ministère ou organisme, cote « Publications gouvernementales ») sont nommées comme des attributs prenant la valeur de la cote qui suit.	F	R
Accessibilité : cet élément regroupe plusieurs sous-éléments qui décrivent comment l'information est rendue accessible.	F	R

- Distributeur : nom (organisation, unité administrative), et les éléments de la section ADRESSE des Pages Blanches, i.e. toutes les coordonnées pour rejoindre le distributeur.
  F U
- Caractérisation : description du document référencé dans le style du distributeur selon ses termes et son style, pour mettre en valeur certains aspects distinctifs.
  F U
- Procédé-de-commande : ensemble de renseignements sur la façon de commander un document de ce distributeur, les supports disponibles, les coûts associés, les modes de paiement et de livraison.
  F U

- Support-technique : Ce sous-élément décrit les condi-tions de support technique pour accéder à l'informa-tion telle que rendue disponible par un distributeur. Par exemple, quel appareil (vidéo, microfilm, etc.) est nécessaire, ou quel type d'ordinateur et de logi-ciel? Pour des données informatiques, il est possible d'ajouter toute spécification d'encodage, de densité d'enregistrement, de parité, de langage de program-mation. Par exemple une version PostScript, PDF, Word est souvent offerte au choix avec une indica-tion de la taille des fichiers. Lorsqu'applicable, et particulièrement pour les documents papier, indiquer le nombre de pages du document.
  F U
- Lien-accessible : Ce sous-élément fournit l'information nécessaire, sous une forme appropriée (URI), pour se relier à une ressource par réseau. Des liens peuvent être établis avec d'autres références, pour faciliter la livraison électronique de produits, ou pour aiguiller l'utilisateur vers les éléments d'analyse et de synthèse de l'information. Sur l'Internet, ces liens sont établis au moyen des URL.
  F R
- Type-de-lien-accessible : Accompagne un lieu et précise le type de contenu MIME.

F	R	
Durée-de-disponibilité : cet élément précise la date limite de la disponibilité du document	F	U
Limites-d'accès : cet élément décrit toute limitation légale ou autre à l'accès ; il peut s'agir de limites gé-nérales comme la protection des renseignements personnels, ou de limites particulières aux documents confidentiels.	F	U
Conditions-d'utilisation : cet élément mentionne toute condition préalable ou toute limite d'usage, notam-ment la protection du droit d'auteur.	F	U
Point-de-contact : identifier une organisation ou éven-tuellement une personne à rejoindre pour obtenir de l'information supplémentaire sur un document référencé (voir section ADRESSES des Pages Blan-ches).	F	R
Raison-d'être : cet élément explique pourquoi cette ressource informationnelle a été produite et est offerte, en vertu de quel programme, projet ou disposition légale. Cette explication peut faire un lien avec son origine ou avec d'autres ressources informationnelles.	F	U
Programme-gouvernemental : cet élément identifie le programme gouvernemental ou le service dont dépend le document référencé.	F	U
Renvoi : Cet élément est un regroupement de sous-éléments qui, ensemble, identifient une autre entrée du répertoire jugée pertinente. Spécifiquement, quand une version du document pointé par une en-trée existe dans une autre langue, c'est dans le renvoi que cette indication est fournie. Cet élément peut aussi servir à établir des références au thésaurus. Il y a quatre sous-éléments :	F	R

- Titre-du-renvoi : une description en quelques mots de ce qui s'y trouve de potentiellement pertinent en relation avec l'entrée d'où est établi le renvoi. Pour un document disponible dans une autre langue, c'est le titre du document dans cette(ces) autre(s) langue(s) qui est présenté ici.
  F R
- Lien-du-renvoi : l'URL ou un identifiant de contrôle du répertoire
  F R
- Type-du-renvoi : accompagne un lien avec le type de contenu MIME de l 'URI référence
  F R
- Relation-avec-l'entrée : ce sous-élément vise à fournir une indication sur le rapport sémantique entre l'entrée et le renvoi tels que série (plus large) ; table des matières (plus étroit), échantillon gratuit, etc.

F	R	
Règle-de-conservation : Cet élément sert à enregistrer, pour une ressource informationnelle, l'identifiant qui lui est associé à des fins de disposition (destruction ou archivage). Ce renseignement doit être conforme au Calendrier de conservation d'une organisation, tel que requis par la Loi québécoise sur les Archives.	F	U
Identifiant-séquentiel-d'entrée : Cet élément est défini par l'organisation qui produit l'information ; chaque entrée sera unique puisque chaque organisation ins-crit son sigle et un numéro matricule ou de contrôle.	O	U
Identifiant-séquentiel-d'origine : cet élément est requis dans le cas d'une entrée qui est une version dérivée d'une autre entrée référence ; l'identifiant de contrôle de cette entrée utilisée comme source est la valeur requise.	F	U
Langue-de-l'entrée : cet élément indique la langue dans laquelle est rédigée l'entrée selon un code où le français est désigné par FR, l'anglais par EN, etc. (RFC 1766)	O	U
Date de révision de l'entrée : Cet élément identifie une date assignée par le producteur de l'entrée pour sa révision.	F	U
Création-horodatée : date à laquelle l'entrée a été crée	O	U
Modification-horodatée : date à laquelle survient une modification de l'entrée	O	R
Nom-du-créateur : nom courant de la personne qui a produit l'entrée	O	U
Nom-du-modificateur : nom courant de la personne qui modifie l'entrée	O	R

5.3.5 Tableau synoptique

Le tableau synoptique suivant offre un aperçu synthétique des trois classes d'objet spécifiées ici en présentant les attributs regroupés en trois sections à des fins explicatives : l'identification de l'objet, sa description, et l'administration de l'entrée elle-même qui décrit chaque objet. Au sein de chaque section d'une classe d'objet, une subdivision est faite pour lister en premier lieu les attributs pour lesquels une valeur est obligatoirement inscrite, et ensuite les attributs facultatifs.

Vue synthèse des attributs

Section de l'entrée	CLASSES D'OBJET		
-	**personne-de-l'organisation**	**unité-organisationnelle**	**document**
identification de l'objet	*obligatoires* nom-courant nom-de-famille prénom-usuel nom-distinctif nom-de-l'unité-organisationnelle *facultatifs* initiales identifiant-unique-X.500 langues langue-préférée titre-personnel photo audio passe-temps	*obligatoires* nom-courant organigramme mandat catégorie-d'affaires mots-clés liste des Rôles-dans-l'organisation *facultatifs* alias-d'unité-organisationnelle	*obligatoires* titre organisation-source langue-du-document *facultatifs* auteur date-de-publication mots-clés-de-source-connue mots-clés-de-source-locale codification résumé référence-géographique-par-coordonnées référence-géographique-par-nom-de-lieu période-couverte

	numéro-d'employé nom-du-rôle mots-clés catégorie-d'utilisateur type-d'employé		autres-agents-de-production source-des-données méthodologie information-supplémentaire
description de l'objet	**(adresses)** *obligatoires* numéro-de-téléphone adresse-postale *facultatifs* numéro-de-télécopieur adresse-de-télémessagerie adresse-d'autre-télémessagerie cellulaire identifiant-d'édifice numéro-de-local téléphone-à-domicile cellulaire-personnel adresse-domiciliaire immatriculation-d'automobile **(sécurité)** *facultatifs* identifiant-d'utilisateur mot-de-passe membre membre-unique certificat-d'utilisateur certificat-d'utilisateur-S/MIME autorisations	*obligatoires* point-de-contact heures-d'ouverture **(programme-service)** *obligatoires* nom-courant description point-de-contact *facultatifs* clientèle définitions formulaires publications cadre-légal dates-début-fin démarches coûts-mode-de-paiement délai-de-traitement Q-R (questions-réponses) renvoi portée-régionale	**(accès)** *facultatifs* **Accessibilité :** distributeur caractérisation procédé-de- commande support-technique lien-accessible type-de-lien-accessible durée-de-disponibilité limites-d'accès conditions- d'utilisation point-de-contact raison-d'être programme- gouvernemental **Renvoi :** titre-du-renvoi lien-du-renvoi type-du-renvoi relation-avec- l'entrée règle-de- conservation
administration de l'entrée	*obligatoires* création-horodatée modification-horodatée nom-du-créateur nom-du-modificateur langue-de-l'entrée identifiant-séquentiel-d'entrée	*obligatoires* création-horodatée modification-horodatée nom-du-créateur nom-du-modificateur langue-de-l'entrée identifiant-séquentiel-d'entrée nom-du-responsable-dans-l'unité-organisationnelle *facultatifs* nom-du-responsable-à-Communication-Québec notes	*obligatoires* création-horodatée modification-horodatée nom-du-créateur nom-du-modificateur langue-de-l'entrée identifiant-séquentiel-d'entrée *facultatifs* identifiant-séquentiel-d'origine date-de-révision

5.4 Conclusion

Pour clore ce chapitre sur le schéma du Répertoire gouvernemental, on peut essayer de dégager une image globale. La figure 5-4 identifie quelques interdépendances pour aider à comprendre comment la synergie du répertoire opère et fait que le tout est égal à plus que la somme de ses parties. On voit que les Pages bleues ont besoin des Pages blanches pour

fournir les adresses des rôles et des points de contact ; on voit aussi que la position hiérarchique vient fournir l'ossature d'autorité nécessaire pour la sécurité en termes de permissions et de certificats de clés publiques. D'un autre côté, les Pages vertes ont également besoin des Pages blanches pour fournir les adresses d'auteurs, de sources ou de points de contact concernant les documents. Entre Pages bleues et Pages vertes, il y a complémentarité entre les publications et formulaires reliés aux programmes et services et le support des métadonnées fournies avec ces documents. Enfin, les trois couleurs de Pages ont en commun des descripteurs des activités gouvernementales.

Annexe 1- Unités organisationnelles de premier niveau

La présente annexe regroupe les ministères du gouvernement et un certain nombre d'organismes et d'institutions assimilées proposés à titre d'unités organisationnelles de premier niveau pour les fins du Répertoire gouvernemental. Tous les organismes listés, comme les ministères, relèvent directement d'un membre de l'exécutif. Un très grand nombre d'organismes relevant directement d'un membre de l'exécutif n'ont cependant pas été retenus dans la présente proposition, compte tenu de facteurs tels leur ordre de grandeur, leur existence temporaire ou leur caractère particulier. Tout organisme non retenu sur la présente liste pourrait, à sa discrétion, faire valoir son droit de figurer à titre d'unité organisationnelle de premier niveau du Répertoire.

Liste des ministères, organismes et institutions

Assemblée nationale (AN)
Bibliothèque nationale du Québec (BNQ)
Bureau d'audiences publiques sur l'environnement
Caisse de dépôt et placement du Québec
Commission administrative des régimes de retraite et d'assurances
Commission d'accès à l'information
Commission de la santé et de la sécurité du travail
Commission de protection de la langue française
Commission des biens culturels du Québec
Commission des normes du travail
Conseil de la langue française
Conseil de la science et de la technologie
Conseil des arts et des lettres du Québec
Conseil du statut de la femme
Conseil du trésor (CT)
Conseil supérieur de l'éducation
Coroner
Directeur général des élections
Fonds pour la formation de chercheurs et l'aide à la recherche
Inspecteur général des institutions financières
Institut de police du Québec
Institut de tourisme et d'hôtellerie du Québec
Ministère de l'Industrie, du Commerce, de la Science et de la Technologie (MICST)
Ministère de la Culture et des Communications (MCC)
Ministère de la Famille et de l'Enfance
Ministère de la Justice (MJQ)
Ministère de la Métropole (MM)
Ministère de la Santé et des Services sociaux (MSSS)
Ministère de la Sécurité publique (MSP)
Ministère de l'Agriculture, des Pêcheries et de l'Alimentation (MAPAQ)
Ministère de l'Éducation (MEQ)
Ministère de l'Emploi et de la Solidarité (MES)
Ministère de l'Environnement et de la Faune (MEF)
Ministère des Affaires municipales, du Sport et du Loisir (MAM)
Ministère des Finances (MF)
Ministère des Relations avec les citoyens et de l'immigration (MRCI)
Ministère des Relations internationales (MRI)
Ministère des Ressources naturelles (MRN)
Ministère des Transports (MTQ)

Ministère du Conseil exécutif (MCE)
Ministère du Revenu (MRQ)
Ministère du Travail (MTRAV)
Office de la langue française
Office de la protection du consommateur
Protecteur du citoyen
Régie de l'assurance-maladie du Québec
Régie des alcools, des courses et des jeux
Régie des rentes du Québec
Société d'habitation du Québec
Société de développement des entreprises culturelles
Société de développement industriel du Québec
Société de l'assurance automobile du Québec
Société de télédiffusion du Québec
Société des alcools du Québec
Société des loteries du Québec
Société immobilière du Québec
Société Innovatech du Grand Montréal
Société Innovatech du sud du Québec
Société Innovatech Québec et Chaudière-Appalaches
Société québécoise d'information juridique
Sûreté du Québec (SQ)
Tribunal administratif du Québec
Vérificateur général

Annexe 2- Caractéristiques et exigences fonctionnelles du Répertoire gouvernemental
La présente annexe présente les principales caractéristiques et exigences fonctionnelles attendues du Répertoire gouvernemental, qu'il s'agisse du système de répertoire dans son ensemble ou de ses composantes client-serveur considérées dans leurs particularités. Elle traduit les besoins perçus et s'appuie en bonne part sur d'importants travaux analogues réalisés au Gouvernement fédéral américain, auxquels se superpose l'analyse de la problématique spécifique au Gouvernement du Québec.

Pour fin de clarté, les éléments de ces caractéristiques et exigences fonctionnelles ont d'abord été regroupés, et affectés d'un numéro séquentiel, selon qu'ils se rapportent au répertoire dans son ensemble (les éléments 1 à 45) ou qu'ils ont trait plus particulièrement au(x) serveur(s) (les éléments 46 à 94) ou à l'interface client (les éléments 95 à 125). Dans chaque cas, les éléments en question ont à nouveau été regroupés cette fois-ci selon certains grands thèmes, soit essentiellement : services, normes, sécurité, gestion (information, système, opérations) et exigences de façon générale.

Le répertoire gouvernemental	Le serveur de répertoires	L'interface client
Exigences générales	Normes	Normes
Normes	Exigences fonctionnelles	Exigences fonctionnelles
Services	Gestion de l'information	Sécurité
Sécurité	Sécurité	Support à la gestion
Exigences fonctionnelles	Performance	
Gestion de l'information	Gestion des opérations	
Gestion du système		

LE RÉPERTOIRE GOUVERNEMENTAL
Le Répertoire gouvernemental devra :

Exigences générales
1. constituer l'outil de référence de base de l'inforoute gouvernementale ;
2. s'inspirer des politiques et pratiques administratives favorisant la responsabilisation des M/O et la gestion répartie des services communs ;
3. privilégier le recours à des normes ouvertes et prévoir l'interfonctionnement entre ensembles de composantes hétérogènes ;

Normes
4. élaborer son architecture de base à partir de la modélisation de l'information, des protocoles, des services et des fonctions spécifiés dans la série de recommandations X.500 de l'UIT/ISO (version 1993 et suivantes) ;
5. intégrer au besoin les protocoles, services et fonctions de répertoire spécifiées par les RFC actuels et à venir de l'Internet, notamment les développements reliés au protocole LDAP ;
6. respecter les exigences de la langue française, notamment en ce qui a trait aux jeux de caractères et au classement alphabétique ;

Services
7. mettre à la disposition de ses utilisateurs, de façon minimale, un service de Pages blanches (information sur les personnes de l'organisation), de Pages bleues (information sur l'organisation et ses services) et de Pages vertes (information sur les documents de l'organisation) ;

8. être accessible au public et aux utilisateurs gouvernementaux ;
9. être conçu de façon à soutenir de multiples applications provenant d'une large gamme d'activités administratives internes ou de prestation de services aux clientèles ;
10. incorporer des outils pour supporter les applications de télémessagerie, telles les listes de distribution ;
11. incorporer des outils pour supporter des applications de travail collaboratif, de workflow et de commerce électronique ;
12. supporter les mécanismes de sécurisation des échanges offerts par une infrastructure à clés publiques (ICP), autant pour usage interne au gouvernemental qu'avec le milieu externe ;

Sécurité

13. se conformer à la politique de sécurité des actifs informationnels en vigueur et l'étendre pour couvrir les caractéristiques de la sécurité en réseau ;
14. être protégé contre l'intrusion, les atteintes à la sécurité physique des données et des systèmes et les pannes et défaillances techniques ;
15. incorporer des procédures pour vérifier l'intégrité des informations à l'entrée et à la sortie ;
16. fournir un contrôle d'accès et des mécanismes de sécurité jusqu'au niveau des attributs ; *Le détenteur de l'information devra déterminer les utilisateurs qui peuvent y avoir accès ainsi que les circonstances et conditions gouvernant cet accès.*
17. supporter l'analyse des tentatives, fructueuses ou infructueuses, d'atteinte à la sécurité ;
18. produire et garder en mémoire pendant 30 jours toutes les vérifications d'atteinte à la sécurité ;

Exigences fonctionnelles

19. être disponible 24 heures sur 24, sept jours par semaine ;
20. démontrer un taux de réponse aux requêtes dépassant les 99,99 pour-cent ;
21. fournir un support à la fois aux utilisateurs stationnaires, quel que soit leur lieu de travail, et à ceux qui ont à se déplacer ;
22. permettre un accès au Répertoire gouvernemental qui soit intuitif et convivial, autant pour les particuliers que pour les utilisateurs dans les établissements publics ou privés ;
23. pouvoir reconnaître et traiter les requêtes selon un ordre de priorité ;
24. informer l'utilisateur lorsqu'il ne sera pas possible de donner suite à une requête ;
25. fournir aux requêtes des réponses en quasi-temps réel ;
26. permettre à ses utilisateurs de mettre fin à leurs recherches en cours d'exécution ;
27. produire un compte rendu et un journal des requêtes faites au Répertoire ;
28. permettre aux utilisateurs autorisés d'accéder aux informations où qu'elles soient dans le domaine du Répertoire gouvernemental ;
29. permettre l'ajout de composantes (matérielles et logicielles), au fur et à mesure de l'accroissement des besoins et des services ;
30. être en mesure d'accueillir des répertoires semblables mis en place dans les secteurs publics et parapublics québécois et de fournir une interface aux répertoires analogues à l'extérieur du domaine du Répertoire gouvernemental ;
31. incorporer les outils pour s'ajuster de manière dynamique aux changements de charges et de conditions sur le réseau, là où c'est techniquement et économiquement réalisable, afin de fournir la livraison des informations du Répertoire dans les délais voulus ;
32 permettre la reproduction de l'information contenue dans l'un ou l'autre des serveurs du Répertoire, afin d'en améliorer la performance ;
33. incorporer des mécanismes de mise des données en mémoire cache ;
34. afficher une interface normalisée ;

Gestion de l'information

35. assurer le caractère unique des conventions d'appellation à l'échelle gouvernementale ;
36. comporter des mécanismes appropriés pour gérer le schéma du Répertoire et notamment régir l'inscription de nouvelles classes d'objets et de nouveaux types d'attributs exigés par les circonstances ;
37. permettre aux administrateurs du réseau d'ajouter et de modifier facilement les données contenues dans le Répertoire ;
    Les administrateurs des systèmes du Répertoire gouvernemental devront utiliser des procédures d'authentification serrée afin d'obtenir l'accès administratif au Répertoire.
38. contenir des données qui soient à jour et précises ;
39. fournir un support pour l'inscription en direct des données, lorsque cela s'applique ;
40. permettre l'utilisation d'alias pour désigner des objets répertoriés ;

Gestion du système

41. adopter une structure de gestion répartie ;
42. supporter la journalisation des informations ayant trait au contrôle de la performance du système ;
43. fournir la journalisation des informations permettant de dépister les erreurs de fonctionnement ;
44. incorporer des dispositifs d'auto-évaluation et de diagnostic, ainsi que la documentation nécessaire à l'entretien du système ;
45. supporter des mécanismes permettant d'effectuer la facturation à l'usage.

LE SERVEUR DE RÉPERTOIRE

Le serveur de répertoire devra :

Normes

46. supporter le protocole d'accès au Répertoire (DAP) tel que spécifié dans les recommandations X.500 de l'UIT/ISO ;
47. supporter le protocole léger d'accès au Répertoire (LDAP) tel que spécifié dans les RFC de l'Internet ;
48. supporter le protocole de liaison opérationnelle du répertoire (DOP) tel que décrit dans les recommandations X.500 de l'UIT/ISO ;
49. supporter le protocole de miroitage (DISP) tel que spécifié dans les recommandations X.500 de l'UIT/ISO ;
50. supporter l'accès au répertoire X.500 via le Web ;
51. supporter la norme ANSI/NISO Z39.50 pour le repérage de documents ;
52. supporter les normes qui assurent le respect des particularités de la langue française : norme canadienne de classement, jeux de caractères (ISO 10646 ou autres) ;

Exigences fonctionnelles

53. accepter les liaisons à partir de toute interface client autorisée, y compris les interfaces d'applications ;
54. supporter les opérations d'interrogation et de modification de la base des entrées ;
55. permettre des recherches floues ;
56. pouvoir transmettre des résultats en différé ;
57. supporter la consultation en mode interactif par des utilisateurs ;
58. pouvoir assurer la gestion des certificats de clés publiques conformément aux spécifications de la recommandation X.509 de l'UIT/ISO ;
59. assurer des passerelles vers d'autres types de répertoires ;
60. fournir des outils pour chercher et récupérer les informations à partir de tout attribut ou combinaison d'attributs ;
61. traiter les requêtes sur la base du premier arrivé, premier servi ;
62. fournir des outils pour exécuter des mises à jour préprogrammées ;

Ceci devra inclure un changement en une seule étape d'une branche entière de l'arborescence du répertoire.

63. fournir des outils pour soumettre les mises à jour du Répertoire par lots, éliminant le besoin d'une liaison continue entre l'interface client et le serveur, le temps que le serveur traite la requête ;
64. fournir des outils pour supporter des listes de distribution ;
65. fournir des outils d'horodatage sur chaque entrée pour indiquer le moment où l'on a modifié les données et le moment où cette modification est entrée en vigueur ;
66. permettre ou interdire sur une base discrétionnaire la reproduction (miroitage) des informations entre les serveurs du Répertoire ;
67. fournir des moyens pour assurer la mise en mémoire cache des informations récupérées telles qu'autorisées par le gestionnaire local ;
68. supporter les opérations de réacheminement, de chaînage et de transmission ciblée avec les autres serveurs ;

Gestion de l'information

69. supporter toutes les classes d'objet et tous les types d'attributs normalisés tels que définis dans les recommandations X.509, X.520 et X.521 ;
70. intégrer les classes d'objets et les types d'attributs pertinents développés dans le cadre de normalisation de l'Internet ;
71. supporter les extensions à la version 1993 de la série de recommandations X.500 de l'UIT/ISO, tels les attributs collectifs et les attributs opérationnels ;
72. supporter la définition de nouvelles classes ou sous-classes d'objets (entité abstraite, structurelle ou auxiliaire) et types d'attributs spécifiques au Répertoire gouvernemental ;
73. supporter le chargement initial de données à partir d'une base de données autres qu'un répertoire X.500 ;
74. fournir des outils permettant de relocaliser et de supprimer des ramifications de l'arborescence gouvernementale ;
75. supporter les entrées d'alias ;

Sécurité

76. assurer la sécurité des informations hébergées et transmises aux utilisateurs ainsi qu'aux autres serveurs ;
77. supporter le modèle de services de sécurité spécifié par la recommandation X.500 (1993) de l'UIT/ISO ainsi que les mécanismes de contrôle d'accès spécifiées par la recommandation X.501 ;
78. disposer des outils appropriés pour procéder, selon le cas, à l'authentification simple ou serrée du point de provenance de chaque accès au Répertoire, qu'il s'agisse d'un autre serveur, d'un utilisateur ou d'une application ;
79. permettre l'application du contrôle d'accès aux entrées, aux attributs ou aux valeurs d'attributs par des utilisateurs sur une base individuelle ou à titre de membre d'un groupe ou d'une catégorie d'utilisateur ;
80. assurer au détenteur des informations contenues dans la base des entrées du Répertoire des outils pour restreindre les recherches dans cette base ;
81. pouvoir assurer l'intégrité des informations contenues dans la base des entrées du Répertoire ainsi que leur protection contre des actions accidentelles, non autorisées ou malicieuses visant à les modifier ou les altérer ;
82. pouvoir assurer la confidentialité des échanges (requêtes, réponses, transferts d'informations) auxquels donnera lieu le fonctionnement du Répertoire ;
83. être en mesure d'assurer la protection requise contre des actions accidentelles, non autorisées ou malicieuses visant à altérer les mécanismes de sécurité ou les niveaux d'accès ;
84. permettre l'acquisition sélective des données de journalisation sur la base des besoins

ainsi que des politiques et pratiques de sécurité en vigueur ;

85. créer et maintenir un registre des accès aux entrées qui font l'objet de restrictions ;
86. comporter la documentation des mesures et mécanismes de sécurité requis pour le fonctionnement du Répertoire ;

Performance

87. afficher une vitesse de traitement adéquate pour satisfaire les requêtes soumises par l'ensemble des applications ;
88. supporter la répartition de la base des entrées du Répertoire de telle manière que le temps de réponse pour les requêtes, les mises à jour et le miroitage soit acceptable ;

Gestion des opérations

89. supporter les agents de gestion spécifiés par la recommandation X.700 de l'UIT ;
90. supporter la production des rapports d'événements tel que défini dans le modèle de répertoire X.500 ;
91. produire des rapports abrégés de gestion ;
92. supporter la cueillette et la déclaration des données sur la performance du Répertoire ;
93. incorporer des outils pour recueillir et maintenir une comptabilité appropriée des transactions et de l'utilisation des ressources du Répertoire afin de supporter l'administration de la facturation ;
94. journaliser les événements et opérations permettant d'assurer la gestion de la sécurité du Répertoire et de l'information qu'il contient.

L'INTERFACE CLIENT

L'interface client devra :

Normes

95. supporter HTTP, HTML, XML, Z39.50, LDAP et, au besoin, DAP ;
96. supporter les normes qui assurent le respect des particularités de la langue française : norme canadienne de classement, jeux de caractères (ISO 10646 ou autres) ;

Exigences fonctionnelles

97. supporter la consultation en mode interactif des informations du Répertoire, la formulation et l'adressage de requêtes, la réception et l'affichage des résultats et la modification de certaines informations par les utilisateurs ;
98. permettre aux utilisateurs de recourir au Répertoire pour supporter le fonctionnement d'autres applications ;
99. disposer d'une ou de plusieurs interface(s) normalisée(s) de programmation d'applications (Application Programming Interface - API) ;
100. permettre d'établir automatiquement, au départ, une liaison avec un serveur prédéterminé, et, en cas d'échec, d'en établir une autre avec un serveur de rechange ;
101. fournir des outils pour assister les utilisateurs dans la préparation des requêtes au Répertoire ;
102. fournir aux utilisateurs des outils pour saisir des informations et les incorporer au Répertoire ;
103. fournir des outils pour les opérations de création et modification par lots d'un ensemble d'entrées du Répertoire ;
104. offrir la possibilité d'effectuer des modifications au Répertoire à des heures préprogrammées ;
105. fournir à l'utilisateur ou à l'application toutes les informations sollicitées ;
106. supporter les attributs nouveaux ou non normalisés spécifiés dans le schéma du Répertoire et qui sont propres au Répertoire gouvernemental ou à ses composantes ;
107. pouvoir interpréter une réponse d'erreur en provenance d'un serveur du Répertoire et présenter à l'utilisateur un message d'erreur facile à comprendre ;

108. être en mesure de soumettre des requêtes pour résultats différés ;
109. pouvoir rediriger une requête à un nouveau serveur du Répertoire à partir d'une référence obtenue du serveur précédent dans le cadre d'un processus de réacheminement d'une requête ;
110. retourner les informations sur l'adresse du nouveau serveur du Répertoire à l'utilisateur, si l'interface client n'est pas configurée pour rediriger la requête automatiquement ;
111. supporter la mise en mémoire cache locale des informations concernant des objets et des attributs donnant lieu à des requêtes fréquentes et fournir à l'utilisateur les outils pour sélectionner et emmagasiner ces entrées et ces attributs ;
112. pouvoir valider les paramètres des requêtes avant de soumettre celles-ci au Répertoire ;
113. fournir une aide contextuelle en direct ;
114. faciliter l'accès aux utilisateurs affectés d'handicaps physiques ;

Sécurité

115. fournir les outils pour l'authentification des utilisateurs ;
116. pouvoir s'authentifier auprès d'un serveur du Répertoire avant d'établir une liaison ;
117. fournir des outils pour supporter un contrôle sélectif d'accès aux informations du Répertoire par les utilisateurs autorisés ;
118. pouvoir assurer l'intégrité des données transmises à un serveur de répertoire et reçues de ce dernier ;
119. pouvoir assurer la confidentialité des données ;
120. interdire les accès non autorisés à ses données de configuration ;

Support à la gestion

121. fournir, au besoin, l'ensemble des outils nécessaires à l'administration du schéma du Répertoire ;
122. supporter la journalisation des activités d'interfaces client et s'assurer que ces dispositifs ne peuvent être contournés ou rendus inopérants ;
123. supporter les agents de gestion chargés de la sécurité et de l'administration du Répertoire gouvernemental ;
124. fournir des outils pour supporter la gestion de la configuration du Répertoire ;
125. fournir les informations nécessaires afin de supporter la facturation de l'utilisation du Répertoire.

Annexe 3- Définition des classes d'objet X.500/LDAP

Le contenu de cette annexe n'est fourni qu'à titre indicatif, à prendre en compte dans un cheminement plus complet à venir. Si les types des classes, leurs attributs obligatoires et leurs règles d'appellation sont des éléments ayant une grande constance, les attributs facultatifs et les règles de structure peuvent être plus aisément modifiés dans les spécifications plus formelles qui doivent être réalisées. Certaines classes ne sont pas décrites aussi complètement que d'autres, en raison même des limites de la conception détaillée présentée dans ce document.

ORGANISATION

Type : structurel
Description : Il n'y a qu'une entrée pour cette classe : le gouvernement du Québec dans son ensemble.
Attribut(s) obligatoire(s) : nom-d'organisation
Attribut(s) facultatifs : catégorie-d'affaires
description
Ensemble d'attributs localisation
Ensemble d'attributs postal
Ensemble d'attributs télécommunications
aide-au-repérage-amélioré
mot-de-passe
renvoi
Règles d'appellation : nom-d'organisation
Règles de structure : Une entrée de la classe Organisation n'a pas besoin d'une entrée supérieure. Toutefois, si c'est le cas, l'entrée immédiatement supérieure doit être l'une des classes d'objet suivantes :

- Pays
- Localité

Une entrée *Organisation* est permise immédiatement en dessous de la racine de la base des entrées.

UNITÉ-ORGANISATIONNELLE

Type : structurel
Description : Les entrées *Unité-organisationnelle* représentent des subdivisions d'une entrée Organisation. Dans le Répertoire, les ministères et organismes gouvernementaux sont de la classe *Unité-organisationnelle*, de même que les directions et services qui les constituent.

Exemples : Ministère de l'Éducation
Régie d'assurance-maladie du Québec
Attribut(s) obligatoire(s) : nom-d'unité-organisationnelle
Attribut(s) facultatifs : catégorie-d'affaires
description
Ensemble d'attributs localisation
Ensemble d'attributs postal
Ensemble d'attributs télécommunications
aide-au-repérage-amélioré
mot-de-passe

Règles d'appellation : nom-d'unité-organisationnelle
Règles de structure : Une entrée de la classe *Unité-organisationnelle* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Localité
- Organisation
- Unité-organisationnelle

RÔLE-DANS-L'ORGANISATION

Type : structurel
Description : Les entrées Rôle-dans-l'organisation représentent les postes ou les rôles au sein d'une *Organisation* et contiennent généralement le nom-distinctif complet de la personne qui occupe ce poste ou exerce ce rôle. Cette valeur peut être mise à jour régulièrement, afin de refléter les changements qui surviennent dans le personnel.
Attribut(s) obligatoire(s) : nom-courant (du poste ou du rôle)
Attribut(s) facultatifs : Ensemble d'attributs localisation
Ensemble d'attributs postal
Ensemble d'attributs télécommunications
mode-préféré-de-livraison
nom-d'unité-organisationnelle
tenant-de-rôle
(nom-distinctif de la personne,
ou d'un objet d'une autre classe
enregistré dans la Répertoire)
renvoi
Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Rôle-dans-l'organisation* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Organisation
- Unité-organisationnelle

PERSONNE-DE-L'ORGANISATION

Type : structurel
Description : Les entrées *Personne-de-l'organisation* représentent les individus qui sont à l'emploi d'une *Organisation* ou associés à celle-ci. Au gouvernement du Québec, outre les employés de tous niveaux et les contractuels, il y a aussi les personnes élues députés, les personnes désignées ou nommées (par exemple sur des Commissions). La classe d'objet *Personne-de-l'organisation* est une sous-classe de *Personne*.
Attribut(s) obligatoire(s) : nom-courant (de l'individu)

Attribut(s) facultatifs : Ensemble d'attributs localisation
Ensemble d'attributs postal
Ensemble d'attributs
télécommunications
nom-d'unité-organisationnelle
rôle-dans-l'organisation
Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Personne-de-l'organisation* doit avoir comme

entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Localité
- Organisation
- Unité-organisationnelle

GROUPE-DE-NOMS

Type : structurel
Description : La classe d'objet *Groupe-de-noms* fournit un mécanisme pour l'emmagasinage d'un ensemble non-ordonné de noms-distinctifs complets d'entrées au répertoire. Ces noms distinctifs peuvent désigner des personnes-de-l'organisation ou d'autres groupes-de-noms. Cette classe sert à supporter des groupes d'intérêt, des regroupements d'individus provenant d'une ou de plusieurs branches de l'arborescence, de communiquer entre eux : groupes de direction, groupes de travail, comités, listes de distribution. Le recours à cette classe permet de faire prendre en charge par le Répertoire les tâches de contrôle d'accès et de distribution d'information inhérentes à de multiples situations courantes de communications administratives et d'affaires.

Attribut(s) obligatoire(s) : nom-courant (par ex : Conseil des ministres);
membre-individuel

Attribut(s) facultatifs :
catégorie-d'affaires
description
détenteur
nom-d'organisation
nom-d'unité-organisationnelle
renvoi

Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Groupe-de-noms* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Localité
- Organisation
- Unité-organisationnelle

PROCESSUS-D'APPLICATION

Type : structurel
Description : La classe d'objet *Processus-d'application* fournit un mécanisme pour documenter une composante fonctionnelle utilisable dans diverses applications.
Attribut(s) obligatoire(s) : nom-courant
Attribut(s) facultatifs :
description
nom-de-localité
nom-d'unité-organisationnelle
renvoi
Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Processus-d'application* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Organisation
- Unité-organisationnelle
- Localité

ENTITÉ-D'APPLICATION

Type : structurel
Description : La classe d'objet *Entité-d'application* est une sous-composante fonctionnelle d'un *Processus-d'application* ; par exemple le routage des messages est une partie récurrente des tâches dans beaucoup de situations.

Attribut(s) obligatoire(s) : nom-courant
adresse-de-présentation

Attribut(s) facultatifs : contexte-d'application-supporté
description
nom-de-localité
nom-d'organisation
nom-d'unité-organisationnelle
renvoi

Règles d'appellation : nom-courant
Règles de structure : Les entrées de la classe *Entité-d'application* doivent avoir comme entrée immédiatement supérieure une entrée de la classe d'objet *Processus-d'application*.

COLLECTION

Type : structurel
Description : La classe d'objet *Collection* fournit un mécanisme qui permet de désigner des rassemblements d'entrées de la classe *Document*.
Attribut(s) obligatoire(s) : nom-courant
Attribut(s) facultatifs : description
nom-d'organisation
nom-d'unité-organisationnelle
nom-de-localité
renvoi

Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Collection* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Localité
- Organisation
- Unité-organisationnelle

DOCUMENT

Type : structurel
Description : La classe d'objet *Document* fournit un mécanisme qui permet de décrire et repérer grâce aux renseignements bibliographiques ou références de documents.
Attribut(s) obligatoire(s) : identifiant-de-document

Attribut(s) facultatifs : auteur
description
diffuseur
version
localisation
nom-courant
nom-d'unité-organisationnelle
nom-de-localité
titre-de-document

renvoi

Règles d'appellation : nom-courant

Règles de structure : Une entrée de la classe *Document* doit avoir comme entrée immédiatement supérieure la classe d'objet *Collection*.

SERVEUR-DE-RÉPERTOIRE

Type : structurel

Description : Cette classe d'objet, *Serveur-de-répertoire*, permet de désigner les entrées qui représentent les serveurs dans l'arborescence du Répertoire. Il s'agit d'une sous-classe de *Entité-d'application* ainsi que du serveur racine.

Attribut(s) obligatoire(s) : adresse-de-présentation
contexte-d'application-supporté
description
nom-courant
nom-d'organisation
nom-d'unité-organisationnelle

Attribut(s) facultatifs : information-de-référence
référer

Règles d'appellation : nom-courant

Règles de structure : Une entrée de la classe *Serveur-de-répertoire* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Pays
- Localité
- Organisation
- Unité-organisationnelle

ÉQUIPEMENT

Type : structurel

Description : La classe d'objet *Équipement* sert à documenter le matériel tel les imprimantes, les ordinateurs ainsi que d'autres périphériques ou matériel de réseau.

Attribut(s) obligatoire(s) : nom-courant

Attribut(s) facultatifs : description
détenteur
nom-d'organisation
nom-d'unité-organisationnelle
nom-de-localité
numéro-de-série
renvoi

Règles d'appellation : nom-courant

Règles de structure : Une entrée *Équipement* doit avoir comme entrée immédiatement supérieure l'une des classes d'objet suivantes :

- Localité
- Organisation
- Unité-organisationnelle

LOCALITÉ

Type : structurel
Description : Les entrées *Localité* peuvent représenter des entités géographiques comme une province ou un état, une ville, un édifice, etc. Elles peuvent par exemple servir à représenter les bureaux locaux ou régionaux d'un ministère ou d'un organisme.
Attribut(s) obligatoire(s) : classe-d'objet
description
nom-de-localité
Attribut(s) facultatifs : nom-de-province-ou-état
numéro-de-porte
guide-de-repérage
renvoi
Règles d'appellation : nom-de-localité
Règles de structure : Une entrée *Localité* peut avoir comme entrée immédiatement supérieure :

- Localité
- Province-état
- Pays
- Organisation
- Unité-organisationnelle

ALIAS

Type : abstrait
Description : L'*Alias* sert de base à la constitution des classes d'objet spéciales qui ne comportent qu'un pseudonyme et effectuent le renvoi à un nom-courant d'une entrée de la classe d'objet identifiée : *Localité*, *Personne-de-l'organisation*, ou *Unité-organisationnelle*. *Alias* ne s'emploie pas seul mais en association avec une classe d'objet existante. Le recours à l'*Alias* pour donner une forme alternative au nom-courant d'un objet permet d'obtenir un deuxième nom-distinctif pour un objet, tandis que plusieurs formes de nom-courant n'ont pas cet effet. Les *Alias* servent à des fins de gestion, par exemple le réacheminement de courrier après un déplacement de personnel, ou pour camoufler l'identité d'entrées spécialement sensibles.
Attribut(s) obligatoire(s) : Pseudonyme-de (nom-courant d'une entrée de la classe d'objet identifiée).
Attribut(s) facultatifs : Aucun
Règles d'appellation : *Alias* doit se combiner avec une classe d'objet, il ne s'emploie pas seul pour la création d'entrées.
Règles de structure : Aucune règle de structure ne limite l'*Alias* en tant que tel ; les règles qui s'appliquent sont celles de la classe d'objet particulière associée à l'*Alias*.

PAYS

Type : structurel
Description : Une entrée de *Pays* n'est créée qu'une fois pour un pays par l'autorité administrative concernée.
Attribut(s) obligatoire(s) : nom-de-pays
Attribut(s) facultatifs : aide-au-repérage
description
Règles d'appellation : nom-de-pays

Règles de structure : Une entrée de la classe *Pays* doit être située immédiatement en-dessous de la racine logique de l'arborescence du répertoire.

PERSONNE

Type : structurel
Description : La classe générique de *Personne* sert à la description des individus humains.
Attribut(s) obligatoire(s) : nom courant/prénom
Attribut(s) facultatifs : description
mot-de-passe
numéro-de-téléphone
renvoi
Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Personne* doit avoir comme entrée immédiatement supérieure la racine logique de l'arborescence du répertoire.

PERSONNE-À-DOMICILE

Type : structurel
Description : Les entrées de la classe *Personne-à-domicile* servent à décrire des personnes dans le contexte de leur résidence personnelle ou leur domicile. Cette classe pourrait éventuellement accueillir la clientèle gouvernementale des personnes vivant au Québec. Pour les *Personnes-de-l'organisation*, le domicile est un objet approprié de renseignements pour les directions des Ressources humaines.
Attribut(s) obligatoire(s) : nom-de-localité
Attribut(s) facultatifs : catégorie-d'affaires
Ensemble d'attributs localisation
Ensemble d'attributs postal
Ensemble d'attributs télécommunications
mode-de-livraison-préféré
Règles d'appellation : nom-courant
Règles de structure : Une entrée de la classe *Personne-à-domicile* doit avoir pour entrée immédiatement supérieure la classe *Personne*.

GROUPE-DE-NOMS-UNIQUES

Type : structurel
Description : La classe *Groupe-de-noms-uniques* sert à définir des entrées qui contiennent une liste non ordonnée de noms d'objets ou d'autres groupes de noms dont l'intégrité est garantie. Cette liste est stable et n'est modifiée que par une action administrative intentionnelle. Le fait d'être membre d'un groupe constitue un laissez-passer dans un contrôle d'accès.

Attribut(s) obligatoire(s) : membre-unique
nom-courant
Attribut(s) facultatifs : catégorie-d'affaires
description
détenteur
nom-de-l'unité-organisationnelle
nom-de-l'organisation
renvoi

Règles d'appellation : groupe-de-noms-uniques
Règles de structure : Une entrée de la classe *Groupe-de-noms-uniques* peut avoir pour classe immédiatement supérieure la racine logique de l'arborescence du répertoire ou :

- Localité
- Organisation
- Unité-organisationnelle

SOURCE-DE-CONTRÔLE-DES-CERTIFICATS-RÉVOQUÉS

Type : structurel
Description :
Attribut(s) obligatoire(s) : nom-courant
liste-de-révocation-de-certificats
liste-de-révocation-d'autorité
Attribut(s) facultatifs :
Règles d'appellation : nom-courant
Règles de structure : A comme classe immédiatement supérieure l'autorité de certification émettrice.

SOUS-ENTRÉE

Type : structurel
Description : La classe *Sous-entrée* sert à décrire les sous-arbres pour l'administration des services x.500.
Attribut(s) obligatoire(s) : nom-courant
spécification-de-sous-arbre
Attribut(s) facultatifs :
Règles d'appellation :
Règles de structure :

DOMAINE

Type : structurel
Description : Un *Domaine* consiste en une branche d'un répertoire, spécifiée par une *Sous-entrée* et son *Sous-schéma*, sous le contrôle d'une autorité administrative.
Attribut(s) obligatoire(s) : nom-courant
Attribut(s) facultatifs : catégorie-d'affaires
description
Ensemble-d'attributs-télécommunications
Ensemble-d'attributs-postal
mot-de-passe
Règles d'appellation : nom-courant
Règles de structure : Directement sous la racine logique.

PERSONNE-BRANCHÉE

Type : structurel
Description : Sous-classe de *Personne-de-l'organisation* pour les exigences courantes dans le déploiement de répertoires Internet et intranet (en ajoutant quelques attributs couramment requis à ceux de X.521 sur *Personne-de-l'organisation*).

Note : Dans la troisième section, cette classe se trouve entièrement intégrée au modèle de *Personne-de-l'organisation*.
Attribut(s) obligatoire(s) : nom-courant
Attribut(s) facultatifs : tous les attributs héritables de Personne-de-l'organisation ainsi que :

- audio
- photo-jpeg
- URI-étiqueté
- adresse-de-télémessagerie
- cellulaire
- certificat-d'utilisateur
- identifiant-d'utilisateur
- certificat-d'utilisateur-S/MIME

Règles d'appellation : personne-branchée
Règles de structure : A comme classe immédiatement supérieure : *Personne-de l'organisation*.

LOCAL

Type : structurel
Description :
Attribut(s) obligatoire(s) : nom-courant
Attribut(s) facultatifs : numéro-de-téléphone
renvoi
description
numéro-de-local
Règles d'appellation : local
Règles de structure : A comme classe immédiatement supérieure :

- Localité
- Organisation
- Unité-organisationnelle

COMPTE

Type : structurel
Description :
Attribut(s) obligatoire(s) : identifiant-d'utilisateur
Attribut(s) facultatifs : ordinateur-hôte
unité-organisationnelle
organisation
renvoi
description
Règles d'appellation : compte
Règles de structure : A comme entrée immédiatement supérieure :

- Localité
- Organisation
- Unité-organisationnelle
- Personne-de-l'organisation

OBJET-RATTACHÉ-À-UN-DOMAINE

Type : structurel
Description :
Attribut(s) obligatoire(s) : domaine-associé
Attribut(s) facultatifs :
Règles d'appellation : objet-rattaché-à-un-domaine
Règles de structure : directement sous la racine

OBJET-SIMPLE-DE-SÉCURITÉ

Type : structurel
Description :
Attribut(s) obligatoire(s) : mot-de-passe
Attribut(s) facultatifs :
Règles d'appellation : objet-simple-de-sécurité
Règles de structure : A comme entrée immédiatement supérieure :

- Personne-de-l'organisation
- Personne

RÉFÉRER

Type : structurel
Description : Cette classe d'objet, *Référer*, sert à représenter de l'information de référence générique dans les répertoires LDAP et peut, via les URI, pointer sur d'autres répertoires, qu'ils soient LDAP ou autre. L'information de référence en cause est relative à l'environnement de serveurs et de services dans l'inforoute. Cette classe d'objet est à l'usage des serveurs et n'est généralement pas visible pour les utilisateurs.
Attribut(s) obligatoire(s) :
Attribut(s) facultatifs : URI-étiqueté
URL
Règles d'appellation :
Règles de structure : Directement sous la racine

SOUS-ENTRÉE-D'ATTRIBUT-COLLECTIF

Type : auxiliaire
Description : Cette classe d'objet est importante dans l'administration des serveurs X.500. Elle contient un ou des attributs dits collectifs, c'est-à-dire qu'ils sont reproduits dans chacune des entrées de cette branche du Répertoire qu'une sous-entrée concerne. En d'autres mots, les attributs collectifs sont partagés par un ensemble d'entrées et contribuent à un emmagasinage plus économique.

Les attributs de télécommunications, postaux, de localisation, d'organisation sont souvent l'objet d'un modèle en cascade des éléments d'information partagés grâce au mécanisme des attributs collectifs à placer à la racine d'un domaine sous une autorité administrative du répertoire.
Attribut(s) obligatoire(s) :
Attribut(s) facultatifs :
Règles d'appellation :
Règles de structure :

SOUS-SCHÉMA

Type : auxiliaire
Description : Cette classe d'objet est importante pour enregistrer des sous-schémas dans les serveurs X.500. Le *Sous-schéma* spécifie les attributs utilisés dans un domaine du répertoire. Il contient les types-d'attributs, les classes d'objet, les règles de structure, les syntaxes et les règles-d'appariement. Le *Schéma* du Répertoire est constitué de Sous-schémas disjoints, sans recouvrement.
Attribut(s) obligatoire(s) :
Attribut(s) facultatifs : règles-de-structure-de l'arborescence
formes-de-noms
règles-de-contenu
classes-d'objet
types-d'attributs
usage-des-règles-d'appariement
Règles d'appellation : nom-courant
Règles de structure :

CONTRÔLE-D'ACCÈS-DE-SOUS-ENTRÉE

Type : auxiliaire
Description : Cette classe d'objet est importante dans l'administration de serveurs X.500. Elle s'utilise en conjonction avec la classe Sous-entrée. Elle contient de l'information prescriptive du contrôle d'accès à exercer dans cette branche du répertoire que la *Sous-entrée* concerne. Les opérations se catégorisent en repérer, lire, modifier, tandis que l'information se catégorise en public, protégé (groupe), confidentiel.
Attribut(s) obligatoire(s) :
Attribut(s) facultatifs :
Règles d'appellation :
Règles de structure :

INFORMATION-DE-SÉCURITÉ-D'UTILISATEUR

Type : auxiliaire
Description : Listes de groupes dont l'utilisateur est membre, et liste des autorisations de l'utilisateur.
Attribut(s) obligatoire(s) : information-de-sécurité-d'utilisateur
Attribut(s) facultatifs : algorithmes-disponibles
Règles d'appellation :
Règles de structure : directement sous la racine logique.

UTILISATEUR-ÉTROITEMENT-IDENTIFIÉ

Type : auxiliaire
Description : La classe *Utilisateur-étroitement-identifié* sert à définir les entrées pour des objets qui peuvent être étroitement identifiés grâce à l'authentification d'identité permise par les certificats de clé publique.
Attribut(s) obligatoire(s) : certificat-d'utilisateur.
Attribut(s) facultatifs :
Règles d'appellation :
Règles de structure : Directement sous la racine.

AUTORITÉ-DE-CERTIFICATION

Type : auxiliaire
Description : La classe *Autorité-de-certification* sert à définir les entrées pour les objets qui agissent comme source de distribution des certificats. Les autorités de certification sont définies dans ISO/IEC 9594-8.
Attribut(s) obligatoire(s) : certificat-d'autorité-de-certification
liste-de-révocation-de-certificats
liste-de-révocation-d'autorité
Attribut(s) facultatifs : paire-de-certification-réciproque
Règles d'appellation : nom-courant
Règles de structure : Directement sous la racine logique.

AUTORITÉ-DE-CERTIFICATION-V2

Type : auxiliaire
Description :
Attribut(s) obligatoire(s) :
Attribut(s) facultatifs :
Règles d'appellation :
Règles de structure : Sous-classe d'*Autorité-de-certification*.

OBJET-URI-ÉTIQUETÉ

Type : auxiliaire
Description : L'utilité de cette classe d'objet est de pouvoir être ajoutée aisément à des objets existants du répertoire en vue de permettre l'inclusion normalisée de valeurs d'URI dans une entrée. Cela n'empêche d'ailleurs pas l'inclusion directe du type d'attribut URI-étiqueté dans d'autres classes d'objets. Défini dans RFC 2079 (janvier 1997). L'étiquette doit avoir valeur indicative pour l'utilisateur.
Attribut(s) obligatoire(s) : aucune
Attribut(s) facultatifs : URI-étiqueté
Règles d'appellation : objet-URI-étiqueté
Règles de structure : Directement sous la racine

Annexe 4- Glossaire

Glossaire français-anglais

A
accès frontal : front-end
accord de miroitage : shadowing agreement
adresse-d'autre-télémessagerie : otherMailbox
adresse-de-présentation : presentationAddress
adresse-de-télémessagerie : mail
adresse-domiciliaire : homePostalAddress
adresse-enregistrée : registeredAddress
adresse-postale : postalAddress
adresse-X121 : x121Address
Agenda : @calendar
aide-au-repérage : searchGuide
aide-au-repérage-amélioré : enhancedSearchGuide
ajouter : Add
algorithmes-disponibles : supportedAlgorithms
Alias : alias
arborescence du répertoire : Directory Information Tree (DIT)
attribut : attribute
audio : audio
Autorité-de-certification : certificationAuthority
Autorité-de-certification-V2 : certificationAuthority-V2

B
base des entrées du répertoire : Directory Information Base (DIB)
biclé : asymetric key pair
borne interactive : kiosk

C
casier-postal : postOfficeBox
catégorie-d'affaires : businessCategory
catégorie-d'utilisateur : userClass
cellulaire : mobile
cellulaire-personnel : personalMobile
certificat-d'autorité-de-certification : cACertificate
certificat-d'utilisateur : userCertificate
certificat-d'utilisateur-S/MIME : userS/MIMECertificate
chaînage : chaining
chemin-de-certification : certificatePath
chiffrement : encryption
classe-d'objet : objectClass
classe-d'objet-extensible : extensibleObject
code-postal : postalCode
Collection : documentSeries
comparer : Compare
Compte : account
consommateur-miroir : shadow consumer
consulter : Browse

contexte d'appellation : naming context
contexte-d'application-disponible : supportedApplicationContext
contextes-d'appellation : namingContexts
Contrôle-d'accès-de-sous-entrée : accessControlSubentry
contrôles-disponibles : supportedControl
convention d'appellation : naming convention
copie-miroir : shadow copy
copies miroir d'information : shadow information
création-horodatée : createTimestamp

D
déchiffrement : decryption
détenteur : owner
deuxième-prénom : middleName
Domaine : domain
domaine de gestion-du-répertoire : directoryManagementDomain (DMD)
domaine-associé : associatedDomain
données référentielles : knowledge information
duplication : replication

E
embranchement : subtree
empreinte : digest
Ensemble-d'attributs-localisation : LocaleAttributeSet
Ensemble-d'attributs-postal : PostalAttributeSet
Ensemble-d'attributs-télécommunications : TelecommunicationsAttributeSet
entente d'association : binding agreement
Entité-d'application : applicationEntity
entrée : entry
entrée-sur-soi : thisEntry
enveloppe numérique : digital envelope
Équipement : device
espace d'appellation : name space
exporter : Export
extensions-disponibles : supportedExtension

F
faire une recherche : search
feuilleter : browse
fiche-de-domaine : dnsRecord
formulaire-de-requête : informationRequestForm
fournisseur-miroir : shadow supplier

G
gestionnaire : manager
gestionnaire-de-serveur-de-répertoire : dSAManager
groupe-d'utilisateurs : userGroup
Groupe-de-noms : groupOfNames
Groupe-de-noms-uniques : uniqueGroupOfNames

H
hachage : hash
heures-d'ouverture : hoursofOperation

I
identifiant-d'édifice : houseIdentifier
identifiant-d'objet : ObjectIdentifier (OID)
identifiant-d'utlisateur : userid (uid)
identifiant-de-terminal-télétex : teletexTerminalIdentifier
identifiant-unique : uniqueIdentifier
identifiant-unique-X500 : x500UniqueIdentifier
immatriculation-d'automobile : carLicense
importer : Import
indicateur-de-destination : destinationIndicator
information-de-protocole : protocolInformation
information-de-référence : knowledgeInformation
Information-de-sécurité-d'utilisateur : userSecurityInformation
informations de référence : knowledge information
initiales : initials
interface client du répertoire : Directory User Agent (DUA)

L
Langage de balisage hypertexte : Hyper-Text Markup Language (HTML)
langue(s) : language
langue-préférée : preferredLanguage
liaison au répertoire : directory binding
lire : Read
liste-delta-de-révocation : deltaRevocationList
liste-de-révocation-d'autorité : authorityRevocationList
liste-de-révocation-de-certificat : certificateRevocationList
Local : room
Localité : locality (l)
logo : thumbnailLogo

M
mécanismes-SASL-disponible : supportedSASLMechanisms
membre : member
membre-de-l'unité-organisationnelle : organizationalUnitMember
membre-unique : uniqueMember
miroitage : mirroring, shadowing
miroitage primaire : primary shadowing
miroitage secondaire : secondary shadowing
mise en mémoire cache : caching
mode-de-livraison-préféré : preferedDeliveryMethod
modification-horodatée : modifyTimestamp
modifier : Modify
mot-de-passe : userPassword

N
nom : name
nom courant : Common Name (CN)
nom distinctif : Distinguished Name (DN)
nom distinctif relatif : Relative Distinguished Name (RDN)
nom-courant : commonName (cn)
nom-d'objet-d'alias : aliasedObjectName
nom-de-bureau-pour-livraison-physique : physicalDeliveryOfficeName
nom-de-domaine-de-gestion-du-répertoire : dmdname
nom-de-famille : surname (sn)
nom-de-l'organisation : organizationalUnit
nom-de-l'unité-organisationnelle : organizationalUnitName
nom-de-localité : localityName
nom-de-modificateur : modifiersName
nom-de-pays : countryName (c)
nom-de-province-ou-état : stateOrProvinceName (st)
nom-distinctif : distinguishedName
nom-du-créateur : creatorName
numéro-d'employé : employeeNumber
numéro-d'identité-organisationnelle : departmentNumber
numéro-de-local : roomNumber
numéro-de-porte : streetAddress
numéro-de-série : serialNumber
numéro-de-télécopieur : facsimileTelephoneNumber
numéro-de-téléphone : telephoneNumber
numéro-de-télex : telexNumber
numéro-RNIS-international : internationalISDNNumber

O
Objet-simple-de-sécurité : simpleSecurityObject
Objet-rattaché-à-un-domaine : domainRelatedObject
Objet-URI-étiqueté : labeledURIObject
option-préférée-de-messagerie : mailPreferenceOption
ordinateur-hôte : host
organigramme : organizationalChart
Organisation : organization
ossature : backbone

P
pagette : pager
pagette-personnelle : personalPager
paire-de-certification-réciproque : crossCertificatePair
partie-d'un-domaine : dc (domainComponent)
« passe-temps » : « drink »
Pays : country (C)
personne : person
Personne-à-domicile : residentialPerson
Personne-branchée : inetOrgPerson
Personne-de-l'organisation : organizationalPerson
photo : jpegPhoto
point d'accès reconnu : Well Known Entry Point (WEP)

point-de-contact : pointofContact
pointeurs référentiels : knowledge reference pointers
prénom-usuel : givenName
Processus-d'application : applicationProcess
production de copies miroir : shadowing
protocole allégé d'accès au répertoire : Lightweight Directory Access Protocol (LDAP)
protocole d'accès au répertoire : Directory Access Protocol (DAP)
protocole de liaison opérationnelle du répertoire : Directory Operational Binding Protocol (DOP)
protocole de miroitage : Directory Information Shadowing Protocol (DISP)
Protocole de transport hypertexte : Hyper-Text Transfer Protocol (HTTP)
protocole du système de répertoire (DSP) : Directory System Protocol

Q
qualificatif-de-domaine : dnQualifier

R
racine : root
racine logique : top
ramification de l'arborescence : subtree
réacheminement : referral (chap. 2)
référence croisée : cross reference
référence immédiatement inférieure : non-specific subordinate reference
référence immédiatement supérieure : immediate superior reference
référence inférieure : subordinate reference
référence supérieure : superior reference
référer-à-supérieur : superior Reference
référer-par-nom : named Reference
référer-sans-nom : unnamed Reference
règles-d'appariement : matchingRules
renommer : Rename
renvoi : seeAlso
repérer-par-filtre : FilterMatch
répertoire : directory
Référer : referral (chap. 5)
résolution : dereferencing
révéler-en-cas-d'erreur : DiscloseOnError
révéler-le-nom-distinctif : ReturnDN
Rôle-dans-l'organisation : organizationalRole

S
secrétaire : secretary
serveur de répertoire : Directory Server Agent (DSA)
serveur maître : master DAS
serveur-de-relève : altServer
Serveur-de-répertoire : directorySystemAgent
serveur-maître : master DSA
serveur-miroir : shadow DSA
signature numérique : digital signature
soi : Self
Source-de-contrôle-des certificats-révoqués : (certificateRevocationList) cRLDistributionPoint
sous-arborescence : subtree

Sous-entrée : subEntry
Sous-entrée-d'attribut-collectif : collectiveAttributeSubentry
(Sous-entrée) entrée-de-sous-schéma : subschemaEntry(Subentry)
Sous-schéma : subschema
suffixe-de-nom : generationQualifier
supprimer : Remove
syntaxes-LDAP-disponibles : ldapSyntaxes

T
télécopieur-à-domicile : homeFax
téléphone-à-domicile : homePhone
tenant-de-rôle : roleOccupant
titre-personnel : personalTitle
tous-les-types-d'attribut-d'utilisateur : allUserAttributeTypes
tous-les-utilisateurs : allUsers
toutes-les-valeurs-d'attribut : allAttributeValues
transmission ciblée : multicasting
type-d'attribut : attributeType
type-d'employé : employeeType

U
unité organisationnelle : organisational unit
Unité-organisationnelle : organizationalUnit
URI-étiqueté : labeledURI
usage-de-règles-d'appariement : matchingRulesUse
Utilisateur-du-gouvernement : governementUser
Utilisateur-étroitement-identifié : strongAuthentificationUser

V
valeur-sur-soi : selfValue
versions-LDAP-disponibles : supportedLDAPVersion

Glossaire anglais-français

A
@calendar: agenda
accessControlSubentry: Contrôle-d'accès-de-sous-entrée
account: Compte
Add: ajouter
alias: Alias
aliasedObject Name: nom-d'objet-d'alias
allAttributeValues: toutes-les-valeurs-d'attribut
allUserAttributeTypes: tous-les-types-d'utilisateur
allUsers: tous-les-utilisateurs
altServer: serveur-de-relève
applicationEntity: Processus-d'application
applicationProcess: Entité-d'application
associatedDomain: domaine-associé
asymetric key pair: biclé
attribute: attribut
attributeType: type-d'attribut
audio: audio
authorityRevocationList: liste-de-révocation-d'autorité

B
backbone: ossature
binding agreement: entente d'association
Browse: consulter
businessCategory: catégorie-d'affaires

C
cACertificate: certificat-d'autorité-de-certification
caching: mise en mémoire cache
carLicense: immatriculation-d'automobile
carLicense: immatriculation-d'automobile
certificatepath: chemin-de-certification
certificatePath: chemin-de-certification
certificateRevocationList: liste-de-révocation-de-certificat
certificationAuthority: Autorité-de-certification
certificationAuthority-V2: Autorité-de-certification-V2
chaining : chaînage
collectiveAttributeSubentry: Sous-entrée-d'attribut-collectif
Common Name (CN): nom courant
commonName (cn): nom-courant
Compare: comparer
country (C): Pays
countryName (c): nom-de-pays
createTimestamp: création-horodatée
creatorsName: nom-du-créateur
cRLDistributionPoint: Source-de-contrôle-des certificats-révoqués
cross reference: référence croisée
crossCertificatePair: paire-de-certification-réciproque

D
dc (domainComponent): partie-d'un-domaine
decryption: déchiffrement
deltaRevocationList: liste-delta-de-révocation
departmentNumber: numéro-d'identité-organisationnelle
dereferencing: résolution
destinationIndicator: indicateur-de-destination
device: Équipement
digest: empreinte
digital envelope: enveloppe numérique
digital signature: signature numérique
directory: répertoire
Directory Access Protocol (DAP): protocole d'accès au répertoire
directory binding: liaison au répertoire
Directory Information Base (DIB): base des entrées du répertoire
Directory Information Shadowing Protocol (DISP): protocole de miroitage
Directory Information Tree (DIT): arborescence du répertoire
Directory Operational Binding Protocol (DOP): protocole de liaison opérationnelle du répertoire
Directory System Agent (DSA): serveur de répertoire
Directory System Protocol (DSP): protocole du système de répertoire
Directory User Agent (DUA): interface client du répertoire
directoryManagementDomain (DMD): domaine de gestion-du-répertoire
directorySystemAgent: Serveur-de-répertoire
DiscloseOnError: révéler-en-cas-d'erreur
distinguishedName (DN): nom-distinctif
dmdname: nom-de-domaine-de gestion du-répertoire
dnQualifier: qualificatif-de-domaine
dnsRecord: fiche-de-domaine
documentSeries: Collection
domain: Domaine
domainRelatedObject: objet-rattaché-à-un-domaine
« drink »: « passe-temps »
DSAManager: gestionnaire-de-serveur-de-répertoire

E
employeeNumber: numéro-d'employé
employeeType: type-d'employé
encryption: chiffrement
enhancedSearchGuide: aide-au-repérage-amélioré
entry: entrée
Export: exporter
extensibleObject: classe-d'objet-extensible

F
facsimileTelephoneNumber: numéro-de-télécopieur
Filter Match: repérer-par-filtre
front-end: accès frontal

G
generationQualifier: suffixe-de-nom
givenName: prénom-usuel
governementUser: Utilisateur-du-gouvernement
GroupOfNames: Groupe-de-noms

H
hash: hachage
homeFax: télécopieur-à-domicile
homePhone: téléphone-à-domicile
homePostalAddress: adresse-domiciliaire
host: ordinateur-hôte
hoursofOperation: heures-d'ouverture
houseIdentifier: identifiant-d'édifice
Hyper-Text Markup Language (HTML): Langage de balisage hypertexte
Hyper-Text Transfer Protocol (HTTP): Protocole de transport hypertexte

I
immediate superior reference: référence immédiatement supérieure
Import: importer
inetOrgPerson: Personne-branchée
informationRequestForm: formulaire-de-requête
initials: initiales
internationalISDNNumber: numéro-RNIS-international

J
jpegPhoto: photo

K
kiosk: borne interactive
knowledge Information: information-de-référence
knowledge information: informations de référence, données référentielles
knowledge reference pointers: pointeurs référentiels

L
labeledURI: URI-étiqueté
labeledURIObject: Objet-URI-étiqueté
language: langue(s)
ldapSyntaxes: syntaxes-LDAP-disponibles
Lightweight Directory Access Protocol (LDAP): protocole allégé d'accès au répertoire
LocaleAttributeSet: Ensemble-d'attributs-localisation
locality (l): Localité
localityName: nom-de-localité

M
mail: adresse-de-télémessagerie
mailPreferenceOption: option-préférée-de-messagerie
manager: gestionnaire
master DAS: serveur maître
matchingRules: règles-d'appariement
matchingRulesUse: usage-de-règles-d'appariement

member : membre
middleName: deuxième-prénom
mirroring: miroitage
mobile: cellulaire
modifiersName: nom-de-modificateur
Modify: modifier
modifyTimestamp: modification-horodatée
multicasting: transmission ciblée

N
name: nom
name space: espace d'appellation
named Reference: référer-par-nom
naming context: contexte d'appellation
namingContexts: contextes-d'appellation
naming convention: convention d'appellation :
non-specific subordinatereference: référence immédiatement inférieure

O
objectClass: classe-d'objet
ObjectIdentifier (OID): identifiant-d'objet
organisational unit: unité organisationnelle
Organization (O): Organisation
organizationalChart: organigramme
OrganizationalPerson: Personne-de-l'organisation
OrganizationalRole: rôle-dans-l'organisation
organizationalUnit: nom-de-l'organisation
OrganizationalUnit: Unité-organisationnelle
OrganizationalUnitMember: membre-de-l'unité-organisationnelle
organizationalUnitName: nom-de-l'unité-organisationnelle
otherMailbox: adresse-d'autre-télémessagerie
owner: détenteur

P
pager: pagette
person: personne
personalMobile: cellulaire-personnel
personalPager: pagette-personnelle
personalTitle: titre-personnel
physicalDeliveryOfficeName: nom-de-bureau-pour-livraison physique
pointofContact: point-de-contact
postalAddress: adresse-postale
PostalAttributeSet: Ensemble-d'attributs-postal
postalCode: code-postal
postOfficeBox: casier-postal
preferedDeliveryMethod: mode-de-livraison-préféré
preferredLanguage: langue-préférée
presentationAddress: adresse-de-présentation
primary shadowing: miroitage primaire
protocolInformation: information-de-protocole

R
Read: lire
referral: réacheminement (chap. 2)
referral: référer (chap. 5)
registeredAddress: adresse-enregistrée
relative distinguished name (RDN): nom distinctif relatif
Remove: supprimer
Rename: renommer
replication: duplication
residentialPerson: Personne-à-domicile
ReturnDN: révéler-le-nom-distinctif
roleOccupant: tenant-de-rôle
room: Local
roomNumber: numéro-de-local
root: racine
root: racine

S
search: faire une recherche
searchGuide: aide-au-repérage
secondary shadowing: miroitage secondaire
secretary: secrétaire
seeAlso: renvoi
Self: Soi
selfValue: valeur-sur-soi
serialNumber: numéro-de-série
shadow consumer: consommateur-miroir
shadow copy: copie-miroir
shadow DSA: serveur-miroir
shadow information: copies-miroir d'information
shadow supplier: fournisseur-miroir
shadowing: production de copies-miroir
shadowing: miroitage
shadowing agreement: accord de miroitage
simpleSecurityObject: Objet-de-sécurité-simple
stateOrProvince Name (st): nom-de-province-ou-état
streetAddress: numéro-de-porte
strongAuthentificationUser: Utilisateur-étroitement-identifié
subEntry: Sous-entrée
subordinate reference: référence inférieure
subschema: Sous-schéma
subschemaEntry(Subentry): entrée-de-sous-schéma (sous-entrée)
subtree: embranchement, ramification, sous-arborescence
superior Reference: référer-à-supérieur
superior reference: référence supérieure
supportedAlgorithms: algorithmes-disponibles
supportedApplicationContext: contexte-d'application-disponible
supportedControl: contrôles-disponibles
supportedExtension: extensions-disponibles
supportedLDAPVersion: versions-LDAP-disponibles
supportedSASLMechanisms: mécanismes-SASL-disponibles
surname (sn): nom-de-famille

T
TelecommunicationsAttributeSet: Ensemble-d'attributs-télécommunications
telephoneNumber: numéro-de-téléphone
teletexTerminalIdentifier: identifiant-de-terminal-télétex
telexNumber: numéro-de-télex
thisEntry : entrée-sur-soi
thumbnailLogo: logo
top: racine-logique

U
uniqueGroupOfNames: Groupe-de-noms-uniques
uniqueIdentifier: identifiant-unique
uniqueMember: membre-unique
unnamedReference: référer-sans-nom
userCertificate: certificat-d'utilisateur
userClass: catégorie-d'utilisateur
userGroup: groupe-d'utilisateurs
userid (uid): identifiant-d'utlisateur
userPassword: mot-de-passe
userS/MIMECertificate: certificat-d'utilisateur-S/MIME
userSecurityInformation: Information-de-sécurité-d'utilisateur

W
Well Known Entry Point (WEP): point d'accès reconnu

X
X121Address: adresse-X121
x500UniqueIdentifier: identifiant-unique-X500

Annexe 5- Répertoires gouvernementaux - Aperçu des services

Aperçu des répertoires gouvernementaux

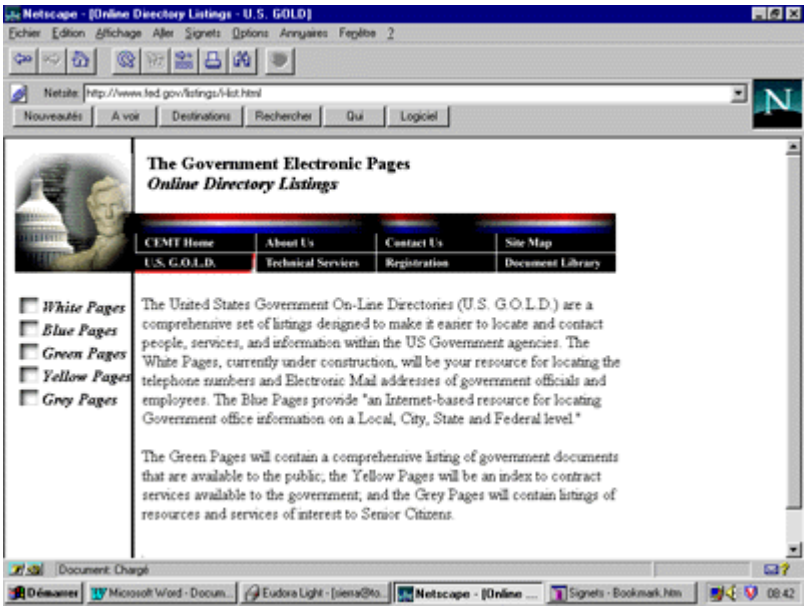


Figure A5-1 Répertoire gouvernemental américain

Figure A5-2 Répertoire gouvernemental australien

Figure A5-3 Répertoire fédéral australien

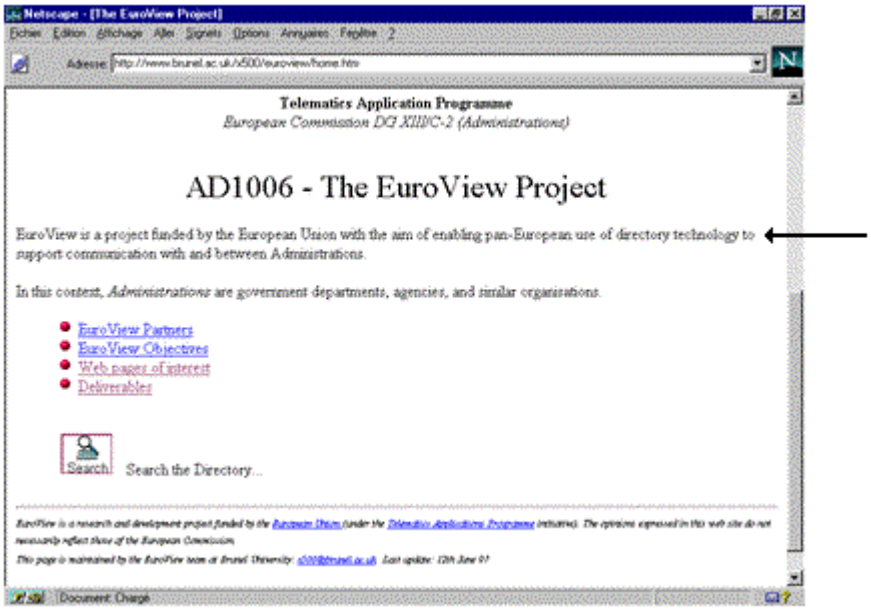


Figure A5-4 Répertoires pour les Administrations européennes

Service Pages blanches
Répertoire gouvernemental américain

Figure A5-5 Page d'accueil

Figure A5-6 Requête

Figure A5-7 Résultat 1)

Figure A5-8 Résultat 2)

Service Pages blanches
Répertoire fédéral australien

Figure A5-9 Page d'accueil

Figure A5-10 Requête

Figure A5-11 Résultat 1)

Figure A5-12 Résultat 2)

Service Pages blanches
Répertoire gouvernemental canadien

Figure A5-13 Page d'accueil

Figure A5-14 Requête

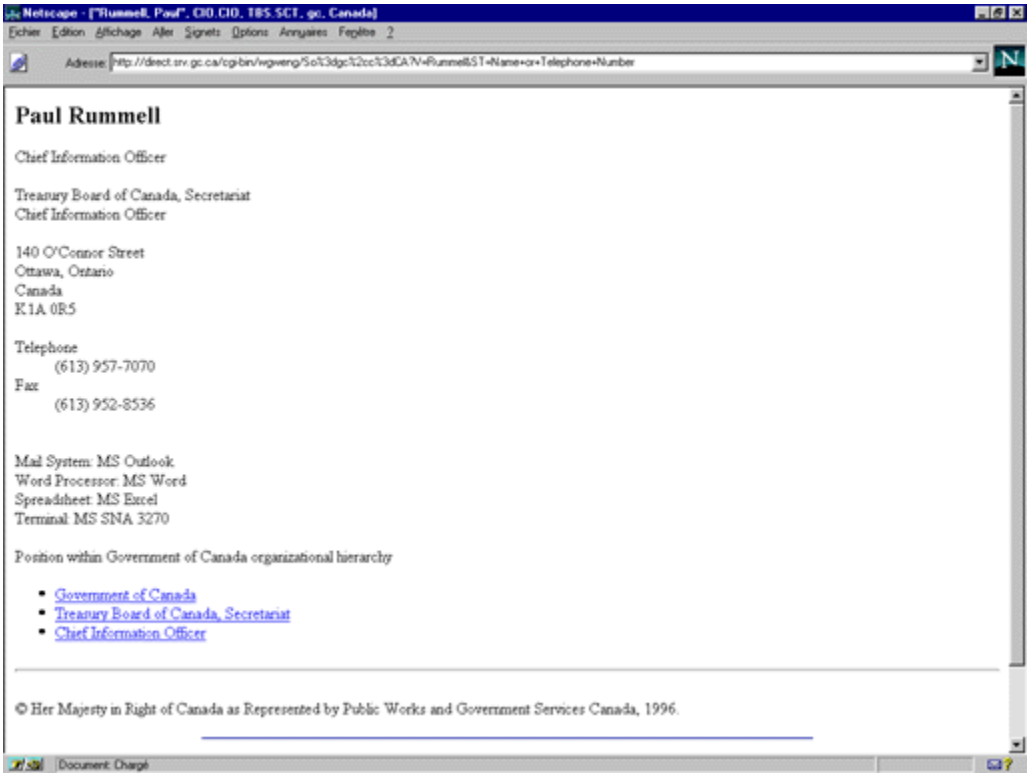


Figure A5-15 Résultat

Service Pages blanches
Gouvernement britannique

Figure A5-16 Page d'accueil

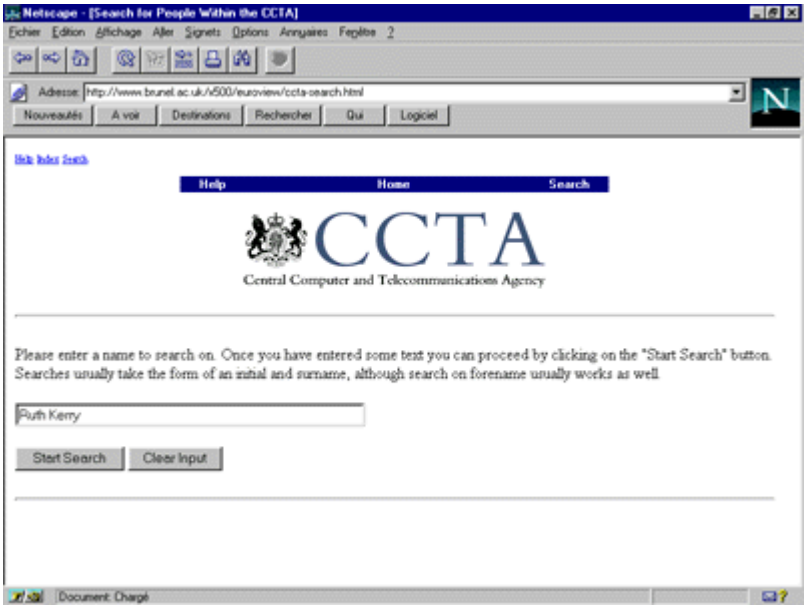


Figure A5-17 Requête

Figure A5-18 Résultat

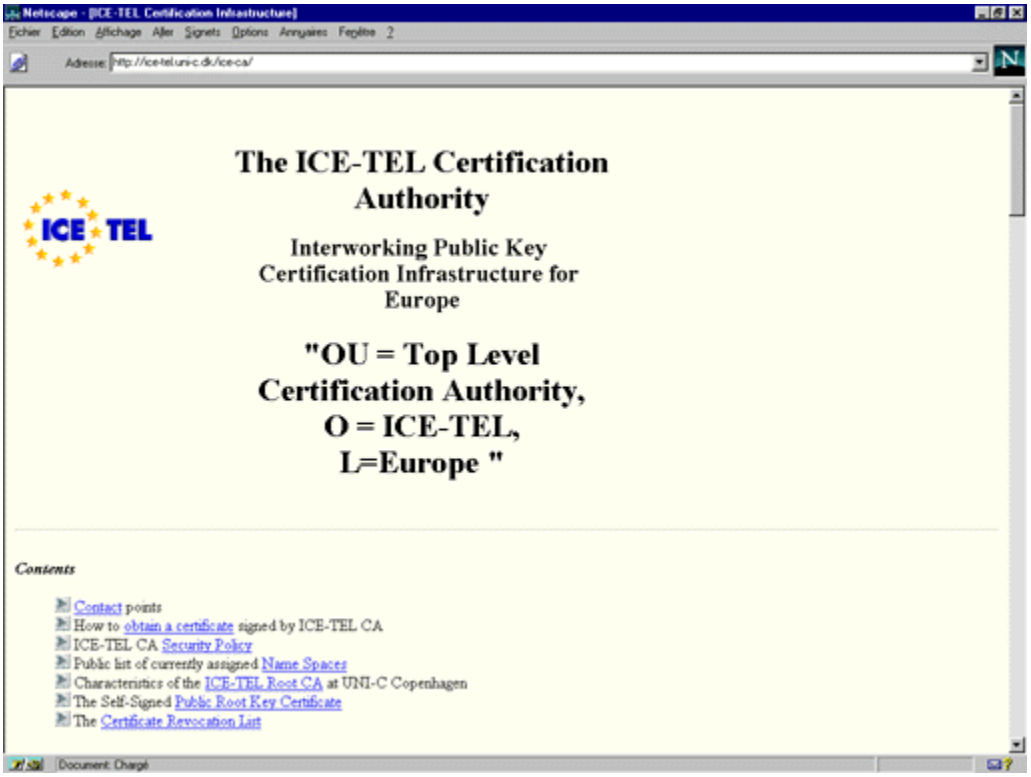


Figure A5-19 Autorité de certification
Page d'accueil

Service Pages bleues
(volet structures administratives et fonctions)
Répertoire fédéral australien

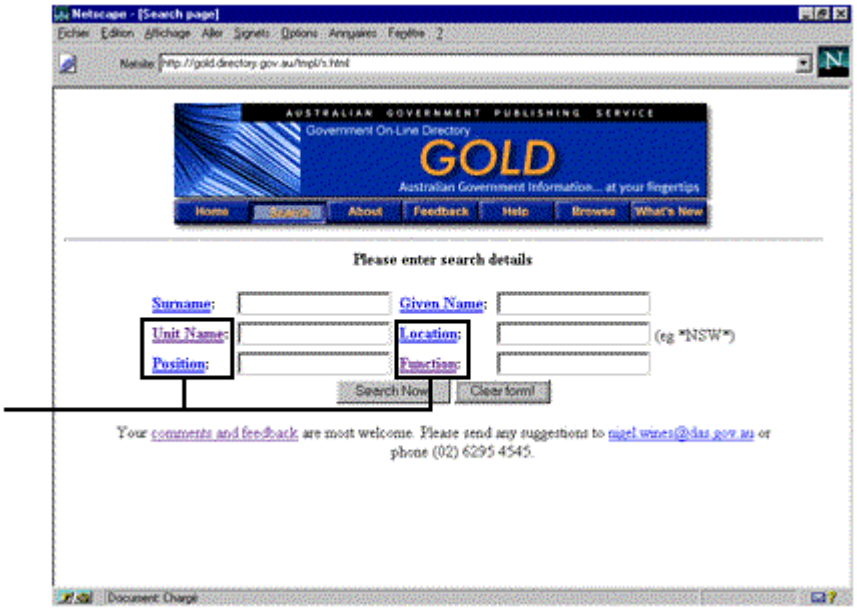


Figure A5-20 Page d'accueil

Figure A5-21 Requête

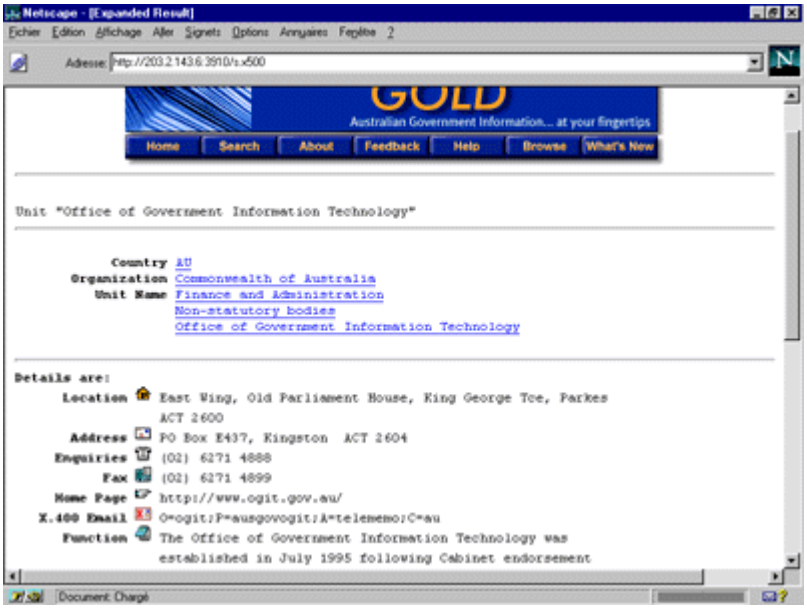


Figure A5-22 Résultat (1 de 2)

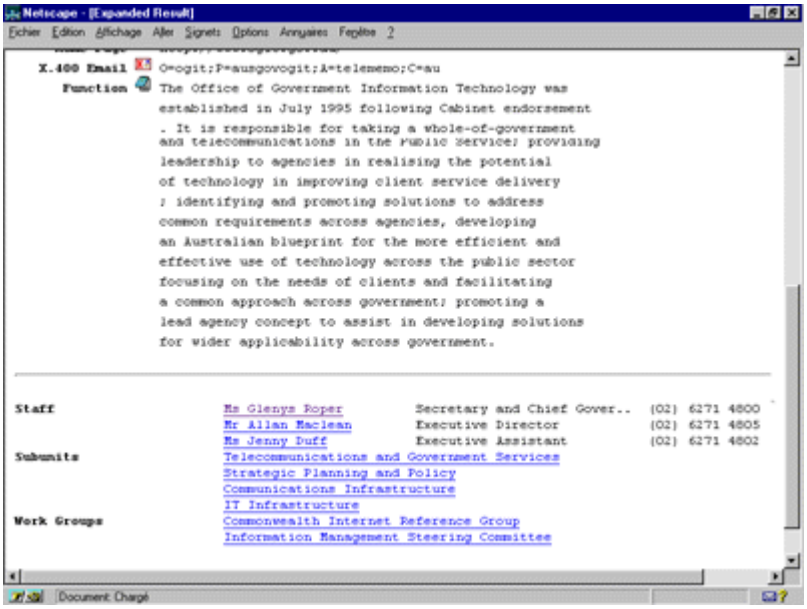


Figure A5-23 Résultat (2 de 2)

Service Pages vertes (GILS)
Gouvernement canadien

Figure A5-24 Page d'accueil

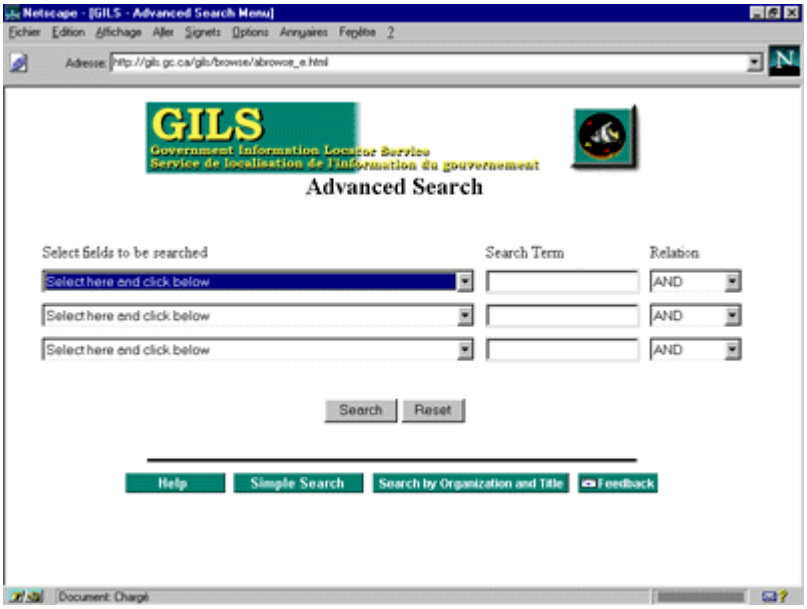


Figure A5-25 Formulaire de recherche avancée (1 de 2)

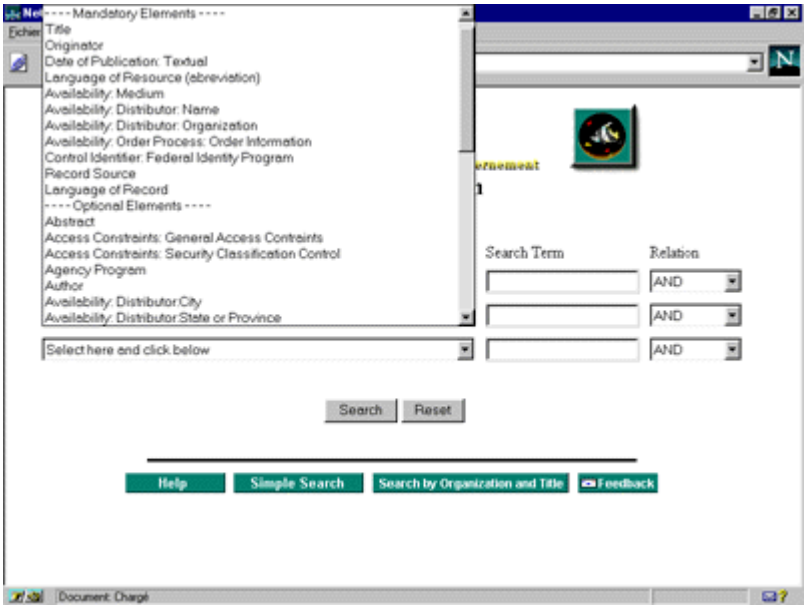


Figure A5-26 Formulaire de recherche avancée (2 de 2)

Figure A5-27 Exemple de résultat