3

Les annuaires LDAP et leurs applications

Introduction

Nous allons décrire les applications pouvant émerger de l'existence d'un standard comme LDAP. En effet, au-delà de la maîtrise des coûts et de la complexité d'administration d'une multitude d'annuaires dans l'entreprise, de nouveaux enjeux se présentent, qui peuvent à eux seuls justifier la mise en place d'un annuaire s'appuyant sur ce standard.

Pour cela, nous allons considérer des domaines d'applications, comme les réseaux d'entreprise, les portails, le commerce électronique ou les extranets, et mettre en avant pour chacun d'eux les applications des annuaires normalisés et la valeur ajoutée qu'ils apportent. Notons qu'il ne s'agit pas ici de pure spéculation, mais d'applications réelles de LDAP dans ces domaines.

Les différents domaines d'application des annuaires LDAP que nous détaillons dans ce chapitre sont les suivants :

- les réseaux et les systèmes d'exploitation ;
- la sécurité des systèmes d'information ;
- le commerce électronique ;
- les extranets ;
- les portails d'entreprise ;
- la fédération des identités.

Et enfin, nous allons donner des exemples d'application des annuaires, et, plus généralement, de la gestion des identités telle que nous l'avons définie dans le chapitre 1, par secteur de

marché, comme les télécommunications, la grande distribution, les banques, l'administration publique, etc.

Les réseaux et les systèmes d'exploitation

L'initiative DEN

DEN *(Directory Enabled Networks)* est une initiative commune des sociétés Microsoft et Cisco, amorcée en 1997. Son objectif est de définir un standard qui permette à une multitude d'équipements constituant un réseau, comme des routeurs, des modems et des serveurs de ressources (fichiers, imprimantes), de mieux coopérer en partageant des informations dans un même annuaire. Les annuaires LDAP sont bien placés pour jouer ce rôle, puisqu'ils sont déjà au cœur des systèmes d'exploitation et des applications. En effet, comme nous le verrons par la suite, Microsoft a mis en place son annuaire Active Directory au cœur de son système d'exploitation Windows 2000. À travers DEN, Microsoft a souhaité mettre en avant son annuaire pour gérer les informations requises par les équipements réseaux de Cisco, pour mieux servir les applications et les utilisateurs.

Mais, le succès de DEN ne pouvant passer que par son adoption par tous les acteurs du marché, l'initiative a été reprise rapidement par le consortium DMTF *(Desktop Management Task Force),* à la demande de Microsoft et de Cisco. Fondé en 1992, DMTF a pour objectif de définir des standards facilitant la gestion et l'administration des réseaux et des systèmes d'entreprise. Parmi ceux-ci, nous pouvons citer DMI *(Desktop Management Interface)*, CIM *(*Common Information Model*)* et WBEM *(Web-Based Enterprise Management)*. Le consortium regroupe plus d'une centaine de membres, et travaille avec des organismes comme l'IETF *(Internet Engeneering Task Force*), l'Open Group et d'autres. Des sociétés telles que Bay Networks, 3 COM, Lucent Technologies, IBM, Sun/Netscape et Novell ont d'ores et déjà adopté ce standard.

Aujourd'hui DEN reste d'actualité mais évolue lentement. Il ne constitue plus une priorité pour les constructeurs comme Cisco et Nortel, qui se concentrent sur des sujets plus prioritaires, comme la voix sur IP par exemple.

En quoi consiste DEN ? En fait, il s'agit de rendre le réseau plus intelligent, en permettant d'une part à chaque équipement d'être en mesure de faire connaître et de partager ses caractéristiques propres, et d'autre part de tirer parti des caractéristiques des autres équipements, ainsi que des applications et des profils des utilisateurs.

Par exemple, si deux utilisateurs se connectent à un même site, l'un pour visualiser une vidéo et l'autre pour télécharger un fichier, le réseau doit être en mesure de fournir plus de bande passante au premier. Cela parce que le ralentissement du débit peut rendre la séquence vidéo inexploitable, alors que le transfert de fichier prendra plus de temps mais aboutira.

En revanche, si ce transfert de fichier concerne une passation de commande à un fournisseur ou encore l'état d'un stock de marchandise qui doit être rafraîchi tous les quarts d'heure, il peut être important de donner la priorité au transfert. Sauf si l'utilisateur qui consulte la séquence vidéo n'est autre que le PDG de l'entreprise en téléconférence avec son trésorier…

On constate que les cas de figure sont variés et peuvent être complexes. Si nous analysons cet exemple, nous constatons que la configuration du réseau dépend des composants suivants :

- *Les équipements réseau* : chaque équipement a ses caractéristiques et ne peut fournir un service que s'il a été conçu pour celui-ci. Par exemple, un modem dédié au réseau téléphonique commuté ne pourra pas fournir un débit au-delà de 56 Kbit/s et n'est pas capable de discerner les flux qui transitent afin d'allouer une bande passante en fonction du service demandé par l'utilisateur. En revanche, un routeur pourra le faire, mais pas tous car cela dépend de ses capacités et de son coût. Il est donc nécessaire de disposer d'une description électronique de chaque équipement, qui peut être lue et partagée avec les autres équipements et les applications.
- *Les applications* : chaque application peut avoir des besoins spécifiques. Par exemple, une application de diffusion de film vidéo nécessitera une qualité de trafic constante. Il ne s'agit pas d'avoir nécessairement des débits élevés (64 Kbit/s peuvent suffire pour une téléconférence), mais surtout d'avoir un débit constant qui ne soit pas altéré par d'autres applications partageant le même réseau. En revanche, une application de transfert de fichier nécessitera un débit élevé mais ponctuel, car requis uniquement lors du transfert lui-même et non lors de la consultation de la liste des fichiers par exemple. Ainsi, chaque application doit être en mesure de communiquer ses besoins au réseau, quel que soit l'équipement sollicité.

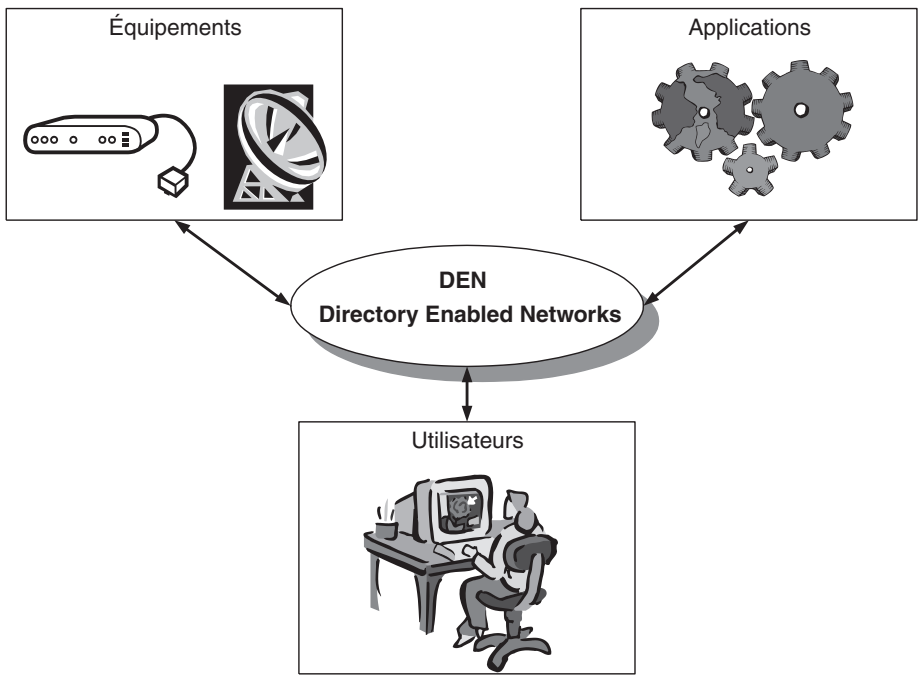


Figure 3.1
DEN au cœur de la qualité de services

- *Les utilisateurs* : ce sont aussi des acteurs importants du réseau. En effet, ce dernier doit s'adapter à leurs profils, assurant à certains plus de sécurité lors de l'accès à une application critique ou encore une priorité maximale pour l'accès à un service donné. Il faut donc disposer d'une base de profils accessible à tous et contenant les informations requises par le réseau, comme la priorité d'accès à un service par exemple.

  C'est la combinaison des trois qui permet d'utiliser de façon optimale les capacités d'un réseau et de fournir la meilleure qualité de service à l'utilisateur.

Comment faire en sorte que des équipements fabriqués par des constructeurs différents puissent dialoguer avec des applications conçues par les éditeurs de solutions du marché ? Et comment faire en sorte que les applications puissent reconnaître les profils des utilisateurs, et partager ces profils?

Les objectifs du standard DEN se décomposent en quatre catégories :

- modéliser les services et les équipements d'un réseau, ainsi que la façon dont ils interagissent ;
- fournir des moyens permettant de construire des solutions qui interopèrent avec le réseau ;
- faire en sorte que les applications tirent parti des capacités d'un réseau de façon transparente pour l'utilisateur ;
- définir des moyens de gestion d'un réseau dans son ensemble, par opposition à la gestion individuelle des équipements.

Le standard DEN offre un modèle indépendant des différents constructeurs à travers l'adoption d'un standard commun. Le modèle doit aussi être extensible afin de prendre en compte des caractéristiques propres à chaque constructeur. Pour atteindre cet objectif, DEN s'appuie sur LDAP. Il permet à chaque ressource de :

- publier ses caractéristiques dans un annuaire LDAP ;
- rechercher d'autres ressources répondant à certains critères à l'aide des fonctions de recherche et de navigation de LDAP ;
- lire les caractéristiques d'une ressource donnée décrite dans un annuaire LDAP.

La modélisation X500 – ou le DIM *(Directory Information Model)* – décrite plus haut, dont dérive LDAP, ne contient aucun objet prédéfini décrivant des équipements réseau ou des services. DEN étend le modèle de données de LDAP pour y ajouter des classes d'objets destinées aux réseaux.

Le modèle d'information de DEN dérive lui-même d'un autre modèle défini par le consortium DMTF : le modèle CIM *(Common Information Model).* On y trouve des classes d'objets telles que : `Chassis` pour décrire un châssis pouvant contenir plusieurs cartes réseaux, `Card` pour décrire une carte, `Slot` pour décrire les connecteurs dans un châssis… On y trouve aussi des classes permettant de décrire des services ou des applications comme la classe `InformationalService` destinée aux services HTTP ou SMTP, ou encore `MultiMediaService` pour les services multimédias.

Mais pour que ceci fonctionne, il faut que les équipements réseau et les applications soient compatibles avec le standard LDAP et soient en mesure d'interroger un annuaire partagé. C'est le cas de certains équipements de la société Cisco, et d'autres constructeurs ayant adopté ce standard. Il faut aussi que l'annuaire LDAP contienne les informations nécessaires aux équipements, et que celles-ci puissent être partagées entre plusieurs annuaires LDAP de marques différentes. L'adoption du standard DEN par Microsoft, Novell, Sun/Netscape, IBM et d'autres vendeurs d'annuaires LDAP, garantit cette interopérabilité pour la gestion des ressources réseau.

Une telle approche dans un environnement réseau apporte un avantage indéniable à celui-ci, tant en termes de qualité de service qu'en facilité d'administration. En outre, elle réduit les coûts d'infrastructure (débits des lignes, disponibilité requise, etc.) puisque chaque service qui décrit ses besoins propres fait en sorte que le réseau optimise ses ressources pour y répondre.

Active Directory et Windows 2000/2003

Le rôle d'Active Directory dans Windows 2000/2003

Les systèmes d'exploitation dédiés aux réseaux d'entreprises tirent parti de LDAP pour fédérer leurs annuaires et en améliorer l'interopérabilité et l'administration. Windows 2000/2003 et son annuaire Active Directory représentent un bon exemple d'utilisation de LDAP.

Les ressources référencées et gérées par un système d'exploitation comme Windows NT ou Windows 2000/2003 sont généralement constituées d'objets de types personnes et groupes, périphériques et machines, applications.

Dans les versions antérieures à Windows 2000, tous ces objets sont gérés dans des domaines Windows NT. Une base de données, nommée SAM *(Security Accounts Manager database*), contient la stratégie de sécurité associée à ces ressources. Cette base est répliquée sur les différents serveurs d'un même domaine. Rappelons qu'un domaine Windows NT est un ensemble de machines (postes de travail, serveurs, imprimantes…) reliées par un réseau local ou étendu, et contrôlées par un même serveur Windows NT. Un serveur principal contient la description de toutes les ressources du réseau, ainsi que celles des utilisateurs pouvant y accéder, et des droits d'accès relatifs à chacun d'eux. Ce serveur est nommé : PDC *(Primary Domain Controler).* Il peut être secouru par un autre serveur Windows NT, contenant une copie de toutes les données du système, et jouant le rôle de contrôleur secondaire. Il est appelé BDC *(Backup Domain Controler).*

La notion de domaine pose des problèmes d'administration pour des réseaux de taille importante. Il est effectivement plus performant avec Windows NT de disposer de petits domaines plutôt que d'un seul contenant des milliers d'utilisateurs. Or ceci nécessite la mise en place d'une stratégie d'approbation entre domaines, leur permettant de partager des ressources sur un même réseau d'entreprise. En outre, la notion de domaine sous Windows NT est plus proche d'une organisation physique de serveurs que d'une organisation logique d'entreprise. Ce qui rend leur administration plus complexe lorsqu'un même département doit gérer plusieurs domaines simultanément.

Par ailleurs, la gestion des différents objets référencés dans ces domaines nécessite l'utilisation de plusieurs utilitaires, chacun d'eux étant dédié à un type d'objet. Par exemple, la gestion des utilisateurs nécessite le Gestionnaire des utilisateurs, et la gestion des machines et de leurs noms nécessite le Gestionnaire WINS et le Gestionnaire de serveur. De plus, certains de ces outils ne sont pas accessibles d'office sur les postes clients, et ne peuvent donc être utilisés que par des administrateurs sur les serveurs. Cela ne facilite ni la recherche des ressources du réseau par les utilisateurs ni l'administration de l'ensemble pour les gestionnaires.

Windows 2000/2003 et son annuaire Active Directory apportent des solutions à ces différents problèmes. Active Directory est une base de données qui tire parti du standard LDAP et contient tous les objets nécessaires à la gestion et l'administration de Windows 2000/2003. On y trouve aussi bien la description des utilisateurs du réseau local, que celle des sites géographiques, des imprimantes partagées et des ordinateurs connectés au réseau.

Active Directory n'est pas un annuaire X500, car il n'implémente pas les couches OSI requises par celui-ci. Les raisons de ce choix par Microsoft sont les mêmes que celles déjà évoquées à propos de la complexité d'implémentation et de la mise en œuvre des annuaires X500.

En revanche, il offre une interface conforme au standard LDAP, qui permet de lire et d'écrire dans celui-ci. Il est complètement intégré à Windows 2000/2003 Serveur, offrant une vue hiérarchique des ressources et une solution extensible, évolutive et distribuée. Notons qu'il est maintenant disponible soit avec une version serveur de Windows 2000 ou 2003, soit en version autonome et indépendante des comptes utilisateurs Windows, désignée par Active Directory Application Mode (ADAM).

Les caractéristiques d'Active Directory

Nous allons décrire dans ce paragraphe les particularités d'Active Directory. Certaines sont dues au fait que c'est un annuaire et qu'il possède une interface LDAP et d'autres lui sont propres et le différencient des autres annuaires.

Un annuaire d'entreprise

Active Directory utilise le modèle de dénomination LDAP pour désigner tout objet d'un serveur Windows 2000/2003. Il offre donc un espace homogène de noms et *unique* pour toutes les ressources du serveur. Il a été conçu aussi bien pour gérer des ressources propres à un système d'exploitation en réseau (imprimantes, disques, etc.), que pour jouer le rôle d'un annuaire capable de répondre aux besoins de certaines applications d'entreprise, comme la messagerie électronique et les portails collaboratifs.

Une administration centralisée

Active Directory offre une administration centralisée pour gérer des fichiers, des périphériques, des connexions réseau, des accès Web, des utilisateurs… Les objets sont organisés de façon hiérarchique dans un arbre constitué d'unités organisationnelles. Comme nous

l'avons expliqué précédemment, l'organisation hiérarchique des données est plus adaptée aux fonctions de recherche et de navigation caractérisant un annuaire.

Il s'appuie sur le protocole DNS *(Domain Name Services)* d'Internet pour la localisation de l'annuaire. C'est-à-dire, qu'un nom de domaine Windows 2000/2003 est identifié de la même façon qu'un nom de domaine Internet (par exemple : `nomsociete.com`). En outre, pour retrouver un serveur Windows 2000/2003 il faut faire appel à un serveur DNS qui va associer au nom de domaine une adresse IP, donc l'adresse physique de la machine. Il est nécessaire de disposer d'un serveur DNS dans un réseau local d'entreprise pour déployer Windows 2000/2003 et Active Directory. Notons que le serveur Windows 2000/2003 contient en standard un serveur DNS.

Un même arbre peut contenir plusieurs domaines. Les notions de PDC *(Primary Domain Controler)* et de BDC *(Backup Domain Controler)* de Windows NT disparaissent au profit d'une notion de contrôleur de domaines unique. Les relations d'approbation entre domaines Windows 2000/2003 sont obligatoirement bidirectionnelles, simplifiant ainsi l'administration de l'ensemble. La compatibilité avec la notion de domaine au sens Windows NT ainsi qu'avec les notions de PDC et de BDC est conservée.

Une base de données dédiée

Active Directory est basé sur un moteur de base de données relationnelle propre à Microsoft (initialement le moteur de stockage de Microsoft Exchange 4.0). Il est adapté aux particularités des annuaires de systèmes d'exploitation, notamment en ce qui concerne la réplication de l'annuaire sur différents sites, la sollicitation intensive en lecture et la recherche multicritère, ainsi que le support d'un volume d'enregistrements correspondant au nombre d'utilisateurs dans une entreprise.

Intégration avec le système d'exploitation Windows 2000/2003

Active Directory est complètement intégré avec le serveur Windows 2000/2003. Il faut savoir qu'il n'est pas obligatoire de le mettre en œuvre, mais qu'il nécessite obligatoirement la version serveur de Windows 2000/2003 pour fonctionner.

Le support de LDAP

Active Directory supporte aussi bien la version 2 du standard LDAP que la version 3. Il est effectivement possible d'interroger l'annuaire avec tout utilitaire compatible avec ce protocole.

Le standard LDAP introduit des concepts comme les *attributs*, les *classes* et les *objets* ; nous décrirons plus en détail ce standard dans les chapitres suivants.

Nous allons exposer rapidement les concepts ci-dessous pour mieux comprendre la suite de ce paragraphe :

- Un attribut est un champ caractérisé par des propriétés comme le type de valeur qu'il peut contenir (entier, chaîne de caractères, etc.). Il est comparable à une colonne d'une

table dans une base de données. Par exemple, LDAP décrit des attributs normalisés comme le nom, le prénom, le numéro de téléphone…

- Une classe permet de décrire un enregistrement de l'annuaire. Elle est constituée d'un ou de plusieurs attributs, et contient des caractéristiques propres (attributs obligatoires…). Par exemple, on trouve dans LDAP des classes normalisées, comme la classe `personnes`, la classe `groupe de personnes`, la classe `organisation`...
- Un objet est l'instance d'une classe. Dans une base de données relationnelles, c'est tout simplement un enregistrement. Chaque objet de l'annuaire doit être associé à une classe, décrivant les attributs facultatifs et ceux qui sont obligatoires.

Active Directory est compatible avec les attributs et les classes décrites dans le standard LDAP. Mais ceci n'exclut pas la personnalisation de ce standard faite par Microsoft dans son annuaire. Par exemple, certaines classes d'objets, comme la classe `top` dont dérivent toutes les autres classes, contiennent des attributs qui ne font pas partie du standard LDAP, bien que ces classes en fassent partie !

Si nous prenons l'exemple de la classe `top`, voici la comparaison entre le standard LDAP et Active Directory :

Standard LDAP (RFC 2256)	Active Directory	Attribut obligatoire	Appartient au standard LDAP (RFC 2256)
• ObjectClass	• ObjectClass	• Oui	• Oui
	• InstanceType	• Oui	• Non
	• NTSecurityDescriptor	• Oui	• Non
	• ObjectCategory	• Oui	• Non

Néanmoins, il est toujours possible de lire tout objet de l'annuaire Active Directory avec n'importe quel outil LDAP (seuls les attributs LDAP seront lus, et qui peut le plus peut le moins…). En revanche, il ne sera pas aisé de créer à partir de l'interface LDAP un objet ayant des attributs obligatoires n'appartenant pas au standard.

Il est aussi envisageable d'accéder à Active Directory à travers toute interface de programmation compatible avec le standard LDAP, en langage C, Java, .Net ou tout autre langage. Microsoft offre également une interface de programmation sous forme d'objets COM ou .Net, nommée ADSI *(Active Directory Service Interfaces),* qui permet d'appeler les services de tout annuaire LDAP, dont Active Directory, à partir de pages ASP et ASPX, de Visual Basic ou de tout programme .Net par exemple. Nous décrirons cette interface plus en détail dans la suite de ce livre.

L'évolutivité d'Active Directory

Afin d'assurer l'évolutivité de l'annuaire et le support d'un grand nombre d'enregistrements, Active Directory crée un espace de stockage dédié pour chaque domaine, à savoir un

fichier contenant une partie de la base de données. On désigne aussi ces espaces de stockage par *partitions*.

Plusieurs domaines peuvent être regroupés dans un même *arbre,* chaque domaine ayant sa propre partition de la base de données. Ainsi les données d'un même annuaire sont réparties sur plusieurs fichiers, qui ne contiennent pas tous une copie complète des données.

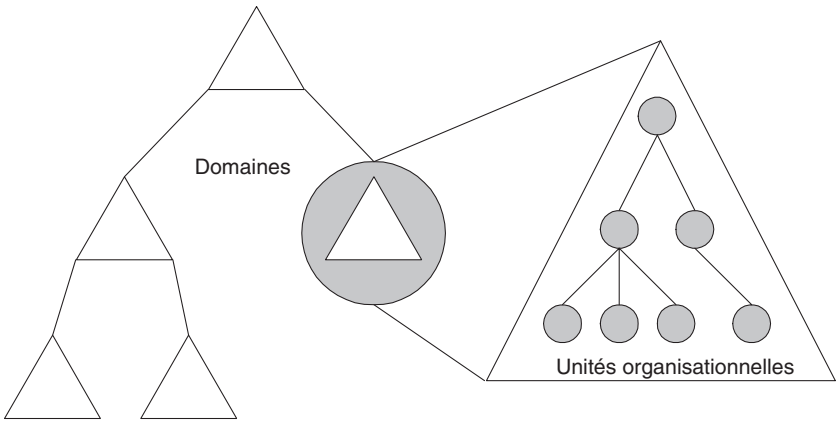
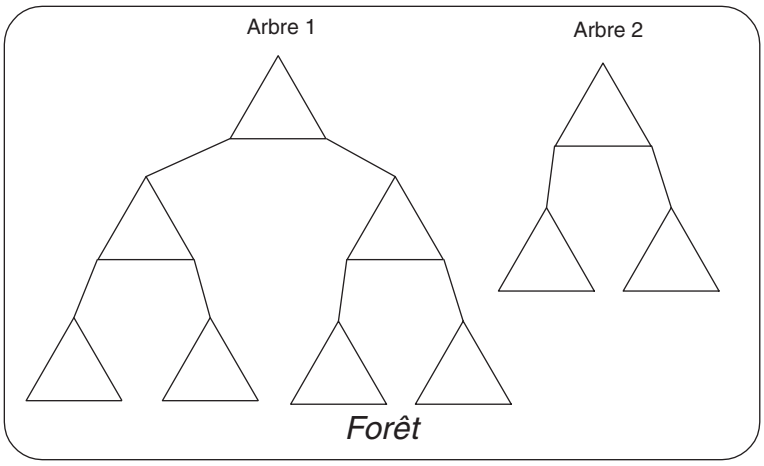


Figure 3.2
Arbre de domaines et unités organisationnelles dans un domaine

Il est possible de regrouper plusieurs arbres comprenant donc un ensemble de domaines reliés hiérarchiquement. Cet ensemble d'arbres forme une *forêt* comme vous pouvez le deviner !

Figure 3.3
Notion de forêt dans Active Directory



Plusieurs domaines dans un même arbre peuvent partager le même nom DNS. Par exemple, dans la figure 3.3, les différents domaines de l'arbre 1 peuvent se trouver sous le même nom DNS (si le nom du DNS de l'arbre 1 est `entreprise.com`, les domaines peuvent avoir des adresses du type `domaine1.entreprise.com`, `domaine2.enteprise.com`...). En revanche, le nom de domaine ne peut pas être le même pour deux arbres.

Rappelons qu'un domaine est un ensemble d'ordinateurs reliés par un réseau local qui partagent la même base de comptes utilisateurs. Tous les domaines de Windows 2000/2003 appartenant à un même arbre ou à une même forêt ont, par défaut, des relations d'approbations bidirectionnelles et transitives, et partagent le même schéma de l'annuaire (c'est-à-dire les classes d'objets et les attributs). La possibilité de modifier ces relations d'approbation pour conserver la compatibilité avec des domaines Windows NT est offerte.

L'extensibilité d'Active Directory

Active Directory contient par défaut une multitude de classes d'objets. Par exemple, on y trouve toutes les informations nécessaires pour sauvegarder un environnement Windows

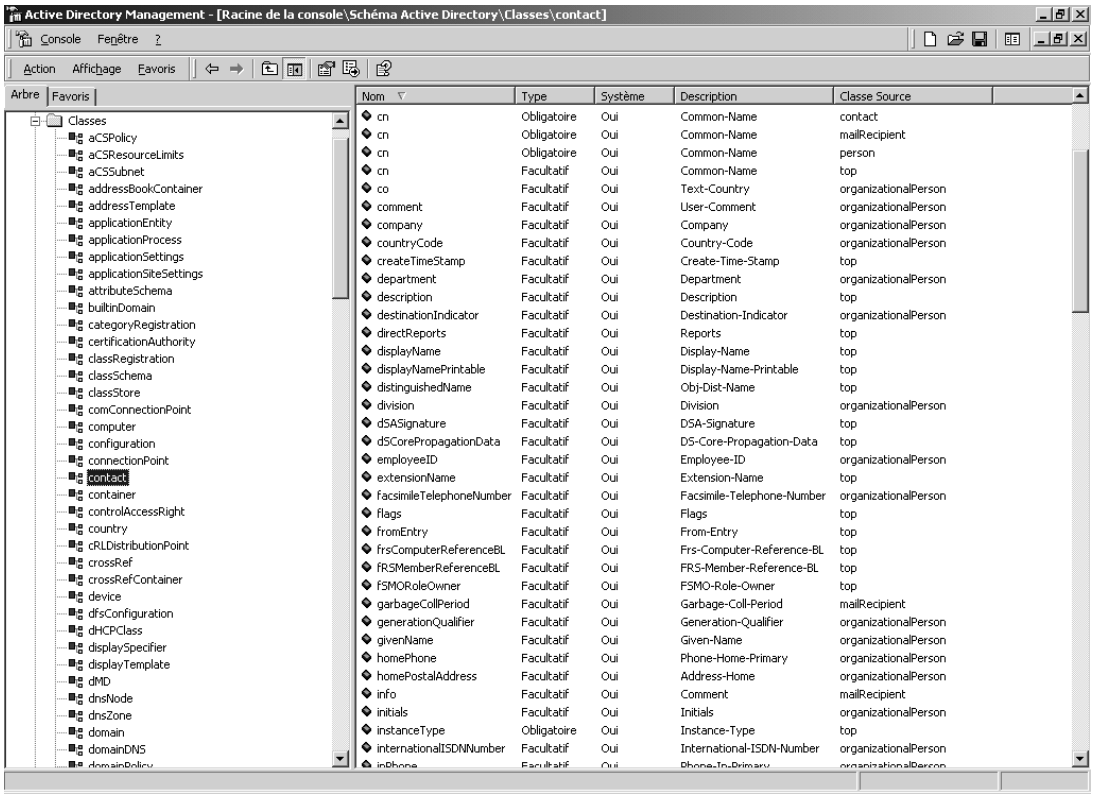


Figure 3.4

Liste des classes d'objets et des attributs prédéfinis dans Active Directory

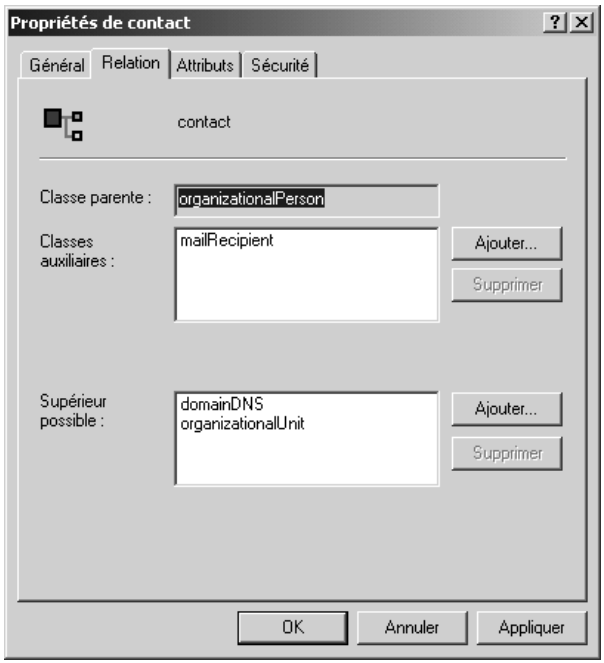
personnalisé par un utilisateur : les répertoires par défaut, les paramètres du bureau, les préférences… Tous ces paramètres sont utilisés pour reconstituer l'environnement de l'utilisateur quel que soit l'endroit à partir duquel il s'identifie.

Il est possible de consulter le schéma de l'annuaire Active Directory à l'aide de la console d'administration MMC *(Microsoft Management Console).* Pour cela il faut rajouter le composant logiciel enfichable appelé Schéma Active Directory à l'aide du menu Console.

Dans la colonne de gauche se trouve la liste des classes, et dans la colonne de droite se trouve la liste des attributs pour la classe sélectionnée (la classe `contact` dans cet exemple).

Toutes ces classes sont reliées par des liens d'héritage (elles dérivent toutes de la classe `top`). Par exemple, la classe `contact` qui permet de décrire une entrée du carnet d'adresses dérive de la classe `organizationalPerson` comme le montre la figure 3.5.

Figure 3.5
Propriétés de la classe `contact`



Dans ce schéma, c'est le champ *Classe parente* qui indique la classe dont dérive la classe `contact`.

On peut également modifier le schéma de l'annuaire et rajouter des attributs et des classes d'objets. Il n'est pas conseillé de modifier les classes existantes car ceci risque d'altérer le fonctionnement de Windows 2000, mais il est envisageable de rajouter une classe d'objet propre à une application.

Par exemple, si vous souhaitez différencier les employés de votre entreprise des prestataires externes, vous pouvez créer deux nouvelles classes dérivant de la classe `user`. Ainsi, vous pourrez rajouter des informations propres à chacun des cas, comme le nom de la société à laquelle appartient le prestataire, tout en bénéficiant des fonctions standards offertes par Windows 2000/2003 (la classe `user` décrit tout utilisateur déclaré par l'administrateur et pouvant accéder aux ressources de Windows 2000/2003).

Notons qu'il faut commencer par ajouter les nouveaux attributs dans la liste des attributs avant de modifier ou de rajouter de nouvelles classes d'objets. En effet, les attributs ne dépendent pas des classes et peuvent être partagés par plusieurs d'entre elles.

Un catalogue global

Afin de faciliter la recherche d'objets dans Active Directory, celui-ci dispose d'une copie d'un sous-ensemble des attributs de tous les objets, répliquée sur toutes les partitions de l'annuaire.

Cette copie s'appelle le *catalogue global.* Il contient la totalité du schéma, et pour chaque objet, la partition qui l'héberge et les attributs les plus communs comme le nom, le prénom, l'identifiant…Toute recherche sur ces attributs peut se faire localement et évite ainsi le parcours de toutes les partitions. Le mécanisme de réplication intégré dans Active Directory assure la synchronisation des catalogues de toutes les partitions d'un même annuaire au sein d'une même forêt uniquement.

La sécurité

Tous les objets d'un annuaire Active Directory sont protégés par le concept des ACL *(Access Control Lists)* décrit dans le standard LDAP. Les ACL permettent de décrire les habilitations de tout utilisateur référencé dans l'annuaire sur les autres objets de l'annuaire. Ils rendent possible le contrôle de ce que peut voir un utilisateur et les actions qu'il peut effectuer (mise à jour, suppression, etc.). Ces droits peuvent s'appliquer aussi bien sur un objet que sur un de ses attributs.

Active Directory offre des mécanismes de délégation des droits sur une branche de l'annuaire à un ou plusieurs utilisateurs. C'est une des plus importantes fonctions d'un annuaire, car elle permet de décentraliser les tâches d'administration tout en s'assurant que les actions exécutées par des tiers restent dans un cadre de sécurité cohérent. Par exemple, pour un annuaire contenant deux sous-branches : le service marketing et le service informatique, l'administrateur global peut déléguer les droits de gestion des utilisateurs du service marketing à une personne donnée du service informatique. Celle-ci pourra créer, supprimer ou modifier des profils d'utilisateurs mais ne pourra pas créer d'autres types d'objets ni créer des utilisateurs dans un autre service.

Conclusion

En résumé, nous pouvons affirmer qu'Active Directory tire parti du standard LDAP de façon significative. Il implémente son modèle de données pour la définition du schéma de l'annuaire. Il respecte l'organisation hiérarchique X500 et le modèle de dénomination

associé pour identifier tout objet de l'annuaire. Il tire parti du modèle de sécurité aussi bien pour l'identification à l'annuaire que pour la définition des habilitations. Enfin, il offre le modèle des services préconisé par le standard qui permet d'effectuer des actions sur l'annuaire à l'aide de toute application externe respectant le protocole LDAP.

Active Directory est étroitement lié à Windows 2000/2003. C'est un annuaire de ressources dédié au système d'exploitation, qui peut par conséquent être moins adapté pour gérer d'autres types d'objets, comme des profils d'utilisateurs externes à l'entreprise (comme des clients ou des partenaires) ou des applications. C'est pour cette raison que Microsoft a réalisé une version autonome d'Active Directory, dénommée ADAM, qui n'est pas liée aux comptes utilisateurs du système d'exploitation. Il est ainsi possible de créer des utilisateurs dans ADAM à des fins d'identification lors de l'accès à un site Internet, sans que ces utilisateurs aient des comptes sur le serveur Windows. Notons qu'ADAM ne fonctionne que sur Windows 2003 Serveur et sur Windows XP.

Signalons également qu'il n'est pas possible de remplacer l'annuaire Active Directory du système d'exploitation Windows par un autre annuaire LDAP, comme celui de Sun ou de Novell.

Rappelons enfin que Microsoft a acquis récemment la société Zoomit, offrant un méta-annuaire nommé Via. Ce produit permet de centraliser dans une même base l'ensemble des données concernant les personnes et les ressources de l'entreprise provenant de tout type d'annuaire, fichier ou base de données. Cet outil s'interface avec Active Directory afin de gérer les habilitations, mais ne l'utilise pas comme base de données pour sauvegarder les informations. La dernière version de ce produit, dénommé MIIS (Microsoft Identity Integration Server), s'appuie sur une base de données SQL Server 2000 et nécessite Windows 2003 Serveur.

Novell eDirectory Server et Netware

NDS/eDirectory et Netware

La société Novell est connue pour son logiciel Netware, dédié au partage de ressources informatiques sur un réseau local d'entreprise. Son rôle consiste essentiellement à référencer l'ensemble de ces ressources (disques, volumes, imprimantes, serveurs…), ainsi que les utilisateurs et leurs profils, puis de contrôler les droits d'accès sur ces ressources. Novell Netware est également un système d'exploitation propriétaire, capable de faire fonctionner des applications, comme des messageries ou des bases de données tirant parti du référentiel des ressources et du gestionnaire des habilitations.

Depuis quelques années, la stratégie de Novell a consisté à mettre en avant les fonctionnalités d'annuaire intégrées dans Netware. Pour cela, Novell a créé un produit séparé de Netware, dénommé NDS *(Novell Directory Server)* puis Novell eDirectory, dont la vocation est d'être un annuaire généraliste.

Depuis la version 8 de son produit, Novell a souhaité couvrir les besoins des entreprises dans le domaine d'Internet et des extranets, et non plus dans le domaine des intranets uniquement, comme dans les versions précédentes.

Quelques caractéristiques de NDS/eDirectory

L'orientation de la stratégie de Novell sur Internet et sa volonté de se positionner comme un acteur majeur des annuaires dans ce domaine sont récentes.

Voici quelques points qu'il est intéressant de connaître à propos de Novell eDirectory :

- Il fonctionne aussi bien dans un environnement Netware que sous Windows NT/2000/2003, Linux et Solaris ;
- Novell eDirectory est compatible avec le standard LDAP v3, incluant les classes auxiliaires, les extensions LDAP et les renvois de références (referrals) ;
- Novell eDirectory prend en charge les fonctions d'authentification et de chiffrement à l'aide d'une infrastructure à clés publiques (PKI) s'appuyant sur SSL et des certificats X509v3 ;
- Novell eDirectory offre un outil permettant d'importer et d'exporter des données au format LDIF ;
- Le moteur de base de données intégré à Novell eDirectory est issu de celui de la suite Groupwise de Novell. Il a été optimisé pour prendre en charge un grand nombre d'enregistrements et pour être performant en lecture. Il est capable de supporter plusieurs millions d'enregistrements et d'utilisateurs simultanés, comme l'atteste le service d'authentification de déclaration des impôts en France, basé sur ce produit !

Il faut aussi noter que la société Novell a racheté SuSE, éditeur de systèmes d'exploitation Linux. Ceci marque le fort engagement de Novell vis-à-vis de cet environnement. La plupart des outils de Novell seront donc disponibles sous Linux, et seront optimisés pour être très performants sur cette plate-forme.

OpenLDAP et Linux

Les récents succès du système d'exploitation Linux, aussi bien comme plate-forme serveur que comme poste de travail bureautique, en font une solution incontournable des technologies informatiques de demain. Linux existe en version poste de travail, comprenant l'ensemble des outils bureautiques de base comme la messagerie, le traitement de texte, le tableur, etc. Mais il existe également en version serveur, pouvant aussi bien héberger des applications Web pour Internet ou les intranets, que jouer le rôle d'un serveur de fichiers et d'imprimantes dans un réseau local d'entreprises.

Les différentes solutions Linux du marché (gratuites ou commerciales) comprennent en standard un annuaire LDAP issu d'un projet de logiciel libre dénommé OpenLDAP. Il fonctionne sur diverses plates-formes, dont Windows, Unix et Linux, et peut être adapté par chacun en fonction de ses besoins propres à partir de son code source, téléchargeable librement sur le site *www.openldap.org*.

Cet annuaire s'intègre avec le système d'exploitation Linux et peut être utilisé pour certaines fonctions, comme l'illustrent les exemples suivants :

- Remplacement de NIS *(Network Information Service)* par un annuaire LDAP : NIS est un service défini par Sun, et utilisé par la majorité des Unix, dont Linux, afin de gérer les utilisateurs, les mots de passe et les groupes du système d'exploitation, ainsi que d'autres informations d'administration.
- Annuaire des services Samba : les services Samba permettent à des postes de travail sous Windows de partager des fichiers et des ressources (imprimantes, disques) sur un serveur Linux. L'annuaire OpenLDAP peut être utilisé pour référencer les utilisateurs du serveur Samba, ainsi que pour les authentifier.
- Annuaire des services Radius : il existe un projet OpenSource (FreeRadius à l'adresse *http://www.freeradius.org*) permettant d'implémenter le protocole RADIUS pour authentifier les utilisateurs se connectant à distance à une machine Linux (ou un autre système d'exploitation). Il est possible d'utiliser un annuaire LDAP soit pour stocker les valeurs des attributs RADIUS, soit pour authentifier les utilisateurs.
- Annuaire DNS : l'annuaire LDAP peut être utilisé comme base de données d'un service DNS, pour la résolution des noms de machine en adresses réseau.

La sécurité des systèmes d'information

Les certificats X509 et les infrastructures à clés publiques

Les infrastructures à clés publiques ou les PKI *(Public Key Infrastructure),* constituent une solution idéale pour authentifier des utilisateurs et des services, et gérer des habilitations dans un environnement réseau distribué et ouvert, comme sur Internet, un intranet ou un extranet. Nous allons dans un premier temps décrire le mécanisme des PKI et leur utilité, puis nous mettrons en avant le rôle des annuaires LDAP dans ce type d'infrastructure.

Le principe des PKI consiste à associer deux clés (deux nombres premiers élevés, n'ayant donc aucun lien entre eux, l'un ne pouvant pas être déduit de l'autre) à un service ou à un utilisateur donné : l'une dite privée qui lui est personnelle et que lui seul connaît et l'autre dite publique qui peut être diffusée à toute autre personne ou service. Ces clés sont alors utilisées pour chiffrer toute information échangée à l'aide d'un algorithme asymétrique : le chiffrement par l'émetteur s'effectue avec l'une ou l'autre des clés (par exemple la clé publique du récepteur) et le déchiffrement avec l'autre clé par le récepteur (par exemple la clé privée du récepteur).

Les applications des certificats

Les certificats sont utilisés à des fins d'authentification, de signature et de chiffrement des données. Nous allons décrire pour chacun des cas les mécanismes utilisés et le rôle d'un annuaire LDAP.

Authentifier l'utilisateur ou le service

Pour cela, il est nécessaire d'associer un certificat à l'utilisateur ou au service, lequel n'est autre qu'un document électronique émis par un tiers contenant des informations d'identification (nom, adresse, etc.) et la clé publique. Ces informations sont chiffrées avec la clé privée de ce tiers, appelée aussi *autorité de certification* ou CA *(Certification Authority).* La clé publique de l'autorité de certification, accessible par tous, permet de décrypter les informations du certificat, et donc de s'assurer de l'identité de l'utilisateur ou du service en y trouvant sa clé publique et des informations qui offrent le moyen de l'identifier, comme son nom ou son adresse.

Ce mécanisme d'authentification est habituellement désigné par authentification forte, par opposition au mécanisme d'authentification élémentaire réalisé à l'aide d'un simple mot de passe.

Note

Afin d'assurer l'interopérabilité des systèmes d'information pour lire et écrire les certificats, il est nécessaire de disposer d'un standard décrivant le format des données du certificat lui-même, et d'une interface d'accès à ce dernier. Ce format est celui décrit dans le standard X509 version 3, et l'interface d'accès est basée sur le standard PKCS#12.

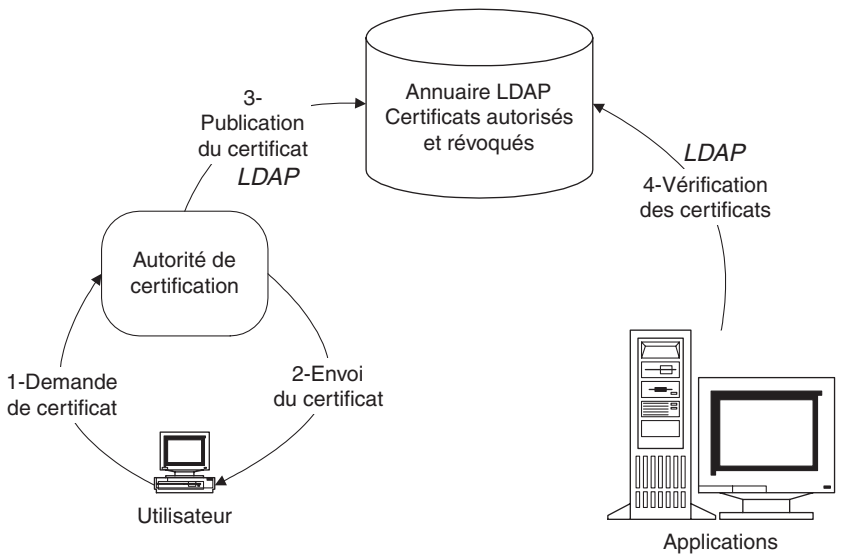


Figure 3.6

Processus de gestion PKI

Authentifier un utilisateur consiste donc à s'assurer que sa clé publique lui appartient bien. Pour cela, il faut obtenir son certificat et s'assurer qu'il contient des informations certifiées correctes par un tiers, qui n'est autre que le CA. Pour authentifier un service il

faut exécuter la même procédure avec sa clé publique. Ainsi, un site Web peut par exemple avoir un certificat utilisé par les internautes en cas de téléchargement de programmes de ce site afin de s'assurer de leur origine ou de leur authenticité (c'est ce qui se produit lorsqu'on télécharge un composant ActiveX dans Internet Explorer). Il peut aussi être utilisé pour signer les fichiers téléchargés et s'assurer ainsi de leur intégrité (par exemple qu'ils n'ont pas été modifiés par un tiers, qu'aucun virus n'a été ajouté, etc.).

Le CA doit aussi conserver les certificats révoqués afin de pouvoir refuser la validité d'un certificat le cas échéant. L'absence d'un certificat dans la base ne signifie pas que celui-ci est invalide ; il peut par exemple se trouver tout simplement dans une autre base gérée par un autre CA. Il est donc important de conserver aussi longtemps que possible dans l'annuaire tous les certificats révoqués.

Signer des documents

Signer un document consiste à s'assurer d'une part de l'intégrité de celui-ci, et d'autre part qu'il appartient bien à son auteur.

Pour vérifier l'intégrité d'un document, il faut calculer une clé à partir de son contenu. Ce calcul doit garantir l'unicité de celle-ci par rapport à ce contenu. Cette clé est ensuite ajoutée au certificat de l'auteur, pour être chiffrée avec sa clé privée, constituant ainsi la signature du document.

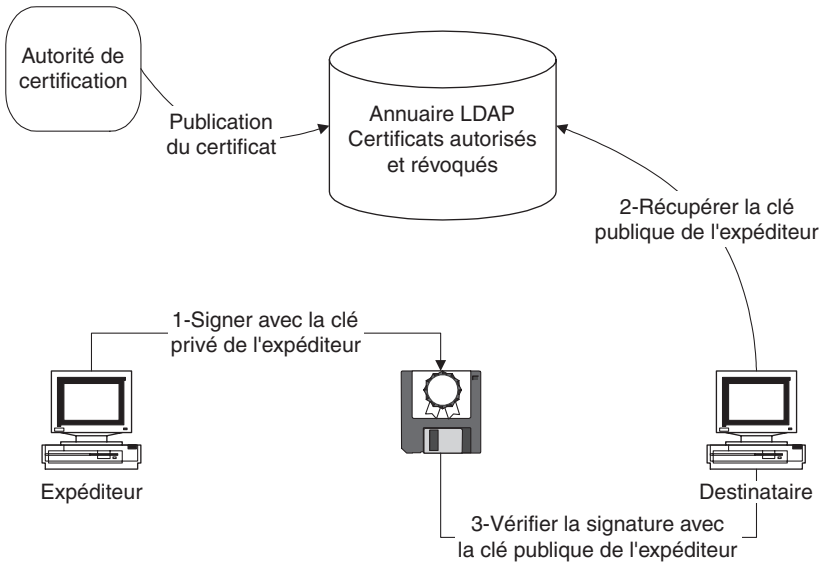


Figure 3.7
Processus de signature PKI

Le destinataire s'assure de la signature du document en déchiffrant celle-ci avec la clé publique de l'auteur. Il recalcule alors la clé associée au contenu à l'aide du même

algorithme et la compare avec la clé contenue dans la signature. Puis il vérifie le certificat qui se trouve dans celle-ci pour s'assurer de l'identité de l'auteur.

Crypter des informations échangées

Pour crypter des informations échangées entre deux personnes et s'assurer de la confidentialité des échanges, il faut que seul le destinataire puisse décrypter les informations reçues. Pour cela, l'expéditeur doit utiliser la clé publique du destinataire pour crypter les informations qu'il souhaite lui envoyer. Seul le destinataire pourra alors les décrypter avec sa clé privée (voir figure 3.8).

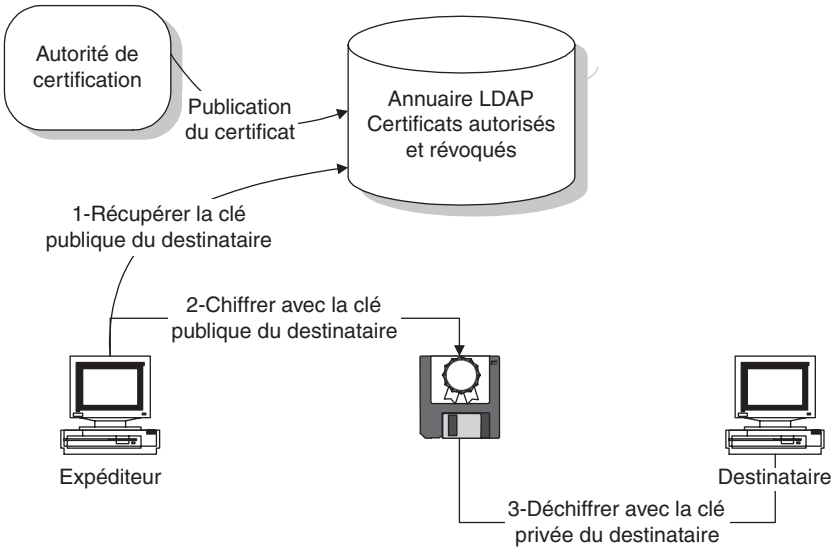


Figure 3.8
Processus de chiffrement PKI

Le rôle de LDAP dans la gestion des certificats

Nous constatons dans ces trois cas qu'il est indispensable que les certificats puissent être partagés entre les différents acteurs ; ceux-ci pouvant être des personnes physiques, des autorités de certification ou des applications informatiques.

Il est donc nécessaire de disposer d'un outil basé sur un standard ouvert permettant de sauvegarder ces certificats et de les lire à partir de différents critères de recherche, comme le nom d'une personne et le nom d'un service, mais aussi d'y accéder de n'importe où et à partir de n'importe quel type d'outil et de plate-forme. Les annuaires LDAP sont bien adaptés à ce besoin et sont utilisés par tous les acteurs du marché offrant des solutions de sécurité. C'est le cas notamment des produits iPlanet de Sun/Netscape, de Novell avec son annuaire NDS et d'IBM avec son offre de sécurité Tivoli et son annuaire.

L'identification unique (ou le Single Sign On)

Avec la multiplication des réseaux et des applications informatiques dans une entreprise, il est courant de devoir s'identifier plusieurs fois et de façon différente pour accéder aux services offerts. L'utilisateur doit en général posséder un nom et un mot de passe pour accéder à son poste de travail, puis un mot de passe pour la messagerie, un autre pour l'intranet, et encore un autre pour accéder aux applications sur les grands systèmes (mainframe)…

Certaines seulement de ces identifications s'appuient sur un même nom et un même mot de passe. Pour rendre les choses encore plus complexes, les administrateurs imposent souvent aux utilisateurs de modifier leurs mots de passe régulièrement (par exemple tous les mois), en prenant bien soin de refuser tout nouveau mot de passe ayant déjà été utilisé ! Chaque utilisateur est donc contraint de retenir trois, quatre ou cinq mots de passe différents, qui doivent changer régulièrement.

Comment arriver à une situation idéale où chaque utilisateur ne s'identifierait qu'une seule fois, malgré la multitude des plates-formes, des réseaux et des applications, tout en garantissant un niveau de sécurité optimal ? Comment faire en sorte que le mot de passe qui transite sur la ligne soit le plus dynamique possible afin d'éviter tout risque de piratage de celui-ci, sans contraindre l'utilisateur à le modifier régulièrement et à en mémoriser plusieurs ? Comment épargner à l'utilisateur d'avoir à ressaisir son mot de passe lorsqu'il sollicite une nouvelle application auprès de laquelle il ne s'est pas encore identifié ?

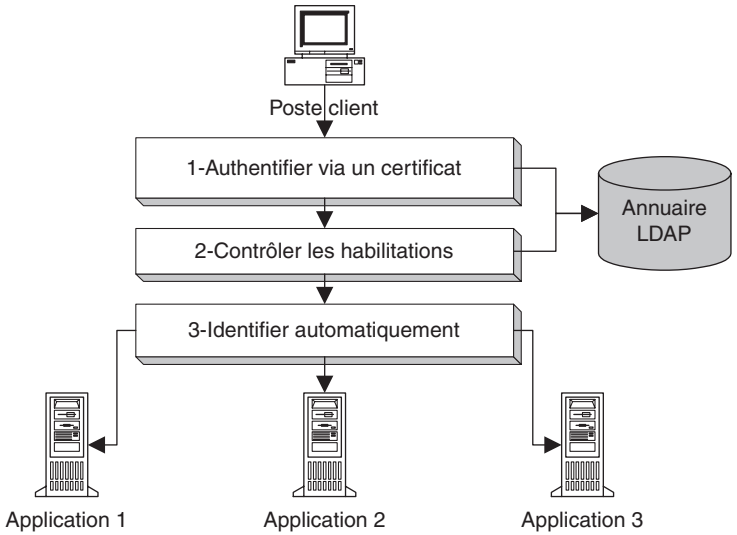
Par ailleurs, comment savoir à quelles applications un utilisateur a droit ? En effet, si chaque application contient la liste des utilisateurs autorisés, il n'est pas possible de savoir, pour un utilisateur donné, à quelles applications il peut accéder, sans avoir à parcourir toutes les applications de l'entreprise ! Comment gérer ces habilitations et assurer une compatibilité et une interopérabilité du plus grand nombre d'applications ?

Une des solutions envisageables (mais ce n'est pas la seule) consiste à utiliser un certificat X509 pour authentifier l'utilisateur et un annuaire LDAP contenant d'une part l'identifiant unique de l'utilisateur et son certificat éventuel, et d'autre part l'ensemble des attributs requis pour assurer son identification dans toutes les applications autorisées. De plus, pour le contrôle et la gestion des habilitations, l'annuaire contiendrait la liste des applications de l'entreprise, et les habilitations des utilisateurs sur celles-ci.

Notons que pour assurer l'identification unique à plusieurs applications, il est nécessaire d'identifier automatiquement l'utilisateur. On ne lui demandera son identité que pour l'accès à l'une d'elles, le portail intranet par exemple, puis il sera identifié automatiquement et sans dissimulation lorsqu'il voudra accéder aux autres services. Pour cela, l'annuaire doit être complété par un outil particulier qui utilisera différents attributs d'un profil utilisateur afin de l'identifier de façon automatique auprès des services sollicités, et ce après en avoir contrôlé l'autorisation de façon totalement transparente pour celui-ci. Ce type d'outil est implémenté généralement sous forme de serveur, nommé Policy Server ou serveur de stratégie de sécurité. On peut citer à titre d'exemple les produits COREid de la société Oblix, SiteMinder de la société Netegrity ou encore GetAccess de la société Entrust.

Ainsi, nous pouvons résumer dans le schéma suivant les différentes composantes de la solution.

Figure 3.9
Identification unique à plusieurs applications



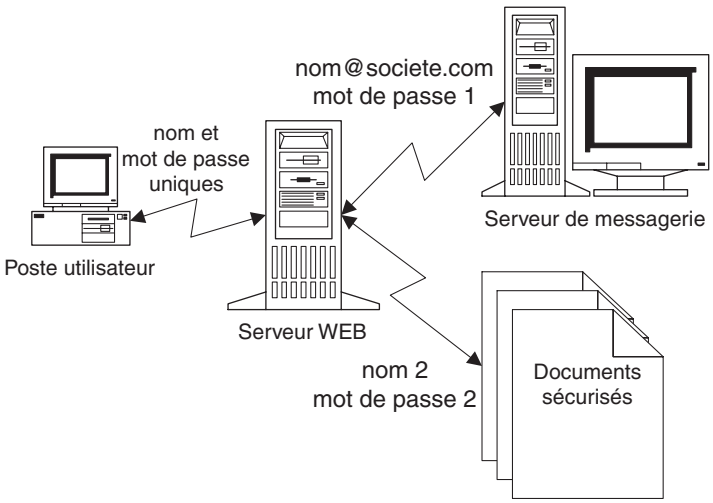
L'authentification *via* un certificat (1) et le contrôle des habilitations (2) sont exposés ci-après. L'identification et l'authentification automatiques (3) vers les différentes applications nécessitent un serveur de stratégie de sécurité comme nous l'avons précisé précédemment.

Prenons l'exemple de deux services accessibles à travers une identification unique : l'accès à des pages sécurisées *via* un navigateur Web, et l'accès à une messagerie électronique *via* ce même *navigateur* (et non à travers un logiciel de messagerie). La plupart des serveurs de messagerie (Microsoft Exchange, IBM Lotus Domino, Sun/iPlanet Messaging Server, etc.) possèdent des passerelles Web permettant de s'affranchir d'un logiciel de messagerie pour accéder à sa boîte aux lettres. L'avantage d'une telle solution est qu'elle offre les moyens de consulter sa boîte aux lettres de n'importe où et à l'aide d'un simple navigateur Web, tout en gardant ses messages sur le serveur.

L'accès à des documents sécurisés à travers un serveur Web nécessite de protéger ceux-ci par un mot de passe et de configurer le serveur pour activer le protocole SSL *(Secured Socket Layer)* lorsqu'un utilisateur demande l'accès à ces documents. Ce protocole chiffre toutes les données échangées entre le navigateur Web et le serveur, quel que soit le sens de cet échange.

Avec un mécanisme d'authentification élémentaire, l'utilisateur devra fournir un premier mot de passe pour accéder à ses messages, puis un deuxième mot de passe pour accéder aux documents sécurisés. En outre, ces mots de passe transitent sur la ligne, ce qui peut présenter un risque de piratage même si le protocole SSL est activé.

Figure 3.10
Exemple de SSO pour l'accès à une messagerie et à des documents



En revanche, avec un mécanisme d'authentification forte à l'aide d'un certificat, l'utilisateur ne devra fournir qu'un seul mot de passe, qui de toute façon ne transitera pas sur la ligne. Les différentes étapes de ce mécanisme sont exposées ci-après.

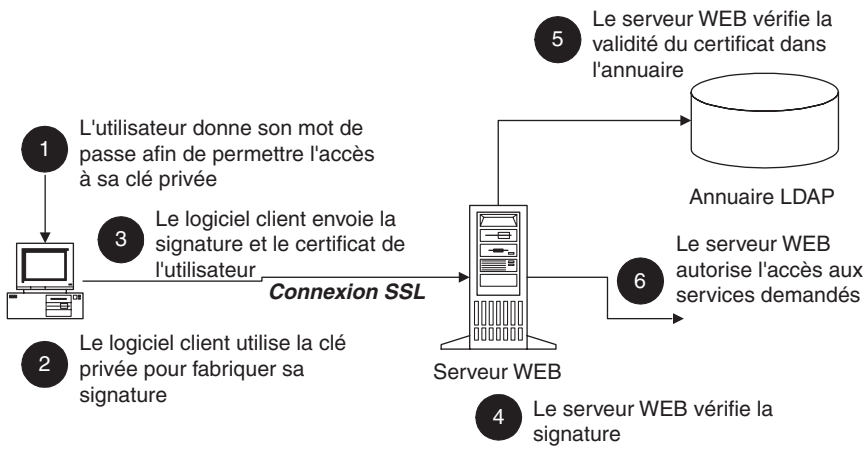


Figure 3.11
Les étapes de l'authentification à l'aide d'un certificat

Voici le processus décrit plus en détail :

1. Le navigateur Web (comme dans Netscape Communicator ou Internet Explorer) ou le poste de travail demande à l'utilisateur de fournir son mot de passe afin d'autoriser l'accès à sa clé privée.

2. Le navigateur fabrique alors une signature de données quelconques à l'aide de la clé privée de l'utilisateur (rappelons que cette signature consiste à calculer un nombre unique associé à ces données qui en garantit l'intégrité). Cette signature et ces données constituent une preuve permettant de s'assurer de l'identité de l'utilisateur puisqu'il a utilisé sa clé privée.
3. Le navigateur envoie le certificat de l'utilisateur contenant sa clé publique, ainsi que les données et la signature au serveur.
4. Le serveur Web vérifie alors la signature envoyée. Pour cela il recalcule une signature à partir des données transmises et à l'aide de la clé publique de l'utilisateur, puis il la compare avec la signature fournie.
5. Le serveur s'assure ensuite de la validité du certificat en se connectant à l'annuaire LDAP. Il vérifie d'une part l'existence de ce certificat pour l'utilisateur désigné, et d'autre part la non-révocation de celui-ci.
6. Si la signature et le certificat sont valides, le serveur autorise alors l'accès au service demandé.

Ainsi, l'utilisateur ne fournit son mot de passe qu'une seule fois dans une même session. S'il demande l'accès à d'autres services, le logiciel client, c'est-à-dire le navigateur, envoie à nouveau le certificat et la signature sans demander le mot de passe de l'utilisateur. L'authentification est donc bien réalisée chaque fois que l'accès à un nouveau service est demandé, mais de façon totalement transparente pour l'utilisateur.

La gestion des autorisations

Nous avons vu le rôle que peut jouer un annuaire LDAP dans l'identification unique à l'aide d'un mécanisme de certificat reposant sur une clé publique et une clé privée. Maintenant, nous allons décrire le rôle des annuaires LDAP dans la gestion des habilitations ou des autorisations pour l'accès aux applications.

Une application n'est autre qu'une ressource d'un système d'information. Elle peut donc être décrite dans l'annuaire LDAP au même titre que toute autre ressource (une imprimante ou un ordinateur). Par exemple, sa description peut contenir les attributs suivants : l'URL si c'est une application Internet ou accessible *via* l'intranet de l'entreprise, un libellé descriptif, un nom abrégé, le nom de la machine où elle se trouve…

L'annuaire peut alors être utilisé pour décrire les droits d'accès des utilisateurs aux applications. Ceci nécessite un outil capable d'exploiter ces informations pour contrôler effectivement l'accès aux applications. L'annuaire n'est en fait qu'une base de données, mais a l'avantage d'offrir un modèle de données faisant partie des standards du marché et une interface d'accès à l'aide d'un protocole normalisé.

À titre d'exemple nous pouvons citer les produits de la société Sun, qui exploitent totalement cette capacité des annuaires LDAP. Le serveur Web de Sun s'appuie sur l'annuaire pour contrôler l'accès aux pages HTML en fonction des profils de chaque utilisateur. Le serveur de messagerie Sun Messaging Server, partage le même annuaire

LDAP pour rajouter au profil de chaque utilisateur le nom de sa boîte aux lettres et ses caractéristiques si celui-ci en possède. Le serveur d'agenda Sun Calendar Server agit de façon identique.

Nous pouvons aussi citer Active Directory dans Windows 2000/2003, dont la vocation est de gérer les utilisateurs et les habilitations des produits de Microsoft, comme Exchange 2000/2003 et Commerce Server 2000/2003.

Il existe aussi des produits généralistes dont la vocation est d'offrir un outil centralisé offrant les moyens de gérer et de contrôler les accès à un ensemble d'applications, voire à la totalité des applications intranet de l'entreprise. Ce sont en général les mêmes outils que ceux utilisés pour l'identification unique, comme le produit COREid de la société Oblix, Tivoli Access Manager d'IBM ou SiteMinder de la société Netegrity.

L'avantage de tels outils est multiple. Il devient possible de centraliser la gestion des autorisations, et par conséquent d'avoir une stratégie de sécurité cohérente entre les différentes applications de l'entreprise, quel que soit le canal d'accès utilisé. Le fait de réaliser de façon spécifique les contrôles d'accès aux services dans chaque application peut induire des divergences ou des incohérences entre les applications. Il est également important d'appliquer les mêmes règles de sécurité lorsqu'un utilisateur accède à une application via Internet, le WAP ou demain l'Internet mobile avec un téléphone portable. Ces outils disposent de connecteurs dédiés à chaque type d'interface qui partagent un même serveur d'autorisations.

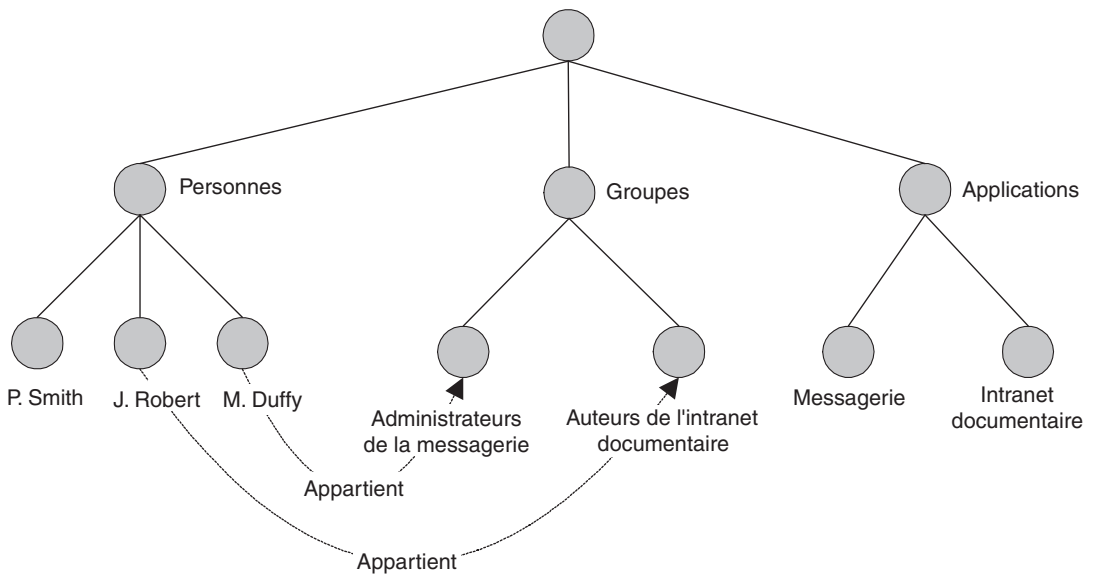


Figure 3.12

Description des habilitations dans un annuaire LDAP

Ceci permet également de réduire les coûts de développement et d'administration des fonctions de sécurité dans les applications. En effet, il ne sera plus nécessaire de développer ces fonctions dans les nouvelles applications et il sera possible d'administrer, à l'aide d'un outil prêt à l'emploi, l'ensemble des règles de sécurité. Enfin, ceci améliore la sécurité car ces outils sont en général largement éprouvé et savent réagir à tous types d'attaques externes à l'instar des antivirus.

Ces outils s'appuient généralement sur les annuaires LDAP. Ils savent d'une part se greffer à n'importe quel annuaire afin de vérifier l'identification de l'utilisateur et son authentification, puis en extraire les informations de son profil nécessaires au contrôle de ces droits. D'autre part, ils s'appuient aussi sur un annuaire LDAP pour sauvegarder les règles d'autorisation. L'avantage est de pouvoir utiliser les fonctions de protection des données offertes par LDAP afin de protéger ces règles, tout en pouvant les partager avec d'autres applications *via* un standard ouvert.

Il existe plusieurs façons de décrire les droits d'accès des utilisateurs à des applications. Le moyen le plus courant consiste à utiliser des groupes statiques ou dynamiques, et à attribuer les droits à un groupe plutôt qu'à un individu, comme le montre la figure 3.12.

Nous décrirons plus en détail les différentes voies possibles dans la suite de ce livre, et nous aborderons une des solutions les plus courantes dans une étude de cas.

Le commerce électronique

L'utilisation des annuaires LDAP dans le commerce électronique se développe de plus en plus. En effet, la plupart des progiciels dédiés à la vente en ligne intègrent en standard une interface LDAP pour l'accès aux profils des utilisateurs. L'avantage d'une telle approche est de pouvoir partager ces profils entre différents sites marchands, et de bénéficier d'un modèle de données prêt à l'emploi.

La plupart des sites de commerce électronique offrent la possibilité aux utilisateurs de passer de l'anonymat ou du stade de visiteur au statut de membre. Un internaute occasionnel peut acheter des produits sur un site et rester anonyme. Il n'a alors pas besoin de fournir des informations sur son profil, hormis son numéro de carte de crédit lors de l'acte d'achat.

En revanche, s'il souhaite être reconnu automatiquement lorsqu'il revient sur ce site pour bénéficier d'offres personnalisées et de ne pas avoir à ressaisir les données de son profil, comme son adresse de livraison, son nom et le numéro de sa carte de crédit, il a tout intérêt à devenir membre du site. Pour cela, il saisit une seule fois les informations le concernant et le site lui attribue un nom et un mot de passe afin de le reconnaître rapidement lorsqu'il se représentera. Ce profil peut aussi être associé à d'autres moyens d'identification comme une carte à puce (ce qui nécessite un lecteur de cartes à puce pour être reconnu) ou encore un cookie, petit fichier résidant sur le poste de travail de l'internaute et contenant un identifiant unique envoyé au site Internet par le navigateur Web.

La base de profils des internautes d'un site marchand constitue un noyau d'information extrêmement précieux. Il permet en effet de connaître les préférences de chacun, les caractéristiques des utilisateurs, leurs comportements d'achat… Bref, tout ce qui permet d'adapter l'offre à la demande, et par conséquent d'optimiser les coûts de publicité du site et d'augmenter les revenus du marchand.

Mais pour que ceci devienne une réalité, il faut que cette base de profils soit la plus large possible. C'est-à-dire qu'il faut qu'elle comprenne un grand nombre d'utilisateurs, et qu'elle contienne un maximum d'informations par utilisateur. Ainsi, un marchand qui offre en ligne aussi bien des billets d'avion que des chambres d'hôtel et des voitures à louer, a tout intérêt à avoir une même base de profils utilisateurs pour ces trois types de produits. Il permettra ainsi à l'internaute de réserver en même temps son billet, sa chambre d'hôtel et sa voiture, associés à une seule facture. Il pourra également lui proposer des hôtels de catégorie supérieure si l'internaute voyage souvent en première classe. Il pourra éventuellement lui offrir une nuit d'hôtel au-delà d'un certain montant d'achats…

Or, vendre des billets d'avion en ligne, réserver des chambres d'hôtel et louer des voitures nécessite des sites Internet et des systèmes d'information différents. Cela exige de se connecter d'une part à des systèmes d'information de compagnies aériennes pour avoir les horaires, et d'autre part à des systèmes de consultation des chambres disponibles dans les hôtels. Il faudra aussi offrir des interfaces homme/machine différentes, adaptées à chaque type de produit. Partager les profils des utilisateurs requiert donc de s'appuyer sur un standard ouvert comme LDAP, assurant l'interopérabilité de ces différents systèmes.

L'apport de LDAP est encore plus manifeste dans le cas de sites marchands destinés aux entreprises (ou BtoB pour Business to Business). En effet, il faudra partager des profils entre différents sites, mais aussi s'adapter à l'organisation des entreprises clientes (voir figure 3.13). Il ne s'agit pas uniquement de gérer le profil d'une personne, mais celui

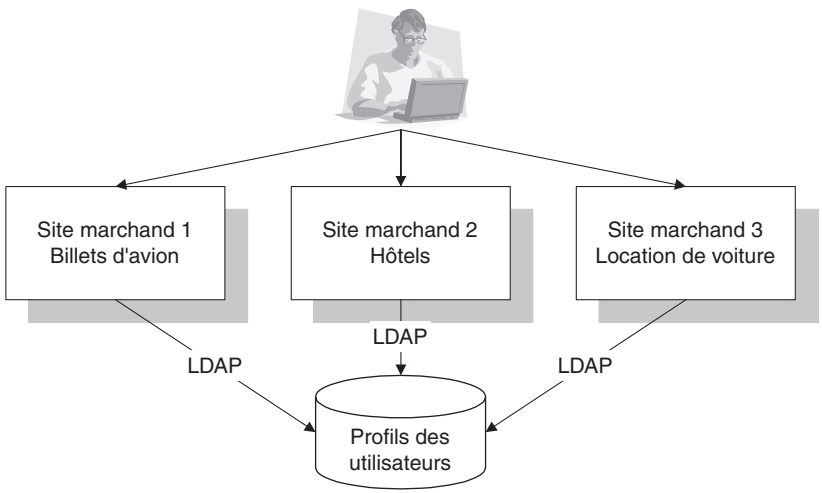


Figure 3.13

Partage des profils utilisateurs avec LDAP entre sites marchands

d'une entreprise, constituée éventuellement de plusieurs filiales ou départements, et de plusieurs acteurs comme des utilisateurs, des acheteurs et des comptables.

Le modèle de données et l'organisation hiérarchique de LDAP sont bien adaptés à ce besoin. Ils permettent d'ajuster la base de profils à chaque entreprise, en tenant compte des rôles de chacun et des services auxquels chaque acteur a droit. Par exemple, seuls les acheteurs pourront effectuer les achats, et seuls certains utilisateurs pourront passer des commandes en ligne. Les comptables recevront les factures et pourront consulter l'historique des achats. L'identification unique et la gestion des habilitations, facilitées par les annuaires LDAP, s'appliquent au commerce électronique BtoB, et y apporte une forte valeur ajoutée.

La plupart des progiciels de commerce électronique du marché sont compatibles avec le standard LDAP pour la gestion des profils des utilisateurs. Nous pouvons citer à titre d'exemple les logiciels suivants :

- le logiciel Commerce Server de la société Microsoft ;
- les produits WebSphere Commerce Suite d'IBM ;
- les logiciels de commerce électronique des sociétés BroadVision, ATG et Vignette.

Les extranets

Qu'est-ce qu'un extranet ? C'est tout simplement l'ouverture d'une partie du système d'information de l'entreprise à ses clients, partenaires et fournisseurs, à l'aide des technologies Internet. Les clients pourront par exemple consulter des factures en ligne ou encore modifier des options d'abonnement. Les fournisseurs pourront également consulter en ligne les appels d'offres d'une entreprise ou encore l'état du stock de certains produits, afin de l'approvisionner automatiquement.

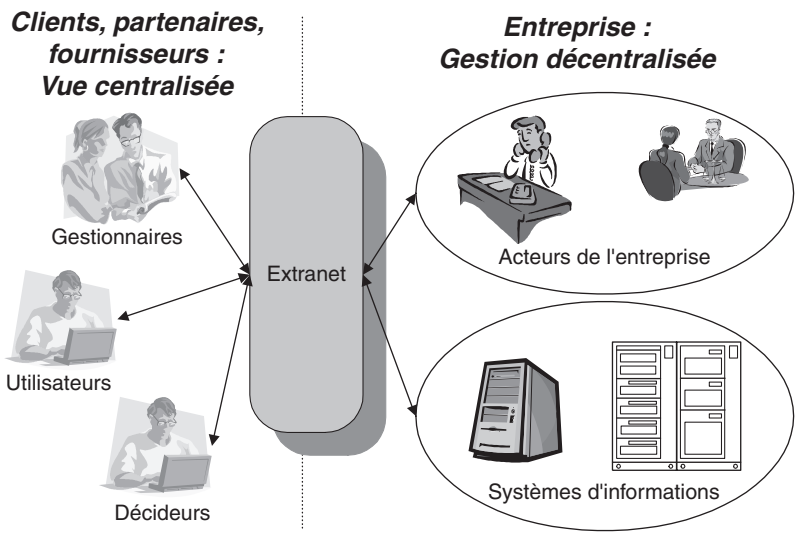
Les apports d'un extranet pour les clients d'une entreprise sont considérables. En effet, il réduit les temps d'attente des clients en leur offrant un accès direct au système d'information sans passer par un opérateur. Il leur donne de l'information quasiment en temps réel comme des encours de consommation ou des relevés de compte. Il facilite l'accès aux services en laissant les clients gérer leurs abonnements et leurs produits de façon autonome (vingt-quatre heures sur vingt-quatre et de n'importe où). En outre, il offre les moyens de personnaliser les informations auxquelles ils ont accès en fonction de leurs profils.

Enfin, l'extranet permet à l'entreprise de réduire les coûts de son service client et de son centre d'appels, de maîtriser les coûts de diffusion d'informations par disquette ou par courrier, d'optimiser le temps passé par les commerciaux à promouvoir de nouvelles offres, d'accroître la fidélisation des clients et de générer des revenus additionnels.

Après les centres d'appels, la mise en place d'un extranet client peut constituer une première étape vers le commerce électronique.

Mais les conditions de succès de l'extranet passent par une vision intégrée de l'offre de l'entreprise et de ses lignes de produits.

Figure 3.14
Qu'est-ce qu'un extranet ?



En effet, il s'agit de donner aux clients une vue centralisée des produits et services de l'entreprise, tout en conservant une gestion décentralisée de ceux-ci dans son organisation actuelle, et tout en intégrant les systèmes d'information existants avec la plate-forme d'un extranet !

L'identification unique, la délégation des fonctions d'administration et la personnalisation constituent des facteurs clés de succès.

- L'identification unique à l'ensemble des services offerts apporte un confort indéniable aux utilisateurs. Elle permet aussi d'améliorer la sécurité de la solution à travers une gestion des habilitations centralisée.

  Le standard LDAP apporte alors un avantage majeur, comme nous l'avons vu précédemment dans le chapitre relatif à la sécurité.

- Un extranet nécessite obligatoirement l'identification des utilisateurs pour des raisons évidentes de sécurité. Mais, plus le nombre d'utilisateurs augmente et plus la gestion des comptes utilisateurs devient fastidieuse et coûteuse pour l'entreprise. Dans le cas du Business to Business, une solution courante consiste à désigner un gestionnaire par client, partenaire ou fournisseur ayant les droits de création d'autres utilisateurs. Celui-ci utilisera l'extranet pour créer, modifier ou supprimer les utilisateurs qui y ont accès. La base des utilisateurs ainsi gérée se trouve toujours dans l'extranet, mais sa gestion est déléguée, ce qui réduit considérablement les tâches d'administration centralisée.

Là aussi, le standard LDAP est tout désigné. Il suffit par exemple de construire un arbre LDAP contenant un nœud pour chaque client, partenaire ou fournisseur ayant accès à l'extranet. Puis il faut déléguer l'administration de cette branche à un utilisateur particulier, qui en sera le gestionnaire.

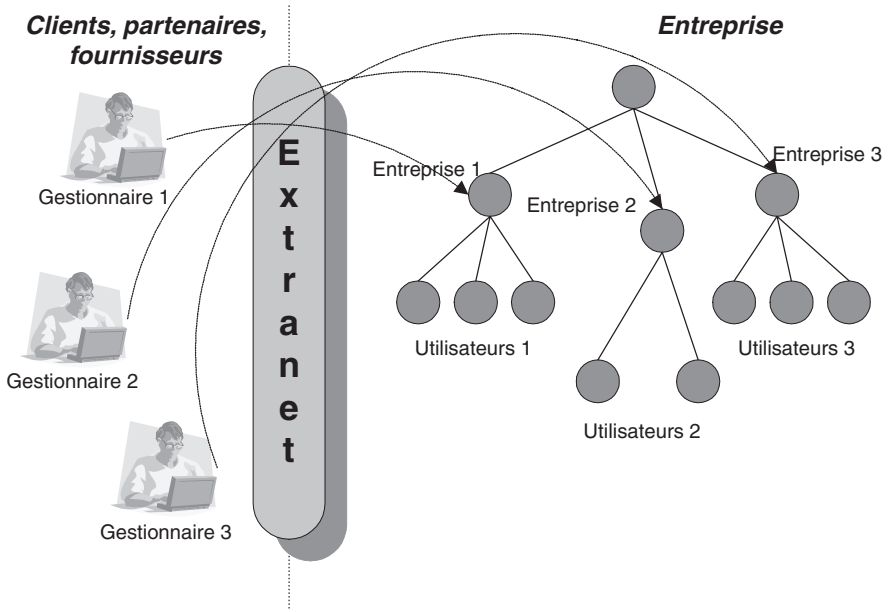


Figure 3.15
Délégation de la gestion des utilisateurs d'un extranet

Dans la figure 3.15, Entreprise 1, Entreprise 2 et Entreprise 3 représentent des entreprises clientes, partenaires ou fournisseurs de l'entreprise mettant à disposition son extranet. Dans chacune de ses entreprises, un utilisateur particulier aura les droits de gérer uniquement les autres utilisateurs de son entreprise dans l'annuaire LDAP de l'extranet.

- La personnalisation a pour objectif d'adapter l'extranet aux besoins de chaque utilisateur. Elle permet de mettre en avant le contenu du site le plus approprié au profil de chacun et de reléguer à un second plan le contenu le moins utilisé.

  La personnalisation comprend :

  – *la présentation de l'extranet* : il s'agit d'afficher uniquement les applications autorisées ou encore les informations éditoriales en fonction des centres d'intérêt sélectionnés ;

– *l'envoi d'informations personnalisées* : comme des alertes sur critères, des messages sur événements, des informations-flashs… ;

– *les contacts* : il s'agit d'offrir la liste des interlocuteurs par client (ingénieur commercial, responsable de compte, support après vente…) avec la possibilité de communiquer et d'échanger des messages et des documents.

La personnalisation apporte une valeur ajoutée par rapport aux services élémentaires d'un extranet. Ses avantages sont les suivants :

– *la fidélisation des clients* : le contenu personnalisé favorise le retour des utilisateurs sur le site, et leur permet de trouver plus facilement des réponses à leurs attentes ;

– *l'enrichissement des profils* : l'analyse du comportement des utilisateurs devient possible en traçant leurs actions sur le site ;

– *les actions marketing ciblées* : il devient possible d'effectuer des segmentations de la clientèle et de rendre plus efficaces les actions marketing ciblées, comme le cross-selling.

Les annuaires LDAP sont bien adaptés à la gestion des profils utilisateurs de l'extranet. Ceux-ci peuvent être des personnes externes à l'entreprise, comme des clients, des partenaires ou des fournisseurs, mais aussi des personnes internes comme des responsables commerciaux ou des responsables après-vente.

La personnalisation en fonction des besoins de chacun peut s'appliquer facilement sur une catégorie d'utilisateurs à l'aide d'une simple requête LDAP, par exemple l'envoi d'une lettre d'information à tous les nouveaux venus ou encore l'envoi par e-mail des coordonnées d'un nouveau contact client dans l'entreprise.

Notons également que LDAP favorise le partage des profils des utilisateurs dans une base de données unique, assurant ainsi une cohérence globale entre les différentes applications offertes et une meilleure réactivité dans le déploiement de nouveaux services sur l'extranet.

Nous présentons dans ce livre une étude de cas sur un extranet clients, décrivant un modèle de données LDAP répondant à ces enjeux.

Les portails d'entreprise

Les annuaires LDAP se situent au cœur des fonctions de communication et de collaboration de l'entreprise à travers son portail car ils en simplifient la gestion et l'administration.

Mais avant tout précisons ce qu'est un portail d'entreprise. C'est l'utilisation des technologies Internet, au sein d'un réseau local d'entreprise, pour des applications de partage d'informations, de communication et de travail de groupe. C'est aussi la fédération des services suivants autour d'une infrastructure commune basée sur les technologies issues d'Internet.

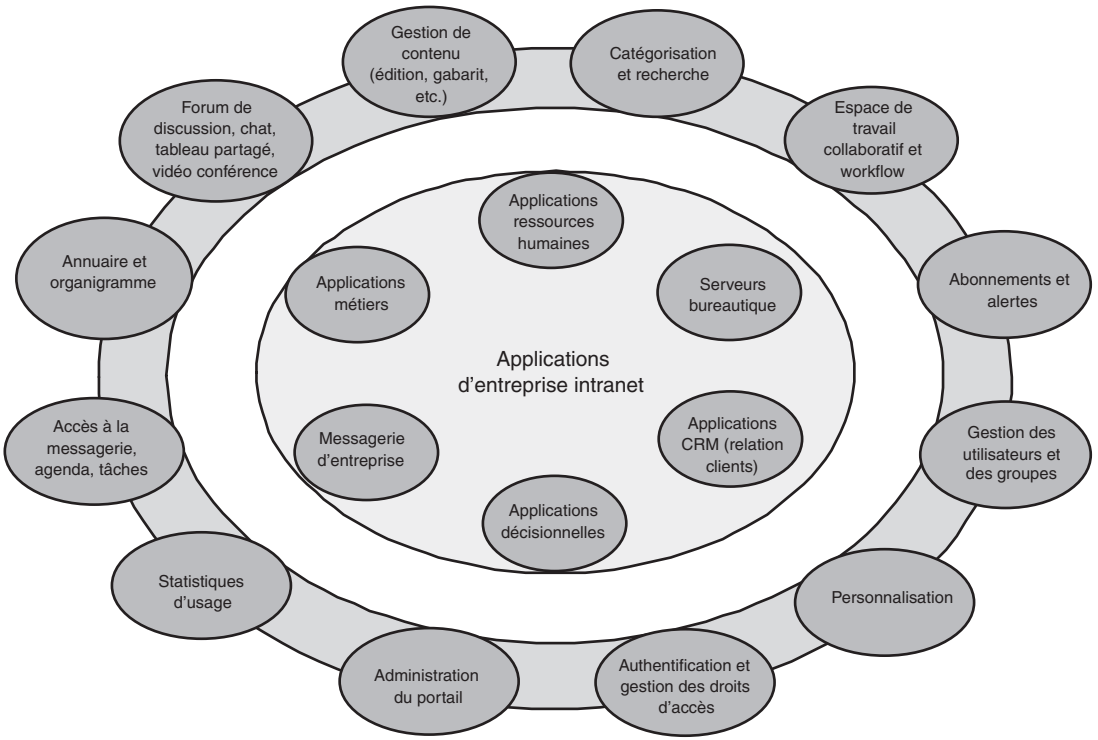


Figure 3.16
Les services d'un portail d'entreprise

Accès à la messagerie électronique, l'agenda partagé et les tâches

Le portail permet généralement l'accès à la messagerie d'entreprise, à l'agenda individuel et aux agendas partagés, ainsi qu'aux tâches individuelles et de groupes. L'accès se fera *via* une interface HTML et un simple navigateur, permettant ainsi la consultation de ses messages à partir d'un accès distant, interne ou externe à l'entreprise.

L'outil de messagerie est souvent couplé à celui de l'agenda partagé, et il possède souvent son propre annuaire. Ce dernier contient les adresses de chacun, mais aussi des listes de diffusion et des adresses de personnes externes à l'entreprise, partagées par tous. L'agenda nécessite, de plus, un annuaire de ressources, comme des salles de réunion.

Annuaire et organigramme

Ici, c'est l'application donnant accès aux informations sur les personnes de l'entreprise, plus communément appelée Pages Blanches. Elle contient aussi l'organigramme de l'entreprise, indiquant les liens hiérarchiques entre les personnes. Cette application possède généralement sa propre base de données. L'exactitude des données de l'annuaire dépendra de l'automatisation des mises à jour à partir de différentes sources, comme

l'application de ressources humaines ou la messagerie d'entreprise, ou bien, à défaut, des fréquences de mise à jour par les administrateurs ou les utilisateurs eux-mêmes.

Forums de discussion, « chat » ou messagerie instantanée, tableau partagé et vidéo conférence

Les forums de discussion nécessitent l'identification de l'utilisateur afin de signaler qui est l'auteur d'un message déposé sur le forum. Si l'outil de forum utilisé est couplé avec la messagerie, ils partagent le même annuaire, mais il peut arriver que ce ne soit pas le cas.

De plus en plus, les entreprises s'équipent d'outils permettant la communication de façon synchrone entre plusieurs personnes. Le « chat », ou la messagerie instantanée, permet d'échanger des messages courts lorsque plusieurs personnes se trouvent connectées au réseau en même temps. Le tableau blanc partagé donne la possibilité de visualiser simultanément un document de travail contenant des textes et des dessins pouvant être modifiés par les personnes en ligne. Avec la vidéo conférence, on communique à travers le son et l'image en utilisant son ordinateur et le réseau de l'entreprise.

Tous ces services nécessitent aussi un référentiel d'utilisateurs partagé.

Gestion de contenu

Elle contient en général des processus rigoureux de publication de documents. Les utilisateurs valident le contenu avant publication, et les complètent par des fiches signalétiques qui permettent de les classer ou d'effectuer des recherches multicritères. Les personnes autorisées à réaliser des publications et à saisir la fiche signalétique doivent être identifiées afin de pouvoir vérifier leurs habilitations.

Par ailleurs, certains documents peuvent être protégés et réservés à un groupe d'utilisateurs. Il est donc nécessaire de les identifier avant de leur donner accès à la base de documents.

Catégorisation et recherche

Il s'agit de moteurs de recherche capables de trouver tout type d'information accessible à travers le portail, à l'aide de critères de recherche multiples. Ces critères peuvent être basés soit sur l'existence de mots dans les documents, soit sur des mécanismes plus élaborés comme la recherche sémantique ou les réseaux bayésiens (similitude entre typologies d'information). Certains moteurs de recherche sont aussi capables de classer automatiquement les informations trouvées dans une catégorie prédéfinie.

Dans tous les cas, la principale difficulté réside dans l'adéquation du périmètre de la recherche aux droits de l'utilisateur qui soumet celle-ci. Le moteur doit être en mesure de tenir compte de ses habilitations sur les catégories de documents auxquels il a droit.

Espace de travail collaboratif et workflow

Il s'agit ici d'un ensemble de services facilitant le travail collaboratif entre différentes personnes, à l'aide d'un réseau local ou étendu comme Internet. Un espace de travail

contient généralement un ensemble de documents concernant un projet ou un sujet donné, des forums de discussion relatifs à la thématique traitée, des tâches affectées aux différents membres du groupe, la description des réunions en cours (agenda, intervenants, lieu), etc.

Des moteurs de workflow sont très utiles dans ce type d'environnement, car ils permettent d'associer des processus à la publication d'informations sur le site. Par exemple, un compte rendu de réunion rédigé par un des intervenants devra être validé par l'organisateur de la réunion avant publication sur le site.

Là aussi, il est important de disposer d'une base d'utilisateurs contenant des informations professionnelles, comme l'adresse de messagerie et le rôle dans l'organisation.

Abonnements et alertes

Afin d'accéder plus rapidement aux informations pertinentes, les utilisateurs peuvent bénéficier, à travers le portail d'entreprise, d'un service d'abonnements. Celui-ci est chargé d'envoyer des alertes lorsqu'un événement survient dans le portail, comme la création d'un nouveau document ou bien d'un forum de discussion relatif à un sujet donné.

Les alertes permettent aux utilisateurs d'accéder aux informations en mode non sollicité (ou en mode *push*) sur divers canaux de communication, comme la messagerie électronique ou les messages SMS sur un téléphone mobile.

De nouveau, il faut disposer d'un annuaire contenant la liste des utilisateurs et leurs adresses en fonction du canal de communication choisi (mobile, messagerie, etc.).

Nous constatons que toutes ces applications partagent les mêmes besoins, à savoir :

1. référencer l'ensemble des utilisateurs ayant accès aux fonctions et associer à chaque utilisateur des informations de profil comme l'adresse de messagerie, d'autres adresses électroniques, comme le numéro de téléphone mobile pour les messages SMS, le rôle, les préférences, etc.
2. identifier l'utilisateur et contrôler ses habilitations aux services offerts ;
3. gérer des groupes d'utilisateurs pour associer des rôles (par exemple valider des documents) ou des services à ces groupes (par exemple, envoyer un message à un groupe, qui devient alors une liste de diffusion).

Pour répondre de façon cohérente à ces besoins, il existe deux possibilités : soit trouver le produit miracle qui répond dans un même outil à l'ensemble des services requis, soit s'appuyer sur un standard ouvert permettant de partager une même infrastructure tout en se servant d'outils dédiés pour chacun de ces services.

Les outils intégrés et offrant l'ensemble des services cités ci-dessus existent bien : nous pouvons citer à titre d'exemple des produits de portail d'entreprise comme ATG, Broadvision, Vignette, Microsoft Sharepoint Server, Lotus Domino de Lotus et d'autres. Mais il existe toujours un besoin non couvert, comme la gestion électronique de documents, la messagerie instantanée, la vidéo conférence, l'identification unique (SSO ou *Single Sign On*) et le contrôle d'accès aux applications existantes. Cela nécessite la mise en œuvre d'un ou de plusieurs outils additionnels.

Le standard LDAP répond ici à cette problématique. Il constitue le socle élémentaire de l'infrastructure de gestion des identités d'un portail sur lequel reposent les outils ou les développements spécifiques couvrant chacun des services cités.

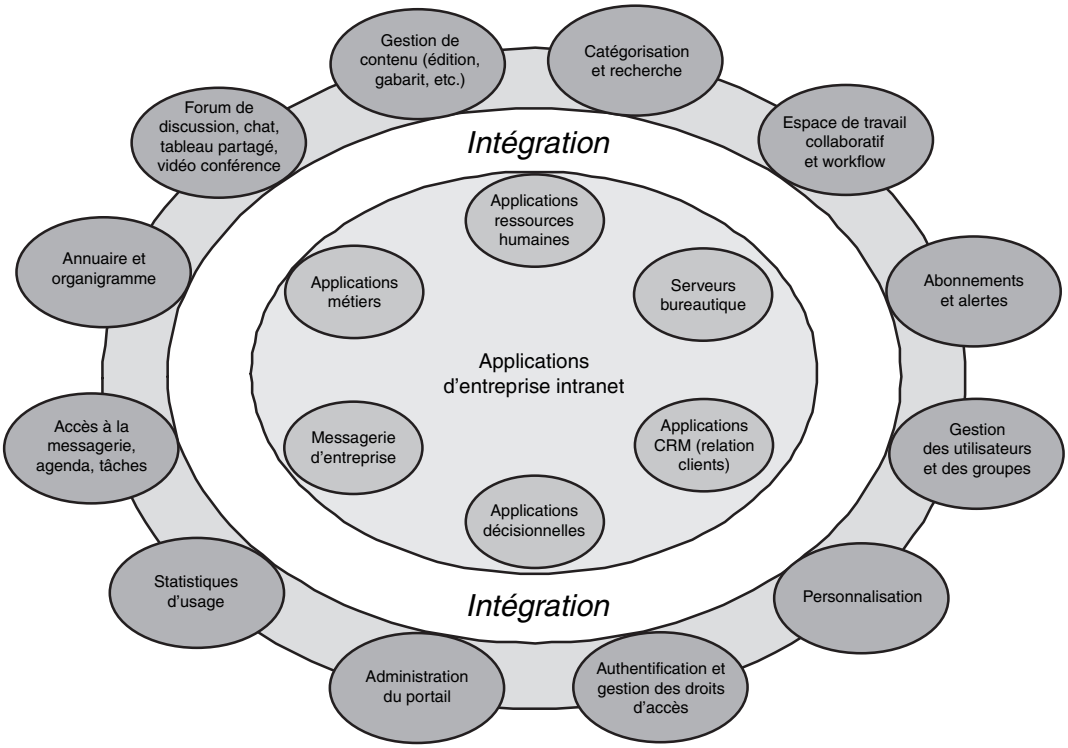


Figure 3.17

Les services d'un portail, fédérés par un annuaire LDAP

En effet, il permet de référencer les utilisateurs et leurs profils dans une base de données partagée par tous. Il rend possible la gestion de l'identification des utilisateurs et de leurs habilitations, comme nous l'avons décrit précédemment dans ce chapitre. Enfin, il permet de gérer et de partager des groupes d'utilisateurs, qu'il est possible de créer de façon dynamique à l'aide de requêtes sur l'annuaire ou de façon statique au moyen de la classe d'objet dédiée aux groupes dans le standard LDAP.

La plupart des outils du marché dédiés aux portails d'entreprise supportent d'ores et déjà le standard LDAP. Il est donc possible de les utiliser simultanément, et de tirer ainsi parti des points forts de chacun, tout en partageant le même référentiel des utilisateurs et des habilitations à l'aide de LDAP.

La mise en œuvre d'un annuaire LDAP au sein d'un portail d'entreprise apporte donc une gestion optimale des utilisateurs et de leurs profils, et la possibilité de partager le référentiel des personnes et des organisations avec l'ensemble des outils du marché dédiés aux applications intranet.

Quelques exemples d'applications par secteur de marché

Nous souhaitons ici donner quelques exemples de mise en œuvre d'annuaires et de gestion des identités, justifiés par les métiers des entreprises et tenant compte de leurs spécificités. Quels sont, par exemple, les usages et les apports des annuaires dans le secteur des télécommunications, des banques, des assurances et de la grande distribution ? Ces exemples sont issus de cas réels. Nous ne citerons pas les sociétés pour des raisons de confidentialité, mais nous pouvons facilement imaginer que les besoins ayant justifié la mise en place d'un annuaire pour l'une d'entre elles, sont les mêmes pour celles ayant un métier similaire.

Les télécommunications

Le secteur des télécommunications est à l'origine des standards comme X500 et LDAP, dont l'objectif initial était de normaliser l'usage des annuaires dans le cadre de la téléphonie et de la messagerie électronique. Aujourd'hui, les annuaires LDAP, la gestion et la fédération des identités, répondent à des enjeux majeurs dans le cadre des services de télécommunications offerts aux clients.

Les portails Internet des ISP (*Internet Service Provider* ou FAI, Fournisseur d'accès Internet) constituent de bons exemples d'usages d'annuaires LDAP, de gestion et de fédération des identités.

En ce qui concerne la gestion des identités et les annuaires LDAP, la plupart de ces portails s'appuient sur ceux-ci pour identifier et authentifier les utilisateurs, offrir des services de messagerie, ainsi que pour y sauvegarder des informations de profils à des fins de personnalisation. L'avantage d'une telle solution est de pouvoir constituer un seul référentiel, basé sur le standard LDAP, permettant de partager la base d'utilisateurs et les services associés (identification, authentification, etc.) entre différents services offerts par l'opérateur, *via* son portail, comme la météo, les nouvelles, les services marchands, etc.

Les annuaires LDAP constituent ainsi une brique essentielle de l'infrastructure de l'opérateur, comme c'est le cas pour la messagerie (référencement des adresses de messagerie, routage, vers le serveur contenant la boîte aux lettres de l'utilisateur, etc.), ou pour le portail Internet, à des fins d'authentification et de personnalisation. La particularité de ces infrastructures est qu'elles doivent supporter une grande quantité d'utilisateurs. En effet, le nombre de clients d'un service de téléphonie mobile, voire ceux d'un ISP s'élève généralement à quelques millions. L'usage d'annuaires LDAP est particulièrement adapté à ce besoin, car ils sont très performants en lecture et sont capables de supporter une charge importante, tout en offrant un haut niveau de disponibilité.

D'autre part, les portails et les services offerts par les opérateurs de télécommunications donnent aussi l'accès à des services fournis par des partenaires (commerçants, fournisseurs de contenu, etc.). Ces derniers doivent généralement pouvoir récupérer des informations concernant l'identité des utilisateurs comme leur adresse de messagerie, leur nom, leur langue préférée, leur fonction dans l'entreprise, etc. De plus, certains opérateurs peuvent établir des relations de partenariat avec d'autres opérateurs, offrant ainsi un service à

l'échelle mondiale à leurs clients respectifs (c'est le cas, par exemple, de Vodaphone et SFR, filiale de Cegetel en France). Dans ces circonstances, le partage d'un seul et unique annuaire LDAP entre l'opérateur et ses partenaires ne sera pas aisé. En revanche, une solution basée sur la fédération des identités, telle que nous l'avons décrite précédemment, offre le meilleur niveau de sécurité, de flexibilité et de facilité d'intégration.

Par ailleurs, les opérateurs de télécommunications offrent des extranets pour leurs clients « entreprises » (dans le cadre d'applications de gestion de la relation clients) et pour leurs distributeurs. Ainsi, il est possible à une entreprise de consulter en ligne la facture de sa flotte de mobiles, de modifier des options d'abonnement et de commander de nouveaux produits à travers un accès sécurisé. Il sera aussi possible à un distributeur de passer commande en ligne et de modifier les abonnements de ses clients. Il sera alors nécessaire d'identifier et d'authentifier l'utilisateur, puis de lui donner accès aux services de façon personnalisée, en tenant compte par exemple du fait que c'est un client particulier, un client entreprise PME, un client entreprise grand compte, ou un distributeur. L'usage d'une solution de gestion des identités, basée sur un annuaire LDAP, ou de fédération des identités, dans le cas de clients de taille importante, apporte des avantages indéniables, aussi bien à l'opérateur qu'aux utilisateurs.

Les assurances

La plupart des assurances offrent, à ce jour, des services sur Internet permettant aux prospects et aux clients d'obtenir des devis en ligne, de déclarer des sinistres, de souscrire à de nouveaux produits, etc. Ces services nécessitent que l'utilisateur s'identifie et s'authentifie, à des fins de mémorisation de son profil et de personnalisation des services offerts, en fonction des abonnements souscrits. L'usage d'un annuaire LDAP pour le site Internet permet de renforcer la sécurité et la confidentialité d'accès aux données personnelles de l'utilisateur. Il permet aussi de faciliter l'intégration de différents progiciels utilisés ou applications développées afin d'offrir à l'utilisateur un mécanisme d'authentification unique. Et enfin, il permet de déléguer la gestion des données à un administrateur, voire à l'utilisateur lui-même, notamment dans le cadre de clients entreprises.

Par ailleurs, les assurances offrent des services en ligne à leurs courtiers leur permettant d'accéder à la gestion de leurs clients, mais aussi à des données contractuelles propres à leurs accords avec l'assurance. Là aussi, l'usage de solutions de gestion des identités et d'annuaire LDAP pour les courtiers permet de sécuriser l'accès aux services en ligne, à travers des mécanismes d'authentification forts (certificat, carte à puce, etc.) si nécessaire, et à travers la possibilité de crypter et de signer des contrats souscrits et échangés en ligne. Notons aussi que les courtiers peuvent être constitués d'une multitude de petits cabinets comprenant quelques personnes, ce qui rend la gestion des utilisateurs par les administrateurs de l'assurance fastidieuse. Il est donc plus commode de déléguer la gestion des utilisateurs aux courtiers eux-mêmes, ce qui est plus facile à faire avec un annuaire LDAP et des outils de délégation d'administration associés.

Enfin, les assurances s'appuient sur un réseau de partenaires, comme des réparateurs ou des experts chargés d'effectuer un devis lors d'un sinistre. Certaines assurances peuvent

fournir des services en ligne à ces partenaires, leur donnant accès, par exemple, à des conditions commerciales personnalisées, ou bien à l'historique des interventions effectuées. Là aussi, l'usage de solutions de gestion des identités et d'annuaire LDAP facilite l'administration des comptes utilisateurs et permet de sécuriser l'accès aux services en ligne, à travers des mécanismes d'authentification forts (certificat, carte à puce, etc.) si nécessaire, et la possibilité de crypter et de signer les informations échangées en ligne.

Les banques

De la même façon que les assurances et les opérateurs de télécommunication, la grande majorité des banques offrent à leurs clients des services en ligne permettant d'accéder à l'état des comptes bancaires, d'effectuer des transactions boursières ou des ordres de virement sur Internet.

Un des principaux enjeux, dans la gestion des identités, est naturellement la sécurité. Les banques se doivent d'assurer un accès protégé, sécurisé et proposant des mécanismes d'authentification forts si nécessaire (cas des accès Internet offerts par les banques privées d'investissement par exemple). Ceci s'applique aussi bien aux clients accédant à des services en ligne, qu'aux employés de la banque. En effet, dans une banque de détail, par exemple, le taux de rotation des chargés de clientèle est assez élevé. Il nécessite donc une gestion rigoureuse des identifiants et mots de passe, et surtout des habilitations d'accès aux applications de gestion de la relation client (consultation des comptes, accès aux offres produits, souscription à de nouveaux produits comme un crédit, etc.). Ces habilitations peuvent dépendre aussi du rôle du chargé de clientèle, de sa position hiérarchique (responsable d'agence ou pas) et de ses compétences. La gestion des identités des employés de la banque à l'échelle de l'entreprise va permettre d'optimiser les tâches d'administration et d'assurer un contrôle global de la sécurité, conformément à la stratégie de sécurité de l'entreprise.

Notons enfin que les banques sont aussi de bonnes candidates pour la fédération des identités. En effet, elles peuvent être amenées à fournir des services en ligne, comme la souscription de crédit à la consommation, à travers des sites de commerce électronique partenaires. Dans ce cas, une solution de fédération des identités apporterait plus de souplesse, une facilité d'intégration avec plusieurs sites marchands, et plus de sécurité et de confort d'utilisation pour le client final.

La grande distribution

Les entreprises de grande distribution sont généralement constituées d'un ensemble de magasins (concessions ou filiales) et d'un siège, répartis dans un ou plusieurs pays. Chaque pays, voire chaque magasin, peut avoir son propre système d'information, offrant des services locaux comme la gestion de stock ou les commandes fournisseurs. D'autres applications peuvent être centralisées au niveau du siège de l'entreprise, comme la messagerie ou les ressources humaines, ou encore des applications décisionnelles permettant de faire une analyse des ventes consolidée par produit ou par saison.

Une des particularités de la grande distribution est le taux de rotation des employés des magasins et l'autonomie de ces derniers. En effet, les personnes en magasin (caissières, chefs de rayon, chefs de produits, prestataires externes, etc.) peuvent changer assez fréquemment, et le magasin peut être un affilié ou avoir sa propre gestion des ressources humaines. Il est indispensable que tout nouvel arrivant ou tout changement de fonction soit intégré rapidement, et ceci, aussi bien au niveau des applications locales, que nationales, afin que la personne puisse devenir opérationnelle le plus vite possible.

Par ailleurs, les chargés de rayon doivent pouvoir accéder rapidement aux informations produits et aux stocks, tout en étant mobiles dans le magasin. Les postes de travail installés en magasin sont généralement vulnérables, que ce soit des postes fixes ou mobiles, comme des Tablets PC équipés de liaison Wi-Fi. Dans le premier cas, ils peuvent être accessibles par toute personne étrangère au personnel, et dans le deuxième cas, un poste mobile sans fil peut être « oublié » et dérobé facilement. Les applications sont donc accessibles en magasin, à partir des PC qui peuvent se trouver dans les rayons fréquentés par des personnes externes à l'entreprise. Il est par conséquent important de pouvoir gérer de façon rigoureuse l'identification et l'authentification des utilisateurs, ainsi que l'ajout, la modification ou la suppression des accès aux applications d'entreprise, et les droits d'accès à celle-ci, afin de minimiser le risque d'erreur et d'interdire tout accès illicite à des données confidentielles.

Là aussi, la solution passe par la mise en place d'un ou de plusieurs annuaires LDAP et par une gestion des identités partagée entre les différentes applications, comme la consultation des stocks, la messagerie, l'accès à des rapports sur l'intranet du magasin, etc. Comme nous l'avons évoqué précédemment, certaines enseignes de la grande distribution étudient d'ores et déjà la possibilité d'équiper les employés mobiles d'ordinateurs portables (type Tablets PC ou PDA) et reliés par un réseau Wi-Fi avec le système d'information du magasin. Ceci permet aux personnes itinérantes de prendre leur PC avec elles, réduisant ainsi les risques d'accès par des tiers. Mais il sera quand même nécessaire de sécuriser l'accès au réseau Wi-Fi en déployant des certificats sur chacun des postes de travail afin de crypter les échanges de données, ce qui nécessite la mise en œuvre d'une solution de gestion des identités et d'annuaires LDAP.

Notons enfin qu'un annuaire commun à l'ensemble des employés d'une entreprise de grande distribution va améliorer la communication sur les rôles et les coordonnées de chacun, à l'aide d'applications de type pages blanches, organigramme et trombinoscope ; ce qui est d'autant plus appréciable que le taux de rotation du personnel est élevé et que l'entreprise est répartie géographiquement sur plusieurs magasins et dans plusieurs pays.

L'industrie

Les entreprises industrielles travaillent de plus en plus avec beaucoup de fournisseurs. C'est le cas par exemple de l'industrie automobile ou de l'aéronautique, qui sous-traitent la fabrication de certains composants comme les moteurs, les tableaux de bord, les pneus ou les vitres des véhicules et des avions. La maîtrise des coûts et la compétitivité de ces entreprises va dépendre essentiellement de l'optimisation de la chaîne logistique, de la

maîtrise du cycle de production et des caractéristiques des produits fournisseurs, et, bien entendu, d'une bonne intégration des systèmes d'information des fournisseurs avec ceux de l'industriel.

Par exemple, il sera nécessaire de fournir des accès extranet aux différents partenaires, leur permettant de suivre en quasi temps réel l'évolution du stock et des prises de commande, afin de pouvoir réguler en conséquence leur production. Dans le cas de plusieurs fournisseurs, l'industriel pourra aussi constituer des places de marché électroniques lui permettant d'obtenir la meilleure offre, et dans les meilleurs délais. Réciproquement, ces fournisseurs vont devoir donner accès à leurs systèmes d'information, afin de fournir, par exemple, des informations détaillées sur les caractéristiques techniques de leurs produits. Ils pourront encore permettre à l'industriel de suivre l'évolution de ses commandes et de s'assurer du bon respect du cadre contractuel et du processus qualité, ainsi que des différentes étapes de fabrication et de livraison, et ceci le plus en amont possible, afin d'anticiper tout retard ou problème.

D'autre part, ces industriels peuvent s'appuyer sur des réseaux de distribution constitués de petites ou moyennes entreprises, chargées de vendre leurs produits dans différents lieux et pays. C'est le cas des constructeurs automobiles. Ils s'appuient sur un réseau de revendeurs à qui ils devront fournir des accès au système d'information, afin de passer des commandes, de consulter l'avancement de la fabrication d'un produit ou de leur communiquer des informations sur les nouvelles offres.

Une solution de gestion des identités des employés, des fournisseurs et du réseau de distribution va permettre de mieux contrôler la sécurité, de personnaliser les accès en fonction du rôle et du profil de chacun. Elle donne ainsi accès plus efficacement à la multitude de services offerts, et apporte une meilleure « agilité » de l'entreprise. Celle-ci sera capable ainsi de s'adapter plus facilement à tout changement d'organisation chez un fournisseur ou un distributeur, voire à toute modification de fournisseurs et de partenaires. De plus, les annuaires associés à chacune de ces catégories de personnes vont permettrent de mieux communiquer sur les fonctions, rôles et coordonnées de chacun.

Par ailleurs, les solutions de fédération des identités vont faciliter l'intégration entre les services offerts aux employés par l'entreprise elle-même et ceux proposés par ses partenaires et fournisseurs. Par exemple, un ingénieur pourra accéder à l'intranet de son entreprise pour rechercher des informations sur la production, et accéder de façon transparente à l'extranet d'un fournisseur pour consulter la documentation d'un produit, ou pour demander un support technique particulier.

L'administration électronique

La plupart des administrations publiques du monde cherchent à tirer profit des nouvelles technologies de l'information et de communication afin de réduire et maîtriser leurs coûts de fonctionnement, d'améliorer les services aux citoyens et aux entreprises, de mieux communiquer avec eux, d'augmenter la réactivité des services publics. Enfin elles assurent plus de cohérence dans les services offerts par différents ministères, comme la santé, les services sociaux, les collectivités locales ou la fiscalité.

L'administration publique est au cœur des interactions entre les agents des différents ministères, des citoyens et des entreprises. Un ministère a besoin de faire communiquer ses services avec ceux d'un autre ministère, comme dans le cas de l'Europe avec d'autres pays et de la Commission Européenne. Il a aussi besoin d'interagir avec les citoyens afin de leur offrir différents types de services comme la déclaration d'impôts, le vote électronique ou la gestion du dossier médical et des remboursements de frais médicaux. Enfin, il a besoin d'interagir avec les entreprises pour des services comme la déclaration de la TVA ou le prélèvement des cotisations sociales.

Tous ces services sont offerts par des systèmes d'information que les administrations cherchent de plus en plus à ouvrir à l'extérieur. C'est-à-dire aussi bien aux agents d'autres administrations qu'aux citoyens et aux entreprises. Comment gérer alors l'ensemble des identités des utilisateurs dans un environnement où le nombre de personnes est particulièrement élevé, où les règles de sécurité et de respect des libertés individuelles doivent être appliquées de façon irréprochable, et enfin où la complexité des organisations et des interactions entre les différentes entités s'ajoute à des procédures administratives qui doivent être rigoureusement suivies ?

Dans ces conditions, il est bien entendu utopique de créer un annuaire ou un référentiel unique contenant l'ensemble des agents d'un ministère, comme celui de l'Éducation nationale (constitué de plus d'un million de personnes en France), et, de surcroît, celui de l'ensemble des ministères. De même, il est aussi extrêmement difficile d'élaborer un annuaire unique, utilisé par l'ensemble des services en ligne offerts aux citoyens. D'une part, ces annuaires seront volumineux et risquent d'évoluer lentement, voire très difficilement face à tout nouveau besoin. D'autre part, ils doivent respecter les libertés individuelles et donc *ne pas permettre* de retrouver les informations sur une personne à partir d'un identifiant unique, comme son numéro de sécurité sociale. Enfin, ils doivent être très robustes car tout problème dans l'annuaire risque d'interrompre l'ensemble des services de l'administration.

La solution passe ici par la fédération des identités qui apporte plus de souplesse dans l'intégration des données issues de différentes applications, et de différents services administratifs. En effet, elle établit des cercles de confiance permettant de partager des informations sur les individus en toute sécurité, voire de façon anonyme (par exemple, seul un identifiant générique et anonyme peut être véhiculé d'un service à l'autre sans communiquer l'identité de la personne auquel il appartient). Elle s'applique aussi bien au cas des citoyens, afin de fédérer leurs données d'identités se trouvant dans différents services administratifs, qu'à celui des relations entre ministères, afin de partager les données et services offerts aux agents, comme un portail de communication ou de travail collaboratif.