

points de vue sur la technologie

Septembre 2008

TABLE DES MATIÈRES

Ce numéro de *Points de vue sur la technologie* de CGI traite de la question de l'identité et du rôle qu'elle joue aujourd'hui dans la conduite des affaires. Il aborde ce sujet sous cinq angles importants :

- l'identité et l'entreprise;
- les utilisations de l'identité;
- les conséquences du Web 2.0;
- l'identité et l'architecture orientée services (AOS);
- l'authentification centrée sur l'utilisateur.

En conclusion, nous présentons les solutions de gestion des identités et des accès de CGI.

Pour nous donner votre opinion sur ces sujets ou pour vous renseigner davantage sur CGI, écrivez-nous à info@cgi.com.

Gérer efficacement l'identité dans le monde en réseau

La gestion des identités est l'un des grands défis qui se posent aux entreprises modernes. Auparavant réservé aux universitaires et aux spécialistes de la sécurité, le débat entourant l'identité, son utilisation et sa protection appartient désormais au domaine public. Ce débat a des ramifications très vastes, touchant par exemple les politiques d'immigration, la prévention du terrorisme, la protection des renseignements personnels, la participation aux réseaux sociaux et le commerce électronique.

Malgré l'importance croissante de ces enjeux, nos solutions informatiques n'apportent pas encore des réponses satisfaisantes aux questions soulevées.

Le commerce électronique a connu une croissance spectaculaire et sa portée continue à s'élargir. Les phénomènes liés au Web 2.0 comme le réseautage personnel et les blogues ont créé de nouvelles tribunes où les gens souhaitent s'identifier. Le nombre de sites augmente et le nombre de personnes qui visitent des sites – offrant entre autres des services personnalisés – augmente davantage. Ainsi, le volume d'ouvertures de session ne cesse jamais de croître et un nombre plus élevé d'entités stockent des renseignements toujours plus nombreux.

Plus la quantité de renseignements personnels circulant sur Internet est grande, plus les risques d'atteinte augmentent. On s'attend à ce que le secteur des TI gère ces risques, ce qui explique en grande partie pourquoi les entreprises n'ont pas cherché à comprendre comment tirer parti des flux de renseignements pour atteindre de nouveaux objectifs d'affaires. Les entreprises qui utilisent intelligemment les mécanismes de gestion de l'identité peuvent en retirer des gains substantiels, en fidélisant leurs clients tout en diminuant les risques et les coûts administratifs. Elles doivent établir un juste équilibre entre la sécurité, la convivialité, la collecte de données sur les clients et la protection des renseignements personnels.

Ce numéro de *Points de vue sur la technologie* de CGI examine l'évolution de la question de l'identité et du rôle qu'elle joue dans les affaires. Le lecteur y trouvera de nouvelles définitions ainsi que des réflexions sur la manière d'utiliser l'identité et les solutions d'authentification pour accélérer la croissance stratégique, à partir des angles suivants :

- **L'identité et l'entreprise** – La gestion de l'identité crée des occasions et des risques. Il faut établir un équilibre qui convient à l'entreprise elle-même, à ses partenaires et à ses clients.
- **Les utilisations de l'identité** – Au début, l'identité ouvrait, littéralement, des portes – d'immeubles ou de systèmes. L'utilisation des TI ayant évolué, les personnes ont acquis plusieurs identités différentes et s'en servent de façons inédites.
- **Les conséquences du Web 2.0** – Les gens veulent révéler leur identité sur Internet. L'afflux de renseignements, dans le monde ouvert en réseau, suscite des inquiétudes relatives à la sécurité, à la protection des renseignements personnels et à la réputation.
- **L'identité et l'architecture orientée services** – L'AOS permet la prestation de services sur mesure, aux bons moments. Il faut toutefois que les entreprises créent de nouvelles architectures pour accéder aux services.


L'authentification centrée sur l'utilisateur – Nous nous approchons de méthodes de gestion de l'identité normalisées qui rendent l'utilisateur maître de ses renseignements

En conclusion, nous présentons les solutions de gestion des identités et des accès de CGI. CGI a élaboré une vision cohérente des moyens que les entreprises peuvent prendre pour retirer des gains stratégiques des activités de gestion de l'identité, tout en demeurant attentives aux occasions et aux risques inhérents à ces activités.

L'identité et l'entreprise

Pour l'entreprise, la gestion de l'identité représente des menaces et des occasions, des entraves et des débouchés. Partout dans le monde, les médias font leurs choux gras des déboires liés aux vols d'identité, par exemple la fraude de 7 milliards \$ dont la Société Générale a été victime. Les chefs de l'exploitation n'ont pas le choix : il faut investir massivement dans des protocoles, dans des systèmes de conformité et dans des projets visant à protéger l'information. Les chefs de l'information non plus : ils doivent satisfaire aux exigences sans mettre en place des systèmes exagérément complexes qui gonfleraient excessivement les coûts et nuiraient à l'agilité de l'entreprise.

Gestion efficace des identités

<p>Avantages</p> <ul style="list-style-type: none"> • Satisfaction accrue des clients • Lancement d'innovations facilité grâce : <ul style="list-style-type: none"> ○ à la personnalisation du service; ○ à la convivialité accrue; ○ à un environnement centré sur les utilisateurs. • Réduction de la fraude et des vols d'identité grâce : <ul style="list-style-type: none"> ○ à des méthodes de gestion des utilisateurs diminuant la complexité et la redondance; ○ aux liens de confiance et à la normalisation. 		<p>Défis</p> <ul style="list-style-type: none"> • Prévenir la fraude sans compromettre la convivialité. • Personnaliser sans empiéter sur la vie privée. • Respecter les exigences de conformité en conservant l'agilité. • Protéger les réputations sans restreindre la liberté ni la créativité.
--	---	---

Aujourd'hui, plus que jamais, toute entreprise doit incorporer sa manière de définir et d'utiliser les identités – pour elle-même, pour ses clients et pour ses partenaires – aux toutes premières étapes de la conception de son architecture fonctionnelle et technologique. D'immenses possibilités s'ouvrent aux entreprises qui font les choses correctement; par contre, les risques sont tout aussi énormes pour celles qui se trompent.

Les utilisations de l'identité

« Identité » n'est pas synonyme de « nom d'utilisateur ». L'identité est l'image que nous nous faisons de nous-mêmes et que les autres ont de nous. Nous pouvons la façonner au moyen des renseignements que nous communiquons. L'identité est aussi un ensemble de caractéristiques uniques qui authentifie qui nous sommes d'une manière satisfaisante pour une autorité ou un fournisseur de services. Tout dépend du contexte et du point de vue.

Qui nous sommes

Dans la plupart des contextes, l'identité fait appel à un nombre restreint de renseignements parmi tous ceux qui nous décrivent. De fait, quand on nous demande de nous identifier, il suffit généralement de fournir une preuve raisonnable que nous détenons légitimement une pièce d'identité pertinente dans les circonstances, par exemple un passeport avec photo, une carte de crédit signée, ou encore un nom d'utilisateur et un mot de passe. Il existe une grande variété d'identifiants et d'authentifiants. De même, nous possédons un vaste éventail d'attributs qui ne servent pas nécessairement à prouver qui nous sommes mais constituent des éléments importants de notre identité personnelle.

Ce que nous pouvons faire

On peut utiliser l'identité pour nous accorder ou nous refuser l'accès à quelque chose – un pays, un édifice, un système informatique, un renseignement ou une bouteille de vin. Les entreprises peuvent aussi tenter de comprendre notre identité pour prédire ce qui nous intéressera, par exemple des produits que nous pourrions apprécier. L'identité peut déterminer notre réputation ou celle de notre employeur. Certains aspects de notre identité sont officiels, vérifiés et contrôlés par le gouvernement, notre banque ou notre employeur. Et nous sommes entièrement maîtres d'autres aspects, qui ne sont pas nécessairement vérifiables.

Qui certifie que nous disons vrai?

La vision que vous avez de votre identité n'est probablement pas identique aux caractéristiques qui intéressent le gouvernement, le vendeur d'alcool ou le service des ressources humaines de votre employeur. Les aspects auxquels vous attachez de l'importance font peut-être partie de ceux que des fournisseurs de services (comme Amazon) ou des sites de réseautage personnel (comme Facebook) utilisent pour détecter des affinités et regrouper des personnes en conséquence.

Vie privée, réputation et confiance

Les façons modernes d'utiliser l'identité, à bon ou à mauvais escient, ont une incidence sur la réputation des personnes et des organisations. Elles façonnent nos relations avec les autres et nos interactions commerciales, comme vendeurs ou acheteurs. Il faut prévoir des mécanismes de sécurité car l'identité est vulnérable au vol et à la fraude. Néanmoins, ces mécanismes peuvent alourdir les modes de fonctionnement et même porter atteinte à la liberté ou à la vie privée. Le modèle

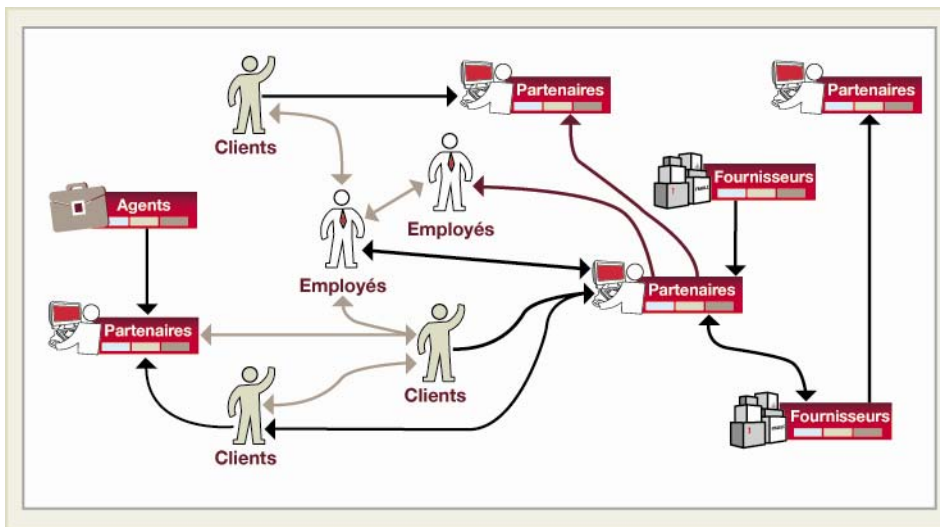
optimal à adopter devra donc rendre à chacun la maîtrise de son identité, ce qui mènera à des liens de confiance permettant à tous d'interagir en toute sécurité.

L'identité dans le monde en réseau

Comme on le sait, de nombreuses entreprises ont transformé leurs processus internes en fonctions réalisées sur Internet. C'est ce que nous appelons « le monde en réseau ».

Notre modèle d'utilisation des identités n'a pas évolué au même rythme que nos processus. La structure de nos TI ne convient tout simplement pas à l'environnement contemporain. Nous avons l'habitude d'utiliser des systèmes fermés auxquels n'ont accès que les gens et les systèmes situés dans les murs coupe-feu de l'entreprise. L'entreprise régit les tâches exécutées sur ces systèmes – qui peuvent être indépendantes de toute autre fonction informatique.

À présent, il peut aussi arriver que les clients ou partenaires de l'entreprise effectuent les mêmes tâches. Il est possible que les employés de l'entreprise soient les clients de ses partenaires, publient un blogue, aient un compte sur Facebook ou LinkedIn, achètent des produits par l'entremise d'Amazon ou de Craigslist et remplissent leurs déclarations fiscales en ligne. Le dessin ci-dessous illustre comment il faut à présent gérer les identités pour faire écho à cet environnement. Il est impensable de simplement « rapiécer » et complexifier les anciennes façons de faire. Nous avons besoin d'une nouvelle approche.



Contrôle de l'accès

Dans le passé, l'identité (ou, plus précisément, l'identifiant) servait surtout à confirmer qui était autorisé à être à un endroit, à lire un document, ou encore à faire, utiliser ou transporter quelque chose – et à quels moments. Cette manière d'utiliser l'identité est devenue monnaie courante. Qu'il s'agisse de traverser une frontière ou d'accéder à une information, nous avons l'habitude de nous munir d'un passeport ou de mémoriser des NIP et des mots de passe. À défaut d'avoir ces identifiants, certaines activités nous sont interdites au travail et dans notre vie privée.

Le contrôle de l'accès comporte deux volets liés à l'identité : l'authentification (*le demandeur semble-t-il être la personne ou l'entité qu'il prétend être?*) et l'autorisation (*le demandeur authentifié est-il autorisé à avoir accès au service, à l'information ou au lieu demandé?*).

Le contrôle de l'accès a de l'importance pour chacun à titre de fournisseur et de consommateur. En tant que fournisseur, je veux déterminer qui peut faire quoi avec chacun des services que j'offre. Je veux recevoir mon paiement, mais aussi protéger mes données et mes actifs. En tant que consommateur, je tiens à mes renseignements personnels comme à la prunelle de mes yeux. Je veux savoir qui peut voir et utiliser les données sur mon argent, mais aussi l'information privée dont ma réputation dépend.

Personnalisation et profils

De nombreux sites Web permettent aux utilisateurs d'adapter leur page personnelle. Dans certains cas, l'internaute peut simplement insérer un message (Bonjour!...). D'autres sites, tels iGoogle, l'invitent à configurer sa page de A à Z. Les utilisateurs aiment trouver rapidement ce qu'ils cherchent et éliminer les éléments auxquels ils n'attachent pas d'importance.

Le commerce électronique occupant une place croissante, les fournisseurs veulent personnaliser l'expérience de chaque client en s'inspirant du profil qui se dégage de ses visites antérieures et en le comparant aux comportements d'autres acheteurs. Dans le monde virtuel, il est possible de créer une boutique particulière pour chaque client, en adaptant l'organisation des étagères, la présentation des produits, les publicités et même les prix. Plus l'offre se moule au profil de l'acheteur, plus l'expérience client est riche et plus les revenus peuvent augmenter.

Les profils peuvent constituer un avantage à long terme pour un fournisseur. Des recommandations efficaces, fondées sur les expériences précédentes de l'utilisateur, permettent de renforcer les liens, surtout si le fournisseur retouche le profil chaque fois que le client visite son site. Un fournisseur peut solidifier sa réputation et ses relations avec ses clients en gérant les profils de manière intelligente et homogène.

Sur les sites de réseautage professionnel (p. ex. LinkedIn et Xing) ou personnel (p. ex. Facebook et Myspace), les transactions s'appuient directement sur les profils. Les utilisateurs et les fournisseurs comptent sur l'évolution continue des profils pour faire croître la valeur du site. Les contacts avec des amis, les nouveaux rapports établis et les commentaires ou recommandations qui rehaussent des réputations permettent de constituer des profils qui ont de la valeur pour les visiteurs, les autres utilisateurs et les fournisseurs. Pensez-y : suivez-vous les recommandations d'un inconnu, ou d'une personne réputée?

Un autre aspect de la personnalisation est la possibilité de créer un personnage reconnaissable – l'image que vous voulez projeter. Cela peut se faire en utilisant votre véritable identité ou un avatar de votre choix. Cette formule est attrayante entre autres parce qu'elle permet d'adopter une identité différente sur chaque site. Par exemple, vous pourriez être une cowgirl de l'espace sur Facebook mais une femme d'affaires sérieuse sur LinkedIn. Parfois, vous pouvez même avoir plus d'une identité sur un seul site. Vous pouvez aussi associer un profil (contenant des renseignements structurés ou non) à chaque personnage. Aucune entité n'a besoin de savoir que toutes ces personnalités vous appartiennent.

Vérification et contrôle

Il faut que les entreprises puissent surveiller, contrôler et certifier l'intégrité et l'exactitude de leurs transactions. Cela est non seulement judicieux sur le plan des affaires, mais aussi nécessaire à l'application des meilleures pratiques juridiques et éthiques. Les médias ont fait largement état des réglementations à cet égard, notamment la loi Sarbanes-Oxley et les normes de Bâle II.

L'identité des parties fait partie des renseignements fondamentaux dans ce contexte. Néanmoins, dans le monde en réseau, cette notion acquiert une complexité beaucoup plus grande que dans les anciens systèmes fermés. L'ouverture des systèmes modernes ainsi que la multitude de points d'entrée, de modalités de paiement et de services internes compliquent les processus de vérification et de contrôle – à moins qu'ils soient conçus d'emblée pour correspondre à la nouvelle réalité.

Les conséquences du Web 2.0

Le réseautage personnel et la réputation

S'il est vrai que la réputation a toujours joué un rôle central dans les affaires et dans la vie privée, le réseautage personnel et le commerce électronique sur Internet renforcent encore ce rôle. Nous avons déjà parlé de la réputation dans le contexte d'Amazon, de Facebook ou d'eBay. Mais de quelle réputation s'agit-il? Vous ne pouvez pas « transporter » votre réputation d'un site à l'autre car l'identité que vous avez sur un site n'est significative qu'à cet endroit. Il se peut que des gens sachent que deux identités appartiennent à la même personne mais ce genre de renseignement n'est pas forcément fiable.

Un autre phénomène important pour les entreprises est le blogage. Un nombre croissant de sociétés se servent de blogues pour promouvoir leur image ou leurs produits sous un vernis d'objectivité. L'identité du blogueur et son lien avec l'entreprise (donc avec l'image de l'entreprise) revêtent par conséquent une importance cruciale. La réputation de la personne et celle de l'entreprise se confondent. Imaginons qu'un blogueur publie assidûment des articles reproductibles sur la Société X. Il se peut que ce blogueur soit perçu comme étant lié à la Société X ou agissant en son nom. Cela est bon pour la réputation de la Société X et du blogueur. Imaginons maintenant que cette personne change d'employeur et crée un blogue pour la Société Y. La Société X pourra-t-elle préserver la réputation du contenu de l'ancien blogue? Le blogueur sera-t-il en mesure de conserver sa réputation antérieure?

Applications composites et accès

Les applications composites permettent de créer assez facilement de la valeur en combinant des applications ou des services déjà disponibles. Si j'amalgame sur mon site des services de Google et de Craigslist, est-ce que j'entremêle la réputation de ces fournisseurs et la mienne? Ces sociétés se sont exposées à des risques de ce genre en faisant des affaires sur la place publique. Je ne touche pas à leurs données protégées. Par contre, si j'associe cette information aux services sécurisés d'une autre entreprise, je crée un nouveau risque car cette entreprise dépendra peut-être de moi pour assurer l'accès sécurisé à ses services. Elle ne connaît ni l'identité ni la réputation

WEB 2.0 ET IDENTITÉ 2.0

Fortement médiatisé, le Web 2.0 est défini de mille et une manières différentes. De quoi s'agit-il, en réalité? « Web-2.0 » est un terme commode servant à désigner l'étape actuelle de l'évolution continue des technologies et des communications liées à Internet. L'une des principales caractéristiques de cette étape est qu'elle privilégie un environnement centré sur les utilisateurs.

De même, le concept « Identité 2.0 », sans faire encore l'objet d'une définition officielle, repose sur le principe que l'utilisateur décide comment, quand et où il fournit de l'information. Les entreprises peuvent aussi y trouver des débouchés, pourvu qu'elles établissent un juste équilibre entre la sécurité, la convivialité, la collecte de données sur les clients et la protection des renseignements personnels.

La normalisation d'Identité 2.0 ne deviendra possible qu'une fois résolus divers enjeux techniques, commerciaux et fort probablement réglementaires. D'ici là, les organisations doivent établir un environnement de confiance qui propose un nombre suffisant d'options aux consommateurs sans engendrer une complexité excessive.

de mes utilisateurs – et quoi qu'il en soit, elle ne souhaite certainement pas entretenir une masse énorme de nouveaux renseignements de ce type. Il faut mettre en place des processus et des normes qui préviendront la réalisation de scénarios de ce genre.

Mobilité

Le branchement continu est un volet important du Web 2.0. Les gens veulent avoir accès aux mêmes services et aux mêmes sites chaque fois qu'ils le désirent, peu importe l'appareil qu'ils utilisent – ordinateur, téléphone cellulaire, console de jeu ou navigateur de la voiture.

Cependant, plusieurs appareils plus récents sont mal adaptés aux écrans et processus traditionnels d'authentification. Dans le cas des téléphones cellulaires, les identifiants classiques sont matériels (carte d'identité de l'abonné ou numéro RNIS de station mobile); on ne peut pas s'y fier pour contrôler l'accès aux services sécurisés. Les fournisseurs de services sans fil sont mis au défi de concevoir de nouveaux mécanismes sécuritaires qui ne nuiront pas à la qualité du service.

La mobilité introduit aussi les concepts d'emplacement et de présence, qui peuvent avoir un impact sur le contrôle de l'accès et sur les profils. On peut aussi présumer que chaque appareil aura ses propres fonctionnalités de gestion des profils et de personnalisation. La mise en commun de tous ces facteurs exige donc de créer des moyens d'authentifier et d'autoriser l'accès qui tiennent compte du contexte.

Confiance

Bien que la confiance soit essentielle à toute interaction significative entre des personnes ou des organisations, elle a jusqu'ici joué un rôle mineur en informatique. Dans un système fermé qui gère et contrôle toutes les règles d'authentification et d'accès, la confiance est superflue. Le monde ouvert en réseau, par contre, ne peut pas se passer de la confiance. Voyons quelques exemples concrets qui le démontrent.

La pièce d'identité la plus officielle est généralement le passeport. Quand les agents d'immigration vérifient un passeport, ils peuvent voir si la photo et la description correspondent à l'apparence de la personne qui le présente et si le document semble authentique. N'accordent-ils pas une foi excessive à un simple document? De fait, cette procédure d'authentification repose sur l'hypothèse que le pays qui a émis le passeport a vérifié tous les documents nécessaires et ne cherche pas lui-même à faire entrer des gens illégalement dans le pays visité. Cette hypothèse se fonde sur des liens de confiance entre les gouvernements du pays visité et du pays émetteur.

Il s'agit donc d'un exemple simple du lien de confiance existant entre deux entités équivalentes, des gouvernements, qui peuvent entretenir des relations diplomatiques entre eux. Voici un cas un peu plus complexe. On utilise fréquemment le permis de conduire comme pièce d'identité pour louer une voiture ou s'abonner à un club vidéo; ce document sert même de preuve d'identité officielle dans certains pays. Cela est possible car il existe un lien de confiance (d'ordinaire implicite) entre l'entité qui authentifie et l'émetteur du permis, souvent une autorité locale. L'autorité locale exige que certains documents soient présentés et validés avant d'émettre un permis. Elle entretient un lien de confiance avec les émetteurs de ces documents – et la chaîne continue généralement jusqu'à ce qu'un organisme gouvernemental national entre en jeu. La chaîne de confiance peut être relativement longue et, même quand il existe un lien de

confiance explicite entre chaque maillon et le suivant, il n'y a habituellement aucune relation directe entre l'entité qui authentifie et l'émetteur de la preuve d'identité initiale.

Aujourd'hui, alors que le nombre de transactions conclues sur Internet augmente, les liens de confiance officiels et implicites jouent un rôle toujours plus important.

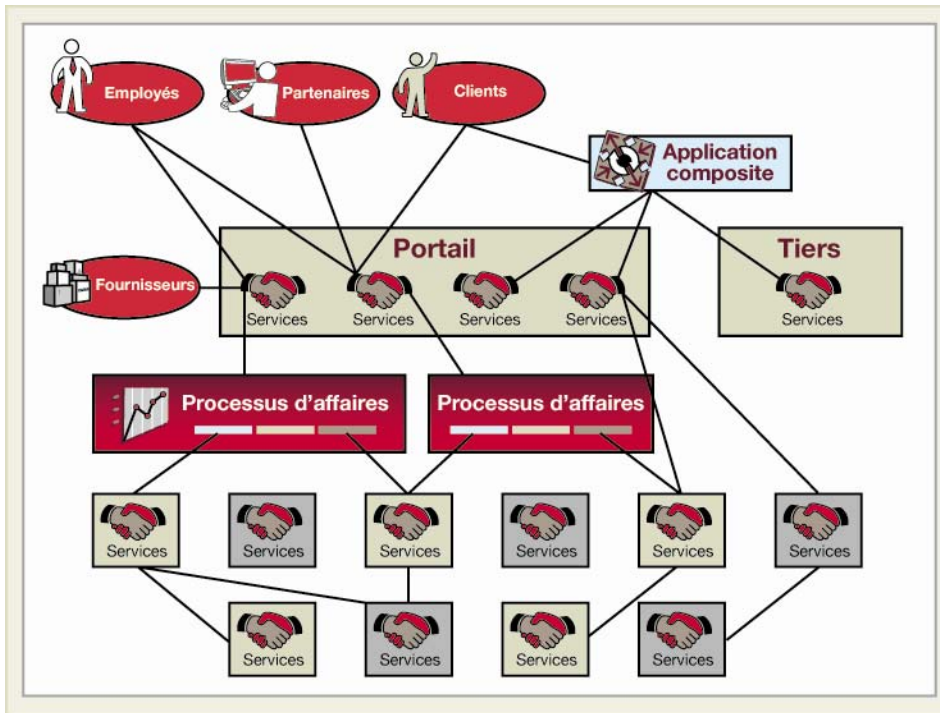
L'identité et l'architecture orientée services (AOS)

L'AOS devient la norme, tant en informatique d'entreprise que sur Internet. Fondamentalement, la promesse de l'AOS est la réutilisabilité. Elle permet aux entreprises de définir des services spécifiques qui seront utilisés dans plusieurs scénarios différents et combinés entre eux. Grâce au couplage faible, il est possible d'assembler et de réassembler les services de manière à les relier uniquement par le contenu utilisé à un certain moment. Chaque nouveau contexte crée un nouvel ensemble de relations.

Ainsi, la pertinence de l'identité d'un consommateur ne peut être déterminée que dans le contexte du service utilisé. Les règles d'accès varient en fonction du caractère critique du processus d'affaires, par rapport au service en question. À quelques exceptions près, il devient impossible de donner aux consommateurs des droits d'accès directs aux services. Et même si nous le pouvions, nous ne voudrions probablement pas gérer les droits d'accès dans cet environnement à base de services où les clients et les employés de nos partenaires interagissent et s'entremêlent de manières toujours renouvelées. Les applications composites doivent être envisagées de la même façon. L'application composite ajoute une « couche » que les consommateurs utilisent pour optimiser les services par le truchement d'un canal indirect qui n'est pas celui du fournisseur d'origine. Dans bien des cas, l'application composite elle-même appartient à un tiers – un partenaire qui n'est peut-être même pas consommateur des services de l'entreprise source... ou qui l'est peut-être.

Ce contexte nous amène à réfléchir sérieusement ce que signifie « l'identité du consommateur ». Si un service est consommé par un autre service, quelle est l'identité pertinente : celle du service qui consomme ou celle du consommateur ultime du processus d'affaires? La réponse à cette question aura des conséquences considérables sur la manière de gérer l'authentification et l'accès au sein du domaine d'un fournisseur.

Le graphique ci-dessous illustre la complexité potentielle de ce genre de situation.



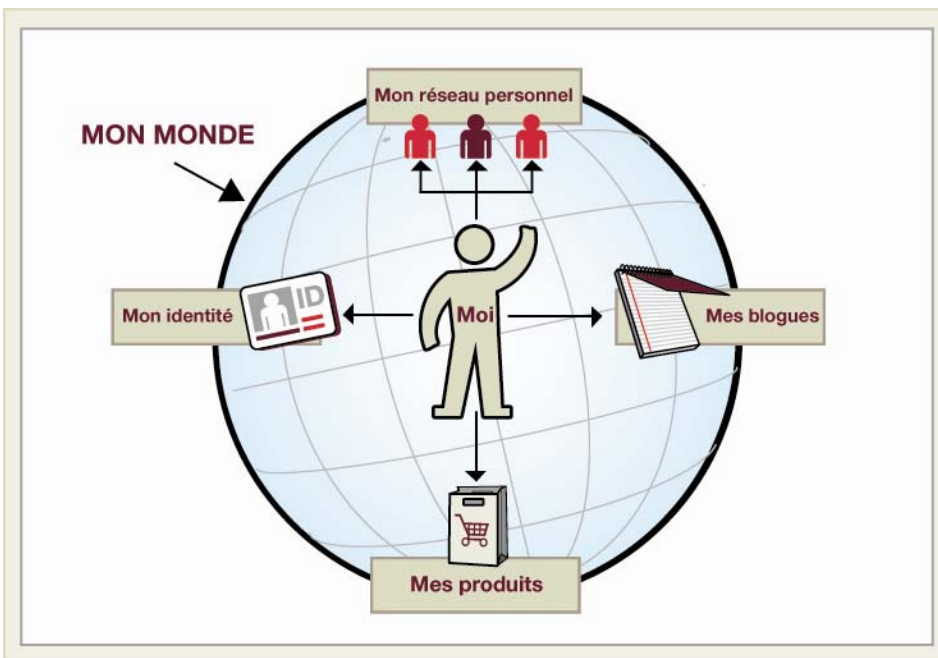
Ce débat mène naturellement à des solutions reposant sur un degré élevé de confiance au sein des réseaux d'entreprise. Dans certains cas, les rapports seront officiels, soutenus par des technologies et des normes. Mais souvent, comme l'illustre notre exemple du passeport, la réputation du fournisseur d'identités sera le facteur déterminant car il n'y aura pas de liens directs entre lui et l'entité qui authentifie.

Authentification centrée sur l'utilisateur

De nos jours, chacun détient des pièces d'identité variées – passeport, permis de conduire, cartes de membre et de crédit – émises par divers fournisseurs et véhiculant des renseignements personnels en plus ou moins grand nombre. Dans une certaine mesure, nous pouvons présenter le document de notre choix, selon les circonstances. Cette décision peut dépendre de la quantité d'information que nous voulons divulguer. Par exemple, quand un jeune homme doit prouver son âge pour acheter de l'alcool, il n'utilisera peut-être pas son permis de conduire (s'il ne souhaite pas dévoiler inutilement son adresse) ni son passeport (qu'il n'a peut-être pas sur lui ou qui renferme peut-être des renseignements privés sur ses voyages récents). Il se servira donc du document le plus discret possible – une carte d'étudiant, peut-être. On est alors en présence d'un modèle d'authentification centré sur l'utilisateur.

Celui-ci, ayant tous les documents en main, utilise la pièce d'identité de son choix; l'échange intervient uniquement entre la personne et le fournisseur de services.

L'authentification centrée sur l'utilisateur va plus loin : elle facilite l'accès aux systèmes informatiques. Dans l'environnement Web 2.0, ce modèle n'est plus un simple concept mais bien une réponse opérationnelle logique. Comme on le voit sur l'illustration, le consommateur passif est devenu un participant de plus en plus actif. Il ne faut donc pas s'étonner qu'on utilise parfois le terme « Identité 2.0 » pour parler de l'authentification centrée sur l'utilisateur.



Normes et solutions d'identification

Outre les solutions exclusives et semi-exclusives, un ensemble évolutif de normes et de solutions d'identification émerge dans l'espace public. En voici quelques exemples.

- **OpenID** : une solution libre et gratuite offerte par plusieurs fournisseurs, y compris de grandes entreprises comme Yahoo. Les sites acceptant OpenID se multiplient mais il s'agit surtout de sites de réseautage personnel ou de blogues. Cette solution ne convient pas encore aux services sécurisés car elle ne vérifie pas les renseignements fournis par les utilisateurs et ne transmet pas les données de manière sécuritaire.
- **InfoCard** : une solution mise au point et déployée principalement par Microsoft. Commercialisée sous le nom de CardSpace, l'InfoCard fait partie du système d'exploitation Vista et des versions récentes de XP. Permettant la transmission sécuritaire de données, elle repose sur le concept de « carte gérée » selon lequel l'utilisateur fournit des renseignements choisis qui peuvent raisonnablement faire l'objet d'une vérification – la date de naissance et le numéro de passeport, par exemple. Il faut qu'un fournisseur d'identités vérifie l'information avant qu'une carte soit émise et une nouvelle vérification est obligatoire en cas de modification. L'utilisateur peut aussi consigner sur sa carte des renseignements non gérés tels que ses préférences et d'autres éléments de son profil. (Voir l'illustration ci-dessous : « L'authentification centrée sur l'utilisateur – Le modèle InfoCard ».)

LA VALEUR DE L'AUTHENTIFICATION CENTRÉE SUR L'UTILISATEUR

L'authentification centrée sur l'utilisateur peut diminuer substantiellement le nombre de noms d'utilisateur et de mots de passe à retenir. Elle ne fournira pas une procédure unique d'identification mais permettra d'utiliser la même procédure sur plusieurs sites. Elle mènera peut-être un jour à une véritable procédure unique d'identification pour l'ensemble du Web.

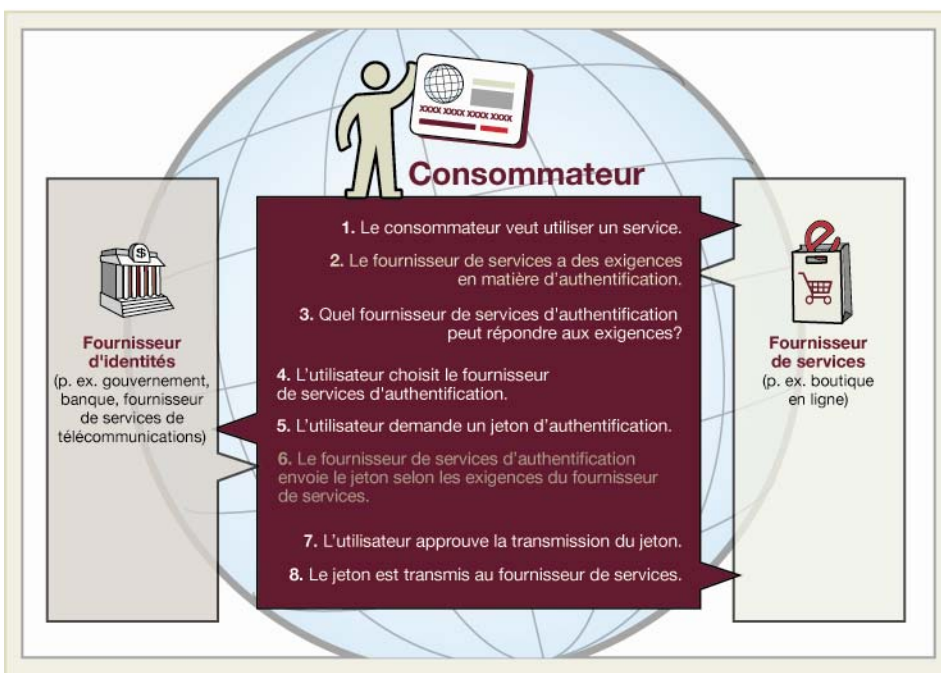
L'authentification centrée sur l'utilisateur contribue à la protection de la vie privée car elle empêche les fournisseurs de services d'obtenir plus de renseignements personnels que ceux que nous souhaitons leur communiquer. Elle procure aussi des bienfaits aux entreprises. Entre autres, elle réduit la complexité des mécanismes à mettre en place pour gérer les droits d'accès des utilisateurs externes.

Si l'utilisateur le veut, l'authentification centrée sur l'utilisateur peut aussi lui permettre de « transporter » sur les divers sites qu'il fréquente la réputation associée à son « identité ».

La normalisation d'Identité 2.0 ne deviendra possible qu'une fois résolus divers enjeux techniques, commerciaux et probablement réglementaires. Ces enjeux comprennent l'établissement de liens de confiance, l'abandon de la propriété exclusive des renseignements sur les utilisateurs et l'acceptation de normes communes.

- **Higgins** : une solution qui vise à compléter l'InfoCard et incorpore une interface permettant de lier des applications à CardSpace, à OpenID ou à toute solution normalisée ou exclusive.

Le dénominateur commun de ces diverses solutions est que les consommateurs – et non les fournisseurs de services – possèdent et gèrent directement les renseignements sur leur identité et leur profil. Elles exigent l'établissement de liens de confiance tacites et explicites entre les fournisseurs d'identités et de services.



Fournisseurs d'identités et confiance

Le succès d'Identité 2.0 dépendra des fournisseurs d'identités. Nous devons trouver un juste équilibre afin de proposer un nombre suffisant d'options aux consommateurs sans rendre l'environnement encore plus complexe.

Il faut que les consommateurs et les fournisseurs de services fassent confiance aux fournisseurs d'identités. Il faut aussi prendre garde aux complications qui surviendront si le consommateur doit faire appel à différents fournisseurs d'identités pour interagir avec différents fournisseurs de services. Idéalement, un fournisseur d'identités devrait être reconnu pour sa fiabilité. Jusqu'ici, la plupart des acteurs en ce domaine sont de petites organisations « point.com » qui ne sont pas aptes à vérifier et à gérer des renseignements vitaux. Les grandes entreprises liées à Internet ont opté pour des solutions exclusives qui utilisent peut-être les normes OpenID mais n'acceptent les identités d'aucun autre fournisseur d'identités du même genre. Pour l'instant, à tout le moins, les organisations traditionnelles demeurent les fournisseurs d'identités les plus crédibles.

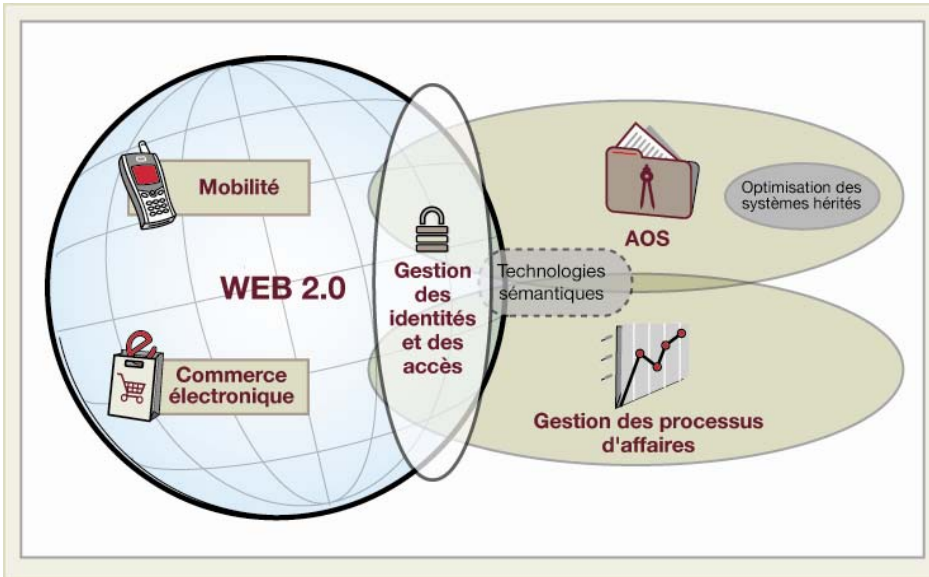
Les gouvernements sont en bonne position pour jouer ce rôle. La réalisation de leur mission fondamentale exige déjà qu'ils collectent et stockent de grandes quantités de renseignements personnels. De plus, en principe, ils sont considérés comme des entités fiables et responsables. Les grandes institutions financières ont aussi la visibilité et les relations nécessaires pour devenir des fournisseurs d'identités respectés. Les sociétés de télécommunications, qui emmagasinent déjà des renseignements sur l'identité et fournissent souvent les services Internet, pourraient aussi être tentées par ce marché. Ultimement, les facteurs décisifs seront la volonté, la réputation et la confiance.

Les solutions de gestion des identités et des accès de CGI

L'authentification et l'autorisation sont les contextes les plus fréquents et les plus exigeants d'utilisation de l'identité. Il est essentiel de déployer ces fonctions de manière efficace, économique et fiable afin d'assurer la sécurité des données et des renseignements personnels ainsi que la conformité réglementaire. Toute nouvelle approche de gestion de l'identité doit donc répondre aux exigences d'authentification et d'autorisation d'organisations très diversifiées.

Il faut également tenir compte des nouveaux modes révolutionnaires d'utilisation des TI qui émergent, tant chez les personnes que chez les entreprises. De nos jours, toutes les transactions en TI doivent être revues à la lumière des occasions et des risques associés à l'identité des personnes.

CGI croit que les solutions de gestion des identités et des accès doivent être conçues pour le monde en réseau, les systèmes ouverts, le Web 2.0 et l'AOS. Même au sein d'une seule entreprise, cette vision peut réduire la complexité et mener à la réalisation de solutions agiles. Pour obtenir des résultats optimaux, il faut traiter la solution de gestion des identités et des accès comme une solution d'affaires, et non comme un ajout à greffer aux systèmes après coup. Voilà pourquoi, comme le démontre l'illustration qui suit (« Architecture pour l'entreprise agile »), CGI considère que les solutions de gestion des identités et des accès sont des technologies clés menant à des débouchés importants. Notre approche combine cette vision stratégique avec des méthodes pratiques de déploiement qui procurent des gains rapides et une souplesse accrue permettant de poursuivre graduellement les investissements, par la suite, afin d'adapter la solution aux besoins de l'avenir.



Caractéristiques de nos solutions

CGI estime qu'Identité 2.0 est le modèle idéal de toute architecture de gestion des identités et des accès. Il ne s'agit pas d'une solution tout-aller mais bien d'un cadre se mouvant aux réalités tangibles de chaque entreprise. Identité 2.0 repose sur des principes directeurs, présentés ci-dessous.

Au sein de l'entreprise

Les fonctionnalités d'authentification et d'autorisation doivent être à base d'agents et s'inspirer du modèle des serveurs de règles et des clients de serveur de règles. Cette approche offre les avantages suivants.

- Les services et applications gèrent les fonctionnalités sans devoir être liés de quelque façon que ce soit à l'infrastructure de gestion de l'accès. Les deux plateformes peuvent donc évoluer indépendamment l'une de l'autre, respectant ainsi l'un des principes de base de tout concept logiciel efficace : la séparation des préoccupations.
- La gestion et l'entretien sont simplifiés car il faut tout au plus un serveur de règles par domaine et toutes les règles d'accès sans exception y sont emmagasinées. Les clients de serveur de règles peuvent être déployés librement selon les besoins (nombre, emplacements, moments) et n'exigent pas d'entretien. Même la redondance, dans le cas des clients de serveur de règles, est un problème mineur.

Les droits d'accès aux processus d'affaires doivent s'appliquer au service initial et non dans une chaîne d'autres services auxquels l'utilisateur n'a pas normalement accès. Notamment, lorsqu'on transforme les applications héritées pour les structurer en services, on devrait éliminer les droits d'accès individuels. Les droits d'accès dépendent du processus d'affaires utilisé. Si on ne s'adapte pas aux contextes, les fonctionnalités de gestion des utilisateurs deviennent inutilement complexes alors que les outils de propagation et de mise en correspondance des identités deviennent difficiles à maintenir. Les avantages de ce modèle sont encore plus manifestes quand on tient compte des accès par les clients et les partenaires.

Il est souhaitable et possible de simplifier grandement le contrôle de l'accès basé sur les rôles car on utilise souvent des renseignements non pertinents lors de l'attribution initiale, par exemple le lieu, le poste ou le service. Le principe de la séparation des préoccupations fournit un cadre aidant à gérer simplement plusieurs fonctionnalités à différents endroits.

La gestion des identités et des accès du point de vue des clients

CGI croit que l'authentification centrée sur l'utilisateur est la bonne approche à utiliser vis-à-vis des clients. Les entreprises doivent se tourner vers l'extérieur et capitaliser sur l'information disponible, ce qui leur permettra d'optimiser l'expérience de leurs clients. À cette fin, il faut qu'elles respectent les critères suivants.

- Adopter des solutions de gestion des identités et des accès compatibles avec OpenID ou InfoCard, et se préparer à intégrer les innovations : le cadre Higgins est la meilleure option globale car elle permet d'élargir progressivement le nombre de plates-formes compatibles sans compromettre la logique sous-jacente. Il existe aussi des produits de pointe tandis que les normes et l'interopérabilité des normes font du chemin.
- Établir des liens de confiance avec les fournisseurs d'identités : il faut que les fournisseurs d'identités soient dignes de confiance et que la vérification de renseignements essentiels sur les clients fasse partie des normes qu'ils intègrent. Ils doivent aussi garantir la transmission sécuritaire des données.

L'une des voies possibles, pour une entreprise, est de devenir elle-même fournisseur d'identités. Certaines le font seules, d'autres s'allient à un partenaire : un intégrateur comme CGI, un partenaire déjà établi de l'entreprise, ou encore une nouvelle division. Cette approche permet à l'entreprise de mieux servir ses clients et de protéger son personnel. L'entreprise tire ainsi le meilleur parti possible des profils et de la réputation tout en rendant possible l'accès multivoie (l'environnement « toujours branché ») et les services axés sur le contexte.

Les entreprises peuvent toujours choisir de maintenir leur propre registre de clients. Si l'approche prescrite de gestion des accès a été adoptée, la gestion des utilisateurs n'a pas à être complexe. Il n'est pas certain, toutefois, qu'il s'agisse là d'une solution viable à long terme.

La gestion des identités et des accès du point de vue des partenaires

La gestion des accès des partenaires peut exiger une approche différente car :

- nous ne pouvons pas présumer qu'une entreprise partenaire est capable d'utiliser l'authentification centrée sur l'utilisateur pour son propre personnel;
- en ce qui a trait aux employés des partenaires, il arrive que les entreprises s'intéressent surtout au rôle qu'ils jouent dans le cadre des processus d'affaires fondamentaux – des aspects sur lesquels les partenaires ont une emprise – qu'à l'identité réelle de chaque employé.

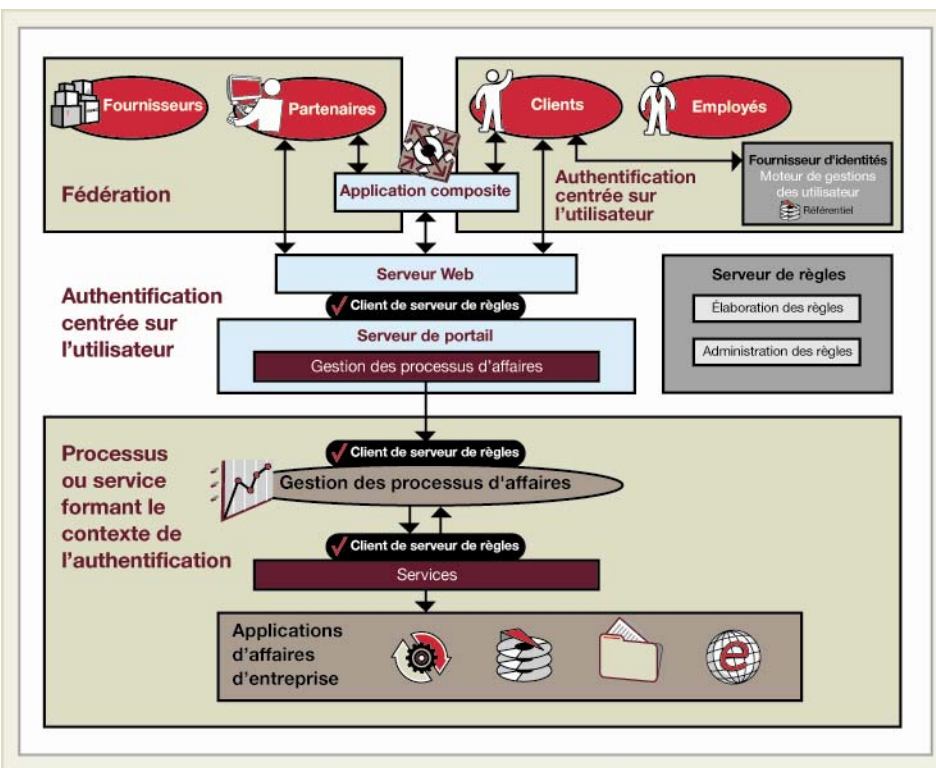
Dans ce cas, la solution idéale peut être une fédération, une technologie mûre assortie de normes établies telles que SAML et ID-FF. Une fédération permet d'accepter les jetons et les preuves d'identité connexes des organisations partenaires avec lesquelles l'entreprise entretient des liens de confiance. Les normes permettent

au partenaire d'authentifier les jetons reçus; il n'est donc pas nécessaire d'établir des identités ni des droits d'accès connexes.

Outre ces normes et d'autres – par exemple WS-Federation, utile dans l'environnement Microsoft – d'autres produits éprouvés compatibles sont disponibles et peuvent offrir des fonctionnalités supplémentaires d'interopérabilité.

Vue d'ensemble

La dernière illustration dépeint une architecture possible utilisant les technologies et l'approche décrites dans ce document pour réaliser une solution sécuritaire et agile. En s'appuyant sur les relations avec les fournisseurs établis, les normes appropriées et une approche agile, CGI réalise des solutions de gestion des identités et des accès qui permettent aux clients de déployer leurs stratégies d'affaires avec succès.



À PROPOS DE CGI

La satisfaction des clients est au premier plan des activités de CGI. Depuis plus de 30 ans, nous sommes solidaires des défis auxquels nos clients font face et nous les aidons à les relever en leur offrant des services de qualité.

Figurant parmi les chefs de file du secteur des services en TI et en gestion des processus d'affaires, CGI maintient une étroite proximité avec ses clients grâce à ses 27 000 professionnels œuvrant à partir de plus de 100 bureaux dans le monde. Par leur entremise, nous fournissons à nos clients la combinaison de valeur et de savoir-faire qui répond le mieux à leurs besoins en alliant judicieusement les partenariats à l'échelle locale et des options de prestation de services à l'échelle mondiale.

Dans le domaine du leadership technologique, CGI s'appuie sur une vision pragmatique de la transformation pour aider les organisations à réaliser le potentiel des technologies innovantes et des concepts modernes de gestion. Nous estimons que nous avons réussi quand nous avons surpassé les attentes de nos clients et quand nous les avons aidés à atteindre une performance supérieure.