

**MATÉRIEL**[Partager sur Viadeo](#) [Commentaire](#)

## Pour un marché du contrôle d'accès plus exigeant !

Vote

**1**Date: 21-06-2010  
Par: Gérard Clech

Qu'est-ce que la gestion des contrôles d'accès physique ? Rien de bien compliqué sur le papier... Il s'agit de s'assurer de la validité que forme le triptyque suivant : une personne, un lieu, une période. Autrement dit, il s'agit de pouvoir répondre de manière efficace à la question : une personne donnée a-t-elle le droit de se trouver à un endroit précis à moment donné ? Si oui, il faut lui faciliter l'accès. Si non, il faut le lui interdire.



Par Sylvain Arts, Responsable de Novento – P&amp;T Consulting

### Des acteurs aux objectifs différents

Cet énoncé simple sur le papier est difficile à mettre en oeuvre sur le terrain. Une multitude d'acteurs s'y intéresse pourtant et y apporte des réponses. Le problème est que cette réponse est souvent partielle, voire handicapante à terme pour le client. Les fabricants de matériels y répondent avec des badges et des lecteurs. Leur force : savoir gérer la partie véritablement physique de l'accès. Ils maîtrisent les technologies d'impression et de lecture, avec ou sans fil, simples ou complexes.

Les éditeurs de solutions y répondent avec leurs logiciels spécialisés. Leur force : savoir gérer les événements imprévisibles, la gestion des droits d'accès, qu'ils soient ponctuels, à court ou à long terme. Ils maîtrisent les problématiques « métier » de l'accès. Les intégrateurs, eux, s'affirment capables de gérer la liaison entre le système d'information « profond » de l'entreprise et les logiciels des éditeurs de solutions métiers.

Le problème du contrôle d'accès physique vient de l'absence de souplesse dans la liaison entre ces acteurs. De facto les clients se retrouvent donc condamnés à choisir par défaut, en fonction de leur contexte. Qu'ils ne veuillent pas renouveler leur matériel, et ils seront limités à certains logiciels, ou ne pourront pas faire appel à leur intégrateur habituel. Qu'ils privilégient leur intégrateur, et ils devront changer leurs logiciels métier. Et souvent qui dit logiciel dit technologie spécifique, et donc difficulté lors du changement... soit pour s'approprier la nouvelle solution, soit pour quitter un ensemble matériel & logiciel fortement imbriqués.

### **Que doit-on attendre d'un système de gestion des accès physiques ?**

Qu'attend-on, en théorie, d'un système informatique aujourd'hui ? Qu'il soit communicant, flexible et adaptable, en enfin qu'il soit personnalisable. Il n'y a aucune raison pour que les solutions de contrôle physique des accès s'affranchissent de ces exigences.

Etre communicant : les données doivent circuler. Une donnée isolée est une donnée inutile. Elle doit pouvoir passer entre les applications, les terminaux, les utilisateurs. La gestion des accès doit être capable de récupérer et transmettre les données non seulement pour remplir sa mission, mais pour faciliter la vie des utilisateurs, et des gestionnaires informatiques. Cela signifie, par exemple, être capable de récupérer des données dans des applications existantes, sans imposer son propre stockage.

Etre flexible et adaptable : le système d'information d'une entreprise est une succession de strates variées. Les langages de programmation varient, les mises à jour sont permanentes, l'infrastructure évolue. La gestion des accès ne doit pas être un bloc monolithique incapable de se fondre dans un environnement particulier. Cela signifie, par exemple, être capable de s'adapter à un nouvel ERP, ou un nouvel outil de gestion des emplois du temps des salariés, sans effort rédhibitoire.

Qu'il soit personnalisable : chaque entreprise est unique. Sa stratégie, son environnement concurrentiel, son infrastructure, ... il est impossible de créer une solution de type « one size fits all ». Certaines solutions, comme les logiciels de gestion intégrés, ont réussi à imposer leurs règles aux utilisateurs. Les grands modules existent, les entreprises doivent les adopter. Mais même dans ce contexte, des développements ad hoc permettent de personnaliser l'utilisation et le fonctionnement du logiciel.

### **Pour que les clients imposent leurs besoins**

Le contrôle d'accès est aujourd'hui considéré comme un marché de renouvellement : à intervalles plus ou moins régulières, les entreprises se mettent en recherche d'un nouveau fournisseur. Elles doivent devenir plus offensives, plus exigeantes. C'est à elles de définir leurs besoins, mais en partant de ce qu'elles connaissent et en listant quelques améliorations possibles. Elles doivent oser la page blanche et exiger de leurs prestataires un service qui corresponde exactement à leurs besoins. Leurs besoins, et non pas les capacités des systèmes actuels.

### **Les trois acteurs du contrôle d'accès**

La construction d'un cahier des charges doit tenir compte des trois parties prenantes de la gestion de la sécurité des accès : le « visiteur », « l'accueillant », et « le surveillant ». Le premier doit, d'une manière ou d'une autre, se déclarer. Qui est-il ? Dans quelle partie des lieux doit-il se rendre ? Rend-il une visite ponctuelle, travaille-t-il là ? De quel service fait-il partie ? Quelle fonction occupe-t-il ?

Le deuxième doit valider les déclarations de l'accueillant. « Oui, c'est un fournisseur, il doit me rendre visite ». « Oui, il fait de la Recherche & Développement, il doit avoir accès au laboratoire d'essai ». « Oui, il est intervenant à notre événement, il doit avoir accès à la salle des Speakers VIP ». Cette validation peut être faite par une ou plusieurs personnes ou services : le responsable hiérarchique, la gestion des ressources humaines, le responsable sécurité... On les désignera sous le terme des « autorités ad hoc ».

Le dernier intervenant, le superviseur, doit avoir les moyens de vérifier si le visiteur qu'il a devant lui est bien qui il prétend être, et si les droits d'accès dont il se prévaut lui ont bien été accordés par les autorités ad hoc. Cet intervenant peut être automatisé – une serrure électronique, un portique, un terminal fixe, etc... – ou humain – un agent de sécurité à l'accueil.

Une solution de gestion de contrôle d'accès moderne doit permettre à ces trois intervenants de jouer chacun leur rôle de la manière la plus simple, la plus transparente, la plus sécurisée et la plus efficace possible.

### **Penser à faciliter et améliorer le contrôle humain...**

Le facteur humain est souvent désigné comme le plus faible maillon de la chaîne. Il peut être débordé par les demandes, absent, ou faire une erreur de lecture. C'est pourquoi, en fonction du contexte, le contrôle doit être fait avec un outil adapté au volume et à l'environnement du moment.

Lors d'une réunion de « taille humaine », des badges classiques, utilisant des impressions holographiques et des codes couleurs peuvent satisfaire une grande partie des besoins. Dans une implantation permanente, accueillant quelques centaines de collaborateurs, des outils plus évolués (terminaux mobiles pour la lecture de badge ou de lecture biométrique), peuvent être plus adaptés.

Quel est le véritable enjeu derrière cela ? D'être capable de facilement gérer l'information, pour permettre à la porte de s'ouvrir devant qui de droit. Le visiteur doit facilement s'inscrire et s'annoncer. Les autorités ad hoc doivent pouvoir facilement attribuer à chaque visiteur le profil pertinent, et pouvoir le faire évoluer dans le temps. Le surveillant doit enfin pouvoir vérifier facilement et efficacement les droits du visiteur qu'il a en face de lui, sans l'importuner et sans diminuer le niveau de sécurité.

La facilitation et l'amélioration du contrôle humain sont directement impactés par les dernières technologies, comme le RFID ou les différents types de code-barre qui existent sur le marché. En plus d'être fortement sécurisées, ces solutions permettent d'enrichir leur utilisation d'une dimension de service... On passe alors du « simple » contrôle d'accès à un support potentiellement complet de tout l'accueil, avec une seule (série de) technologie... Si les prestataires veulent bien enrichir les fonctionnalités de leurs solutions...

#### **Pour une prise de conscience des entreprises utilisatrices**

Le critère principal des entreprises dans leur choix de prestataire doit être la fluidité qu'apportent leurs fournisseurs dans la gestion des visiteurs. Et surtout, elles doivent refuser les systèmes trop contraignants. Encore une fois, c'est à elles d'énumérer leurs besoins et aux fournisseurs de s'adapter.

Un système trop rigide ou trop fermé les obligera à créer des doublons lors de manifestations « hors les murs », alors que la simple mise à jour d'un profil existant doit suffire. De la même manière, elles doivent choisir des solutions qui permettent de communiquer avec le maximum de périphériques, indépendamment de leurs marques. Les technologies sont aujourd'hui ouvertes, les systèmes de contrôle d'accès doivent l'être également, aussi paradoxal que cette affirmation puisse paraître...

Toute énumération supplémentaire est inutile, et revient à dire cela : les systèmes de contrôle d'accès physique ne doivent pas s'affranchir de la souplesse et de l'interactivité que l'on exige aujourd'hui de tout le système d'information. Le temps où ils pouvaient se considérer à part et aujourd'hui révolu. La sécurité est un des domaines où les nouvelles technologies apportent une plus-value, et elle passe par la souplesse et la réactivité... Même dans le domaine de la sécurité.