STid
Electronic Identification

Novembre - 2016

Contrôle d'accès : La dématérialisation est-elle l'avenir ? Sous certaines conditions...

PSM - Novembre/Décembre 2016 - N°238

La généralisation des objets connectés permet aujourd'hui au contrôle d'accès de dématérialiser le badge. Mais cela ne doit pas se faire au détriment de la sécurité et de l'ergonomie de la solution de contrôle d'accès.

Aujourd'hui, nous utilisons tous des smartphones ou des accessoires connectés, dont nous ne nous séparons jamais. Parallèlement, la recherche de l'ergonomie pour faciliter l'acceptation des mesures de sécurité a conduit les professionnels du contrôle d'accès à réfléchir à la possibilité de remplacer le badge par notre téléphone portable ou autre objet connecté. Car contrairement au badge qu'il nous est tous arrivé d'oublier un jour, nous oublions rarement notre téléphone. *« Si vous oubliez votre badge chez vous, vous n'irez probablement pas le chercher, mais s'il s'agit de votre smartphone vous n'hésiterez pas à faire le détour. Le téléphone portable nous est devenu indispensable. Ce dernier peut même faciliter l'acceptation de la sécurité en entreprise à condition que la solution soit si ergonomique qu'elle en devient instinctive »* explique Vincent Dupart, directeur général de STid.
C'est une des raisons pour lesquelles on s'intéresse beaucoup à l'utilisation du téléphone en tant qu'identifiant pour le contrôle des accès. Mais, il faut se demander si en intégrant des solutions d'accès mobile dans les architectures de contrôle des accès physiques on ne va pas accentuer vulnérabilité du système ?

Un identifiant numérique aussi sûr qu'un badge

Pour le directeur général de Stid, il faut, avant tout déploiement de ce type d'application, se demander si l'identifiant numérique sera aussi sécurisé que le badge traditionnel. Pourra-t-on copier l'identifiant facilement ? La transmission radio des clés est-elle vraiment fiable ? La voie de communication entre un mobile et un lecteur peut-elle être détournée à des fins malhonnêtes ?

« le choix d'une solution dématérialisée ne doit pas compromettre la philosophie même de votre politique de sécurité : Pourquoi accepteriez-vous de confier à un tiers vos clés de sécurité ? Où sont stockées vos clés de sécurité ? Qui peut y avoir accès ? Suis-je indépendant dans la gestion de ma sécurité en me connectant à un cloud pour accorder des droits ? Aucune limite technique ou technologique ne doit empêcher un directeur sécurité d'être autonome et de garder la liberté d'héberger ses données sensibles... »

Un cryptage draconien

Pour rassurer les utilisateurs, le cryptage des informations transmises entre le cœur du système de contrôle d'accès et le téléphone sera cryptée via des protocoles de sécurité certifiés par des organismes reconnus.

Dans sa politique de transparence et fort de sa certification Anssi, STid a fait le choix d'utiliser des méthodes et algorithmes publics conformes au RGS. Les échanges de données sont ainsi sécurisés autant en authenticité qu'en confidentialité. *« Cette sécurité est démontrable car non privée. Elle est uniquement basée sur des éléments fournis par l'utilisateur et toutes les méthodes sont publiques »*, explique Vincent Dupart.

Création d'une culture sécurité

C'est un intérêt qui mérite d'être souligné : les systèmes de contrôle d'accès mobile créent également une culture de la sécurité, même si les collaborateurs n'en sont pas conscients.

De ce fait, la sécurité physique de l'entreprise est vulnérable puisqu'un badge valide peut virtuellement tomber entre de mauvaises mains. Le collaborateur, en revanche, fait davantage attention à ses équipements mobiles : la perte comme le vol d'un téléphone sont signalés immédiatement, et l'identifiant mobile peut être révoqué dans la foulée afin d'empêcher tout accès non autorisé.

LE POINT DE VUE D'UN FABRICANT

VINCENT DUPART
Directeur général chez Stid


© DR

« C'EST LA MAIN QUI RÉVEILLE LE LECTEUR. »

« La solution STid a été primée lors de la dernière édition des trophées de la sécurité. Un Jury de 17 experts a ainsi choisi notre solution STid Mobile ID parmi 17 autres. C'est la solution de contrôle d'accès par mobile qui permet de garder totalement le contrôle et qui offre des modes d'identification si ergonomiques qu'ils en deviennent instinctifs. Avec le lecteur Architect Blue et le « slide mode », un simple passage de la main sur le lecteur ouvre les portes. Cette action éveille le lecteur et lui indique de communiquer avec le smartphone qui peut être en veille dans la poche ou en communication dans la main. L'utilisateur a le choix d'activer ou non les 5 modes d'identification : mode contact, mains-libres, tap tap, télécommande ou enfin le slide mode. »