face au RISQUE

Article
Contrôle d'accès et identification par smartphone, les réponses de Vincent Dupart

FACE AU RISQUE - N°563 - Juillet 2020

Contrôle d'accès et identification par smartphone, les réponses de Vincent Dupart

(Lien article : faceaurisque.com/2020/06/10/controle-d-acces-et-identification-par-smartphone-les-reponses-de-vincent-dupart/)

Vincent Dupart, CEO de STid. (Crédit photo STid)

L'identification par smartphone est un thème qui a fait l'objet d'un article dans le numéro 563 de Face au Risque (juin 2020). En complément de celui-ci, Vincent Dupart – CEO de STid – a accepté de répondre à nos questions.

Entreprise française spécialisée dans la conception et la fabrication de têtes de lecture de contrôle d'accès sans contact, **STid** – créée en 1996 et qui dispose aujourd'hui de 70 collaborateurs – a notamment été le premier fabricant à obtenir la certification de sécurité de 1er niveau de la part de l'Anssi (Agence nationale de la sécurité des systèmes d'information).

Architect, sa gamme de lecteurs de contrôle d'accès, est dans sa catégorie celle qui a été la plus récompensée au monde avec 11 distinctions remportées en Europe, au Moyen Orient et aux Etats-Unis.

Des éléments parmi tant d'autres qui suffisent à attester de la légitimité de cette entreprise sur la question du contrôle d'accès et de l'identification par smartphone.

---

face au RISQUE

Article
Contrôle d'accès et identification par smartphone, les réponses de Vincent Dupart

FACE AU RISQUE - N°563 - Juillet 2020

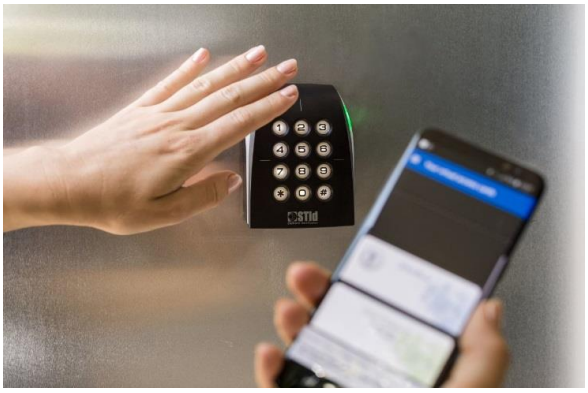
Face au Risque. Quels sont les principaux apports du smartphone dans le contrôle d'accès par rapport aux badges matérialisés ?

Vincent Dupart. *Il y a 5 ans, nous avons développé une forte politique d'innovation pour réinventer le contrôle d'accès en entreprise car nous sommes partis du constat, en échangeant avec les directeurs de sûreté, que la plus grande contrainte était de faire adhérer l'ensemble des collaborateurs d'une entreprise à la politique de sûreté de cette entreprise. Et le contrôle d'accès est perçu comme une contrainte, un mal nécessaire, pour les utilisateurs.*

Aujourd'hui, un utilisateur doit badger entre 12 et 14 fois par jour en moyenne pour s'identifier au sein de son entreprise. Rentrer dans le bureau, aller à la machine à café, rentrer de nouveau dans le bureau… Cela nécessite un certain nombre d'identification. Comme cela est perçu comme une contrainte, nous nous sommes aperçus que les failles de sécurité ne sont pas technologiques mais humaines avant tout. Pour éviter de rebadger, un utilisateur va par exemple bloquer la porte de son bureau avec une corbeille… Le fait d'effacer les contraintes perçues par l'utilisateur facilite son adhésion à cette politique de sécurité de l'entreprise.

Partant de ce constat, nous avons commencé à développer différents modes d'identification. Cela a pris tout son essor à partir du moment où nous avons pu dématérialiser l'identifiant dans le téléphone portable. Imaginons que vous êtes en ligne et que vous vous dirigez vers un lecteur de contrôle d'accès… Avec un badge matérialisé, vous allez devoir chercher votre badge dans votre poche. Et avec les solutions dématérialisées dans les téléphones portables qui existent aujourd'hui sur le marché, vous allez devoir couper votre conversation pour pouvoir ouvrir votre porte car votre téléphone devient votre carte d'accès. Donc cela représente une nouvelle contrainte car vous pouvez être amené à couper plusieurs conversations dans la journée.

« Enlever les contraintes du contrôle d'accès » avec l'identification par smartphone



Un des lecteurs développés par STid permettant l'identification par smartphone pour le contrôle d'accès. (Crédit photo STid)

N*ous avons donc créé des modes « instinctifs ». Par exemple, vous êtes déjà en ligne et plutôt que d'interrompre votre conversation, vous allez simplement passer votre main à quelques centimètres du lecteur (Ndlr : voir photo ci-contre). Cela va réveiller le lecteur, qui va communiquer avec votre smartphone et valider votre accès.*
Vous n'êtes plus obligé de chercher votre badge ou de stopper votre conversation… Cela enlève toutes vos contraintes.

face au RISQUE

Article
Contrôle d'accès et identification par smartphone, les réponses de Vincent Dupart

FACE AU RISQUE - N°563 - Juillet 2020

La deuxième problématique des directeurs de sécurité est de fluidifier l'accès, notamment aux heures de pointe sur les parkings. L'accès d'une moto peut par exemple générer une file d'attente le temps que le motocycliste enlève ses gants et cherche son badge. Nous avons ainsi inventé ***le mode « Tap Tap »*** *qui permet par exemple à un motard – sans enlever les gants et simplement en tapant deux fois sur la poche qui contient son smartphone – de pouvoir obtenir cet accès rapidement.*

Nous avons développé plusieurs modes comme ceux-là visant à rendre le contrôle d'accès beaucoup plus instinctif et beaucoup plus agréable pour l'utilisateur. Le smartphone, c'est avant tout la possibilité de réinventer le contrôle d'accès et d'obtenir l'adhésion des collaborateurs. C'est également une très belle vitrine technologique très appréciée des sièges sociaux.

L'utilisation par smartphone permet aussi de transférer des droits à distance, par exemple pour obtenir un accès à un parking sur un créneau horaire précis. Ce sont ces types d'utilisations qui sont assez recherchés aujourd'hui.

Quels sont les différents acteurs qui composent ce secteur ? Et quelles sont les relations entre eux ?

V.D. *Si on prend la chaîne de valeur, vous avez le client final : le directeur sûreté. Il va être en relation directe avec l'installateur, qui est la personne qui vient sur site pour installer les points de lecture. Juste avant les installateurs, il y a les éditeurs ou intégrateurs de logiciels, synonymes de « constructeurs de systèmes de contrôle d'accès ». Ils développent des logiciels de supervision de contrôle d'accès et vont intégrer des équipements comme des caméras ou des lecteurs de contrôle d'accès.*

Chez STid nous nous situons en amont de cette chaîne de valeur, nous ne vendons pas directement au client final. Nous restons cependant très proches des clients finaux afin de nous assurer que nos solutions répondent bien à leurs besoins, mais également pour les former sur les outils et technologies pour qu'ils restent autonomes et maître de leur sécurité. Nous accompagnons les entreprises à définir leur cible de sécurité et à implémenter des technologies ouvertes et pérennes.

Quel est le futur pour cette identification par smartphone à moyen et long terme ?

V.D. *Aujourd'hui, il y a deux technologies. La première, le NFC, offre des niveaux de sécurité avancés comparables aux technologies de badges type DESFire EV2. La limite du NFC réside dans sa lecture à courte distance, ce qui limite les modes d'identification. La lecture du smartphone sur un lecteur est ainsi limitée à quelques centimètres comme c'est le cas pour un badge classique.*

L'autre technologie, c'est le Bluetooth. Lorsque le canal est sécurisé, vous allez pouvoir vous identifier sur des distances supérieures que le directeur de sûreté pourra définir en fonction des points d'accès. Cela va de quelques centimètres pour des accès sur PNG (portillons

face au RISQUE

Article
Contrôle d'accès et identification par smartphone, les réponses de Vincent Dupart

FACE AU RISQUE - N°563 - Juillet 2020

d'accès automatiques) à une dizaine de mètres pour des accès véhicules. Cela peut être intéressant de le faire comme sur les parkings, pour vous éviter de tendre le bras pour récupérer un ticket par exemple. Mais une technologie va progressivement remplacer le Bluetooth, c'est l'ultra wideband (UWB). Il est beaucoup plus précis que le Bluetooth. Nous sommes capables d'identifier le sens du passage avec l'ultra wideband, ou encore de mesurer avec beaucoup plus de précision la distance de lecture. C'est une technologie qui est progressivement intégrée dans les nouveaux smartphones.

« Anticiper les évolutions futures »

*Nous avons déjà investi sur cette technologie à travers notre **gamme de lecteurs Architect**. L'un des axes forts de différenciation de cette gamme de lecteurs haute sécurité, c'est sa modularité et son évolutivité. Aujourd'hui si vous installez un contrôle d'accès pour la lecture de badges ou de téléphones, et que demain vous avez un besoin de sécurité avancé et que vous voulez ajouter de l'authentification avec de la biométrie, vous pouvez connecter un module biométrie au lecteur. Il en est de même avec l'ultra wideband. Si demain vous voulez ajouter cette technologie, il vous suffira de la connecter au lecteur déjà installé pour toujours être à jour en matière de sécurité. Et demain, vous pourrez également upgrader votre lecteur en intégrant des technologies qui n'existent peut-être pas encore.*

Les clients veulent anticiper les futures évolutions. Nous savons que les niveaux de sécurité évoluent extrêmement rapidement. Lorsque vous investissez dans un système de contrôle d'accès, vous investissez pour les 5 et 10 prochaines années. Donc l'idée, c'est d'avoir des lecteurs qui vont supporter les technologies futures afin de répondre aux enjeux de sécurité à venir.

Eitel Mabouong