


**L'actu des risques
professionnels, naturels &
industriels**
**L'actu des risques malveillance &
incendie**
Expoprotection : le salon
[Actualités](#) [Marchés](#) [Technologies](#) [People](#) [Réglementation](#) [Métiers](#) [Agenda](#) [Dossiers](#) [Annuaire fournisseurs](#)
[Accueil](#) > [L'actu des risques malveillance & incendie](#) > [Contrôle d'accès : jusqu'où iront les badges ?](#)

16-02-2016

 Recevez gratuitement la newsletter
Sécurité et feu

Réagir Imprimer Envoyer

Partager :

Contrôle d'accès : jusqu'où iront les badges ?

Le succès des cartes sans contact et multiservices ne se dément pas dans l'univers du contrôle d'accès. Mais la tendance actuelle met en lumière la montée en puissance des exigences sécuritaires ainsi qu'une plus grande flexibilité des terminaux d'accès.



Sandrine du Caurroy, directrice commerciale d'Alcea. © D.R.

Pas une entreprise, ou presque, qui n'en fasse encore l'économie : le badge s'est imposé comme l'accessoire quasi-indispensable de tout système de contrôle d'accès. Sauf rarissimes exceptions, il est sans contact. Autrement dit, il fonctionne grâce à des liaisons radio. Par ailleurs, le badge de contrôle d'accès est également, dans la plupart des cas, multi-services : le même macaron de plastique sert à ouvrir les portillons d'accès, payer la cantine, les boissons au distributeur, faire des photocopies, voire accéder à certains équipements comme des blouses de travail ou des accessoires professionnels.

Si la technologie utilisée varie un peu selon les cas - accès à des parkings ou à des bureaux -, la carte Mifare classic, développée par NXP, a connu un succès planétaire et s'est imposée comme solution dominante pour les badges à courte portée. Revers de ce succès : elle a été "craquée" dès la fin de la première décennie du millénaire. Du coup, la cloner ne relève plus de l'exploit informatique. Progressivement, le marché a commencé à migrer vers des générations de cartes plus évoluées et plus conformes à la norme ISO 14443. Et notamment vers la carte Mifare Desfire EV1, toujours développée par NXP mais plus sécurisée. « *La Mifare Classic était une carte à mémoire. La Desfire est une carte à microprocesseur au fonctionnement bien plus proche de celui d'une carte bancaire. Elle communique de façon cryptée avec le système de contrôle d'accès* », explique Laurent Rouyer, responsable produit chez Til Technologies, qui conçoit et commercialise des systèmes de contrôle d'accès.

Le mouvement a longtemps été lent. Mais les préconisations faites par l'Agence nationale pour la sécurité des systèmes d'information (Anssi) en novembre 2012 commencent à porter leurs fruits. On recommandait, notamment, d'utiliser en priorité les cartes répondant à la norme ISO 15415, et au moins, une authentification à cryptographie symétrique. « *Depuis 2015, la migration vers les cartes Desfire EV1 s'est vraiment accélérée* », témoigne, par exemple, Sandrine du Caurroy, directrice commerciale du constructeur français Alcea, qui conçoit des badges de contrôle d'accès sous supervision et des contrôleurs. « *Désormais, les grands comptes font le choix de cette technologie* », confirme Laurent Rouyer. Même si le mouvement est en cours, Emmanuel Brunet, directeur marketing d'ARD, concepteur de logiciels de supervision, tient à préciser : « *Pour certains usages, la carte Mifare ultralight C, également très sécurisée mais bien meilleur marché, peut faire l'affaire.* »

Des fonctionnalités sécuritaires de plus en plus utilisées

Les nouveaux badges ne changent pas grand chose aux usages. « *Théoriquement, on peut héberger sur une carte Desfire jusqu'à 28 applications contre 16 sur les cartes Mifare classic 1k (et 40 sur les cartes classic 4k)* », explique Laurent Rouyer chez Til Technologies. En réalité, peu d'entreprises éprouvent de tels besoins ! Le fonctionnement de la carte en multiservices, en revanche, est un peu différent : « *Dans la carte Classic, on affecte à chaque application un secteur précis de la partie électronique*, explique Vincent Dupart, directeur général de STiD, un fabricant de systèmes de contrôle d'accès. *Dans la Desfire EV1, le fonctionnement est plus ergonomique : comme dans une clé USB ou un disque dur, on loge chaque application dans un dossier.* »

Toutefois, Laurent Rouyer note un point négatif : la plus grande puissance de la carte réduit la


[Ajoutez à votre agenda](#)
[Réservez votre badge gratuit](#)
[Consultez la liste des exposants](#)
[Réservez votre stand](#)
[Consultez le programme](#)
[Découvrez la Galerie des Nouveautés](#)

Suivez-nous



Ils soutenaient Expoprotection en 2014



distance de lecture à quelques centimètres. Il faut donc bien approcher son badge très près du lecteur, à 3 ou 4 cm, pour qu'il soit reconnu. Si l'adoption du format Desfire ne signifie donc pas nécessairement la multiplication des services hébergés, « *l'enjeu principal est bien la sécurité* », estime Ali Mahmoud, directeur opérationnel de Castel, qui, outre ses produits d'interphonie, est également présent dans le contrôle d'accès.

Par ailleurs, le Desfire offre une communication cryptée entre le badge et le lecteur. Mais le cryptage n'est pas la seule sécurité offerte : « *Ces cartes ouvrent en outre la voie à ce que l'on appelle la diversification des clés* », explique Vincent Dupart. Autrement dit, chaque carte est dotée d'un identifiant propre, certes, mais aussi d'une clé spécifique que le lecteur calcule à chaque passage. La clé du badge A est donc différente de celle du badge B. Enfin, la carte peut gérer différentes clés selon les applications considérées : contrôle d'accès, cantine, etc.. Le cryptage des communications d'une part, et la diversification des clés de l'autre, permettent un renforcement considérable de la sécurité des systèmes de contrôle d'accès. Les nouvelles cartes répondent ainsi aux préoccupations sécuritaires accrues du moment. En témoigne Camille Fayard, responsable commerciale du fabricant de systèmes de contrôle d'accès Axiom : « *Ces cartes constituent un outil précieux pour gérer la sécurité draconienne à laquelle sont soumis, par exemple, les sites classés Seveso.* » Attention cependant, prévient Laurent Rouyer : « *En contrepartie, ces fonctionnalités exigent une très bonne organisation dans la gestion du contrôle d'accès et de l'encodage des cartes. Il ne s'agit pas de créer des systèmes de clés et d'oublier comment ils ont été construits ! Et plus la sécurité est aboutie, et plus il faut être rigoureux dans la gestion des droits d'accès.* »



Laurent Rouyer, responsable produit chez TII Technologies. © D.R.

Ajuster les systèmes de contrôle d'accès



Idéalement, les lecteurs de badges doivent ne contenir aucune information confidentielle. © Gunnebo

Bien entendu, les cartes Desfire peuvent, tout comme avant elles les cartes Mifare Classic, être utilisées à la fois pour ouvrir les accès dans les systèmes de contrôle d'accès centralisés mais aussi les portes protégées par des serrures électroniques autonomes. Evidemment, ces systèmes d'accès off-line restent d'un niveau de sécurité inférieur puisque le blocage d'un badge, suite à une mise en opposition, par exemple, ne peut pas être transmis au lecteur en temps réel. « *Plus que jamais, il faut veiller à ne protéger de cette manière que des accès non stratégiques comme les salle de réunion, par exemple. Et faire en sorte que les badges voient leurs droits d'accès rechargés très fréquemment* », conseille Emmanuel Brunet d'ARD. « *Car il serait incohérent d'aller, d'un côté vers plus de sécurité avec des badges Desfire, et, de l'autre, tolérer une sécurité bien moindre* », résume Sandrine du Caurroy d'Alcea.

De la même façon, l'adoption de badges plus sécurisés n'est pas sans influence sur les équipements installés devant et derrière les portes protégées. Dans ses recommandations, l'Anssi conseille en effet de ne stocker aucune information sensible dans les lecteurs situés devant les portes, par définition moins protégés que les contrôleurs, placés, eux, en zone "militarisée". « *Le décodage et le traitement sécurisé des badges et la lecture doivent, idéalement, se faire côté protégé* », explique ainsi Dominique Auvray, directeur marketing EMEA de l'activité sécurité électronique de Gunnebo. Autrement dit, le lecteur ne doit être qu'un élément transparent du réseau, servant essentiellement d'antenne de communication.

L'émergence de badges hybrides

Autre tendance récente : le mariage des badges de contrôle d'accès, contenant des puces sans contact de type Desfire, avec des puces avec contact, similaires à celles qui sont intégrées, par exemple, dans les cartes bancaires. « *Tel est le cas des cartes "agent ministériel", déployées par le ministère de l'Intérieur ou encore de la Carte d'identité multi-services (CIMS) déployée par le ministère de la Défense* », explique Ali Mahmoud de Castel. « *On trouve souvent ce type de cartes dans les hôpitaux* », complète Emmanuel Brunet d'ARD. « *Celles-ci permettent à leur porteur, tout à la fois, d'accéder aux locaux, mais aussi de justifier de leur identité, d'accéder aux systèmes d'information et de communication, de payer des services et de sécuriser des échanges électroniques. En effet, ces cartes embarquent la signature électronique des documents* », explique Dominique Auvray de Gunnebo qui travaille notamment sur la carte agent ministériel pour la gestion des accès physiques.



Emmanuel Brunet, directeur marketing d'ARD. © D.R.

Le smartphone, badge du futur ?

Tweets by @InfoProtection

Expoprotection Retweeted

Prévention Carsat AM
@prevention_am

62 salariés sur 1000 ont un accident dans l'année pour le BTP
Presque le double / moyenne !
carsat-alsacemoselle.fr/sites/carsat-a...



5h

Expoprotection Retweeted

Dr Ababacar FALL
@dianbar28

#Crues et #inondations : des animations pour comprendre les risques sco.lt/5L0xkn Some animations to understand #floods

Embed

View on Twitter



Yves Ackermann, responsable EMEA du développement commercial de HID Global. © D.R.

Autre grande tendance : utiliser les smartphones pour ouvrir les accès. « *On n'oublie jamais son smartphone* », explique Yves Ackerman, responsable EMEA du développement commercial de HID Global. Le passage du rêve à la réalité n'est cependant pas toujours aisé. Assez naturellement, les spécialistes du contrôle d'accès souhaitent utiliser le protocole de communication sans fil *Near Field Communication* (NFC) des smartphones. D'autant qu'il fonctionne dans la même gamme de fréquences que celles des cartes de type Mifare (13,56 MHz). Mais les iPhones - sauf les iPhone 6- n'ont pas cette fonctionnalité. Ou, pour ceux qui en disposent, celle-ci n'est utilisable que pour une seule fonction : Apple Pay. Des limitations que ne subissent pas les smartphones sous Android.

Les premiers systèmes de contrôle d'accès fonctionnant avec un smartphone ont donc été mis en place par des opérateurs téléphoniques comme Orange et SFR. Ou des fabricants de cartes SIM comme Gemalto. Lesquels ont

pu équiper leurs personnels de smartphones choisis par eux afin d'implémenter eux-mêmes les fonctionnalités de contrôle d'accès directement sur la carte SIM.

Pour les entreprises ne pouvant pas intervenir sur la carte SIM, et ne voulant pas priver leurs personnels d'iPhones, l'équation est différente. Les constructeurs comme STiD et HID ont donc travaillé sur la technologie Bluetooth, qui équipe, cette fois, tous les portables. Mais le bluetooth fonctionne, quant à lui, à bien plus grande distance. « *Il ne faudrait pas que l'on puisse, à dix mètres, ouvrir une porte et laisser rentrer toutes les personnes qui se trouvent devant* », note Yves Ackerman. Si cette fonctionnalité peut être utile pour les parkings, il faut donc "brider" la distance d'ouverture. « *Il suffit de programmer le lecteur pour lui intimer de ne lire que les badges situés à 1 m, 50 cm ou à une distance inférieure* », explique Vincent Dupart, chez STiD.

Mais ce système est-il sécuritaire ? « *En réalité, le téléphone se comporte exactement comme une carte Desfire notamment concernant la diversification des clés utilisant le numéro de série unique du smartphone IMEI et en sauvegardant l'identifiant de façon chiffrée et authentifiée. Les mêmes applications sont installées sur le smartphone et sur la carte Desfire*, assure Vincent Dupart. *Car désormais, l'identifiant n'est plus nécessairement lié à son support physique.* »



Quelques entreprises commencent à adopter des systèmes de contrôle d'accès actionnés via smartphones. © STiD.

« *Exactement comme l'on peut désormais jouer à un jeu vidéo sur son PC ou sur une console* », renchérit son concurrent Yves Ackerman, chez HID Global. Autre avantage : le téléphone pouvant être lu à une distance un peu plus importante que le badge, il peut tout à fait rester dans le sac ou la poche de son propriétaire. « *Sauf si l'on rajoute des fonctionnalités de sécurité, comme exiger son déverrouillage pour permettre la lecture* », complète Vincent Dupart. Ce système commence à s'implanter, par exemple, pour donner l'accès à un client à une salle de sport ou encore gérer la location de bungalows

En revanche, hormis les exemples précités (SFR, Orange, ..), les entreprises ayant adopté les smartphones ne l'ont fait que pour une partie de leur personnel à laquelle elles fournissent des smartphones de société : pas question encore d'utiliser les smartphones personnels des salariés. « *Cela viendra* », promet Vincent Dupart. « *Mais il reste tout de même un problème : si le système ne fonctionne pas, comment savoir si le défaut vient du contrôle d'accès ou du smartphone qui est totalement personnalisé par son propriétaire ?* », interroge Emmanuel Brunet, chez ARD. En attendant une plus grande maturité du marché, des applications utilisant le téléphone portable - mais sans sa fonctionnalité NFC ou bluetooth - voient déjà le jour.

« *Ainsi nous proposons, par exemple pour les parkings avec réservation, d'équiper leurs entrées de carte SIM. Le numéro de téléphone du visiteur ayant été préalablement enregistré, celui n'a plus qu'à appeler - sans surcoût - pour ouvrir la barrière* », explique Camille Fayard d'Axiom. Le téléphone, c'est sûr, n'a pas fini de s'imposer !

Recevez gratuitement la newsletter
Sécurité et feu

Réagir Imprimer Envoyer

Partager :

Ce site modère les commentaires. Votre commentaire sera visible uniquement s'il est validé par la rédaction.

Vos réactions (0)

Réagir

Soyez le premier à réagir / Signaler un abus

Réagissez

Votre nom/prénom ou pseudo *

Titre de votre commentaire *

Votre commentaire *

Votre e-mail *

Votre adresse email ne sera pas publiée



Ajouter

*Ce site modère les commentaires.
Votre commentaire sera visible uniquement
s'il est validé par la rédaction.*

Suivez-nous

Recevez gratuitement nos newsletters

 Reed Expositions

Site certifié



© 2015 Reed Expositions France | Reed recrute | Données personnelles | Plan du site | Contacts | Mentions légales | Publicité