La lettre d'information #2 – Avril 2018

EDITO

La proximité, une affaire de moyens

Les solutions de sécurité, contrôle d'accès, vidéo-surveillance ou anti-intrusion, sont des applications sensibles qui ne tolèrent pas de rester en panne trop longtemps.

C'est une exigence qui est prise en compte dès la conception des produits. Les électroniques sont robustes et protégées, les architectures sont redondantes. Toutefois la panne ou simplement le dysfonctionnement ne sont pas exclus. Ce jour-là, il faut répondre présent.

ARD a vérifié l'importance que vous attachez à ce point lors de l'analyse de son enquête de satisfaction annuelle. Nous avons donc décidé d'accélérer nos investissements dans deux directions.

Nous avons recruté plus de techniciens en hot line sur notre site de Gap qui collecte l'ensemble des appels clients. Le temps d'attente pour avoir le technicien au bout du fil diminue donc régulièrement. Or c'est le premier maillon de la chaîne qui va permettre que tout rentre dans l'ordre. Le technicien de hot line est capable d'effectuer un premier diagnostic : lecteur défaillant, paramètre erroné ou problème informatique !

Généralement lorsque la partie logicielle est en cause, il est capable d'agir et de réparer le dysfonctionnement, voire de trouver une solution paliative temporaire si le problème s'avère complexe à résoudre.

Néanmoins, il est des cas où le déplacement sur site s'avère nécessaire. Pour réparer le problème (produit à changer, patch à installer, …) ou même pour valider un diagnostic, quelquefois avec un oscilloscope à la main !

Or, plus la distance entre le technicien et le site est faible, plus le temps de réaction sera bon. La Palice n'aurait pas dit mieux. Partant de ce constat pertinent, ARD améliore son maillage du territoire national. En 2017, par exemple, nous avons ouvert un bureau à Mulhouse afin de mieux couvrir l'Est de la France. Nous avons fait de même avec un bureau à Reims. Nous avons également ajouté un technicien itinérant à Nantes. En 2018 nous continuerons notre travail d'araignée tissant sa toile. Lyon est d'ores et déjà un point planifié. D'autres suivront.

La croissance régulière d'ARD et donc votre confiance nous donnent les moyens de cette politique d'investissement, dont nous savons que les dividendes seront au rendez-vous ; pour nous et pour vous.

Frédéric Spagnou - Président

Importance de la volumétrie dans le contrôle d'accès

Les architectures particulières employées dans les solutions de contrôle d'accès peuvent engendrer des limitations quantitatives que l'architecte et le gestionnaire de ces solutions doivent absolument prendre en compte.

ARD S'AGRANDIT …

ERRATUM LETTRE D'INFORMATION OCTOBRE 2017 : NOTRE COLLABORATEUR À REIMS EST MOUAD **MEDROUB** ET NON BEDROUB.

UN NOUVEAU DIRECTEUR POUR LE SERVICE DÉVELOPPEMENT : **BERTRAND GASNIER,** IL REMPLACE **CHRISTOPHE BALISKY** PROMU DIRECTEUR TECHNIQUE.

PLUS DE TECHNICIENS D'INSTALLATION ET DE MAINTENANCE : **ERIC DELEBARRE** À NANTES ET **JÉRÉMY RAMBAUD** À GAP.

PLUS DE COMMERIAUX : **JULIEN NEUILLY** A REJOINT L'ÉQUIPE COMMERCIALE ILE DE FRANCE ET **STÉPHANE MUFFAT** CELLE DU SECTEUR OUEST.

ET AUSSI **CHRISTINE STERBECK** ET **SABINE DIETSCHE** À LA DIRECTION ADMINISTRATIVE ET FINANCIÈRE, **HUBERT LENTREIN** POUR L'INFORMATIQUE INTERNE ET **PHILIPPE SPAGNOU** COMME ASSISTANT MARKETING.

LE GROUPE DEPASSE DÉSORMAIS LES 75 PERSONNES.

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX FRANCE
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – **www.ard.fr**

ARD INVESTIT …

UNE NOUVELLE VERSION DE NOTRE SITE WEB A VU LE JOUR EN JANVIER 2018, PLUS COMPLÈTE, MODERNE ET SURTOUT ADAPTÉE A UNE CONSULTATION SUR ORDINATEUR DE BUREAU, PORTABLE, TABLETTE ET SMARTPHONE.

ARD ENRICHIT SON OFFRE …

UN NOUVEAU **TÉLÉTRANSMETTEUR** DE MESSAGES ET ALARMES INTRUSION A ÉTÉ COMMERCIALISÉ EN FÉVRIER 2018. IL N'EST PLUS NECESSAIRE DE DÉDIER UNE LIGNE TÉLÉPHONIQUE RTC, L'ADRESSE IP ET LE NUMÉRO DE PORT DU TÉLÉSURVEILLEUR SUFFISENT.

CONÇU PAR ARD, CET ÉQUIPEMENT IMPLÉMENTE LE PROTOCOLE CONTACT-ID.

ARD SE MET EN CONFORMITÉ…

LE MODULE DE CAISSE DE LA SOLUTION DE **RESTAURATION GEC** SATISFAIT À L'ARTICLE 88 DE LA LOI DE FINANCE 2015-1785 DU 29 DÉCEMBRE 2015. GEC RÉPOND AUX CONDITIONS D'INALTÉRABILITÉ, SÉCURISATION, CONSERVATION ET ARCHIVAGE, EN VUE DU CONTRÔLE DE L'ADMINISTRATION FISCALE DANS LA LUTTE CONTRE LA FRAUDE À LA TVA.

L'informatique traditionnelle nous a habitué à dépasser régulièrement ses limites, mémoire centrale, puissance des processeurs, chaque année on peut avoir plus pour moins d'argent. On fait donc de moins en moins attention aux optimisations de code pour limiter l'usage des calculateurs ou bien la taille de la mémoire centrale. La bande passante croissante des réseaux évolue également dans le même sens.

Or l'architecture spécifique des solutions de contrôle d'accès nous oblige à revenir sur ces nouvelles habitudes. Cette architecture inclut des éléments essentiels qui ne sont pas aussi extensibles qu'un ordinateur central.

Il faut en retenir 3, l'unité logique, la carte à puce, et le réseau de terrain.

L'unité logique (UTL), c'est cette carte électronique, en fait un petit ordinateur, qui fait tampon entre l'ordinateur central et les lecteurs qui permettront d'identifier les usagers en vue d'ouvrir ou non les portes. Son rôle, éviter que si l'ordinateur central s'arrête, toutes les portes restent ouvertes ou restent fermées. Les droits d'accès sont chargés dans ces unités logiques et en cas de panne du serveur, elles prennent le relais et permettent un fonctionnement quasi normal du site.

On installe habituellement une unité logique pour 2 à 8 portes et sur un site d'importance, la volumétrie des unités logiques devient importante. Or, pour de simples problèmes de coût, la mémoire et le processeur de ces cartes sont loin d'atteindre les caractéristiques d'un serveur. Il faut donc éviter de créer des architectures où chaque unité logique devra stocker des droits complexes attachés à 100.000 badges par exemple. En outre, au-delà des problèmes de stockage, le temps de chargement de ces droits deviendra potentiellement problématique.

La carte à puce est aussi, à son échelle, un petit ordinateur. Sur des applications filaires, elle n'a à stocker qu'un identifiant du porteur. Aussi complexe et aussi crypté soit-il, la carte à puce n'aura aucun problème de place pour le stocker ni de problème de temps de réponse pour le déchiffrer et dialoguer avec le lecteur.

Par contre, les serrures autonomes fonctionnent de manière différente. Les droits d'accès sont partagés entre la serrure et la carte. C'est sur cette dernière que l'on écrira les accès possibles pour le porteur. On imagine facilement que stocker les droits sur 500 portes et y ajouter des plages horaires par exemple (le porteur peut ouvrir la porte 12 mais uniquement entre 8 heures et 17 heures), peut représenter un volume important d'informations, à l'échelle de la carte. Et si on augmente alors la taille mémoire de la carte, c'est le processeur qui deviendra le maillon faible et donnera des temps de réponse en lecture de plusieurs secondes.

Il existe des solutions, comme par exemple dans les serrures au format OSS qui consistent à enregistrer les droits sur des groupes de porte et non porte par porte, mais le coût à payer est non négligeable, il faut alors organiser et gérer son site d'une façon qui rappelle les organigrammes de clés à l'ancienne.

Enfin, le contrôle d'accès filaire irrigue l'ensemble des bâtiments jusqu'aux portes les plus éloignées des gaines principales. On relie alors les lecteurs aux unités logiques non plus par des liaisons IP mais par des

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX FRANCE
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – **www.ard.fr**

DE NOUVEAUX ETABLISSEMENTS SONT ÉQUIPÉS AVEC LES SOLUTIONS ARD

PARMI EUX, LES PALAIS DE JUSTICE DE POITIERS, SAINT-MALO, POINTE-À-PITRE, L'HOTÊL DE POLICE DE FORT-DE-FRANCE, LA COMMUNAUTÉ D'AGGLOMÉRATION DU DOUAISIS, L'INSTITUT MGEN DE LA VERRIERES, LE CH ROMAIN BLONDET À SAINT-JOSEPH EN MARTINIQUE, LE CH D'ABBEVILLE, L'EHPAD DE EQUERDREVILLE, LE CH DE BLAY, IFPS DE GRENOBLE (UGA), MÉDIPOLE DE VILLEURBANNE, L'IFPS DE L'UNIVERSITÉ DE GRENOBLE ALPES, LES BÂTIMENTS HEXAGONE ET TPR1 ET 2 À AIX MARSEILLE UNIVERSITÉ (SITE DE LUMINY), LE CNRS DE MARSEILLE MAIS AUSSI L'ENSMM DE BESANÇON, LE CROUS G. FAURÉ À GRENOBLE, LA COMUE DE VILLENEUVE D'ASCQ, ETC.

cables électriques gérés par des bus de terrain aux caractéristiques de vitesse, et de débit qui sont une nouvelle limite technique inconnue des réseaux informatiques standards.

En conclusion, il est important pour les responsables de ces solutions de contrôle d'accès, de bien avoir en tête ces limites. Sur un site étendu à plusieurs bâtiments, avec de très nombreux porteurs de badges, il pourra être opportun de répartir les usagers dans plusieurs instances de contrôle d'accès lorsque seule une minorité d'entres eux ont des accès autorisés un peu partout. Cette logique est à reconduire sur des sites à forte volumétrie de serrures autonomes.

Ces questions sont complexes et c'est l'un des rôles de sociétés comme ARD de vous assister dans ces phases amont d'études afin que vous n'ayez pas à subir les mauvais choix en phase d'exploitation.

Le conseil du technicien : N'oubliez pas vos batteries

Votre solution de contrôle d'accès est prévue pour résister à une panne d'alimentation électrique ! Elle comprend un ensemble de batteries qui vont suppléer au courant électrique et assurer sur une période bien entendue limitée, un fonctionnement non dégradé du système. Vous pourrez ainsi continuer à entrer et sortir avec le même niveau de contrôle et de sécurité, le temps de rétablir le courant.

Comme pour votre véhicule, ces batteries ne sont pas vraiment visibles et on a tendance à les oublier … jusqu'au jour ou la panne électrique survient et que leur vetustée ne permet plus de garantir une autonomie acceptable !

Il faut anticiper ! Une batterie est un élément dont la durée de vie dépend des sollicitations qu'elle endure mais au-delà de trois ans il est normal de la remplacer. C'est une opération à planifier. Surtout ne l'oubliez pas !

Le contexte est le même si vous avez installé des béquilles ou des cylindres électroniques. Ils fonctionnent à l'aide de piles qu'il faut également prévoir de changer.

Ces équipements étant dotés d'un indicateur de défaut batterie faible, vous pouvez les remplacer au cas par cas. Mais cette solution nécessite que tout le monde soit formé à comprendre et interpréter le signal émis et que vos équipes soient prêtes à intervenir avant l'arrêt complet de la serrure.

Nous conseillons plutôt de remplacer régulièrement vos piles de façon préventive.

Nos techniciens, en hot line sont à votre disposition pour vous donner plus d'informations. Les piles et batteries sont des éléments standards. Vous pouvez les acheter chez un revendeur proche de chez vous ou bien auprès d'ARD.

Les piles et batteries sont en promotion du 15 avril 2018 au 15 juin 2018 chez ARD.

Les architectures haute sécurité : l'ANSSI Niveau 1

Le métier du contrôle d'accès nous ramène au vieux concept de la concurrence entre le canon et le blindage. Chaque année les hackers progressent et leurs méthodes d'attaque se sophistiquent. Pour répondre à ce challenge, il faut réfléchir à des produits et des architectures de plus en plus robustes.

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX FRANCE
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – **www.ard.fr**

Les services du Premier Ministre, au travers du SGDSN et de l'Agence Nationale de Sécurité des Systèmes d'information (l'ANSSI) ont travaillé pour parvenir à un ensemble de recommandations dédiées aux systèmes de contrôle d'accès et aux technologies sans contact.

Ses conclusions aboutissent notamment à une classification des architectures utilisées par les solutions de contrôle d'accès, du plus sûr (type 1) au plus vulnérable (type 4).

L'administration française prend en compte ces recommandations et demande des architectures de niveau 1 sur ses sites les plus sensibles, comme des gendarmeries, des préfectures, etc.

Ces préconisations sont tout aussi pertinentes dans le secteur des universités, dans les établissements d'enseignement supérieur privé, dans les centres de recherche mais aussi dans le secteur privé tertiaire et industriel.

Le point commun à tout ces secteurs est l'usage d'une carte sans contact à capacité cryptographique telle que la technologie NXP Desfire, et à un degré moindre NXP Mifare Ultralight C.

ARD a développé une version de sa solution de sûreté conforme aux préconisations de l'ANSSI architecture n°1. C'est un investissement lourd car dans ce schéma, par exemple, l'identification du badge ne se fait plus dans le lecteur, qui se situant à l'extérieur du périmètre sécurisé pourrait être arraché puis analysé, mais par l'UTL. L'ensemble des messages et communications est crypté , les clés secrêtes sont stockées dans des modules de sécurité physiques (SAM) se trouvant dans chaque UTL. La solution ARD est aujourd'hui opérationnelle et déjà déployée sur un site public « sensible ».

Cette architecture optimisée sur le plan de la sécurité, implique un surcoût à l'installation et une exploitation légèrement plus complexe à cause de la gestion de la cryptographie. Il faut donc s'assurer que le choix de la sélectionner ou non est pertinent dans votre contexte.

ARD est à votre service pour vous aider à conduire cette analyse afin de valider l'intérêt ou non de sélectionner une architecture ANSSI 1.

La carte CPS Santé dans ce contexte ANSSI

La carte CPS, telle qu'elle est utilisée actuellement dans les systèmes de contrôle d'accès physique, correspond du point de vue sécuritaire à une carte Mifare Classic 1K. Cette technologie n'offre plus qu'une sécurité relative face au **rejeu** ou au clonage depuis qu'elle a été « crackée » il y a quelques années. Elle a été bannie par les administrations Françaises au profit de la technologie NXP Desfire selon les recommandations de l'ANSII (Agence Nationale de Sécurité des Systemes d'Information).

Dans le but de réduire les vulnérabilités des systèmes de contrôle d'accès physiques dans les établissements de santé, l'ASIP étudie les différentes solutions visant à mettre en oeuvre les capacités cryptographiques très évoluées de la carte CPS. L'exploitation de la bi clé RSA 2048bits associée au certificat X509 de la carte permettrait une authentification mututelle très solide et une communication sécurisée SSL entre la carte de l'usager (CPS) et le lecteur de contrôle d'accès.

L'enjeu est à la fois de renforcer la sécurité tout en préservant des temps de réponse acceptables pour un usager du contrôle d'accès et de ne pas augmenter trop les coûts.

La première piste consisterait à spécifier un lecteur de contrôle d'accès IAS ECC autonome du point de vue authentification et dialogue avec la carte de l'usager. Ce lecteur permettrait la mise en œuvre de l'architecture de contrôle d'accès recommandée en choix n° 2 par l'ANSSI. Par contre cette solution aboutit à un lecteur plus « intelligent » et malheureusement exposé aux risques d'attaque car il se situe en dehors du périmètre protégé.

La seconde viserait à définir un lecteur transparent se comportant comme un simple modem chargé de véhiculer le signal radio entre la carte et l'UTL. Il délèguerait donc la responsabilité de l'authentification et du chiffrement à l'UTL. Cette option aboutit à une architecture beaucoup plus sécurisée et de ce fait fortement recommandée par l'ANSSI. En effet, l'intelligence est concentrée dans les UTL qui sont protégées des attaques physiques puisqu'installées dans des zones sous contrôle d'accès.

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX FRANCE
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – **www.ard.fr**

Quelle que soit la solution retenue, une seconde question se pose. Faudra-t-il preserver le schéma de sécurité standard à chaque transaction avec une carte (authentification selon la structure pkcs#15, récupération du certificat) au risque d'introduire des temps de réponse incompatibles avec le contrôle d'accès ? Ou bien faudra-t-il s'orienter vers un schéma intermédiaire, laissant le serveur de contrôle d'accès vérifier le statut des certificats de chaque carte périodiquement et charger sur les UTL uniquement des listes blanches de cartes avec le minimum d'information pour assurer l'authentification (ex : la clé publique associé à l'UID de la carte) ?

ARD suit attentivement les travaux de l'ASIP et veillera à faire évoluer sa solution ARD Access haute sécurité pour répondre aux spécifications retenues. Les impacts seront à la fois au niveau du module de gestion des cartes (enrôlement, mise en opposition, interfaçage avec l'autorité de certification, etc.) mais aussi au niveau matériel et logiciel embarqué dans les UTL, à l'image du processus de certification initialisé recemment auprés de l'ANSSI.

Toutefois, il y a deux grands absents dans ces réflexions : le contrôle d'accès au moyen de serrures électroniques radio et au moyen de serrures autonomes, le premier pour des questions de temps de réponse, le second tant que l'interdiction d'écrire les droits d'accès dans une carte CPS n'est pas levée.

RGPD

Le 25 mai 2018 le Règlement Général sur la Protection des Données (RGPD) s'applique aux 28 membres de l'Union européenne et donc à la France. Ce nouveau règlement augmente les obligations des éditeurs comme ARD et des utilisateurs comme vous-même, quant à la sécurisation des données personnelles.

Dans ce cadre, nous avons planifié le développement des quelques modifications à apporter à nos produits pour les rendre conformes à ces nouvelles exigences. Nous les mettrons rapidement à votre disposition. Pour nos clients sous contrat de maintenance, cette mise à jour sera gratuite.

Nous sommes également à votre disposition pour vous apporter notre expertise sur le sujet, si nécessaire.

Au delà des évolutions logicielles, ce nouveau règlement peut avoir des impacts sur l'exploitation que vous en faites. Nous vous conseillons d'approfondir vos connaissances sur le sujet en consultant le site https://www.cnil.fr/fr/reglement-europeen-protection-donnees.

Parmi les éléments (entre-autres) à retenir : ne collecter que les données essentielles, ne pas obliger à remplir des champs qui s'avèreraient facultatifs, donner un droit d'accès à leurs données aux personnes enregistrées dans la base de données et formaliser un droit à l'oubli, purger automatiquement et sélectivement les données d'une base active lorsqu'il n'y a plus de raisons de les conserver, etc.

Nous aurons également à faire évoluer le cadre des relations entre ARD et les utilisateurs de ses solutions : il nous faudra un accord formalisé de votre part avant que nous puissions accéder à vos bases de données (maintenance/hot line). Cette obligation pourra conduire à un avenant au contrat de maintenance ou des échanges formalisés avant que notre service de maintenance puisse accéder à votre application.

Nous aurons aussi l'obligation de vous informer, si nous constatons une violation des règles en matière de protection des données (exemple conservation de données trop anciennes).

Dans ce contexte, nos salariés seront formés à cette nouvelle règlementation. Ainsi, cette sensibilisation jointe aux évolutions logicielles et aux modifications contractuelles déjà mentionnées, permettra à ARD d'être en mesure d'offrir à ses clients des garanties suffisantes quant à la bonne application de ce nouveau règlement lors de l'utilisation de ses solutions et services.

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX FRANCE
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – **www.ard.fr**