UNE INTRODUCTION AUX TECHNIQUES D'IDENTIFICATION

La technique d'identification est un paramètre déterminant du niveau de sécurité garanti par un système de contrôle d'accès ; elle fixe aussi les modalités d'exploitation à mettre en œuvre pour gérer la distribution des badges.

Les badges de proximité

Les techniques de proximité fonctionnant à la fréquence de 125 Khz permettent une portée de lecture de 10 cm à 1 mètre. Leur utilisation est donc « confortable ». Que ce soit des cartes HID™ ProxCard II™, HID ISOProx II™, Indala® FlexPass, STid™ ou EM Microelectronic™, ces techniques n'ont néanmoins pas une résistance forte contre l'écoute frauduleuse des codes transmis et la duplication soit du badge, soit du code. Leur sécurité est en effet limitée par la technologie et la taille des puces de ces badges. NCS® offre une méthode de protection dite VHR™ (Very High Reliability) qui dissocie le code physique écrit dans le badge du code logique utilisé pour gérer les habilitations.

Les technologies 13,56 MHz

Les techniques à 13,56 Mhz représentent un important progrès en termes de sécurité et de capacité des mémoires, des unités de traitement et des vitesses des échanges. Le prix à payer est une moindre portée de lecture qui ne dépasse pas 10 cm. On y trouve des techniques comme MIFARE® de NXP® et tous ses dérivés (comme MIFARE DESFire® EV1), iCLASS™ de HID, des applications spécifiques comme les cartes CPS3, La carte agent Ministérielle (FR), Calypso et d'autres encore. Les nouvelles capacités permettent d'utiliser des processus sécurisés de chiffrement (Cryptage) et d'authentification pour stocker et protéger les données et pour sécuriser les échanges badge-lecteur-automate. Grâce à ces processus, ces badges sont effectivement « multi-services », chaque application étant individuellement sécurisée. La gamme Scaline® de NCS® propose un large éventail de solutions, des plus simples aux plus sécurisées. De même pour la série Architect™ de STid et la plateforme iCLASS SE® de HID.

Les cartes MIFARE®

La technologie MIFARE, développée par NXP®, est une technologie de lecture/écriture pour badges à puce sans contact et lecteurs, conforme à la norme ISO 14443A ; MIFARE qui utilise des technologies de communication sécurisées en radiofréquence à 13.56 MHz entre les badges et les lecteurs, est devenue un des standards de l'industrie.
Dans la gamme, on trouve MIFARE Classic® et MIFARE Plus®, conformes à ISO 14443A-3 qui offrent une organisation prédéfinie des mémoires des badges en secteurs pour permettre de faire cohabiter de façon sécurisée plusieurs applications sur la même carte. On accède aux données soit par la sélection des numéros des secteurs qui les contiennent soit par le code de l'application enregistré dans le MAD (MIFARE Application Directory).

On trouve aussi MIFARE DESFire EV1 et EV2. C'est un système opératoire pour badges à puce sans contact conforme à la norme ISO 14443A-4. Le système opératoire gère l'organisation interne des mémoires des badges et la sécurisation, notamment par cryptage DES, 3DES ou AES. La structure permet de faire cohabiter plusieurs applications sur la même carte. On accède aux données par le code de l'application enregistré dans l'AID (Application IDentifier).

National Control Systems S.A.
Paepsem Business Park, Bat. 1
Blvd Paepsemlaan, 18C
1070 Bruxelles
Belgique
ncs.belgium@ncs-scaline.com
Tel : +32 2 245 22 39
Fax +32 2 245 16 25

National Control Systems S.A.R.L.
Les Flamants ZAC Paris Nord II
Rue de la Perdrix
93290 Tremblay-En-France
France
ncs.france@ncs-scaline.com
Tel : +33 1 48 17 81 86
Fax +33 1 49 38 02 88

www.ncs-scaline.com

Chacun de ces badges possède un UID (Unique Transponder Identification Number) ; c'est un numéro unique identifiant la puce contenue dans un badge. Appelé abusivement « numéro de série », l'UID qui n'est pas sécurisé, est parfois utilisé comme identifiant pour des applications de sécurité moyenne.

La sécurisation des identifiants dans SCNET4™ SECURE

La version SECNET4™ SECURE utilise les badges MIFARE DESFire EV1 dans le mode le plus sécurisé. La sécurité du badge est renforcée :

- Par l'utilisation d'une identification (dite abusivement « numéro de série ») aléatoire (Random ID) de la carte au lieu de l'UID fixe qui n'est pas accessible. Celle-ci n'est utilisée que pour permettre le lien lecteur – carte pendant la communication. Une fois la communication établie, une authentification est réalisée avec la carte de manière à pouvoir déterminer l'UID réel de celle-ci.

- Par l'utilisation de clés diversifiées d'accès au contenu pour la lecture, l'écriture ou le changement; ainsi chaque badge contiendra des clés différentes. Ces clés sont calculées, pour chaque carte, en utilisant un diversifiant pouvant dépendre, par exemple, de l'UID réel de la carte, de paramètre de l'application ainsi que des clés maîtres de l'application.

- Par l'utilisation d'un code d'identification de la personne accompagné d'une signature cryptographique appariant le code et le badge (Anti clonage). Cette appariement peut-être réalisé à l'aide d'une signature numérique ou d'une fonction de scellement, utilisant comme données, une combinaison de l'identifiant de la personne et de l'UID réel de la carte.

National Control Systems S.A.
Paepsem Business Park, Bat. 1
Blvd Paepsemlaan, 18C
1070 Bruxelles
Belgique
ncs.belgium@ncs-scaline.com
Tel : +32 2 245 22 39
Fax +32 2 245 16 25

National Control Systems S.A.R.L.
Les Flamants ZAC Paris Nord II
Rue de la Perdrix
93290 Tremblay-En-France
France
ncs.france@ncs-scaline.com
Tel : +33 1 48 17 81 86
Fax +33 1 49 38 02 88

www.ncs-scaline.com