NFC: kekseksa?

Thomas Engel (texte et illustration)

NFC est le sigle américain pour *Near Field Communication* pour «communication dans un champ proche». C'est une norme internationale pour l'échange de données par ondes radio dans un rayon de quelques centimètres. Le débit maximum est de 424 kbit/s. Cette technique s'est fait connaître par les systèmes de paiement sans espèces. De plus en plus d'appareils mobiles sont aujourd'hui dotés d'une interface NFC qui permettra à l'avenir et malgré la faible vitesse de transmission le développement de nombreuses et intéressantes applications. J'ai évoqué la technique RFID dans l'un de mes précédents articles. NFC repose sur le même principe technologique.

NFC

La technique NFC a fait l'objet de nombreux essais depuis bien des années, mais au début pas encore sous son nom actuel. A l'origine, ce sont surtout des groupes de l'électronique de divertissement, tels que Sony, qui ont participé à son développement. Les premières certifications à l'Organisation internationale de normalisation (ISO) datent de 2010. De nouvelles inscriptions arrivent jour après jour sous la rubrique «Technologies de l'information – télécommunications et échange d'informations entre systèmes» avec de nouvelles évolutions et applications.

La vitesse de transmission des données est trop faible pour permettre le transfert en temps utile de grandes quantités de données, telles qu'images ou vidéos. Les applications typiques de la technique NFC sont l'échange d'informations brèves entre deux appareils tout proches l'un de l'autre.

De plus en plus de fabricants utilisent une combinaison de Bluetooth (BT) et de NFC dans le but de simplifier l'interconnexion des appareils. Le signal NFC transmet les «données utilisateur» pour connecter les deux appareils, puis le signal BT se charge de la transmission des données. Il n'est dès lors plus nécessaire de procéder à l'interconnexion manuelle de la paire émetteur et récepteur BT. Le signal NFC active l'interconnexion BT à condition que les deux appareils soient très proches l'un de l'autre. Il faut aujourd'hui regretter que les téléphones mobiles soient les seuls à disposer simultanément des deux techniques. Nul doute qu'à l'avenir, de plus en plus d'appareils mobiles seront équipés de la technique NFC qui est si commode.

A côté des paiements sans espèces ou de la simple interconnexion de deux appareils, la technique NFC permet d'échanger simplement et rapidement des cartes de visites par exemple. On peut aussi imaginer que votre propre téléphone portable enregistre les informations NFC de différentes cartes de visite, cartes d'identité, cartes d'assurance-maladie et autres documents. A l'avenir, c'est votre téléphone qui portera vos cartes et pièces d'identité. Mais ces applications si utiles sont également très dangereuses car, en théorie, quiconque est versé en NFC pourrait lire et enregistrer ces informations sans que leur légitime propriétaire ne s'en aperçoive.

Technique NFC

La technique NFC repose sur l'induction électromagnétique. Les champs magnétiques rayonnent à haute fréquence (à env. 13 MHz). La porteuse est modulée par déplacement d'amplitude *(Amplitude Shift Keying – ASK)*. Les débuts de cette technique se reflètent dans le codage qui repose soit sur la technique développée par Philips (MIFARE), soit sur celle de Sony (FeliCa). Ces deux techniques recourent toutes deux à un transpondeur passif. Comme je l'ai décrit dans mon article sur les dispositifs RFID, ces systèmes ne possèdent pas d'alimentation électrique propre. L'antenne travaille ainsi en même temps comme un transformateur et produit à partir du signal d'induction qu'elle reçoit le courant nécessaire au fonctionnement du transpondeur.

Aujourd'hui, les deux systèmes sont principalement utilisés pour les paiements sans espèces où la sécurité joue un rôle essentiel. Nul doute que bien d'autres applications verront le jour à l'avenir.

Technique NFC et sécurité

La sécurité est à ce jour mise en doute, et on la décrit constamment comme insuffisante. En avril 2008 notamment, on a appris que son algorithme de cryptage avait été «cassé» …

Cependant, les attaques à distance ne sont pas possibles en raison du très faible rayon d'action des signaux NFC. Ceci réduit considérablement les risques. De plus, il existe aujourd'hui des étuis spéciaux qui bloquent les signaux. Quelques systèmes associent le signal NFC à l'introduction d'un code. Parmi les nombreuses applications qui reposent aujourd'hui sur cette technique, il en est pour lesquelles la sécurité passe à l'arrière-plan, alors qu'elle est vitale pour d'autres. Les systèmes de paiement sans espèces, contrôle des accès, etc. font partie des plus sensibles, tout comme les clés de voitures sans contact et les dispositifs utilisés dans la santé.

Le développement des méthodes de chiffrement s'est poursuivi, et elles ont été améliorées afin d'assurer la sécurité. Les systèmes actuels de paiement sans espèces sont cryptés AES-128 et satisfont aux normes internationales sur la sécurité des systèmes informatiques.

A suivre …