springcard
YOUR EXPERT IN CONTACTLESS SOLUTIONS

January / Janvier 2016

technological watch

ENSURING SECURITY IN THE INTERNET OF THINGS

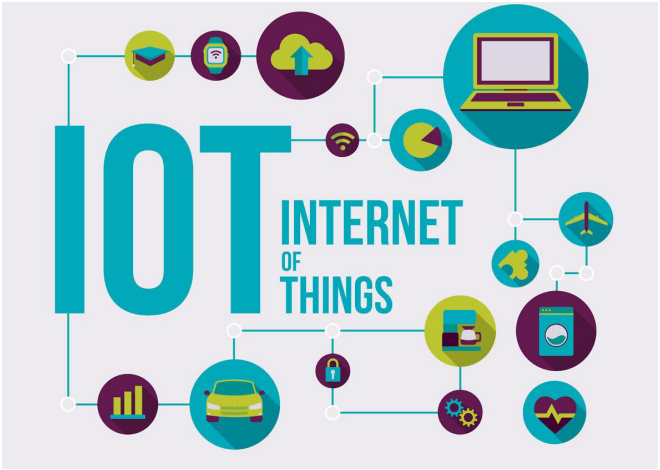
In everyday life, anyone want to be sure that his **personal data** used and registered by connected things are **safe**, and that the connected things themselves can't get hacked. But above all, anyone wish this **security to be invisible** and not to make life more complicated because of passwords to remember.

From their part, **equipment manufacturers** don't want to be pointed if a product comes to get hacked. And **brands** have to get it right otherwise their image will suffer.

The Internet of Things is probably the begining of a new economic phase. Frameworks will gradually be defined, but questions of **costs related to security** are already put forward and impacts in terms of **image** for brands seems to be major.

A cryptographic software stack seems not to be sufficient because of all the examples of security breaches in softwares.

The major step towards a strong security then begins with **secured modules**, providing strong authentication and protection. The **NXP A70CM module** answers all these needs.



JUST ASK SPRINGCARD!

SpringCard is able to implement this module for any kind of project that needs a strong security level.

Please contact info@springcard.com

Reference: NXP blog, *Enabling trust in the Internet of Things era*, June16, 2015, [online] http://blog.nxp.com/security/enabling-trust-in-the-internet-of-things-era/

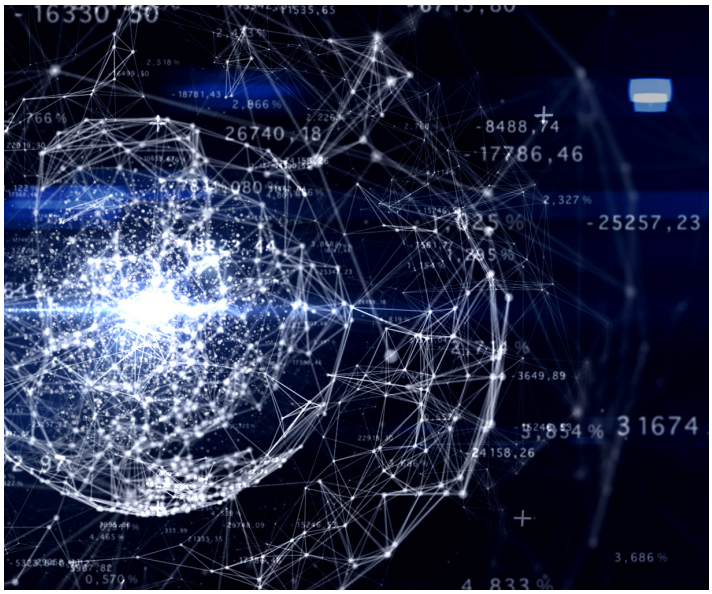


Image provenant du blog de NXP

DEMANDEZ-LE NOUS, NOUS LE FERONS !

SpringCard peut intégrer le module de NXP pour tout projet aux exigences en sécurité fortes.

Pour nous contacter : info@springcard.com

GARANTIR LA SÉCURITÉ DES OBJETS CONNECTÉS

Dans la vie quotidienne, chacun attend que ses **données personnelles**, utilisées et stockées par les objets connectés qui l'entourent, soient **en sécurité**, et que les objets eux-mêmes soient protégés du piratage. Mais surtout, chacun attend que cette **sécurité passe inaperçue** et qu'elle n'implique pas de retenir quantité de mots de passe.

De leur côté, les **fabricants de ces objets** ne veulent pas être tenus responsables au cas où leurs produits viendraient à être piratés. Quant aux **marques**, elles doivent être vigilantes pour que leur image ne souffre pas en cas de piratage.

L'Internet des objets constitue le début d'une nouvelle ère économique. Les cadres vont progressivement se mettre en place, mais les **questions des coûts liés à la sécurité** et les impacts en termes d'**image** pour les marques sont d'ores et déjà mis en avant.

L'empilement de logiciels de cryptographie n'apparaît pas une réponse convaincante aux problèmes de sécurité en raison d'exemples passés de brèches de sécurité dans ces mêmes logiciels.

L'étape essentielle vers une sécurité sans faille commence avec l'intégration de **modules sécurisés** dans les objets, à même d'apporter protection et solide authentification. Le **module A70CM de chez NXP** répond justement à ces attentes.

Référence : blog de NXP, *Installer la confiance dans l'Internet des Objets*, 16 juin 2015, [en ligne] http://blog.nxp.com/security/enabling-trust-in-the-internet-of-things-era/