Les problèmes sociétaux liés à la technologie RFID

Remarque préliminaire

Les craintes ressenties et exprimées du public augmentent au fur et à mesure du déploiement des applications RFID.
Elles couvrent trois domaines (par ordre décroissant d'inquiétude):

-) protection des données individuelles (flicage)

-) problème de santé publique (exposition aux champs électromagnétiques)

-) souci d'environnement (recyclage des produits)

Environnement règlementaire

2008: An 1 de l'implication des Pouvoirs Régaliens Mondiaux dans les problèmes Sociétaux liés à la technologie RFID lors de la réunion ministérielle de l'OCDE à Séoul les 17 et 18 Juin (1).

Ont été prises en considération les notions de sécurité des données et de protection des libertés individuelles. Des mesures de protection sont proposées.

(1) www.oecd.org/dataoecd/19/42/40892347.pdf

Environnement légal

Il est indispensable de protéger de façon légale les individus contre tout abus liés à l'utilisation d'une technologie qui permet de les tracer (déplacements et comportements) à leur insu, et de conduire à des discriminations.

Environnement légal

Au niveau Européen la protection des données individuelles est couverte par la Directive 95/46 EC du 23/11/95 et complétée par la Directive ePrivacy 2002/58 EC publiée en 2002.

Les équipements RFID (Interrogateurs et tags actifs et passifs) tombent dans le domaine d'application de la Directive 1999/5/EC (dite Directive R&TTE) (1)

(1) Radio & Telecommunications Terminal Equipement

Environnement légal

Selon la Directive 1999/5/EC, les besoins de protections des individus couvrent les mécanismes de lecture des données et de désactivation des tags et la nécessité d'information des personnes sur l'existence d'applications RFID.

Ces mesures de protection ont également pour but principal de créer la confiance du public dans la technologie RFID

Sécurité des informations

Elle concerne 3 volets:

Disponibilité: En temps voulu par les personnes autorisées.

Intégrité: Assurance que les informations n'ont pas été altérées

Confidentialité: Assurance que l'accès est réservé aux personnes autorisées.

Les attaques peuvent concerner les tags, les interrogateurs, l'interface air et la liaison avec le S.I..

Sécurité des informations

Il est important de noter que les risques sur la sécurité des données deviennent des menaces sur la protection des données personnelles lorsque les individus peuvent être identifiés ou identifiables.

La Commission Européenne

La Commission Européenne, au nom des Pays membres, répond de deux façons:

- Publication du Mandat 436 le 8 décembre 2008 chargeant les 3 Organismes Européens de Standardisation de développer des Standards Européens
- Publication le 12 mai 2009 d'une Recommandation couvrant l'analyse des risques et l'information du public

La Recommandation

Elle est entrée en application. Elle développe deux concepts:

Un PIA (Private Impact Assessment) qui oblige tout opérateur d'une solution RFID a étudier les risques encourus et à soumettre les résultats à la DPA. (1)

Une signalétique normalisée au niveau Européen visant à informer le public de l'existence d'une application RFID

(1) Data Protection Authority (En France la CNIL)

Le Mandat M436 EN

Un contrat a été signé avec les trois organismes de standardisation européens (CEN, CENELEC et ETSI) le 1er Janvier 2010. Il comprend deux phases:

Phase 1: Préparer un programme de travail de développement normatif

Phase 2: Effectuer le travail normatif tel que défini en phase 1

Le Mandat M436 EN

Note importante: Le Mandat 436 couvre les problèmes de sécurité des données et de « Privacy » mais également les problèmes de santé (exposition aux champs électromagnétiques) et d'environnement (recyclage des équipements RFID)

Phase 1

Création du Groupe de Coordination (RFID-CG) composé de membres des 3 Organismes et recrutement d'un groupe d'experts (STF) pour rédiger le programme de recommandations.

-) 1ère téléconférence le 22 Janvier 2010

-) Kick Off meeting le 1er Février 2010

Fin du contrat 31 Mars 2011

Les tâches du RFID-CG

Tâche 1: Mettre en place la STF

Tâche 2: Consolider les travaux qui concernent la sécurité des données et la protection des données personnelles dans le cadre des règles de l'OCDE

Tâche 3: Chaque Expert consulte son environnement personnel et fait des propositions

Les tâches du RFID-CG

Tâche 4: Analyse des différentes applications et proposition de PIA adéquats.

Tâche 5: Développer des signes et/ou des logos destinés à alerter le public, en concordance avec la Recommandation du 12 mai 2009.

Tâche 6: Promotion des travaux dans le monde actif

Phase 2

Chaque Organisme Européen développe les standards tels que définis dans la phase 1

Démarrage de la phase 2: 1er Avril 2011

Fin de la phase 2: 31 Mars 2013

Conclusions

- Le pouvoir législatif devient de plus en plus exigeant et pressant
- Toutes les applications RFID sont concernées
- Tout opérateur potentiel devra connaitre les directives et faire un PIA
- Toute application RFID incluant un risque devra être signalée selon les normes qui seront publiées.