CNRFID
CENTRE NATIONAL DE REFERENCE

Le CNRFID, de l'innovation au déploiement de solutions RFID

LES PUBLICATIONS DU CNRFID
NORMES, REGLEMENTATIONS ET STANDARDS

CNRFID'S APPLICATIONS
STANDARDS AND REGULATIONS

Évaluation de l'impact des applications RFID sur la vie privée

RFID and Privacy Impact Assessment (PIA)

Le CNRFID est soutenu par / CNRFID is supported by:

dgcis

CONSEIL GENERAL BOUCHES-DU-RHÔNE

Ville de ROUSSET

LE CENTRE NATIONAL DE RÉFÉRENCE RFID

Initié par le Ministère de l'Economie, de l'Industrie et de l'Emploi, le Centre National de référence RFID (CNRFID) a l'ambition de faciliter l'adoption de la RFID et d'en développer les usages.
Il favorise le déploiement de solutions entre offreurs, utilisateurs de solutions RFID, institutions et organismes de recherche.

Il les accompagne selon leurs besoins et intérêts respectifs en :
- Identifiant les valeurs apportées dans chaque métier
- Développant l'usage de la technologie RFID
- Accélérant l'appropriation de la RFID
- Multipliant les opportunités business
- Fédérant les initiatives au niveau national

Le CNRFID est membre de plusieurs comités de normalisation : le CEN, l'ETSI et l'ISO. Il regroupe désormais 125 acteurs au niveau national et international impliqués dans la RFID.

En savoir plus sur le Centre National de Référence RFID : www.centrenational-rfid.com

VERSION FRANÇAISE

SOMMAIRE

01. HISTORIQUE DE L'ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE

Le terme RFID sous-entend plusieurs technologies dont les applications peuvent être nombreuses et variées. Dans certains cas, les individus sont directement concernés. On peut mentionner, par exemple, les badges d'accès, les titres de transport, les documents officiels comme les passeports électroniques ou, plus récemment, l'introduction des systèmes de paiement électronique sans contact et la technologie NFC. Même s'ils ne sont pas toujours conscients du type d'informations traitées dans le cadre de ces applications, ni du niveau de sécurité mis en place, les citoyens peuvent tout de même évaluer les risques et les avantages de ces solutions. Pour d'autres applications, les individus ne sont pas concernés par ces technologies.

Certaines applications, principalement basées sur la technologie UHF, ciblent les besoins en logistique depuis le lieu de fabrication jusqu'au point de vente. Bien que ces applications n'apportent quasiment aucune valeur ajoutée aux consommateurs, force est de constater que les individus ne peuvent pas vivre sans être en contact direct avec ces étiquettes. La méfiance du grand public envers la technologie RFID et ses enjeux en matière de vie privée sont liés à deux problèmes : le manque de sensibilisation du public à cette technologie et l'impossibilité de désactiver simplement les dispositifs RFID.

C'est la raison pour laquelle, en réponse à la mise en place croissante de système RFID en Europe, la Commission Européenne a publié en 2007 le document COM/2007/0096[1] «L'identification par radiofréquence (RFID) en Europe : vers un cadre politique».

Ce document proposait les étapes nécessaires à mettre en place pour promouvoir l'adoption de la technologie RFID tout en respectant le cadre légal

1 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:FR:HTML

afin de protéger les valeurs fondamentales que sont la santé, l'environnement, la protection des données, la vie privée et la sécurité.

Deux ans plus tard, en mai 2009, la Commission Européenne a publié une recommandation «sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence»[2].

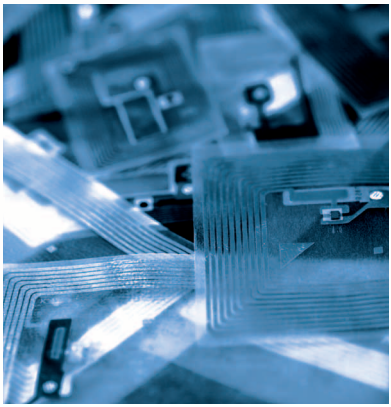
Cette recommandation identifie plusieurs objectifs en matière de vie privée et de données à caractère personnel que les 27 États membres sont encouragés à respecter. Dans ce document, il est suggéré d'informer les consommateurs de la présence d'étiquettes RFID dans les produits (sur les produits ou directement intégrés dans les produits) et que ces étiquettes peuvent être retirées ou désactivées directement sur le point de vente.

L'étiquette peut être laissée active seulement à la demande expresse de l'acheteur. Néanmoins, la désactivation des étiquettes pourrait ne pas être systématique si les commerçants évaluaient les risques en matière de respect de la vie privée et de protection des données.

Selon l'article 4 de la recommandation, les entreprises, en collaboration avec les acteurs concernés de la société civile, doivent élaborer un cadre d'évaluation de l'impact sur la protection des données à caractère personnel et de la vie privée.

Après de longues et difficiles discussions, le document «Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données»[3] a été publié, après l'obtention de l'aval du groupe de travail «Article 29» en février 2011.

En décembre 2008, la Commission européenne a adressé un mandat M/436[4] au CEN, au CENELEC et à l'ETSI dans le domaine des TIC appliquées aux systèmes RFID.



Le mandat M/436 a été validé par les organismes de normalisation européens début 2009.

2 - http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
3 - http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
4 - http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/m436EN2.pdf

Le mandat traite de la protection des données, de la vie privée et des informations dans le cadre de la technologie RFID et sa mise en place se décline en deux étapes distinctes.

L'étape 1.

Qui s'est terminée en mai 2011, a permis d'identifier le travail nécessaire pour établir un cadre complet des futures normes en matière de RFID. Les résultats de l'étape 1 sont repris dans le rapport technique TR 187 020 publié en mai 2011.[5]

L'étape 2.

Concerne la mise en place du programme de travail de normalisation identifié lors de la première étape. Cette deuxième étape se terminera fin 2014 avec la publication de plusieurs rapports techniques et de deux normes européennes : «Processus d'évaluation de l'impact des applications RFID sur la vie privée» et «Notification de la RFID : signalisation et informations supplémentaires devant être fournies par les opérateurs d'applications de capture de données via RFID».

La norme européenne sur l'évaluation de l'impact privé sera basée sur le Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données. Cette norme permettra de définir des procédures normatives ou informatives de manière à promouvoir une méthodologie européenne commune.

Elle proposera un ensemble de procédures normalisées en vue du développement de modèles d'évaluation de l'impact privé, notamment des outils compatibles avec la méthodologie d'évaluation de l'impact de la RFID sur la vie privée.

En outre, elle permettra d'identifier les conditions nécessitant la révision, la modification ou le remplacement d'une évaluation de l'impact sur la vie privée existante par une nouvelle méthode d'évaluation.

5 - http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

02. CONSIDÉRATIONS PRÉALABLES

A. VIE PRIVÉE

La première question à laquelle il faut répondre avant d'aller plus loin dans la réflexion est la suivante : «Qu'est que la vie privée ?».
Le concept de «vie privée» est toujours difficile à définir de manière claire.
Selon la culture et les personnes concernées, l'accent peut être mis sur la réputation ou sur les droits de l'homme. Reconnue par la majorité des experts en la matière, la définition suivante de «vie privée» d'Alan F. Westin[6] est communément utilisée : «le droit des individus (…) de pouvoir décider librement quand, comment et dans quelle mesure des informations les concernant sont communiquées à des tiers» et un moyen «d'atteindre des objectifs individuels dans le cadre d'un épanouissement personnel».

L'une des raisons pour laquelle le concept de vie privée pose un problème est que les différents aspects de ce concept touchent plusieurs domaines comme la protection des données (collecte, exactitude, protection et utilisation des données collectées par une organisation) et la sécurité des données (protection des données collectées).
La vie privée peut généralement être divisée en 5 catégories. Ces formes de vie privée sont définies dans l'Article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales.[7]

Vie privée physique.
Cette forme de vie privée garantit l'intégrité du corps de chaque individu. Elle concerne particulièrement les fouilles corporelles, les vaccins obligatoires, les transfusions sanguines sans consentement, l'obligation de fournir des échantillons de fluides corporels et de tissus biologiques, les exigences en matière de mesures biométriques et les stérilisations obligatoires.

Vie privée comportementale.
Cette forme de vie privée concerne l'observation des actions des individus et inclut les questions de vidéosurveillance, également appelée «vie privée médiatique». Elle affecte tous les aspects du comportement, y compris l'intimité de l'individu, le comportement sexuel, les activités politiques ou syndicales et les pratiques religieuse en lieu public ou en privé.

Vie privée des communications personnelles.
Pour les individus, il est important d'être libre de pouvoir utiliser tous les outils de communications à leur disposition sans prendre de risque d'être surveillé par une autre personne physique ou morale. Cette forme de vie privée est également connue sous le nom de «vie privée d'interception».

Vie privée des informations personnelles.
Cette forme de vie privée est également connue sous le nom de «données à caractère personnel». Chaque individu a un droit de regard sur les

6 - Westin, A., 1967, Privacy and Freedom, New York: Atheneum
7 - http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm

informations le concernant. Ces informations ne devraient pas être automatiquement mises à disposition d'autres personnes physiques ou morales et, au cas où ces informations seraient disponibles, l'individu lui-même doit avoir la possibilité d'exercer un droit de contrôle sur ces informations et l'utilisation qui en est faite.

Vie privée spatiale.
Garantit le respect d'un espace personnel.

B. DONNÉES À CARACTÈRE PERSONNEL

Les Directives 95/46/CE[8] et 2002/58/CE[9] (directives sur la protection des données personnelles) sont applicables uniquement en cas de traitement de données à caractère personnel.

Les données à caractère personnel sont définies comme suit : toute information concernant une personne physique identifiée ou identifiable («personne concernée») ; une personne identifiable est une personne pouvant être identifiée, directement ou indirectement, notamment par le biais d'un numéro d'identification ou d'un ou plusieurs traits physiques, physiologiques, psychologiques, financiers, culturels ou sociaux. Le traitement de données à caractère personnel peut être défini comme suit : toute opération ou série d'opérations effectuées sur une ou plusieurs données à caractère personnel, qu'il s'agisse d'une opération automatisée ou non, comme la lecture, la collecte, l'enregistrement, le classement, le tri, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation, la divulgation par communication, la publication ou tout autre méthode de diffusion, l'alignement ou l'association, la suppression ou la destruction.

Au sein d'une organisation, la personne responsable du traitement des données à caractère personnel doit le faire dans le respect des directives relatives à la protection des données à caractère personnel. Il est clair que la technologie RFID, comme tout autre processus d'identification automatique et de collecte de données, doit respecter ces directives si des données à caractère personnel sont traitées. Ces directives concernent donc les étiquettes, l'interface radio hertzienne, les interrogateurs et les connexions au système back-end.

L'Article 17 de la Directive 95/46/CE et l'Article 4 de la Directive 2002/58/CE imposent à la personne chargée du traitement de données à caractère personnel de mettre en place des mesures techniques et structurelles adaptées pour protéger ces données en cas de destruction accidentelle ou illégale, de perte accidentelle, de modification, de diffusion ou mise à disposition

8 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
9 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

non autorisée (particulièrement lorsque le traitement de ces données implique un transfert via un réseau informatique) et de traitement illégal sous toute forme que ce soit. Les mesures doivent garantir un niveau de sécurité adapté aux risques encourus dans le cadre du traitement et à la nature des données à caractère personnel à protéger.

En s'intéressant aux données à caractère personnel, il est évident que certains aspects de la protection de la vie privée et de la protection des informations se chevauchent tout en restant deux domaines distincts. C'est pour cette raison que le concept d'évaluation de l'impact sur la vie privée est de plus en plus utilisé. Voici la définition ISO de la différence entre une évaluation de l'impact sur la vie privée et un audit de respect de la vie privée[10] :

Un audit de respect de la vie privée se démarque d'une évaluation de l'impact sur la vie privée dans le sens qu'un audit permet de déterminer le niveau de conformité légale d'une institution en matière de respect de la vie privée et d'identifier les étapes à mettre en place pour éviter des non-conformités futures. Bien qu'il existe des similitudes entre une évaluation de l'impact sur la vie privée et un audit de respect de la vie privée, notamment en matière des compétences et des outils utilisés pour éviter les violations de vie privée, l'objectif premier d'un audit est simplement de vérifier que les exigences légales sont respectées, alors qu'une évaluation de l'impact sur la vie privée a pour but d'effectuer une évaluation plus poussée afin d'identifier des moyens de protection de la vie privée plus efficaces.

L'évaluation de l'impact sur la vie privée n'est donc pas un audit de respect de la vie privée ni, de ce fait, un audit de sécurité.

C. OPÉRATEUR RFID

Avant d'approfondir la question de l'évaluation de l'impact sur la vie privée, il faut tout d'abord définir ce qu'est un opérateur RFID. En effet, l'opérateur RFID est la seule personne chargée de réaliser l'évaluation de l'impact sur la vie privée sur l'application RFID qu'il prévoit d'installer. La définition est donnée dans la Recommandation.[11]

«Opérateur d'application RFID» ou «opérateur» signifie la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou en collaboration avec d'autres tiers, détermine le but et les moyens de fonctionnement d'une application, y compris les contrôleurs des données à caractère personnel collectées via une application RFID.

Cette définition indique que toute organisation effectuant une lecture (décodage) ou une écriture (encodage) sur une étiquette RFID est concernée par cette Recommandation et doit donc réaliser une évaluation de l'impact sur la vie privé. Reste à savoir comment réaliser cette évaluation de l'impact sur la vie privée et quel est le niveau d'analyse requis pour chaque application RFID.

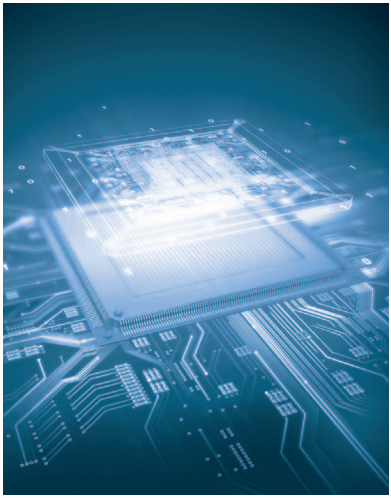
10 - ISO 22307:2008, Financial services -- Privacy impact assessment
11 - http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

03. LE PROCESSUS D'ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE

A. QUAND EFFECTUER UNE ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE ?

Dès qu'un opérateur prévoit d'installer une application RFID, il doit se poser la question de l'évaluation de l'impact sur la vie privée. Le processus d'évaluation de l'impact sur la vie privée d'une application RFID ne doit pas se limiter au contexte interne, c'est-à-dire aux communications planifiées entre l'étiquette RFID et l'application au sein de l'organisation. Il doit également prendre en compte le contexte externe, c'est-à-dire le cas de figure où l'étiquette RFID quitte l'environnement de travail initial tout en restant active. C'est pour cette raison que la Recommandation s'intéresse au secteur de la vente où les étiquettes sont utilisées pour un usage interne type inventaire ou réassort ou pour lutter contre le vol. Si l'étiquette n'a pas été désactivée avant de quitter le point de vente, elle reste opérationnelle.

Bien entendu, l'évaluation de l'impact sur la vie privée ne s'applique pas uniquement lors de l'installation d'une nouvelle application RFID. Il existe d'autres cas de figure où l'évaluation de l'impact sur la vie privée est nécessaire. L'évaluation de l'impact sur la vie privée peut être considérée comme un processus continu qui doit être renouvelé pour chaque nouveau projet ou nouvelle configuration, ce qui constitue une approche plus avantageuse et plus économique.



Compte tenu de l'investissement important requis pour mettre en place une application RFID et des risques en matière d'image inhérents à la mauvaise utilisation de cette technologie, l'évaluation de l'impact sur la vie privée apporte de nombreux avantages. Ces avantages sont d'autant plus importants et faciles à démontrer si des risques en matière de vie privée ont été identifiés et validés avant la mise en place finale de l'application RFID. C'est la raison pour laquelle la Commission européenne et de nombreux experts sur la question de la vie privée soulignent l'importance d'intégrer dès la conception le concept de vie privée.

B. LES NIVEAUX D'ANALYSE DES ÉVALUATIONS DE L'IMPACT SUR LA VIE PRIVÉE

Le Cadre d'évaluation de l'impact sur la vie privée suggère 4 niveaux d'analyse (0 à 3) et énonce explicitement «les entreprises peuvent affiner ces niveaux d'analyse et leurs conséquences sur les évaluations de l'impact sur la vie privée à l'aide de retours d'expérience».

Afin de savoir quel type d'évaluation de l'impact sur la vie privée mettre en œuvre, le Cadre propose un arbre de décision simple basé sur plusieurs questions, comme les suivantes :

«L'application RFID traite-t-elle des données à caractère personnel ? OU L'application RFID reliera-t-elle les données RFID à des données à caractère personnel ?»
«Les étiquettes RFID utilisées par l'application RFID contiennent-elles des données à caractère personnel ?»
«Les étiquettes RFID traitées seront-elles amenées à être portées par des individus ?»

Les réponses à ces questions permettent de définir différents niveaux d'analyse. Malheureusement, ces questions peuvent être interprétées de diverses manières et les différents niveaux d'analyse des évaluations de l'impact sur la vie privée (évaluations à petite ou grande échelle) ne sont pas clairement définis dans le Cadre d'évaluation de l'impact sur la vie privée. C'est pourquoi la future norme européenne proposera les définitions suivantes :

- **Niveau 0** : pas d'évaluation de l'impact sur la vie privée. Si l'étiquette RFID n'est pas portée par un individu ni associée à un individu, le processus d'évaluation de l'impact sur la vie privée peut donc être arrêté ici et l'opérateur doit simplement préparer la déclaration de fonctionnement RFID.

- **Niveau 1** : évaluation de l'impact sur la vie privée à petite échelle. Si l'étiquette RFID est portée par un individu ou associée à un individu de manière permanente ou temporaire, l'évaluation de l'impact sur la vie privée doit être réalisée dans son intégralité. Lorsqu'aucun actif ni aucune donnée associée n'est définie dans la catégorie de données à caractère personnel, la partie restante du processus de l'évaluation des risques est simplifiée.

▪ **Niveau 2** : évaluation de l'impact sur la vie privée de la partie de l'application pilotée par l'opérateur. Ce niveau d'évaluation de l'impact sur la vie privée est requis lorsque l'application traite des données à caractère personnel mais que ces données ne sont pas stockées sur l'étiquette RFID.

L'évaluation des risques d'une évaluation de l'impact sur la vie privée de niveau 2 ne s'applique que pour la partie de l'application qui est pilotée par l'opérateur. L'évaluation ne concerne pas l'interface radio hertzienne entre l'interrogateur et l'étiquette, ni entre l'interrogateur et l'application.

▪ **Niveau 3** : évaluation de l'impact sur la vie privée des parties de l'application pilotées et non pilotées par l'opérateur. Ce niveau d'évaluation de l'impact sur la vie privée est requis lorsque la RFID traite des données à caractère personnel pouvant être identifiables.

L'évaluation des risques d'une évaluation de l'impact sur la vie privée de niveau 3 s'applique à la partie de l'application qui est pilotée par l'opérateur, tout comme pour le niveau 2. Mais le niveau 3 inclut également une évaluation des risques concernant les données des étiquettes RFID dans la partie de l'application non pilotée par l'opérateur.

C. LE PROCESSUS D'ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE

Si l'opérateur doit réaliser une évaluation de l'impact sur la vie privée (niveaux 1, 2 ou 3), conformément aux niveaux définis précédemment, il peut suivre les 9 étapes qui seront contenues dans la prochaine norme européenne :

ÉTAPE 1

Préparer une description détaillée de l'application.

ÉTAPE 2

Identifier et attribuer une valeur de risque aux actifs de vie privée comme suit :

- Les actifs à caractère personnel d'un individu en possession d'une étiquette RFID utilisée par l'application RFID et pouvant être utilisées au-delà du périmètre d'utilisation prévu pour l'application.
- Les actifs de la société pouvant être à l'origine d'une violation ou d'une perte de données à caractère personnel dans le cadre d'un traitement de données RFID.

ÉTAPE 3

Identifier et évaluer les menaces associées aux actifs de vie privée. Ce niveau s'applique aux actifs personnels allant au-delà du périmètre d'utilisation prévu pour l'application afin de s'assurer que la protection de la vie privée est garantie. Ce niveau s'applique également, ou du moins est lié, aux menaces relatives aux données à caractère personnel détenues par l'opérateur RFID ou le contrôleur des données.

ÉTAPE 4

Identifier les vulnérabilités associées aux menaces et aux actifs.

ÉTAPE 5

Réaliser une évaluation des risques des actifs, où le risque est une fonction de l'actif/la menace/la vulnérabilité, tout en sachant que plusieurs risques peuvent être pris en compte.

ÉTAPE 6

Identifier les mesures de contrôle existantes et les nouvelles mesures de contrôle à mettre en place afin de limiter les risques.

ÉTAPE 7

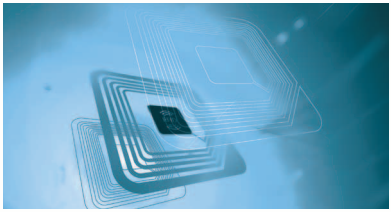
Déterminer les risques résiduels. Si les risques résiduels restent élevés, reprendre l'évaluation à partir de l'étape 2.

ÉTAPE 8

Remplir et signer le rapport d'évaluation de l'impact sur la vie privée.

ÉTAPE 9

Remplir et signer le résumé d'évaluation de l'impact sur la vie privée à rendre public.



Les étapes 2 à 7 font partie du processus d'évaluation des risques. Les opérateurs doivent faire attention à ce qu'ils considèrent comme données à caractère personnel et doivent se référer au paragraphe 2.2 du présent document.

a. Identification et classement des actifs de vie privée

En considérant les différents aspects de la vie privée mentionnées au paragraphe 2.1, il apparaît évident que l'identification des actifs de vie privée n'est pas une tâche simple. Il est beaucoup plus facile de se référer aux données traitées par l'application RFID. Toutes les données traitées par le système back-end ou stockées directement dans la mémoire de l'étiquette RFID doivent être prises en compte. Le type de données identifiées peut alors être associé à un actif de vie privée. Deux catégories d'actifs doivent être identifiées comme appropriées pour l'application, en fonction du type ou de l'implication des données stockées dans l'étiquette RFID ou dans l'application :

- Les actifs directement identifiables, pour lesquels les données encodées comprennent les informations suivantes :
  - Nom d'un individu
  - Identifiant de puce unique
  - Tout identifiant permettant de créer un lien unique avec l'individu

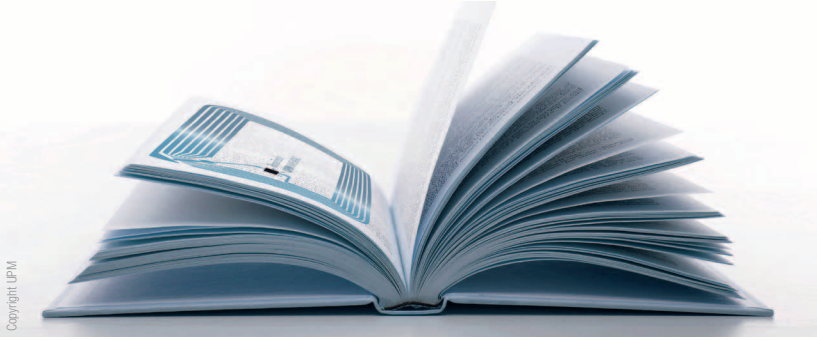
- Les actifs indirectement identifiables et spécifiques à l'identité de l'individu (trait physique, physiologique, psychologique, financier, culturel ou social), comme précisé dans la définition des données à caractère personnel de la Directive 95/46/CE.

Qu'il s'appuie sur un modèle d'évaluation de l'impact privé basé sur un secteur d'activité ou une application, ou bien qu'il parte de zéro,

l'opérateur doit utiliser la description complète de l'application RFID indiquée à l'étape 1 pour identifier les actifs de vie privée concernés. Ensuite, l'opérateur doit classer les actifs et les trier selon leur importance. En fonction de la taille de la société et du niveau de l'évaluation de l'impact sur la vie privée, tous les actifs identifiés, ou tous ceux qui sont pertinents pour l'évaluation, seront à considérer.

Bien entendu, le processus d'identification des menaces pour une application RFID doit considérer les éléments suivants :

- Les aspects technologiques : données encodées sur l'étiquette, protocole d'interface radio hertzienne, interface de l'appareil et couche applicative ;
- Les aspects sécuritaires : confidentialité, intégrité et disponibilité des données



b. Identifier et classer les menaces

Comme pour la vie privée, il existe de nombreuses définitions d'une en fonction de l'intégration ou non de l'agent de menace, de ses motivations et parfois d'une partie de vulnérabilité. La définition proposée dans le présent document provient d'une version adaptée de celle de l'ENISA[12] :

Des mécanismes physiques ou de type matériel informatique et logiciel pouvant potentiellement avoir un impact négatif sur un actif par le biais d'un accès non autorisé, d'une destruction, d'une diffusion, d'une modification de données et/ou d'un déni de service.

Comme pour les actifs de vie privée, toutes les menaces identifiées et concernées par l'évaluation doivent être classées en fonction de leur importance. Voici une liste non exhaustive des menaces RFID les plus connues : reproduction d'étiquette, écoute clandestine, «attaque man in the middle», déni de service, code malveillant, etc. Pour une liste exhaustive, se référer au rapport de phase 1 du Mandat M/436[13] ou à la prochaine norme européenne sur l'évaluation de l'impact sur la vie privée.

Dans le cadre de l'évaluation des menaces, il est important de prendre en compte les motivations de la personne à l'origine de l'attaque et des

12 - http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
13 - http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

compétences requises pour réaliser ces attaques. La probabilité de ces attaques est également un critère important.

c. Identification et classement des vulnérabilités

Comme pour les menaces, il est important de définir ce qu'est une vulnérabilité. Voici, entre autres, une définition proposée par la norme ITSEC[14] (Information Technology Security Evaluation Criteria) :

L'existence d'une faiblesse, d'une erreur de conception ou de mise en œuvre pouvant entraîner un événement inattendu ou indésirable nuisible pour la sécurité du système informatique, du réseau, de l'application ou du protocole concerné.

Un autre moyen d'identifier une vulnérabilité RFID est d'évaluer l'utilisation ou non de fonctionnalités spécifiques (commande «kill», protection lecture/écriture par mot de passe, commande intraçable, utilisation d'algorithmes de chiffrage spécifiques, etc.). L'objectif de l'évaluation de l'impact sur la vie privée sera d'identifier les vulnérabilités et d'évaluer les risques. Ce type de fonctionnalités pourra permettre de limiter les risques de vulnérabilité. Une liste exhaustive des vulnérabilités est disponible dans le rapport de phase 1 du Mandat M/436.

Pour le classement des vulnérabilités, l'opérateur peut faire appel aux règles suivantes :
S'il est impossible de mettre en œuvre une menace, le niveau de risque de vulnérabilité peut être considéré comme «faible». Par exemple, une attaque chiffrée ne peut pas être effectuée sur une étiquette RFID ou sur un protocole d'interface radio hertzienne qui n'est pas compatible avec des fonctionnalités cryptographiques. Si une menace est possible, alors les critères définis à l'étape suivante sont applicables.

Si une menace est identifiée et s'il est possible de l'appliquer à la technologie RFID utilisée par l'application, alors le niveau de risque de vulnérabilité est considéré comme «moyen» pour indiquer que la menace et les vulnérabilités associées ont été identifiées dans les documents de recherche.

Le niveau de vulnérabilité «élevé» ne s'applique que lorsque des failles connues ont été identifiées dans des cas de figure réels.

d. Évaluation des risques

Lorsque les actifs, les menaces et les vulnérabilités ont été identifiés et classés, la dernière étape est l'évaluation des risques. Il

14 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile

existe plusieurs méthodes pour attribuer une valeur à un risque. OCTAVE[15] (Operationally Critical Threat, Asset, and Vulnerability Evaluation) est une méthode développée par l'université de Carnegie Mellon en 2001.
Cette méthode consiste en une gamme d'outils, de techniques et de méthodes permettant d'analyser et de planifier de manière stratégique la sécurité des informations sur la base des risques. Une autre méthode, l'algorithme DREAD, consiste à calculer la valeur du risque à partir de l'équation suivante : Risk_DREAD = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5.

Une autre méthode encore est proposée par le NIST (National Institute of Standards and Technology) dans la publication spéciale 800-30[16]. Toutes ces méthodes et ces algorithmes de calcul ciblent plus ou moins la sécurité informatique et ne sont pas vraiment adaptés à l'évaluation des risques en matière de vie privée.

Dans le présent document et dans la prochaine norme européenne, nous proposons une méthode basée sur la norme ISO/IEC 27005:2011[17].
Dans cette méthode, les actifs peuvent avoir une valeur entre 0 et 5. Pour les menaces et les vulnérabilités, les valeurs peuvent être «faible», «moyen» ou «élevé».
L'équation permettant de calculer la valeur de risque est basée sur l'addition des valeurs d'actif, de menace et de vulnérabilité. Elle est synthétisée dans le tableau ci-dessous. Dans ce tableau, plus le chiffre est élevé, plus le risque est élevé.

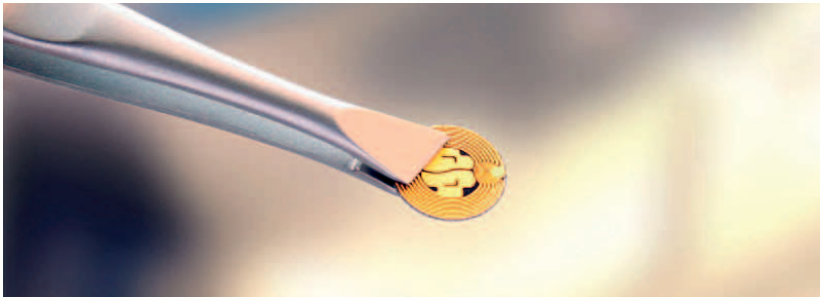
e. Limitation des risques et mesures de contrôle

Chaque opérateur doit définir son propre seuil de valeur de risque au-delà duquel une action doit être entreprise. Si un ou plusieurs risques possèdent une valeur supérieure à ce seuil, l'opérateur doit limiter le risque en mettant en place une contre-mesure. Les contre-mesures peuvent être classées comme suit :

Matrice d'évaluation des risques basée sur la norme ISO 27005

	PROBABILITÉ DE LA MENACE	FAIBLE			MOYEN			ELEVÉE		
	FACILITÉ D'EXPLOITATION DE FAILLE VULNÉRABILITÉ	F	M	E	F	M	E	F	M	E
VALEUR D'ACTIF	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

15 - http://www.cert.org/octave/octavemethod.html
16 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
17 - http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742



- Fonctionnalités encodées dans les étiquettes et dans les appareils associés à un protocole d'interface radio hertzienne spécifique ;
- Fonctionnalités déjà disponibles via la technologie utilisée mais nécessitant une action délibérée de l'opérateur RFID ;
- Fonctionnalités non associées au matériel informatique qui doivent être mises en œuvre par l'opérateur RFID ;
- Actions qui relèvent de l'individu pour protéger sa vie privée.

Une fois qu'une ou plusieurs mesures de contrôle ont été mises en place, l'opérateur doit évaluer à nouveau la valeur de risque et vérifier que cette valeur reste sous le seuil qu'il a défini.

f. Risques résiduels

Tous les acteurs du secteur de la RFID s'accordent à dire que le risque zéro n'existe pas en matière de vie privée. En fonction du seuil défini par l'opérateur, certains risques restent non résolus. Ces risques sont appelés «risques résiduels». Ce concept est défini dans le Guide ISO 73:2009, Management du risque, Vocabulaire[18] : risques résiduels après le traitement des risques.
Bien entendu, plus la valeur des risques résiduels est faible, plus les individus utilisant l'application RFID peuvent être assurés que leur vie privée est protégée. L'opérateur RFID doit calculer le retour sur investissement de la mise en place de mesures de contrôle et de contre-mesures supplémentaires.

g. Rapport et résumé de l'évaluation de l'impact sur la vie privée

Une fois l'évaluation des risques terminée, la prise de décision finale de mise en place de l'application devra être documentée dans le rapport d'évaluation de l'impact sur la vie privée, accompagnée d'éventuelles remarques concernant les risques, les mesures de contrôle et les risques résiduels.

Les signataires du rapport d'évaluation de l'impact sur la vie privée devront disposer des compétences nécessaires pour comprendre le fonctionnement de l'application RFID et/ou l'autorité requise pour exiger une modification du système, le cas échéant.

18 - http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651

Un rapport d'évaluation de l'impact sur la vie privée peut contenir des informations confidentielles concernant la mise en place de la technologie RFID par l'opérateur. L'opérateur devra rédiger un résumé d'évaluation de l'impact sur la vie privée s'il désire communiquer les résultats de l'évaluation aux acteurs concernés externes à la société. Ce résumé devra contenir au moins les éléments suivants : la date du rapport d'évaluation de l'impact sur la vie privée, le nom de l'opérateur RFID, les généralités concernant l'application RFID, les données encodées dans les étiquettes RFID, le score d'évaluation de l'impact sur la vie privée (calculé grâce au Tableau 1), les limitations des risques et les mesures de contrôle.

Comme indiqué précédemment, l'évaluation de l'impact sur la vie privée est un processus continu qui doit être renouvelé à chaque nouvelle étape de projet ou nouvelle configuration. Les critères de renouvellement du processus pourront être, notamment :

- Des modifications importantes de l'application RFID, comme l'extension du champ d'application.

- Des modifications au niveau du traitement de l'information, au niveau de l'étiquette ou de l'application.

- Des signalements de violations de la vie privée identifiées dans des applications RFID similaires.

- La disponibilité d'un nouveau modèle sectoriel, ou d'une mise à jour du modèle utilisé.

- La disponibilité d'une technologie RFID plus avancée. Il est tout de même recommandé de prendre en compte la valeur résiduelle des investissements en cours et la migration vers de nouvelles technologies.

- La réévaluation périodique, au moins une fois par an si possible, de l'évaluation de l'impact sur la vie privée. Si aucun changement important ne s'est produit, il suffit simplement de mettre à jour la date de publication de l'évaluation de l'impact sur la vie privée.

04. CONCLUSION

Le travail réalisé par la Commission européenne et les nombreux autres acteurs de l'industrie et de la recherche en matière de RFID et de vie privée peut être considéré comme une première étape permettant de promouvoir une utilisation intelligente et respectueuse de la vie privée de la technologie RFID. Pour l'instant, la Recommandation relève de ce que l'on appelle le «droit mou». Le Cadre d'évaluation de l'impact sur la vie privée est un premier jet en vue de proposer un processus clairement défini aux opérateurs RFID. Grâce à ce premier Cadre, les opérateurs RFID peuvent évaluer les risques en matière de vie privée inhérents aux applications RFID et ainsi identifier des mesures de contrôle ad hoc et des méthodes de limitation des risques.

On entend souvent dire que la technologie RFID n'est pas la technologie la plus dangereuse en matière de respect de la vie privée. Il n'empêche que les opérateurs RFID ont aujourd'hui une occasion de mettre en place un exemple en matière de respect de la vie privée que d'autres secteurs pourraient suivre. La prochaine norme européenne permettra aux opérateurs RFID d'être encore plus efficaces dans ce domaine en proposant des procédures et des étapes clairement définies. Cette norme pourrait aider à établir un référentiel garantissant une conformité. Une telle conformité au niveau européen renforcera la confiance des citoyens envers la technologie RFID. Pour les organismes comme le Centre National RFID, la création de ce type de norme est la meilleure récompense qu'un opérateur, et par extension, que tout constructeur de solutions RFID, puisse recevoir.

THE FRENCH NATIONAL RFID CENTER

Initiated by the French Ministry of Economy, Industry and Employment to facilitate adoption and use of RFID technology and develop its applications, the French National RFID Center (CNRFID) is a non-profit organization for RFID providers, users, integrators, laboratories.

It supports their specifics needs and interests:

- To clarify the added value for each vertical market
- To facilitate take-up of the RFID technology
- To develop new fields for RFID use
- To boost business opportunities
- To coordinate ideas and projects on a nationwide scale

The CNRFID is a member of several international standardization committees, including CEN, ETSI and ISO. It federates more than 125 RFID key players.

More about the French National RFID Center (CNRFID) : www.centrenational-rfid.com

ENGLISH VERSION

SUMMARY

01. HISTORY OF RFID PRIVACY IMPACT ASSESSMENT (PIA)

Behind the word RFID, we can find several technologies whose characteristics allow considering many diverse applications. In some cases, individuals are directly involved. We can mention the cases of access badges, transport cards, official documents such as e-passports or more recently the introduction of electronic contactless payment cards and NFC.

If citizens are not always aware of the information that this kind of application can process or the level of security implemented, they can nevertheless balance the risks and the benefits of such applications.

For other applications, individuals are currently excluded from the value chain. We can mention applications, mainly based on UHF technology, devoted to logistics from manufacturers to point of sale. Even if there is no or very little added value for the customer, this does not prevent people from getting stuck with or surrounded by some of these tags.

The reason why RFID can cause public distrust and privacy concerns is the combination of two issues: public unawareness and impossibility to switch off RFID devices. That's the reason why, in response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96[1] «RFID in Europe: steps towards a policy framework».

This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values

1 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0096:EN:NOT

such as health, environment, data protection, privacy and security.

Two years later, in May 2009, the European Commission issues a Recommendation 'on the implementation of privacy and data protection principles in applications supported by radio-frequency identification'[2].

This document outlines data privacy objectives recommended for use in the 27 member states.

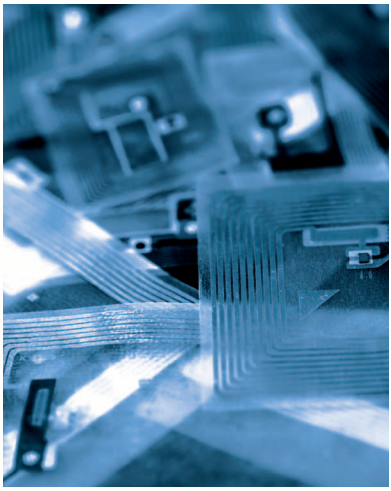
It is proposed that consumers should be informed of the presence of RFID tags placed on or embedded in products, and that tags should be removed or deactivated immediately at the point of sale.

The tag can be kept operational only if purchasers expressly agree (Opt-in). However, deactivation could be not systematic if the retailer assesses the privacy and data protection risks.

According to Article 4 of the Recommendation, industry, in collaboration with relevant civil society stakeholders have to develop a framework for privacy and data protection impact assessments.

After long and sometimes difficult discussions, but finally endorsed by the Article 29 Working Party in February 2011, the «Privacy and Data Protection Impact Assessment Framework for RFID Applications»[3] has been published.

Meanwhile, in December 2008, the European Commission addressed the Mandate M/436[4] to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems.



The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information

2 - http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
3 - http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
4 - http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/m436EN2.pdf

aspects of RFID, and is being executed in two phases.

Phase 1.

Completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020[5], which was published in May 2011.

Phase 2.

Is concerned with the execution of the standardisation work programme identified in the first phase.

This second phase will end in 2014 with the publication of different technical reports and the publication of two European standards: «RFID Privacy Impact Assessment (PIA) process» and «Notification of RFID: The information sign and additional information to be provided by operators of RFID data capture applications».

The European norm on PIA will be based on the Privacy and Data Protection Impact Assessment Framework for RFID Applications. It will define aspects of that framework as normative or informative procedures to enable a common European method for undertaking a RFID PIA.

It will provide a standardised set of procedures for developing PIA templates, including tools compatible with the RFID PIA methodology. In addition, it will identify the conditions that require an existing PIA to be revised, amended, or replaced by a new assessment process.

5 - http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

02. PRELIMINARY CONSIDERATIONS

A. PRIVACY

The first key question we have to answer before going deeper in the process is: «What is privacy?» Privacy, as a concept, is always difficult to define with clear boundaries. Depending on the culture and individuals, emphasis can be put on reputation or human rights.

Generally accepted by most privacy experts, Alan F. Westin's definition of privacy is commonly used[6]: "the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others" and as a mean "(...) for achieving individual goals of self realization".

One of the reasons why privacy creates conceptual problems is that different aspects of privacy are belonging to different sectors like data protection (collection, accuracy, protection and use of data collected by an organisation) and data security (protection of collected data).

Privacy can generally be discerned into five categories. These types of privacy are covered by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[7].

Physical privacy.

This is to ensure the integrity of the body of the individual. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissues, requirements for submission to biometric measurement and compulsory sterilization.

Privacy of personal behavior.

This relates to the observation of what individuals do, and includes such issues as optical surveillance also called as «media privacy». This affects all aspects of behavior, including intimacy, sexual behavior, political or trade union activities and religious practices both in private and in public spaces.

The privacy of personal communications.

For individuals, it is important that they can use a variety of media to communicate without their communications being watched by other persons or organisations. This form of privacy is also known as «interception privacy».

The privacy of personal information.

Is referred to variously as «data privacy» and «information privacy». Individuals claim that data about themselves, not necessarily should be automatically available for other individuals and organisations, and that, even though others obtain such data, the individual himself must be capable to exercise a considerable degree of

6 - Westin, A., 1967, Privacy and Freedom, New York: Atheneum
7 - http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm

control over these data and the use of these data.

The spatial privacy.
As a shield of its own territory.

B. PERSONAL DATA

The Directives 95/46/EC[8] and 2002/58/EC[9] (privacy directives) are applicable only when the processing of personal data is taking place.

Personal data are defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Processing personal data can then be defined as any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as reading, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

Within an organisation, the controller is responsible that the processing of personal data is performed in compliance with the privacy directives.
Of course, RFID, like any other mean of automatic identification and data capture technique, if processing personal data, has to be compliant with the law.

This include the tags, the air interface, the interrogators and the connection to the backend system.

Article 17 of 95/46/EC and Article 4 of 2002/58/EC obliges the controller to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

8 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
9 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

When focusing on personal data, it is clear that privacy protection and information security overlap each other but are not similar.

That is one of the reasons why the concept of privacy impact assessment (PIA) is more and more widely used. Following the ISO definition of the difference between a PIA and a privacy compliance audit[10]:

A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution's current level of compliance with the law and identifies steps to avoid future non-compliance with the law. While there are similarities between privacy impact assessments and privacy compliance audits in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is simply to meet the requirements of the law, whereas a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.

It is clear that a Privacy Impact Assessment is not a regulatory compliance audit and, by extension, it is neither a security audit.

C. RFID OPERATOR

Before entering much deeper in the PIA process, we need to define clearly the concept of RFID operator because he is the only one responsible in undertaking a PIA for the RFID application he intends to set up. The definition is given in the Recommendation[11]:

'RFID application operator' or 'operator' means the natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using a RFID application.

This means that any organisation that carries out a reading (decoding) process on a RFID tag or that carries out a writing (encoding) process on a RFID tag is concerned by the Recommendation and by undertaking a PIA.
The question is to know how to undertake a PIA and what is the level of detail requested for a given application.

10 - ISO 22307:2008, Financial services -- Privacy impact assessment
11 - http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

03. THE PIA PROCESS

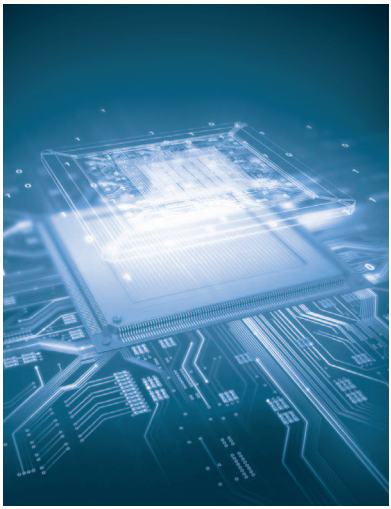
A. WHEN UNDERTAKING A PIA?

As soon as a RFID operator intends to set up a RFID application, he has to ask the question of undertaking a PIA.
The RFID PIA process shall not only deal with the internal context, in terms of all the planned communication between the RFID tag and the business application.
The PIA process has to take into consideration the external context, in terms of the RFID tag leaving the organisation's application environment and still being functional.
That's why the Recommendation focused on the retail sector where a tag used for internal purpose like inventory, re-assort or anti-theft can go through the point of sale and continue to be functional if not deactivated.

Of course, undertaking a PIA for a brand new RFID application is not the only case. There are other different situations when a RFID PIA has to be considered.

A beneficial and cost-effective approach may be to consider the RFID PIA as a continual process which has to be re-visited at each new project phase or new situation.

Given the significant investment that any organisation makes in a RFID application, and the reputation risks of inherent features in the technology not being addressed, there are numerous business advantages in undertaking the RFID Privacy Impact Assessment.



These advantages are even greater and easy to demonstrate if privacy concerns have been identified and mitigated before the complete implementation of the RFID application.

That's why the European Commission and a lot of privacy experts consultants emphasize the principle of privacy by design.

B. DIFFERENT PIA LEVELS OF DETAIL

The PIA Framework suggested four levels of PIA

(0 to 4) and explicitly stated «Industry may further refine these levels and how they impact the PIA process with further experience.»

To know what kind of PIA has to be undertaken, the PIA Framework proposed a simple decision tree based on simple questions like:

«Does the RFID application process personal data? OR Will the RFID Application link RFID data to personal data?»

«Do the RFID tags used in the RFID Application contain personal data?»

«Is it likely that the RFID tags you process are carried by an individual?»

Answering these questions leads to different PIA scales. Unfortunately, these questions can be differently interpreted and furthermore, the different PIA scales (small or full scale PIA) are not well defined in the PIA Framework.
That's why, the future European standard will propose the following definitions:

- **Level 0:**

No PIA: If a RFID tag is not carried by, or is associated with, an individual then the PIA process may stop before entering the PIA process itself and the operator has only to prepare the RFID functional statement.

- **Level 1:**

Small scale PIA: If a RFID tag is carried by, or is associated with, an individual on a permanent or temporary basis, then all the PIA process has to be done.
Where no asset or associated data type is defined in the category of personal privacy, the remaining risk analysis process is simplified.

- **Level 2:**

PIA of the controlled domain of the application: This level of PIA is required when the application processes personal data, but such personal privacy data is not held on the RFID tag.
The risk assessment process for a level 2 PIA is

only applied to the part of the application which is controlled by the operator.
This does include the communications interfaces between the interrogator and tag, and interrogator and application.

- **Level 3:**

PIA of the controlled and uncontrolled domain of the application:
This level of PIA is required when the RFID holds personally identifiable data. The risk assessment process for a level 3 PIA is applied to the controlled part of the application as for level 2.

In addition, a risk assessment is required for the data on the RFID tag in the uncontrolled part of the application.

C. THE PIA PROCESS

If, following the proposed defined levels of PIA, the operator has to undertake a PIA (levels 1, 2 and 3), he can follow the 9 steps defined in forthcoming European standard:

STEP 1

Prepare a detailed description of the application.

STEP 2

Identify and assign a risk value to the privacy assets as follows:

- The personal privacy assets of an individual in possession of a RFID tag used by the RFID application, and also in the individual's possession beyond the bounds of the application.

- The organisation's assets that might be implicated with a privacy breach or loss of personal data associated with RFID data processing.

STEP 3

Identify and assess the threats to the privacy assets. This applies to individual assets beyond the domain on the application, i.e. ensuring the privacy protection is addressed.
It also applies, and is linked to, threats to sets of personal data held by the RFID operator / data controller.

STEP 4

Identify the vulnerabilities associated with the threats and assets.

STEP 5

Carry out a risk assessment of the assets, where risk is a function of (asset, threat, vulnerability), taking account that there can be a number of risks.

STEP 6

Identify existing and new controls that can be applied to mitigate risks.

STEP 7

Determine the residual risks. If assessed too high re-start form step 2.

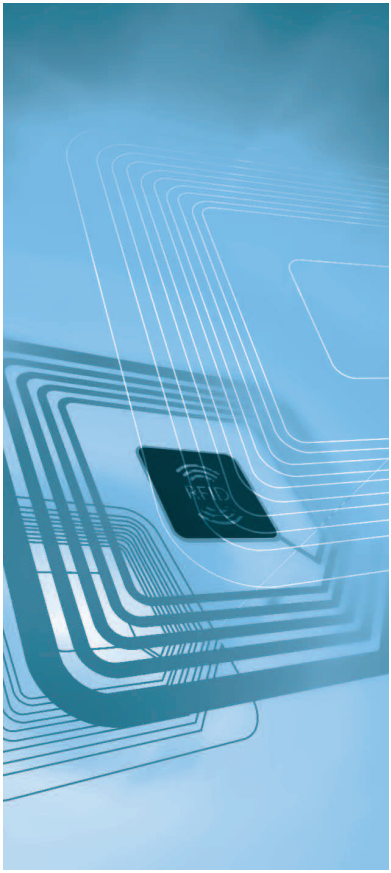
STEP 8

Complete and sign-off the RFID PIA report.

STEP 9

Complete and sign-off the RFID PIA summary report to be made available in the public domain.

Steps 2 to 7 are considered as the risk assessment process. Operators have to be careful of what they consider to be personal data and have to refer to clause 2.2 of this document.



a. Identifying and ranking privacy assets

Referring to different aspects of privacy defined in 2.1, identifying privacy assets is not an easy task. It much more easier to refer to the data processed by the RFID application.

All the data either processed in the back-end system or stored directly into the memory of the RFID tag have to be considered. The type of data can then be linked to a particular privacy asset.

Two categories of assets have to be identified as appropriate for the application, based on the type or implication of the data on the RFID tag or stored on the application:

- Directly identifiable assets, where encoded data includes:

- An individual's name
- A unique chip ID
- Any identifier that has a one-to-one relationship with the individual

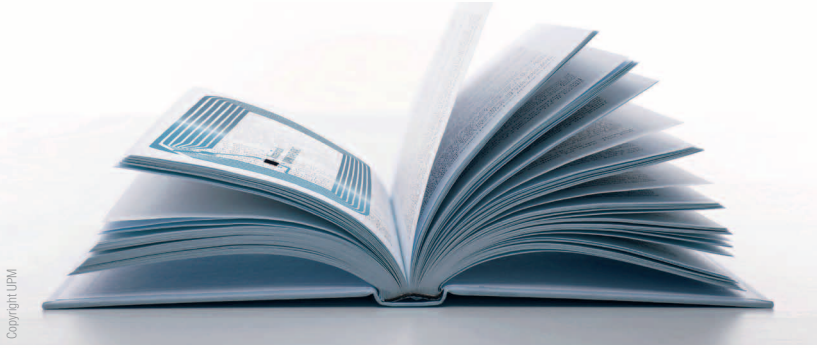
- Indirectly identifiable factors specific to the individual's physical, physiological, mental, economic, cultural or social identity, as included in Directive 95/46/EC for the definition of personal data.

Using a sector-based or application based PIA template or starting from scratch, the operator has to use the full description of the RFID application prepared in step 1 to identify all the relevant privacy assets.

The next work is to classify assets and sort them by order of importance. Depending on the PIA level and organisation's size, most relevant or all identified assets will have to be considered.

- Security aspects like confidentiality, integrity and availability.

Like for privacy assets, all identified relevant



b. Identifying and ranking threats

As for privacy, we can find a lot of definition of a threat depending on whether we integrate or not the agent, his motivation and sometimes a piece of vulnerability.
The one we propose in this document is derived and adapted from ENISA[12]:

Physical, hardware, or software mechanism with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and / or denial of service

Of course, the identification of threats for a RFID application has to consider:

- Technological aspects like the data encoded in a tag, the air interface protocol, the device interface and the application layer.

threats have to be sorted by importance. Among others, we can cite the most known RFID threats: tag cloning, eavesdropping, man in the middle, denial of service, malicious code, etc.

For a more complete list of threats, the reader may refer to the M436 phase 1 report[13] or to the forthcoming European standard on PIA.

In the evaluation of threats, it is important to take into account the motivation and the required skills of the attacker. The probability of such an attack is another important criterion.

c. Identifying and ranking vulnerabilities

Like for threats, it is important to have a definition of vulnerabilities. Among others, the one proposed by Information Technology Security

12 - http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
13 - http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf

Evaluation Criteria[14] (ITSEC) is:

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Another way to identify RFID vulnerabilities is to evaluate the use or not of special features like kill command, read/write password protection, untraceable command, use of particular cryptographic algorithms, etc.

The goal of the PIA process will be to identify the vulnerabilities and to assess the risk. One way of mitigating the risk will be to use these kind of features. A more complete list of vulnerabilities can be found in the M436 phase 1 report.

For scoring the vulnerabilities, the operator can use the following rules:
If it is impossible to implement a threat, then the vulnerability risk level shall be defined as 'low'. For example, a crypto attack cannot be implemented on an RFID tag and air interface protocol that does not support cryptographic features.

If the threat is possible, then the criteria set out in the next step apply.

If a threat is identified and if it is feasible to apply this to the RFID technology used in the application, then its vulnerability risk level shall be 'medium' to indicate that the threat and implied vulnerabilities have been identified in research documents.

The vulnerability level of 'high' shall only be applied when known exploits have been identified in real applications.

d. Risk evaluation

Once the assets, the threats and the vulnerabilities have been identified and ranked, the last step is the risk assessment.

Different methods can be used to assign a value to a given risk. We can cite here the OCTAVE[15] method developed by Carnegie Mellon University in 2001. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.

Another method is the DREAD algorithm where the value of the risk is derived from the equation:

14 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile
15 - http://www.cert.org/octave/octavemethod.html

Risk_DREAD = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5. Another method is proposed by NIST in the special publication 800-30[16].

All these methods and scoring algorithms are more or less devoted to computer security and are not well suited to privacy risk assessment. In this paper, and in the future European standard, we propose a method based on the ISO/IEC 27005:2011[17] standard.

In this method, assets can have a value between 0 and 5. For threats and vulnerabilities, values are whether low, medium or high.

The equation that gives the risk value is based on the addition of asset, threat and vulnerability values and can be summarised in the table below.

Of course, the higher the number, the more serious the risk.

e. Mitigation and controls

Each operator has to define his own threshold for risk value that imply an action to be done.

If one or more risks have a value above this threshold, the operator has to mitigate the risk by implementing a countermeasure. Countermeasures can be classified as follow:

- Features embedded in the tags and devices associated with a particular air interface protocol.

- Features available in the technology but require a conscious action by the RFID operator.

- Features independent of the hardware and can be implemented by the RFID operator.

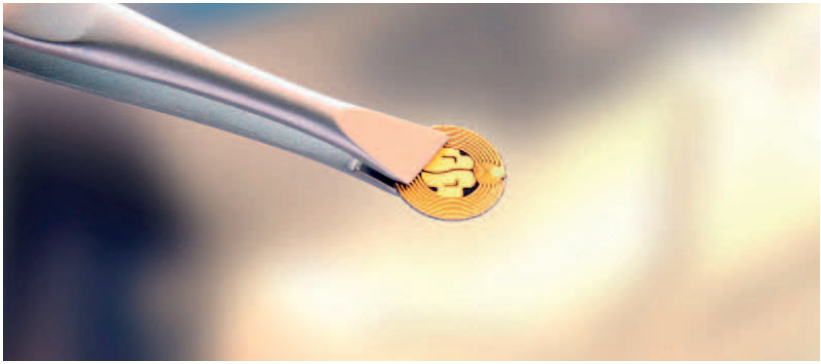
- Action that the individual has to do to protect his or her privacy.

Once one or more controls have been

Matrix approach to determine a risk value based on ISO 27005

	LIKELIHOOD OF THREAT	LOW			MEDIUM			HIGH		
	EASE OF EXPLOITATION VULNERABILITY	L	M	H	L	M	H	L	M	H
ASSET VALUE	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

16 - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
17 - http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742



implemented, the operator has to re-assess the risk value and verify that this time, the value is below the threshold he decided to set.

f. Residual risks

It is generally agreed upon RFID stakeholders that a zero privacy risk RFID application is something that cannot be achieved.

Depending on the threshold defined by the operator, there still are risks that have not been mitigated. These are called residual risks. This concept is defined in ISO Guide 73:2009, Risk management – Vocabulary[18]: Risk remaining after risk treatment.

Of course, the lower the value of residual risks, the higher the confidence of individuals in the RFID application.

The RFID operator has to calculate the ROI of the implementation of even more controls and countermeasures.

g. The PIA report and summary

Once the risk assessment has been completed, the final resolution about the application should be documented in the PIA Report, along with any further remarks concerning risks, controls and residual risks.

Those signing off should have the necessary skills to understand the RFID application and/or have the authority to require a system change should this be necessary.

Such PIA report may contain confidential information on how RFID is implemented by a given operator.

In order to communicate with involved stakeholders out of the organisation, the operator has to draft a PIA summary report. This summary shall at least include: the PIA report date, the name of the RFID operator, the RFID application overview, the data embedded in the

18 - http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651

RFID tags, the RFID privacy impact assessment score (derived from Table 1), RFID controls and mitigations.

As it has been said earlier, PIA is a continual process which has to be re-visited at each new project phase or new situation. The criteria for a review may include:

- Significant changes in the RFID application such as expanding on the original purpose.

- Changes in the type of information process either as held on the tag or on the application.

- Reports of privacy breaches in similar RFID applications.

- The availability of a new or enhanced sector template.

- The availability of improved RFID technology. However, it is acknowledged that the residual value of existing investments and the migration to the new technology need to be taken into consideration.

- Periodically; ideally no more than one year should elapse, the existing PIA should be re-assessed. If no material changes have occurred, then all that is required is to indicate this fact with an updated date.

04. CONCLUSION

The work done by the European Commission and numerous industrial and academic stakeholders on privacy related to RFID application can be seen as a first step to promote smart and privacy friendly use of RFID.

For the moment, the Recommendation is what we can call a soft law.

The PIA Framework is a first attempt to propose a defined process to RFID operators.

It allows RFID operators to assess how the application can harm individual's privacy and help them in indentifying ad hoc controls and mitigation methods.

We can often ear that RFID is not the most dangerous technology for privacy. Never mind, the RFID operators have now the opportunity to set up an example and induce other sectors.

The forthcoming European standard will surely help RFID operator even more by a well defined set of procedures and steps.

Such a standard can help to implement a repository for ensuring compliance. Such compliance, across Europe, will lead to greater confidence from the citizens towards RFID.

This, seen by an organisation like French RFID National Centre, is the best reward that an operator and by consequence all RFID manufacturers, can obtain.

Rédaction :
Claude Tételin
Directeur Technique de CNRFID / CTO at CNRFID

EN SAVOIR PLUS SUR LES PUBLICATIONS ET LES ACTIONS DU CNRFID :
MORE ABOUT CNRFID'S PUBLICATIONS AND SERVICES:

www.centrenational-rfid.com

Centre National de Référence RFID
5 avenue de Manéou - 13790 Rousset - France
Tél : +33 (0)4 42 37 09 37
Fax : +33 (0)4 42 26 40 10
contact@centrenational-rfid.com