ARTICLE 29 Groupe de travail protection des données

10107/05/FR
WP 105

Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)

19 janvier 2005

Le présent groupe de travail a été créé en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses tâches sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction E (Services, droits d'auteur, propriété industrielle et protection des données) de la Commission européenne, direction générale Marché intérieur, B-1049 Bruxelles, Belgique, Bureau N° C100-6/136.

Site web: www.europa.eu.int/comm/privacy

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3 de ladite directive,

vu son règlement intérieur, notamment les articles 12 et 14,

A ADOPTÉ LE PRÉSENT document de travail:

1. Introduction

L'utilisation de la radio-identification, ou identification radio fréquence (communément appelée RFID, de l'anglais Radio Frequency Identification) pour des finalités et des applications différentes peut profiter aux entreprises, aux particuliers et aux services publics (gouvernements inclus). Comme cela est illustré plus loin dans le présent document, la RFID peut aider les détaillants à gérer leurs stocks, renforcer l'expérience des consommateurs en matière d'achats, et améliorer la sécurité des médicaments, tout en permettant de mieux contrôler l'accès des personnes dans des zones réglementées.

Tandis que les avantages liés à l'utilisation de la technologie RFID paraissent évidents, le vaste déploiement de cette technologie n'est pas sans comporter des inconvénients potentiels. Sur le front de la protection des données, le groupe de travail de l'article 29 se préoccupe de la possibilité pour certaines applications de la technologie RFID de porter atteinte à la dignité humaine et aux droits en matière de protection des données. En particulier, d'aucuns redoutent que des entreprises et des gouvernements puissent utiliser la technologie RFID pour fouiller dans la vie privée des personnes. La possibilité de collecter subrepticement diverses données toutes liées à la même personne ; de suivre à la trace des personnes se déplaçant dans des lieux publics (aéroports, gares ferroviaires, magasins) ; d'étoffer des profils en surveillant le comportement des consommateurs dans les magasins, de lire les données détaillées des vêtements et des accessoires que portent les clients et des médicaments qu'ils transportent sont autant d'exemples d'utilisation de la technologie RFID qui suscitent des inquiétudes en matière de protection de la vie privée. Le problème est aggravé par le fait que, en raison de son coût relativement faible, cette technologie sera à la portée non seulement d'acteurs de premier plan mais aussi d'éléments de moindre rang et de simples citoyens.

La conscience de ce nouveau risque a poussé le groupe de travail de l'article 29 à étudier les implications de la technologie RFID dans le domaine de la protection de la vie

[1] Journal officiel L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

privée et d'autres droits fondamentaux. À cette fin, notamment, le groupe de travail de l'article 29 a consulté les parties intéressées, notamment les fabricants et les utilisateurs de cette technologie ainsi que les défenseurs du droit de la vie privée. Le résultat de l'analyse réalisée ensuite par le groupe de travail de l'article 29 est le présent document de travail qui a les deux grands objectifs suivants : premièrement, fournir à ceux qui exploitent la technologie RFID des orientations concernant l'application des principes fondamentaux définis dans les directives communautaires, en particulier la directive Protection des données[2] et la directive Vie privée et communications électroniques[3] et deuxièmement, fournir des orientations aux fabricants de cette technologie (tags, lecteurs et applications RFID) ainsi qu'aux organes de normalisation de RFID concernant leur responsabilité en matière de conception d'une technologie respectueuse de la vie privée afin de permettre à ceux qui exploitent la technologie de s'acquitter de leurs obligations au titre de la directive Protection des données.

Tenant compte du niveau d'expérience relativement faible de l'utilisation de technologie RFID, le groupe de travail de l'article 29 considère le présent document comme une première évaluation de la situation. Le groupe de travail continuera à examiner cette situation et, au fil de l'expérience, fournira d'autres orientations. Cela sera plus particulièrement nécessaire si la technologie RFID devient, comme prévu, l'une des « pièces » maîtresse du futur environnement de l'intelligence ambiante. En somme, il s'agit d'un document de départ, et le groupe de travail de l'article 29 continuera à travailler sur cette question.

2. La technologie de radio-identification: aperçu de la technologie et de ses utilisations[4]

1. Les éléments fondamentaux de la technologie de radio-identification

Les principaux éléments de la technologie ou de l'infrastructure de radio-identification sont un *tag* (à savoir une puce) et un *lecteur*. Le tag (étiquette, marqueur ou transpondeur) comprend un circuit électronique qui stocke des données et une antenne qui communique les données au moyen d'ondes radio. Le lecteur possède une antenne et un démodulateur qui traduit l'information analogique par liaison radioélectrique en données numériques. L'information numérique peut alors être traitée par un ordinateur.

Comme cela est illustré dans la prochaine section, la technologie RFID peut fonctionner de différentes façons en fonction des types de tags et de lecteurs. Ceux qui exploiteront la technologie devront choisir entre les différentes possibilités techniques suivant leurs besoins. Ces opérateurs devront décider s'ils utilisent des tags actifs ou passifs. Les tags « passifs » ne possèdent pas de source d'énergie (pile) et peuvent donc

---

[2] Directive 95/46/CE du 24 octobre 1995 relative à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[3] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[4] Une plus ample description de la technologie RFID et les utilisations auxquelles elle convient figurent en annexe à la fin du présent document.

être réveillés plusieurs dizaines d'années après avoir été fabriqués. Le tag est alimenté en courant par le signal radioélectrique. Un lecteur RFID émet des signaux radioélectriques qui réveillent le tag à une certaine distance, déclenchant une réaction consistant à transmettre l'information stockée sur le tag. Les tags « actifs » possèdent leur propre pile, ce qui réduit leur cycle de vie. Ils peuvent soit diffuser leur information sans être interrogés par le lecteur, soit rester en sommeil jusqu'à ce qu'ils soient déclenchés par un lecteur.

2 Des utilisations multiples dans de nombreux secteurs - exemples

L'utilisation de la technologie RFID est en train de décoller dans divers *secteurs* (par exemple les soins de santé, l'aviation, les transports). En outre, les *fonctions* spécifiques que peuvent assurer les tags RFID dans les différents secteurs sont elles aussi en augmentation et leurs possibilités commencent tout juste à se dégager. La présente section vise à illustrer les principales fonctions que peut assurer la technologie RFID dans différents secteurs ou applications, à savoir les transports et les soins de santé. Tandis que certaines des applications RFID décrites ci-après en sont encore aux premiers essais, d'autres sont une réalité, parfois à l'insu des personnes concernées.

Transports/Distribution. Les systèmes RFID sont bien adaptés à certaines applications de transports. Avec une répartition appropriée des lecteurs RFID, les véhicules équipés d'un tag peuvent être suivis sur leur trajet jusqu'à destination. De nombreux billets de transports publics reposent déjà sur la technologie RFID. D'après des sources dans l'industrie, il existe des millions de clés de voiture de par le monde qui incorporent la radio-identification.

Aviation. La technologie RFID peut être utilisée pour le traitement des bagages. Au guichet de contrôle, le bagage sera muni d'un tag et les lecteurs installés dans différentes parties des aéroports suivront les déplacements du bagage d'un aéroport à l'autre et à l'intérieur de l'aéroport lui-même. Il existe des projets visant à équiper les cartes d'embarquement de tags permettant de localiser les passagers en retard.

Soins de santé. Des systèmes RFID sont utilisés dans l'industrie pharmaceutique pour faciliter le traçage des médicaments et prévenir la contrefaçon et les pertes dues à des vols au cours du transport. Ce traçage peut être réalisé par des fabricants qui insèrent des tags dans chaque médicament, en authentifiant ainsi leur origine. Les pharmaciens ou les commerces vendant les médicaments seront équipés de lecteurs qui vérifieront que le médicament provient de l'entreprise présentée comme le fabricant. L'agence FDA (Food and Drug Administration), aux Etats-Unis, a déjà publié des orientations pour la radio-identification sur les emballages des médicaments aux fins du traçage et de la lutte contre la contrefaçon[5]. Dans les hôpitaux également, en attachant des tags à certains objets, la radio-identification améliore la sécurité des patients et fait réaliser des économies aux hôpitaux, par exemple en éliminant le risque de laisser un objet à l'intérieur du corps d'un

[5] Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; Guidance for FDA Staff and Industry; Compliance Policy Guide; Sec. 400.210; Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; November 2004.

patient après une opération. Des étiquettes RFID peuvent aussi être attachées aux patients eux-mêmes pour vérifier leur identité, le lieu où ils se trouvent et la procédure exacte à exécuter par le personnel hospitalier. Ce personnel peut aussi être suivi à la trace de manière à être facilement localisé en cas d'urgence. La FDA vient d'autoriser une application d'une entreprise (VeriChip) fondée sur l'injection/implantation sous la peau d'un être humain d'un tag RFID fournissant la référence du dossier médical d'un patient, utilisable en cas d'urgence[6].

Sécurité et contrôle de l'accès. Les déplacements et l'utilisation d'équipements précieux peuvent être suivis avec des systèmes RFID, des tags diffusant une information concernant le lieu où ils se trouvent à des lecteurs dans le rayon approprié. Par exemple, dans l'industrie automobile, la radio-identification est déjà utilisée comme composant d'un système d'immobilisation des véhicules. Dans le secteur de la consommation et du commerce de détail, des tags RFID spéciaux peuvent être utilisés pour vérifier l'origine d'un article. De cette façon, les biens de grande valeur peuvent faire l'objet d'une vérification pour détecter les contrefaçons. La sécurisation des billets de banque avec la technologie RFID a fait l'objet de recherches au cours de ces dernières années.

D'après les travaux réalisés au sein de l'OACI[7], la technologie RFID sera aussi utilisée dans les passeports[8]. L'accès des personnes aux zones réglementées peut aussi être géré en les munissant d'un tag RFID ou en les équipant de cartes intelligentes sans contact comme celles qui sont utilisées pour le Sommet mondial sur la société de l'information ou pour un congrès du Parti communiste chinois.

Applications pour le commerce de détail. Plusieurs grandes entreprises de commerce de détail ont demandé aux fabricants de marquer leurs produits. Le détaillant peut profiter de l'utilisation de produits marqués dans plusieurs contextes. Par exemple, la radio-identification améliore les fonctions de gestion des stocks des détaillants. Comme chaque produit est identifié séparément à diverses étapes (à savoir lors de son arrivée au magasin, sur l'étagère, au point de vente), la RFID fournit au détaillant un outil flexible pour gérer et suivre la disponibilité des produits dans le magasin et en entrepôt. La RFID a le potentiel d'améliorer l'efficacité des stocks, en profitant à la fois aux détaillants et éventuellement aux consommateurs. Par exemple, l'installation de lecteurs aux issues permettant l'abandon des opérations de vérification au moment de quitter l'établissement réduira le temps que doit passer un consommateur dans un commerce. La RFID peut contribuer à la traçabilité des produits, en permettant des rappels plus efficaces de produits défectueux ou dangereux ou de produits pour lesquels la date de péremption est dépassée.

---

[6] Department of Health and Human Services; Food and Drug Administration; 21 CFR Part 880; Docket No. 2004N–0477]; published in Federal Register / Vol. 69, No. 237 / Friday, December 10, 2004 / Rules and Regulations

[7] Organisation de l'aviation civile internationale.

[8] En 2003, l'OACI a spécifié les exigences techniques pour la technologie RFID utilisées dans les passeports électroniques. Ces spécifications ont été publiées dans le document OACI 9303.

S'agissant de la radio-identification dans le secteur du commerce de détail, il importe de prendre en compte le travail de normalisation réalisé par EPC Global dans le sens de la création de « codes de produit électroniques » qui identifieront chaque objet[9].

3. Implications pour la protection des données et de la vie privée

Tandis que certaines applications de la radio-identification ne risquent pas de susciter des inquiétudes en matière de protection des données, comme cela est illustré plus loin, nombre d'entre elles sont préoccupantes. La présente section vise à donner un aperçu des principales implications pour la protection des données qui découlent de différentes utilisations de la technologie RFID.

3.1. Utilisation de la radio-identification aux fins de la collecte d'informations liées à des données à caractère personnel

Un premier type de préoccupations concernant la protection des données apparaît lorsque l'exploitation de la technologie RFID sert à collecter une information qui est directement ou indirectement liée à des données à caractère personnel. Premièrement, il est possible d'envisager le cas où le numéro d'un produit figurant sur le tag RFID est lié au fichier du client qui l'a acheté. Par exemple, un magasin de produits électroniques de consommation pourrait marquer ses produits avec des codes de produit uniques que le commerçant combine systématiquement avec les noms des clients relevés lors du paiement avec des cartes de crédit et ultérieurement liés avec la base de données clients du commerçant. Cette opération pourrait être réalisée, entre autres, à des fins de garantie. Comme deuxième exemple, il est possible d'envisager le cas où un supermarché marque des cartes de fidélité ou des dispositifs comparables qui identifient les personnes par leur nom afin de connaître et d'enregistrer les habitudes de consommation pendant que les consommateurs se trouvent dans le magasin, y compris le temps passé dans un secteur donné du supermarché, le nombre de fois où le consommateur se rend dans le supermarché sans faire d'achats, etc.

Dans les cas ci-dessus, dans la mesure où l'information collectée au moyen de la technologie RFID est liée à des données à caractère personnel, les implications pour la vie privée sont manifestes. En plus de renforcer la capacité existante de connaissance des habitudes de consommation et de réalisation de profils individuels que permettent les cartes de fidélité, la technologie RFID accroît le potentiel de démarchage direct avec un marquage au niveau de l'objet, les personnes pouvant être reconnues au moment de leur entrée dans un magasin et leurs habitudes observées dans l'établissement. En outre, une exploitation à grande échelle de la technologie provoquera un gonflement du type et du nombre de données à traiter par un vaste éventail de responsables du traitement, dont il y a lieu de s'inquiéter.

[9] Voir le paragraphe 5.2 pour plus de renseignements concernant EPC Global.

3.2. Utilisation de la radio-identification aux fins du stockage de données à caractère personnel sur chaque tag

Un deuxième type d'implications sur la protection de la vie privée apparaît lorsque des données à caractère personnel sont stockées dans des tags RFID. La billetterie des transports pourrait constituer un exemple de cette utilisation. Il conviendrait d'envisager le cas hypothétique où une entreprise décide de mettre en œuvre un système de billetterie sans contact fondé sur la technologie RFID pour les abonnements mensuels dans lequel le nom et les coordonnées du titulaire de l'abonnement sont insérés dans le tag. Ceci aurait pour effet de permettre à l'entreprise d'avoir connaissance à tout moment des déplacements d'une personne identifiée. Ceci a manifestement des répercussions sur la vie privée des individus. Non seulement l'entreprise posséderait cette information, car n'importe qui peut détecter la présence de tags RFID particuliers avec un lecteur standard, des tiers pourraient aussi subrepticement obtenir la même information. Il est à noter que les systèmes de radio-identification sont très sensibles aux attaques. Comme ils fonctionnent hors de tout contact visuel et physique, un malfaiteur peut travailler à distance et des lectures passives passeront inaperçues.

3.3. Utilisation de la radio-identification aux fins d'un repérage en l'absence d'éléments d'identification "traditionnels"

Un troisième type d'implications pour la protection des données apparaît avec des utilisations de la technologie RFID qui impliquent un repérage des personnes et l'accès à des données à caractère personnel. Plusieurs exemples illustrent de quelle façon la technologie de radio-identification peut avoir des répercussions sur la vie privée d'une personne.

Par exemple, il est possible à une chaîne d'épicerie de donner aux clients des dispositifs marqués (comme par exemple des jetons) permettant de se servir de chariots, que les clients réutilisent à chaque fois qu'ils se rendent dans le magasin. Un tel mécanisme permettrait au commerce d'établir un fichier utilisant le numéro d'identification stocké dans le dispositif marqué lui permettant d'observer quels produits achète une personne (identifiée par le jeton), avec quelle fréquence ces produits sont utilisés et dans quels établissements de la chaîne d'épicerie le consommateur les achète. Le magasin pourrait déduire des hypothèses concernant les revenus, l'état de santé, le style de vie, les habitudes d'achat, etc. d'une personne. Cette information pourrait servir à différents processus de décision, comme la commercialisation, les objectifs voire la fixation dynamique des prix. Comme ce dispositif identifierait la personne à chaque fois qu'elle pénètre dans le commerce, le consommateur pourrait être démarché à la lumière des habitudes de consommation enregistrées. Non seulement le commerce serait en mesure de collecter l'information précitée, mais un tiers pourrait éventuellement se procurer aussi cette information. De cette façon, différentes décisions pourraient être prises concernant cette personne identifiée sans qu'elle y consente en toute connaissance de cause. Comme cela se produit avec l'utilisation de « cookies » dans l'environnement en ligne, même si la personne n'est pas immédiatement et directement identifiée au niveau de l'information sur l'objet, elle peut être identifiée par association à cause de la

possibilité de l'identifier sans difficulté par l'intermédiaire de la grande masse d'informations qui l'entoure ou qui est stockée autour d'elle. En outre, les données collectées auprès d'elle peuvent influencer la façon dont elle est traitée ou évaluée. Cette utilisation de la radio-identification comporte aussi de graves implications en matière de protection des données.

Un autre exemple pourrait être le cas où l'utilisation de tags RFID peut aboutir au traitement de données à caractère personnel, même lorsque la technologie de radio-identification n'implique pas l'utilisation d'autres éléments d'identification explicites. Prenons l'hypothèse dans laquelle M. Z pénètre dans la boutique C avec un sac de produits marqués par RFID des boutiques A & B. La boutique C scanne son sac et les produits qu'il contient (plus probablement des numéros en vrac) sont révélés. La boutique C conserve ces numéros. Lorsque M. Z retourne à la boutique le lendemain, il est scanné à nouveau. Le produit Y, qui avait été scanné la veille, est révélé ce jour-là – le numéro correspond à la montre qu'il porte toujours. La boutique C crée un fichier utilisant le numéro du produit Y comme « clé ». Ceci permet à la boutique de repérer quand M. Z entre dans le magasin, en utilisant le numéro RFID de sa montre comme numéro de référence personnel. Ceci permet à la boutique C d'établir un profil de M. Z (dont le nom ne lui est pas connu) et de repérer ce qu'il transporte dans son sac lors de ses passages ultérieurs dans la boutique C. Ce faisant, la boutique C traite des données à caractère personnel et la loi sur la protection des données s'appliquera.

Enfin, prenons l'exemple de l'utilisation de tags sur certains objets qui contiennent des informations révélant la nature de l'objet. Les effets personnels sont très intimes et constituent des renseignements dont la connaissance par des tiers porterait atteinte à la vie privée de la personne qui en est propriétaire. Les exemples suivant illustrent cette hypothèse. Envisageons le cas où toute personne en possession d'un lecteur peut détecter des billets de banque, des livres, des médicaments ou des objets précieux de passants. La connaissance de ces renseignements par des tiers portera atteinte à la vie privée de la personne propriétaire de ces objets. Les mêmes préoccupations s'appliquent lorsque des terroristes seraient en mesure de détecter des nationalités spécifiques dans des foules. L'intrusion dans la vie privée serait encore plus grave quand le dispositif lui-même contient des informations personnelles importantes comme par exemple des renseignements relatifs au passeport ou des informations hautement sensibles.

Comme l'illustrent ces exemples, certaines des grandes préoccupations en matière de protection des données et de la vie privée suscitées par l'utilisation de la technologie RFID tiennent au repérage clandestin indésirables réalisé par un accès non autorisé à la mémoire du tag ou à l'information qu'il révèle.

Comme cela est encore décrit dans les sections suivantes, il importe de fournir des orientations quant à l'application des principes de base définis dans les directives communautaires, en particulier la directive Protection des données, aux opérations précitées de traitement des données.

4. Application de la législation de l'Union en matière de protection des données à l'information collectée au moyen de la technologie de radio-identification

4.1. Orientations concernant l'application de la directive Protection des données à la collecte et au traitement ultérieur de données au moyen de la technologie RFID

Le champ d'application de la directive Protection des données recouvre le traitement de toutes les données à caractère personnel. Cette directive donne une définition très large des « données à caractère personnel » qui inclut « *toute information concernant une personne physique identifiée ou identifiable* ». On peut alors se demander si cela signifie que la directive Protection des données s'applique nécessairement à la collecte de données par la technologie RFID. La réponse dépendra en général de l'application concrète spécifique de la technologie de radio-identification, et plus particulièrement du point de savoir si l'application RFID spécifique comporte le traitement de données à caractère personnel telles quelles sont définies par la directive générale Protection des données.

Lorsque nous évaluons si la collecte de données à caractère personnel par une application spécifique de RFID est couverte par la directive Protection des données, nous devons impérativement déterminer a) la mesure dans laquelle les données traitées concernent une personne et, b) si ces données concernent une personne qui est *identifiable* ou identifiée. Les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée. Pour évaluer si une information concerne une personne identifiable, il faut appliquer le considérant 26 de la directive Protection des données qui établit qu'« *il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ».

À la lumière de ce qui précède, s'il est évident que les collectes de données par technologie RFID n'entreront pas toutes dans le champ d'application de la directive Protection des données, il est aussi manifeste qu'il se trouvera de nombreux scénarios dans lesquels l'information personnelle est collectée par la technologie RFID, dont le traitement est couvert par la directive Protection des données.

Ceux qui envisagent d'utiliser l'information collectée par technologie RFID devront, avant de le faire, procéder à une évaluation préalable pour déterminer si cette information est considérée comme « donnée à caractère personnel » au sens de la directive Protection des données. Si l'information identifiée par radiofréquence ne contient aucun renseignement personnel et n'est pas non plus combinée avec des données à caractère personnel définies plus haut, alors la disposition de la directive Protection des données ne s'appliquerait pas. De fait, si l'information du tag n'est pas combinée avec d'autres éléments d'identification, par exemple la photographie ou le nom et l'adresse

d'une personne, ou avec un numéro de référence récurrent, alors la directive Protection des données ne s'appliquera pas.

Dans les trois scénarios décrits dans la section 3, les dispositions de la directive Protection des données s'appliqueraient. Dans le premier cas, la raison en est que l'information au niveau de l'objet collectée par la technologie RFID est directement liée à des données à caractère personnel figurant soit dans une carte de crédit, soit dans des cartes de fidélité. Dans le deuxième scénario, l'application de la directive Protection des données est déclenchée dès lors qu'une information personnelle comme un nom est intégré dans les tags RFID. Enfin, l'utilisation de la technologie RFID aux fins du repérage des déplacements d'une personne qui, étant donné l'agrégation massive des données, la mémoire d'ordinateur et la capacité de traitement, sont sinon identifiés, identifiables, déclenche aussi l'application de la directive Protection des données.

4.2 Orientations concernant la conformité avec les exigences de la protection des données

Les responsables du traitement des données collectées par technologie RFID seront tenus de respecter les obligations de la directive Protection des données (tout au long du présent document, il est souvent question d'« exploitants de la technologie »). S'il n'est pas possible d'établir comment ces exigences s'appliquent dans chaque scénario de radio-identification, on peut éventuellement fournir quelques orientations générales que les responsables du traitement des données peuvent suivre et adapter à la lumière des circonstances du traitement de données. Comme cela est encore décrit plus loin dans la section 5, il incombe directement aux fabricants de veiller à ce qu'existe une technologie respectueuse de la vie privée pour aider les responsables du traitement des données à remplir leurs obligations au titre de la directive Protection des données et faciliter l'exercice des droits d'une personne.

Principes:

Le groupe de travail aimerait souligner que le cadre s'appliquant à l'utilisation de la technologie de radio-identification, ainsi que toute autre technologie, est défini au considérant 2 de la directive Protection des données, selon lequel « *les systèmes de traitement de données sont au service de l'homme ; (...) ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus* ».

Principes concernant la qualité des données: les responsables collectant des données dans le contexte d'applications RFID doivent impérativement respecter plusieurs principes de protection des données, notamment les suivants:

Principe de la limitation de l'utilisation (principe de la finalité): ce principe en partie incarné par l'article 6, paragraphe 1, point b), de la directive Protection des

données, entre autres, interdit un traitement ultérieur qui est incompatible avec la ou les finalité(s) de la collecte.

Le principe de la qualité des données: ce principe, dans la directive, exige que les données à caractère personnel soient pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. Ainsi, toute donnée non pertinente ne doit pas être collectée et, si elle a été collectée, doit être éliminée (article 6, paragraphe 1, point c)). Ce principe exige aussi que les données soient exactes et mises à jour.

Le principe de conservation: ce principe exige que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

Légitimation des traitements: conformément à l'article 7 de la directive Protection des données, les données à caractère personnel ne peuvent être traitées que si ce traitement se fonde sur l'un des motifs légitimant le traitement des données [10].

Dans la plupart des scénarios où est utilisée la technologie RFID, le consentement des personnes sera le seul motif légal que pourront invoquer les responsables du traitement des données pour légitimer la collecte d'informations par radio-identification. Par exemple, un supermarché qui marque des cartes de fidélité devra, soit expliciter les règles contractuelles, soit obtenir le consentement de la personne pour lier l'information personnelle obtenue dans le contexte de la délivrance de la carte de fidélité avec l'information collectée au moyen de la technologie RFID. Néanmoins, le consentement n'est pas toujours le motif légal approprié pour légitimer le traitement de données à caractère personnel collectées dans le contexte de systèmes RFID. Par exemple, un hôpital qui utilise la radio-identification dans les instruments de chirurgie pour éliminer le risque de laisser un objet à l'intérieur d'un patient après une opération n'a pas besoin d'obtenir le consentement du patient dans la mesure où ce traitement pourrait être légitimé par les intérêts vitaux de la personne concernée, ce qui constitue un autre motif légal prévu par l'article 7 de la directive Protection des données[11].

Si le consentement est invoqué, conformément à l'article 2 et à l'article 7, point a), de la directive, certaines exigences doivent être respectées. (i) Le consentement doit avoir été donné librement, c'est-à-dire en l'absence de « tromperie ou contrainte ». (ii) Il doit être spécifique, en d'autres termes, il doit concerner une finalité particulière. (iii) Le

[10] L'article 7 énumère les motifs juridiques légitimant le traitement de données: (i) La personne concernée a indubitablement donné son consentement ; (ii) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ; (iii) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; (iv) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ; (v) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ; (vi) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection de la vie privée de la personne.

[11] Le groupe de travail de l'article 29 note que, en dernier ressort, le motif légal approprié prévu par l'article 7 de la directive Protection des données pour légitimer un traitement de données précis dépendra des circonstances spécifiques de ce traitement.

consentement doit être une indication de la volonté effective de la personne. (iv) Le consentement doit être donné en toute connaissance de cause. Enfin, le consentement doit être « indubitable », ce qui signifie qu'un consentement qui peut avoir plusieurs sens ne serait pas considéré comme un consentement.

Exigences d'information: Conformément à l'article 10 de la directive Protection des données, les responsables traitant des données au moyen de la technologie RFID doivent fournir les informations suivantes aux personnes concernées : l'identité du responsable du traitement, les finalités du traitement et, entre autres, l'information sur les destinataires des données et l'existence d'un droit d'accès[12]. Conformément à cette obligation dans le contexte du scénario décrit au point 4, le commerce de détail devra fournir aux personnes concernées des informations claires concernant au moins les points suivants :

(i) la présence de tags RFID sur les produits ou leur emballage et la présence de lecteurs ;

(ii) les conséquences de cette présence du point de vue de la collecte d'informations ; en particulier, les responsables devraient très clairement informer les personnes que la présence de ces dispositifs permet aux tags de diffuser une information sans que la personne se livre à une action intentionnelle ;

(iii) les finalités pour lesquelles il est entendu d'utiliser l'information, notamment a) le type de données avec lesquelles l'information RFID sera associée et b) si l'information sera mise à la disposition de tiers, et

(iv) l'identité du responsable du traitement des données.

En outre, en fonction de l'utilisation spécifique de RFID, le responsable du traitement devra informer les personnes concernant : (v) la façon d'abandonner, de neutraliser les tags ou de les détacher des produits, en les empêchant ainsi de communiquer d'autres informations et (vi) la façon d'exercer le droit d'accès aux informations. Par exemple, cette information sera nécessaire dans les scénarios décrits au paragraphe 3.1. Tandis que les avis tels que ceux qu'il est proposé de donner dans les produits de consommations pour EPC Global servent à communiquer l'information décrite plus haut au point I, ces avis devraient être complétés par une autre documentation fournissant en plus l'information visée ci-dessus[13].

Le principe d'un traitement loyal reconnu à l'article 6, paragraphe 1, point a), de la directive Protection des données exige que l'information soit communiquée à la personne concernée de façon claire et compréhensible.

---

[12] L'information sur les destinataires des données, l'obligation de réponse et l'existence de droits d'accès et de rectification doit être fournie dans la mesure où elle est nécessaire au regard des circonstances spécifiques dans lesquelles les données sont collectées, pour garantir un traitement loyal par rapport à la personne concernée.

[13] Voir le paragraphe 5.1 pour un aperçu des activités de EPC Global.

Enfin, en communiquant l'information ci-dessus, le groupe de travail estime important de souligner que la personne concernée devrait être en état de comprendre facilement les effets de l'application de radio-identification.

Droit d'accès de la personne concernée aux données: L'article 12 de la directive Protection des données donne aux personnes concernées la possibilité de vérifier l'exactitude des données et de s'assurer que les données sont mises à jour. Ces droits s'appliquent intégralement à la collecte de données à caractère personnel par la technologie RFID. Si nous revenons à l'exemple du supermarché qui marque des cartes de fidélité, le droit d'accès implique la communication de *toute* l'information relative à une personne, ce qui peut inclure le nombre de fois où la personne a pénétré dans le magasin, les objets achetés, etc.

Si les tags RFID contiennent des informations personnelles décrites au paragraphe 3.2, les personnes devraient être en droit de connaître l'information contenue dans le tag et de procéder à des corrections en utilisant des moyens aisément accessibles.

Obligations en matière de sécurité: L'article 17 de la directive Protection des données impose aux responsables du traitement des données une obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre une destruction accidentelle ou illicite ou une diffusion sans autorisation. Ces mesures peuvent être organisationnelles ou techniques. Cette exigence est développée dans la section 5 concernant la radio-identification et la nécessité d'utiliser une technologie respectueuse de la vie privée.

5. Exigences techniques et d'organisation pour assurer la mise en œuvre adéquate des principes de protection des données

Le respect des principes définis plus haut, ainsi que le principe de la minimisation des données incarné par l'article 6, paragraphe 1, de la directive Protection des données est essentiel pour les exploitants des applications RFID.

Le groupe de travail de l'article 29 considère que la technologie peut jouer un rôle essentiel en assurant le respect des principes de la protection des données dans le contexte du traitement des données à caractère personnel collectées au moyen de la technologie RFID. Par exemple, la conception des tags, des lecteurs et des applications RFID sous l'effet d'initiatives de normalisation peut avoir un impact puissant en réduisant au minimum la collecte et l'utilisation de données à caractère personnel et aussi en empêchant toute forme illicite de traitement en mettant des personnes non autorisées dans l'impossibilité technique d'accéder à des données à caractère personnel.

Dans ce contexte, le groupe de travail de l'article 29 souhaite souligner que si les exploitants d'une application RFID sont en fin de compte responsables des données à caractère personnel collectées au moyen de l'application en question, il incombe aux fabricants de produits RFID et aux organismes de normalisation de veiller à ce que des produits RFID respectueux de la protection des données et de la vie privée soient mis à la disposition de ceux qui exploitent la technologie. Il conviendrait de mettre au point des

mécanismes pour garantir que ces normes soient largement observées dans des applications pratiques. En particulier, il faut disposer de normes RFID respectueuses de la vie privée pour garantir que les responsables du traitement des données à caractère personnel au moyen de la technologie RFID disposent des outils nécessaires pour mettre en œuvre les exigences figurant dans la directive Protection des données. Le groupe de travail préconise donc aux fabricants de tags, de lecteurs et d'applications RFID et aux organismes de normalisation de prendre en compte les recommandations suivantes.

5.1 Répercussion de la normalisation et de l'interopérabilité sur la mise en œuvre des principes de la protection des données.

Quelle que soit la technologie envisagée, le processus de normalisation constitue généralement le principal moteur de l'interopérabilité, ce qui est important pour réussir à faire adopter et mettre en œuvre de nouvelles technologies. La normalisation peut aussi faciliter l'adoption des exigences en matière de protection des données et de la vie privée.

Tous les composants d'un système RFID font ou feront l'objet d'une norme, comme la conception du tag et du lecteur, les données stockées dans le tag, le protocole de communication (interface air) entre le lecteur et le tag, la gestion des données collectées par le lecteur, etc. Les organismes de normalisation et d'autres groupes ont déjà entrepris certains travaux dans le domaine de la radio-identification. Il est à noter que la normalisation de la RFID aura une influence sur un nombre considérable de marchés qui affecteront en particulier les opérations sur les marchandises.

Alors que le système a été introduit à l'origine en réaction à la crise de la vache folle, l'Organisation internationale de normalisation (ISO) a mis au point des normes spécifiques aux secteurs (conteneurs, unités de transport, animaux, etc.) pour les tags RFID et des normes plus génériques pour l'interface air (séries ISO 18000) et pour la gestion des objets (ISO/CEI 15963:2004).

EPCglobal Inc[14], entreprise commune constituée entre EAN International et Uniform Code Council (UCC), est dirigée par le conseil d'administration de EPCglobal qui est composé de grandes sociétés. Cette entreprise travaille à la création de codes de produit électroniques (Electronic Product Codes - EPC) qui identifieront des objets. Chaque produit sera équipé d'un tag comportant le numéro du produit auquel il est attaché. Le prédécesseur de ce système est le code universel de produit (Universal Product Code - UPC) ou le système de code à barres, que EPC vise à remplacer. La différence entre les deux systèmes est que le code électronique de produit UPC identifie un type de produits sans que chacun des différents objets soit numéroté. En outre, le réseau EPC Global crée des normes pour connecter les serveurs contenant des informations relatives à des objets identifiés par des numéros EPC. Ces serveurs, appelés

[14] http://www.epcglobalinc.org/

en anglais EPC Information Services ou EPCIS sont accessibles via l'Internet et mis en liaison, autorisés et rendus accessibles via un ensemble de services de réseau[15].

Dans la plupart des initiatives de normalisation RFID, il sera possible d'inclure des caractéristiques de protection des données dans les spécifications techniques. Par exemple, il a été récemment proposé[16] de modifier la norme du protocole lecteur-tag mis au point par l'ISO pour inclure les pratiques d'information loyale mises au point par l'OCDE[17].

Récemment, l'Institut européen des normes de télécommunication (ETSI) a approuvé une nouvelle norme européenne pour l'utilisation de systèmes RFID en augmentant la puissance autorisée du lecteur et le nombre de fréquences disponibles dans la bande UHF, la plus prometteuse dans le secteur du commerce de détail pour l'identification au niveau des objets. Cette évolution augmentera en particulier la distance de lecture depuis le lecteur vers le tag[18].

L'interopérabilité des systèmes RFID (matériels, logiciels et données produites) résulte logiquement du processus de normalisation. D'un point de vue commercial, l'interopérabilité des systèmes RFID est positive. De fait, pour un modèle économique durable, il conviendrait qu'un détaillant évite de mettre en œuvre plusieurs lecteurs de tags différents pour scanner des tags produits par différents fabricants. Du point de vue de la protection des données, si l'interopérabilité peut augmenter la qualité technique des données et contribuer au respect des dispositions de l'article 6, paragraphe 1, point d), de la directive, l'interopérabilité RFID peut en même temps avoir certains effets collatéraux négatifs pour la protection des données si des mesures appropriées ne sont pas prises. Par exemple, le principe de la limitation des finalités peut être plus difficile à appliquer et à contrôler. En outre, la gestion des droits d'accès concernant la protection de la vie privée peut aussi devenir plus critique avec l'augmentation du nombre d'intervenants manipulant les données.

5.2 Mesures techniques et d'organisation pour l'information sur la présence de RFID, sa visibilité et son état de veille

Comme cela a été souligné au paragraphe 4, les exploitants de technologies RFID sont tenus de fournir aux personnes concernées une information concernant non seulement les finalités du traitement de données, mais aussi la présence de dispositifs RFID et ils doivent aussi se conformer aux dispositions suivantes:

---

[15] Jusqu'à présent, les préoccupations de l'Union ont été sous-représentées dans ces initiatives de normalisation où prédominent les parties prenantes de l'industrie américaine. Il n'est toujours pas sûr non plus que le marché chinois adoptera une des normes citées et ne mettra pas au point ses propres normes.

[16] Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan.

[17] ISO 18000 Part 6 Type A

[18] La distance du lecteur et sa puissance peuvent affecter la mesure dans laquelle une application RFID donnée porte plus particulièrement atteinte à la vie privée.

Premièrement, les personnes doivent être informées de la présence de dispositifs d'identification radiofréquence ou de lecteurs RFID activés. À cette fin, des pictogrammes allant dans le sens d'une norme mondiale ainsi que d'autres moyens d'information allant dans le même sens constituent un besoin manifeste. Il est essentiel de fournir ce type d'informations pour empêcher la collecte clandestine et non autorisée de données à caractère personnel par la technologie RFID. Par exemple, si un magasin ou un hôpital a activé les lecteurs, les personnes devraient en être informées.

Deuxièmement, pour les mêmes raisons définies plus haut (éviter la collecte clandestine de données à caractère personnel) l'identification de l'existence de dispositifs d'identification radiofréquence autour d'une personne (par exemple dans les vêtements et les objets) est une autre exigence car la taille de ces dispositifs les rend quasiment invisibles. Les méthodes pour satisfaire à cette exigence peuvent prendre différentes formes: il peut s'agir d'avis standards mais aussi de mesures techniques.

Troisièmement, informer de la présence de dispositifs RFID seulement ne suffira pas en pratique. La possibilité d'activation ou l'activation en temps réel de ces dispositifs constituent aussi des informations à fournir aux personnes en vertu de la directive Protection des données. Donc, des techniques simples permettant une indication visuelle de l'activation ou de l'état de veille sont aussi nécessaires. La présence et la nature de technologies PET (essai de planification concernant les technologies des télécommunications) (par exemple dispositifs de neutralisation temporelle, caractère amovible du tag, etc.) et les mesures organisationnelles dans un environnement donné devraient figurer parmi les informations facilement accessibles.

Le groupe de travail de l'article 29 souligne qu'il est toujours nécessaire de poursuivre les travaux de recherche et de développement sur ces trois thèmes d'information par toutes les parties.

5.3 Mesures techniques et d'organisation pour l'exercice des droits en matière d'accès, de rectification et d'effacement

Comme cela est décrit plus loin, la constitution de la technologie RFID peut avoir un impact important pour garantir la mise en œuvre effective des droits d'accès, de rectification et d'effacement reconnus par l'article 12 de la directive Protection des données.

a) Accès au contenu des tags (article 12, point a), de la directive Protection des données)

Fait inhérent à cette technologie, l'accès au contenu d'un tag RFID exige un lecteur fonctionnant avec le protocole du tag et un affichage destiné à la personne. Mais pour de nombreuses applications, le tag contient uniquement une identité dont la sémantique ne peut être abordée que par l'intermédiaire d'un environnement complet d'applications de la télécommunication. À notre connaissance, seul un petit nombre de tags RFID comporte une information sémantique (décrivant l'objet, l'identifiant du responsable du traitement,

la finalité de la collecte des données, etc.), ce qui pose aussi le problème de l'accès des personnes au contenu.

Une possibilité pour rendre cette information précieuse est de définir des normes sémantiques en utilisant par exemple XML. Quelle que soit la forme qu'elles prennent, ces descriptions sémantiques posent toujours le problème de l'accès par des tiers non autorisés (voir la section 3 plus haut).

b) Rectification du contenu (article 12, point b) de la directive Protection des données)

À la différence de l'accès au contenu, la rectification exige un lecteur fonctionnant avec le protocole du tag et un système de technologie de l'information permettant à la personne de suivre à la fois la lecture du contenu et sa modification.

Une possibilité particulière proposée consiste à intégrer dans le tag une fonction qui effacera ou brouillera le numéro de série de l'objet et ne rendra disponible en tout ou partie que la description du type de classe d'objet (le contraire est aussi possible mais avec des implications différentes en matière de protection de la vie privée).

c) Effacement du contenu (article 12, point b), de la directive Protection des données)

Le point de savoir s'il conviendrait de mettre en œuvre des neutraliseurs de tag pour permettre aux personnes de mettre fin au traitement de leurs données à caractère personnel lorsque ce tag entre dans le champ d'un lecteur dépend des motifs juridiques qui légitiment le traitement de ces données. Par exemple, cette mesure ne serait pas raisonnable pour ce qui concerne l'intégration de tag RFID dans des passeports tandis qu'elle serait nécessaire – d'un point de vue de protection des données – dans des tags RFID attachés à des produits de consommation. Cette question a été examinée dans le contexte de la Conférence des commissaires à la protection des données et de la vie privée de Sydney, comme cela ressort de la déclaration de Sydney sur la radio-identification[19].

Au cours des dernières années, il a été fait état de diverses solutions proposées. Une démarche concerne l'introduction d'une commande « destruction ». En d'autres termes, le tag peut être désactivé de façon permanente ou temporaire en envoyant un ordre de « destruction ». La désactivation permanente peut être réalisée par effet fusible, brouillage de mémoire ou détachement du tag. La désactivation temporaire pourrait être réalisée mécaniquement ou au moyen d'un verrouillage logiciel. Un problème avec cette démarche est que l'avantage de la réutilisation du dispositif RFID en dehors de la boutique est perdu. Il a donc été proposé d'autres démarches.

---

[19] Résolution sur la radio-identification, 25ème Conférence internationale des commissaires à la protection des données et à la vie privée, Sidney 2003, http://www.privacyconference2003.org selon laquelle : « …à partir du moment où les étiquettes RFID sont en possession des individus, ceux-ci devraient avoir la possibilité de supprimer les données, de désactiver ou de détruire les étiquettes ».

Une variante de ce qui précède consiste à « écraser » les données stockées sur un tag RFID avec des zéros. Le tag reste actif mais n'émet en retour que des zéros au lieu d'un nombre lorsqu'il est interrogé. Ce système ne « neutralise » pas vraiment la radio-identification. Le tag continue de répondre et informe que la personne transporte un objet marqué, ce qui peut avoir les conséquences suivantes : premièrement, tant que les tags de radio-identification qui n'émettent que des zéros ne sont pas très répandus, la simple existence d'un tel tag constitue une information précieuse. Elle démontre que la personne a fait un achat dans une boutique qui marque les objets. Une entreprise bien informée peut faire une supposition éclairée. Deuxièmement, il apparaît que pour commencer, les tags RFID vont être utilisés sur des objets de prix. Pendant quelques années, la simple présence d'un tag RFID (même s'il émet des zéros ou des données inintelligibles) aidera les voleurs dans leur recherche d'objets valant la peine d'être dérobés dans des vestiaires ou des parcs de stationnement. Enfin, au fur et à mesure que les tags RFID deviendront plus nombreux, les commerces risquent de ne pas apprécier tous ces tags qui répondent aux interrogations mais émettent des données sans valeur.

Une autre démarche consiste à protéger matériellement le tag, ce qui peut être utilisé délibérément par l'usager. Par exemple, des porte-monnaie avec des protections peuvent être utilisés, de telle sorte que les billets de banque marqués ne puissent être détectés. De même, une feuille d'aluminium incorporée dans la couverture du passeport RFID pourrait suffire à assurer la protection de son contenu, sauf lorsque le passeport est ouvert. Néanmoins, cette protection ne convient pas bien à toutes les applications. Par exemple, les vêtements équipés de tags ne peuvent pas être enveloppés avec un matériau protecteur lorsqu'ils sont portés. En outre, cette démarche paraît imposer de façon indue des fardeaux aux personnes qui sont en dernier recours les seules à être chargées d'empêcher le tag de révéler une information.

En définissant comment les neutraliseurs de tags devraient fonctionner, en plus de ce qui précède, les organismes de normalisation, les fabricants et les exploitants de la technologie RFID devraient tenir compte du fait que les personnes choisissant de détacher le tag ne devraient être pénalisées d'aucune façon.

Là encore, le groupe de travail de l'article 29 souligne qu'il est encore nécessaire de mener de nouveaux travaux de recherche et de développement sur ces thèmes par toutes les parties.

5.4. Légitimation du traitement

Neutraliseurs des tags : En plus de la nécessité de neutraliseurs des tags dans le contexte de la section 5.3, d'autres dispositions de la directive Protection des données exigent la présence de cette fonction (neutralisation d'un tag). De fait, lorsque, aux termes de la directive Protection des données, le consentement est le seul motif légal légitimant la collecte de données à caractère personnel au moyen de la radio-identification (voir la section 4.2), les personnes peuvent toujours retirer leur accord au traitement de données à caractère personnel (article 7, point a)). S'il n'existe pas de dispositif permettant à la

personne de neutraliser le tag, toute personne qui ne souhaite pas que le tag continue à fournir des informations la concernant sera empêchée d'exercer ce droit. Lorsqu'il est prévu que les données à caractère personnel intégrées dans les tags RFID sont collectées sur une base juridique autre que le consentement, il n'est pas toujours nécessaire que ces tags possèdent des dispositifs de neutralisation. Par exemple, l'information à caractère personnel contenue dans les tags utilisés dans le contexte professionnel à des fins de contrôle d'accès au lieu de travail n'exige pas nécessairement que des dispositifs de neutralisation des tags soient disponibles dans la mesure où le traitement de données est fondé sur la relation de travail.

Dans certains applications RFID, par exemple lorsque la personne a le droit de retirer son consentement ou de s'opposer au traitement (article 14, point a)) et le droit subséquent de désactiver le tag, les fabricants et les exploitants de technologie RFID devraient veiller à ce que cette opération de désactivation du tag soit facile à réaliser. En d'autres termes, pour la personne concernée, la tâche consistant à désactiver le tag devrait être facile.

5.5 Sécurité des données

Utilisation du cryptage sur les tags et applications: Lorsque les tags RFID contiennent des données à caractère personnel, ils doivent, conformément à l'article 17 de la directive Protection des données, faire l'objet de mesures techniques destinées à empêcher la diffusion non autorisée des données. Au cas où ces mesures ne seraient pas mises en œuvre, toute personne équipée d'un lecteur pourrait « réveiller » un tag et obtenir l'information stockée sur ce dispositif. Ces mesures sont aussi nécessaires au titre de l'article 6, paragraphe 1, point d), de la directive Protection des données pour garantir l'intégrité des données conservées dans le tag, en évitant ainsi des modifications sans autorisation.

Le type de moyens techniques mis en œuvre dépendra de la nature des données. Comme cela est illustré plus loin, la plupart du temps, ces tags pourraient exiger le cryptage des données et l'authentification du lecteur pour empêcher des tiers équipés de lecteurs de lire l'information. Si nous envisageons le scénario où des étiquettes d'identification radio-fréquence contenant l'identité du patient, le nom du docteur responsable et la procédure à exécuter par le personnel hospitalier, on comprendra aisément qu'il soit imposé à l'hôpital de garantir que cette information n'est pas lisible pas des lecteurs de tiers, ce qui rend à son tour nécessaire l'utilisation de mesures techniques comme le cryptage pour empêcher cette lecture.

La démarche la plus générale et la plus sûre est l'utilisation de protocoles d'authentification standards (par exemple ISO/CEI 9798). Ces protocoles sont déjà largement utilisés dans des réseaux ou avec des cartes intelligentes. Dans ces protocoles standardisés, des primitives cryptographiques sont utilisées. Pour les méthodes d'authentification symétriques, c'est-à-dire lorsque les clés sont égales pour l'émetteur et le récepteur, il est utilisé des codes authentification de messages ou des algorithmes de cryptage symétriques (par exemple DES, AES). Pour les méthodes asymétriques, c'est-à-

dire où chaque partie a une clé privée et une clé publique, il est utilisé des algorithmes de cryptage asymétriques (par exemple RSA, ECC) ou des systèmes avec signature.

Certaines méthodes d'authentification cryptographiques sont déjà mises en œuvre dans les immobiliseurs d'automobile ou les systèmes de contrôle d'accès, mais elles utilisent souvent des algorithmes exclusifs, car ils sont souvent plus faciles et moins coûteux à mettre en œuvre que les algorithmes standards. Néanmoins, pour la sécurité renforcée qui peut être nécessaire à la protection de données sensibles, il conviendrait de mettre en œuvre des algorithmes et protocoles standards. L'avantage de ces protocoles et algorithmes est qu'ils sont déjà largement utilisés et donc testés et éprouvés par de nombreuses parties différentes. De cette façon, leur caractère sûr est à présent largement accepté.

Il existe déjà des publications indiquant que les algorithmes symétriques (comme AES) conviennent pour des tags RFID[20]. Le problème que pose l'utilisation d'algorithmes d'authentification symétriques est que l'établissement des clés et leur gestion sont complexes. Les méthodes asymétriques évitent ce problème mais sont plus coûteuses que les méthodes symétriques.

6. Conclusion

Étant donné l'utilisation croissante de la technologie de la radio-identification pour toutes sortes de finalités et d'applications, dont certaines ont des implications énormes en matière de protection des données, le groupe de travail a estimé qu'il était nécessaire à ce stade de publier le présent document de travail et de contribuer à la discussion en cours sur les questions de l'identification par radio-fréquence. Le groupe de travail espère que le contenu du présent document constitue une contribution utile au débat sur la RFID et invite les parties prenantes à adhérer aux principes évoqués dans le présent document.

Ce document de travail a été préparé sur la base de l'information disponible, considérant l'état de mise au point de la technologie et en particulier son application actuelle dans divers secteurs. Néanmoins, le groupe de travail est conscient que l'utilisation de la RFID est en constante évolution. Il se produit constamment des développements dans ce domaine et, plus l'expérience acquise augmente, plus la connaissance des questions en jeu s'accroît. Pour cette raison, le groupe de travail s'engage à continuer de suivre les développements technologiques dans ce domaine en collaboration avec les parties intéressées. Plusieurs questions identifiées dans le présent document pourront nécessiter un réexamen à la lumière de l'expérience acquise. En outre, en fonction de l'évolution de la technologie RFID et de ses applications, le groupe de travail décidera peut-être ultérieurement de se concentrer en détail sur des

[20] Feldhofer M., Dominikus S., Wolkerstorfer J., "Strong Authentication for RFID Systems using the AES Algorithm", In the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004, August 11-13, 2004, Boston, USA), Lecture Notes in Computer Science (LNCS) Vol. 3156, Springer Verlag, 2004, ISBN 3-540-22666-4, pp. 357-370.
http://www.iaik.tugraz.ac.at/research/publications/2004/CHES2004_AES.htm

domaines/applications spécifiques en fournissant des orientations supplémentaires pour des applications spécifiques.

ANNEXE

LA TECHNOLOGIE RFID

La communication sans fil est une technologie émergente qui couvre à présent une gamme étendue d'applications. Parmi ces applications figure la création de réseaux locaux sans fil (WLAN) ou les connexions sans fil dans la bande des basses fréquences entre divers dispositifs comme des ordinateurs portables, des assistants numériques personnels (PDA), des téléphones mobiles, etc. (technologie Bluetooth).

Au cours de ces dernières années, une nouvelle technologie est devenue de plus en plus populaire. Il s'agit de la RFID, c'est-à-dire l'identification par radio-fréquence ou radio-identification. L'idée principale à l'origine de cette technologie a consisté à donner à chaque objet porteur d'un tag RFID une identité unique qui peut être communiquée à un lecteur par fréquence radio. Cela permet diverses applications dans la chaîne d'approvisionnement et d'autres applications industrielles. Au début, les tags RFID étaient destinés à être utilisés en remplacement des codes barres. Les avantages de leur utilisation étaient évidents : ils n'ont pas besoin d'être visibles et le processus d'enregistrement peut donc être réalisé automatiquement. À présent, avec les progrès de cette technologie, il est possible d'envisager d'autres applications plus perfectionnées. Avant de discuter d'éventuelles applications, il est fourni un aperçu de cette technologie.

Le système RFID le plus simple consiste en deux composants : un tag, qui est attaché à un objet, et un lecteur qui est capable de récupérer les données du tag. Ces composants communiquent l'un avec l'autre au moyen d'une liaison radio. Le tag et le lecteur possèdent tous deux une antenne et un démodulateur (niveau d'entrée analogique). Le niveau d'entrée « traduit » l'information analogique entrante communiquée par la liaison radio en données numériques. Ces données peuvent encore être traitées par la partie numérique du lecteur du tag.

Côté tag, le traitement numérique peut être réalisé soit par un matériel spécial soit par un microprocesseur. Pour traiter les données récupérées à partir des tags, il est possible d'utiliser un ordinateur serveur attaché au lecteur. Il est demandé à ce serveur de mettre en œuvre des applications spéciales en utilisant les données du tag. La figure suivante présente un système RFID actuel.

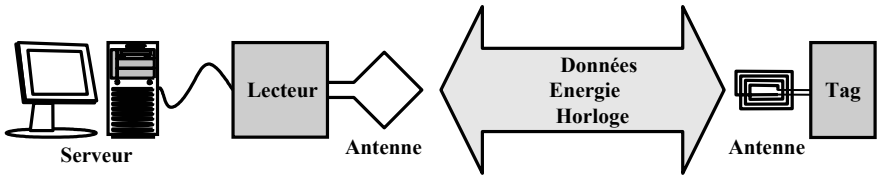

Figure: Structure d'un système RFID

Divers paramètres technologiques peuvent être utilisés pour décrire un système RFID particulier. En fonction de ces paramètres, les systèmes RFID permettent différentes applications.

- *Tags RFID actifs/passifs*. Les tags de base fonctionnant sur un mode passif reçoivent l'énergie et le signal d'horloge pour traiter et transmettre des données via le champ électromagnétique du lecteur. L'intensité de ce champ est limitée par des règlements nationaux et internationaux. Ainsi, la consommation d'énergie du tag doit être limitée pour garantir une fonctionnalité correcte. La grandeur des champs diminue avec la distance par rapport au lecteur, et une consommation d'énergie plus faible du tag aboutit donc à des distances de lecture plus longues. En d'autres termes, le lecteur et le tag sont capables de communiquer sur une plus grande distance : les tags actifs transmettent des données même si aucun lecteur n'est présent ou détecté. En conséquence, ils sont équipés d'une pile. Pour que la description soit complète, il est à signaler que certains tags peuvent incorporer un dispositif de contrôle ou de mesure enregistrant des valeurs, comme un thermomètre pour détecter des ruptures dans la chaîne du froid. Dans ce cas précis, une pile est aussi nécessaire mais sans que cela ait une conséquence directe sur la nature active/passive du tag.

- *Fréquences de fonctionnement:* Les systèmes RFID peuvent fonctionner avec des fréquences, des distances de lecture et des types de couplage différents. Ces paramètres dépendent souvent fortement l'un de l'autre. Les fréquences varient de 135 kHz à 5,8 GHz. En l'occurrence, il faut impérativement prendre en considération les restrictions internationales et les exigences physiques. Le couplage peut être électrique, magnétique ou électromagnétique. Le type de couplage affecte la distance de fonctionnement, qui peut varier de quelques millimètres à 15 mètres et plus. Plus particulièrement, il est possible d'établir une distinction entre :

- ✓ Les systèmes à couplage ferme, utilisant des tags avec une distance de lecture courte allant jusqu'à 1 cm. Ces systèmes fonctionnent avec des fréquences comprises entre CC et 30 MHz et doivent être placés à l'intérieur ou sur le lecteur pour communiquer. Dans ces systèmes, il est possible d'avoir une forte consommation d'énergie et des taux de transmission élevés des données.

- ✓ Des systèmes de couplage à distance avec une distance de lecteur d'environ 1 m. La plupart des systèmes RFID utilisent le couplage à distance avec des fréquences comprises entre 135 kHz et 13,56 MHz.

- ✓ Les systèmes à longue distance, avec une distance de lecture supérieure à 1 m. Ils fonctionnent sur des fréquences comprises entre 868 MHz et 5,8 GHz.

Les systèmes RFID peuvent créer des interférences avec d'autres installations radios. En conséquence, il importe qu'ils utilisent d'autres fréquences que les services de radio-audio, de télévision ou de radio mobile. Les fréquences les plus importantes utilisées pour les systèmes RFID sont de 0 à 135 kHz et les fréquences des appareils industriels, scientifiques et médicaux (ISM) sont de 6,78 MHz, 13,56 MHz, 27,125 MHz, 40,68 MHz, 869,0 MHz, 2,45 GHz, 5,8 GHz et 24,125 GHz.

- *Possibilité de lecture/écriture:* La complexité des systèmes RFID varie. Elle est souvent limitée par les possibilités du tag.

- ✓ Dans les systèmes de bas de gamme, les tags ont une mémoire morte. Le lecteur peut uniquement lire le contenu du tag, qui consiste en général en un numéro de série de quelques bytes. Ces tags simples sont souvent utilisés en raison de leur faible prix et de la faible taille de leur mémoire. Ils peuvent être utilisés pour remplacer des

systèmes à code barres lorsque les objets doivent être identifiés, le plus souvent pour la gestion d'entrepôts ou l'acheminement de marchandises tout au long du processus de production. Le traçage des animaux peut également être réalisé avec ce type de tag.

- ✓ Dans la gamme moyenne des systèmes RFID, les tags peuvent contenir une mémoire inscriptible. La capacité de la mémoire varie actuellement de quelques bytes à plusieurs dizaines ou centaines de kBytes avec une mémoire morte modifiable électriquement (EEPROM[21] pour les tags passifs et du type RAM partagée[22]) pour les tags actifs. Dans cette gamme, des capteurs (de température, de pression, etc.) peuvent aussi être intégrés dans les tags, par exemple pour détecter les accidents environnementaux, qui peuvent être enregistrés sur le tag. Ces tags peuvent en outre être utilisés pour le contrôle d'accès. Une autre application qui a déjà été mise en œuvre et testée est le traçage des bagages dans les aéroports. La destination du bagage peut être inscrite sur la mémoire du tag et l'acheminement peut se faire automatiquement. Une autre application se situe dans les soins de santé. Ces tags peuvent être utilisés dans les hôpitaux, pour enregistrer le détail du traitement des patients ou observer plusieurs paramètres de l'état de santé d'un patient.

- ✓ Les cartes intelligentes sans contact équipées d'un microprocesseur et d'un système d'exploitation sont qualifiées de systèmes haut de gamme. Ces systèmes peuvent aussi contenir un certain volume de mémoire, qui est généralement supérieur à celui des tags RFID moyens. Des fonctions complexes doivent être mises en œuvre sur la carte. Des programmes peuvent être conservés dans la mémoire du tag puis exécutés par le microprocesseur. En raison de la forte consommation d'énergie de ces cartes, la distance de lecture de ce système se limite à l'heure actuelle à quelques centimètres. Des applications plus complexes peuvent être mises en œuvre avec ces cartes. Elles sont utilisées pour des applications caractéristiques de cartes intelligentes comme le contrôle d'accès. Elles peuvent aussi servir de cartes d'identité ou d'assurance maladie. Les documents de voyage dotés d'une puce électronique (ICC[23]) définis par l'OACI ou les visas et les permis de séjour équipés d'une puce constituent les exemples où des systèmes RFID haut de gamme sont en cours d'examen.

Fait à Bruxelles, le 19 janvier 2005
Par le groupe de travail
Le président
Peter SCHAAR

---

21 Electrically Erasable Programmable Read Only Memory
22 Static Random Access Memory
23 Integrated Circuit Chip