Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1275

(12/2010)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

Lignes directrices relatives à la protection des informations d'identification personnelle dans les applications utilisant la technologie RFID

Recommandation UIT-T X.1275

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1275

Lignes directrices relatives à la protection des informations d'identification personnelle dans les applications utilisant la technologie RFID

Résumé

La Recommandation UIT-T X.1275 reconnaît que la technologie d'identification par radiofréquence (RFID) comporte un risque en ce sens que les informations se rapportant spécifiquement aux articles et produits portés ou transportés par les particuliers peuvent être utilisés à des fins abusives, même si cette technologie facilite grandement l'accès à ces informations et la diffusion de celles-ci à des fins licites. L'abus consiste, par exemple, à localiser un individu ou à s'immiscer dans sa vie privée par un autre moyen illicite. La présente Recommandation fournit par conséquent des lignes directrices applicables aux procédures RFID qui peuvent être utilisées pour tirer parti des avantages de cette technologie tout en assurant la protection des informations d'identification personnelle.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1275	2010-12-17	17

Mots clés

Application RFID, protection des informations d'identification personnelle.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT [avait/n'avait pas] été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Recommandation UIT-T X.1275

Lignes directrices relatives à la protection des informations d'identification personnelle dans les applications utilisant la technologie RFID

1 Domaine d'application

La présente Recommandation a pour objet de fournir aux utilisateurs et aux vendeurs de systèmes d'identification par radiofréquence (RFID) (y compris les fournisseurs de services et fabricants de systèmes RFID) des lignes directrices pour la protection des informations d'identification personnelle afin d'assurer le respect de la vie privée des personnes dans un environnement RFID.

Ces lignes directrices peuvent s'appliquer aux cas dans lesquels le système RFID peut être utilisé pour s'immiscer dans la vie privée des personnes; par exemple, les informations d'identification personnelle sont enregistrées dans une étiquette RFID et sont collectées ultérieurement, ou bien les informations relatives aux objets, collectées au moyen de la technologie RFID, sont reliées aux informations d'identification personnelle. Toutefois, ces lignes directrices ne s'appliquent pas aux cas dans lesquels les informations relatives aux objets sont collectées et utilisées sans aucun risque de divulgation des informations d'identification personnelle ou d'atteinte à la vie privée.

Elles visent à protéger les informations d'identification personnelle en cas de risque d'atteinte à la vie privée des personnes au moyen d'un système RFID, et à promouvoir des conditions d'utilisation sûres de la technologie RFID. Elles ont pour objet d'énoncer les règles de base relatives à la protection de la vie privée que devraient suivre les fournisseurs de services RFID, et de donner à ces derniers, ainsi qu'aux fabricants et aux utilisateurs de systèmes RFID, des conseils en la matière et s'inscrivent dans le cadre de la législation locale ou nationale.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[ISO/CEI 18000] ISO/CEI 18000-6 (2004), *Technologies de l'information – Identification par radiofréquence (RFID) pour la gestion d'objets – Partie 6: Paramètres de communications d'une interface hertzienne entre 860 MHz et 960 MHz.*

[ISO/CEI 19762-3] ISO/CEI 19762-3 (2005), *Technologies de l'information – Techniques automatiques d'identification et de saisie de données (AIDC) – Vocabulaire harmonisé – Partie 3: Identification par radiofréquence (RFID).*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 informations d'identification personnelle (PII) [UIT-T X.1171]: informations relatives à une personne physique, permettant de l'identifier (y compris les informations permettant d'identifier

une personne lorsqu'elles sont combinées avec d'autres informations, même si elles n'identifient pas clairement la personne).

3.1.2 système d'identification par radiofréquence (RFID) [ISO/CEI 19762-3]: système d'identification automatique et de saisie de données comprenant un ou plusieurs lecteurs/interrogateurs et un ou plusieurs transpondeurs, par lesquels le transfert de données est assuré au moyen de porteuses électromagnétiques à induction ou à rayonnement modulées de façon appropriée.

3.1.3 étiquette d'identification par radiofréquence (RFID) [ISO/CEI 19762-3]: tout transpondeur associé au mécanisme de stockage d'informations relié à un objet donné.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 consentement: disposition d'un accord d'acceptation expresse ou d'exclusion expresse quant à la collecte, le transfert, l'utilisation, le stockage, l'archivage ou la suppression d'informations PII particulières par un maître de fichier; il définit un accord particulier et limité.

3.2.2 maître de fichier: entité reliant les informations d'objet enregistrées dans l'étiquette RFID aux informations PII, ou enregistrant des PII dans l'étiquette RFID, ou collectant les PII enregistrées dans cette dernière.

3.2.3 personne concernée: entité qui peut être identifiée par une ou plusieurs données relatives à ses attributs physiques, physiologiques, mentaux, financiers, culturels ou sociaux.

3.2.4 formule de l'acceptation expresse ("*opt-in*"): consentement exprès donné par un individu à un contrôleur de PII pour collecter, transférer, utiliser, stocker, archiver ou supprimer des informations PII particulières, à des fins spécifiques.

3.2.5 formule de l'exclusion expresse ("*opt-out*"): choix d'un individu, à sa demande, de refuser la collecte, le transfert, l'utilisation, le stockage, l'archivage ou la suppression de données particulières.

3.2.6 données à caractère personnel: voir informations d'identification personnelle. Ces deux termes sont synonymes.

3.2.7 fabricant de systèmes d'identification par radiofréquence (RFID): toute entité assurant la fabrication et la vente de puces/étiquettes RFID ou la fabrication (y compris le traitement ou le conditionnement) et la vente d'objets intégrant des étiquettes RFID.

3.2.8 fournisseur de services d'identification par radiofréquence (RFID): toute entité offrant un service fondé sur des objets auxquels sont intégrées ou jointes des étiquettes RFID.

3.2.9 utilisateur: personne qui acquiert un objet auquel est intégrée ou jointe une étiquette RFID, ou qui utilise le service fondé sur un objet auquel est intégrée ou jointe une étiquette RFID.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AES norme de chiffrement perfectionné (*advanced encryption standard*)

NFC communication en champ proche (*near field communication*)

PDA assistant numérique personnel (*personal digital assistant*)

PIA évaluation des incidences sur la vie privée (*privacy impact assessment*)

PII informations d'identification personnelle (*personally identifiable information*)

RFID identification par radiofréquence (*radio frequency identification*)

5 Conventions

Sans objet.

6 Principes relatifs à la vie privée

Les lignes directrices décrites dans la présente Recommandation reposent sur les principes relatifs à la vie privée énoncés dans les documents suivants: [b-Conseil de l'Europe], [b-CE1], [b-CE2], [b-OCDE] et [b-HCNUR]. Il s'agit notamment des principes de:

– Limitation en matière de collecte: il conviendrait d'assigner des limites à la collecte des données à caractère personnel, et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

– Qualité des données: les données à caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

– Spécification des finalités: les finalités en vue desquelles les données à caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

– Limitation de l'utilisation: les données à caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe ci-dessus.

– Garanties de sécurité: il conviendrait de protéger les données à caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation ou divulgation non autorisés.

– Transparence: il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données à caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données à caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

– Participation individuelle: toute personne physique devrait avoir le droit:

  a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

  b) de se faire communiquer les données la concernant dans un délai raisonnable; moyennant, éventuellement, une redevance modérée; selon des modalités raisonnables; et sous une forme qui lui soit aisément intelligible;

  c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet; et

  d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

– Responsabilité: tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

7 Menaces et atteintes pour les informations PII dans l'environnement RFID

Les menaces et atteintes pour les informations PII dans l'environnement RFID peuvent être imputables aux caractéristiques de la technologie RFID "sans contact", aux vulnérabilités de la communication hertzienne et, éventuellement, à la collecte d'informations par un tiers au moyen d'un lecteur RFID. L'Appendice II décrit en détail les caractéristiques de la technologie RFID.

En outre, il existe un risque accru d'atteinte aux informations PII imputable à la mise en œuvre de la technologie RFID, dans la mesure où les informations obtenues par un maître de fichier à partir de l'étiquette RFID peuvent être utilisées dans l'ensemble du réseau, sans se conformer à la législation, aux politiques et aux règlements nationaux ou régionaux. Ces informations peuvent également être modifiées de manière à obtenir les informations PII. Le paragraphe qui suit décrit les principales menaces et atteintes pour les informations PII liées à la technologie RFID.

Il convient toutefois de souligner qu'il peut être difficile d'intégrer certains mécanismes de sécurité dans l'étiquette RFID, en raison des ressources que celle-ci peut utiliser, par exemple, l'alimentation électrique, le temps de traitement, l'espace de stockage, etc. Les Appendices I et II décrivent les restrictions liées à la technologie RFID et les mesures techniques nécessaires pour assurer la protection des systèmes RFID.

7.1 Invisibilité de la collecte de données

En raison des caractéristiques particulières de la technologie RFID, des données peuvent être collectées sans que la personne concernée n'en soit informée. Il est possible de lire les données d'une étiquette RFID sans visibilité directe, car les ondes radio pénètrent des obstacles, tels que des sacs ou des vêtements, et toute personne en possession d'un lecteur peut lire les données contenues dans une étiquette RFID. En outre, les étiquettes et les lecteurs RFID peuvent être de très petite taille et leur utilisation peu passer inaperçue. Cette particularité de la technologie RFID peut être une des causes d'atteinte pour les informations PII.

7.2 Profilage

L'accès aux informations d'étiquette RFID d'un objet détenu ou transporté par une personne concernée peut révéler les aspects privés de ses préférences. En particulier, les profils et les inférences pouvant être extraits d'un groupe d'étiquettes RFID transportées par une personne concernée pourraient révéler des informations importantes. Dans des applications, comme le passeport électronique ou les soins de santé, la technologie RFID pourrait permettre également de révéler des informations encore plus sensibles, comme la nationalité, les données biométriques ou les dossiers médicaux, informations qui pourraient être directement utilisées pour établir les profils et les inférences se rapportant à la personne concernée.

7.3 Traçage

Il est possible de tracer des personnes transportant une étiquette RFID, dans la mesure où un identificateur unique est attribué à cette étiquette.

Ce traçage se fait par la collecte ou le traitement des données de localisation et de temps, soit a posteriori, les données étant déjà stockées dans une base de données, soit en temps réel.

8 Applications RFID

La technologie RFID est largement utilisée dans diverses applications, telles que les soins de santé, le transport et la logistique, le cybergouvernement ou les services d'information, dans la chaîne de vente au détail et de distribution. Le Tableau 1 présente les menaces pour les informations PII qui peuvent exister dans des applications types utilisant la technologie RFID.

Tableau 1 – Applications RFID types et menaces possibles pour les informations PII

Domaine	Applications types	Informations contenues dans une étiquette RFID	Menaces possibles pour la vie privée
Chaîne de distribution	Gestion des stocks	Produit	Traçage, profilage de personnes, réalisation d'inventaires
	Vente au détail (p. ex., supermarché)	Produit	Traçage, profilage (après l'achat de marchandise)
Transport et logistique	Billet de transport public	Identificateur de l'utilisateur, tarification, etc.	Traçage, profilage
	Péage autoroutier	Identificateur de l'utilisateur, tarification, etc.	Traçage, profilage
	Traçage du véhicule	Produit	Traçage, profilage
	Gestion de parcs de véhicules/de conteneurs	Produit	Traçage, profilage de personnes, manipulation de conteneurs
Soins de santé	Traçage de patients	Identificateur du patient, antécédents médicaux, etc.	Traçage, profilage, invisibilité
	Prévention d'erreurs de médication	Identificateur du patient, antécédents médicaux, ordonnances, etc.	Traçage, profilage
	Traçage d'échantillons sanguins ou de médicaments à des fins de lutte contre la contrefaçon	Produit	×
Cybergouvernement	Passeport électronique	Identificateur, nationalité, données biométriques d'individus	Traçage, profilage, contrefaçon PII
Services d'information	Affiche intelligente	Produit	×

Comme le montre le Tableau 1, toutes les applications RFID ne suscitent pas des craintes d'atteinte pour les informations PII (ni d'éventuels problèmes). Si l'application RFID ne concerne pas l'utilisateur, par exemple, dans certaines applications de chaîne de distribution, il n'y aura probablement pas de risques d'atteinte pour les informations PII.

Cependant, si, par exemple, des travailleurs manipulent des conteneurs dans le cadre d'autres applications relatives à la chaîne de distribution, leur activité peut être contrôlée à l'aide des étiquettes RFID.

Les paragraphes qui suivent présentent certains exemples d'applications concernant des scénarios de services pouvant susciter des craintes d'atteinte pour les informations PII.

La combinaison de lecteurs RFID avec d'autres applications (par exemple, mobiles) permet d'établir diverses relations de communication pouvant donner lieu à des capacités améliorées de traçage et de profilage.

8.1 Gestion de chaînes de distribution

La technologie RFID est largement utilisée depuis longtemps pour la gestion de chaînes de distribution. Parmi les applications commerciales essentielles de la gestion de chaînes de distribution utilisant la technologie RFID figure la gestion de stocks/de biens ou encore le commerce de détail. Cette dernière application est la plus représentative des applications utilisant la technologie RFID. La Figure 1 donne un exemple d'utilisation de la technologie RFID dans une application de commerce de détail, illustrant le changement d'une étiquette RFID.

Les applications de commerce dedétail utilisant la technologie RFID peuvent être mises en œuvre après qu'un fabricant a créé une étiquette RFID, a saisi des informations d'objet dans cette étiquette et a joint cette étiquette à l'objet. Dans cet exemple, le détaillant en question est un fournisseur de services RFID vendant à un utilisateur un objet auquel est apposée une étiquette RFID. Dans le cas de la gestion de chaînes de distribution, les étiquettes passives sont généralement utilisées par le système RFID, au moyen notamment des mots de passe "kill", afin de protéger les informations PII de la personne concernée. Dans certains cas, comme les applications concernant des articles individuels, la gestion de la chaîne de distribution nécessite souvent l'utilisation d'étiquettes passives avec une longue portée de communication, et ceci même pour des articles unitaires.

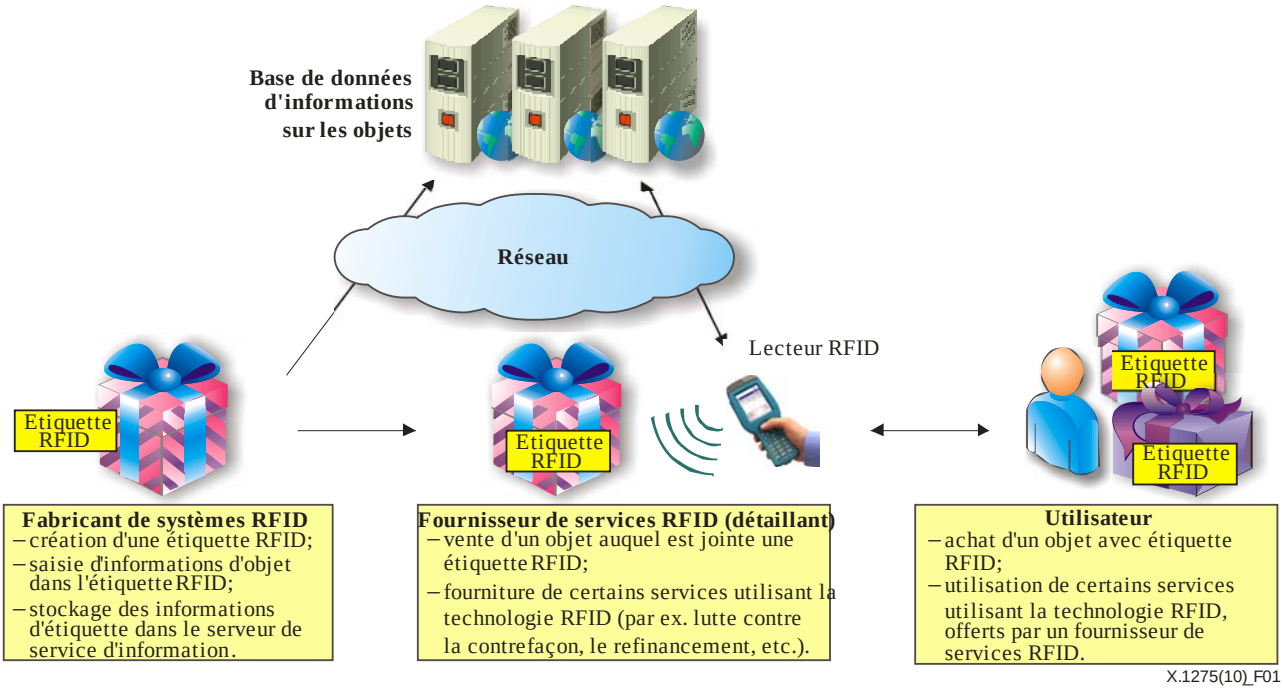


Figure 1 – Exemple d'utilisation de la technologie RFID dans des applications de commerce de détail

Une application de commerce de détail suscite des craintes d'atteinte aux informations PII essentiellement après qu'un utilisateur a acheté un objet auquel est jointe une étiquette RFID, étant donné que la participation de l'utilisateur au point de vente intervient uniquement à ce moment-là. Lorsqu'un utilisateur achète un objet auquel est jointe une étiquette RFID, le détaillant peut identifier les préférences de cet utilisateur en reliant les informations d'objet stockées dans l'étiquette RFID aux informations de paiement de l'utilisateur ou à sa carte de fidélité et en observant et analysant de façon continue le profil d'achat de l'utilisateur. Dans ce cas, le fournisseur de services RFID devient le maître de fichier et l'utilisateur la personne concernée. A moins qu'elle soit supprimée ou détruite, l'étiquette RFID peut alors être lue par quiconque est en possession d'un lecteur.

8.2 Transport et logistique

Les systèmes RFID sont bien adaptés à certaines applications de transport et logistique. Compte tenu d'une répartition appropriée de lecteurs RFID, les véhicules équipés d'une étiquette peuvent être tracés dans une petite zone, par exemple un entrepôt ou une usine. En revanche, les billets de transport public et les systèmes de péage autoroutier, tels que ceux qui sont décrits dans le Document [b-E-Zpass], sont des applications qui peuvent susciter des craintes liées à la vie privée dans les secteurs du transport ou de la logistique.

On distingue plusieurs applications de technologie RFID dans les secteurs du transport et de la logistique. En particulier, un nombre de billets de transport public et de systèmes de péage autoroutier utilisent déjà la technologie RFID. La Figure 2 donne un exemple d'application de transport illustrant la manière dont une étiquette RFID est utilisée pour l'identification et le traçage d'un véhicule dans le système de péage autoroutier.

Dans une application de péage autoroutier, le fabricant de systèmes RFID réalise simplement une étiquette RFID et la vend au fournisseur de services RFID. Le fournisseur de services RFID qui offre et gère un service de péage autoroutier peut saisir, dans certains cas particuliers, les informations de paiement d'un utilisateur dans une étiquette RFID. Ces informations sont des informations PII qui peuvent être utilisées pour identifier facilement cet utilisateur.

Si les informations de paiement de l'utilisateur sont associées aux informations de localisation de l'utilisateur, telles qu'elles sont enregistrées par le système de péage autoroutier, elles peuvent alors constituer une menace sérieuse pour sa vie privée. Dans ce cas, le fournisseur de services RFID (le système de péage autoroutier) devient le maître de fichier et l'utilisateur, la personne concernée.

Dans les secteurs du transport et de la logistique, les systèmes RFID utilisent généralement des étiquettes passives. En ce qui concerne le transport, des systèmes cryptographiques simples (basés sur un système de chiffrement symétrique) sont souvent utilisés pour authentifier réciproquement l'étiquette et le lecteur et sécuriser la transmission de données qui s'ensuit.

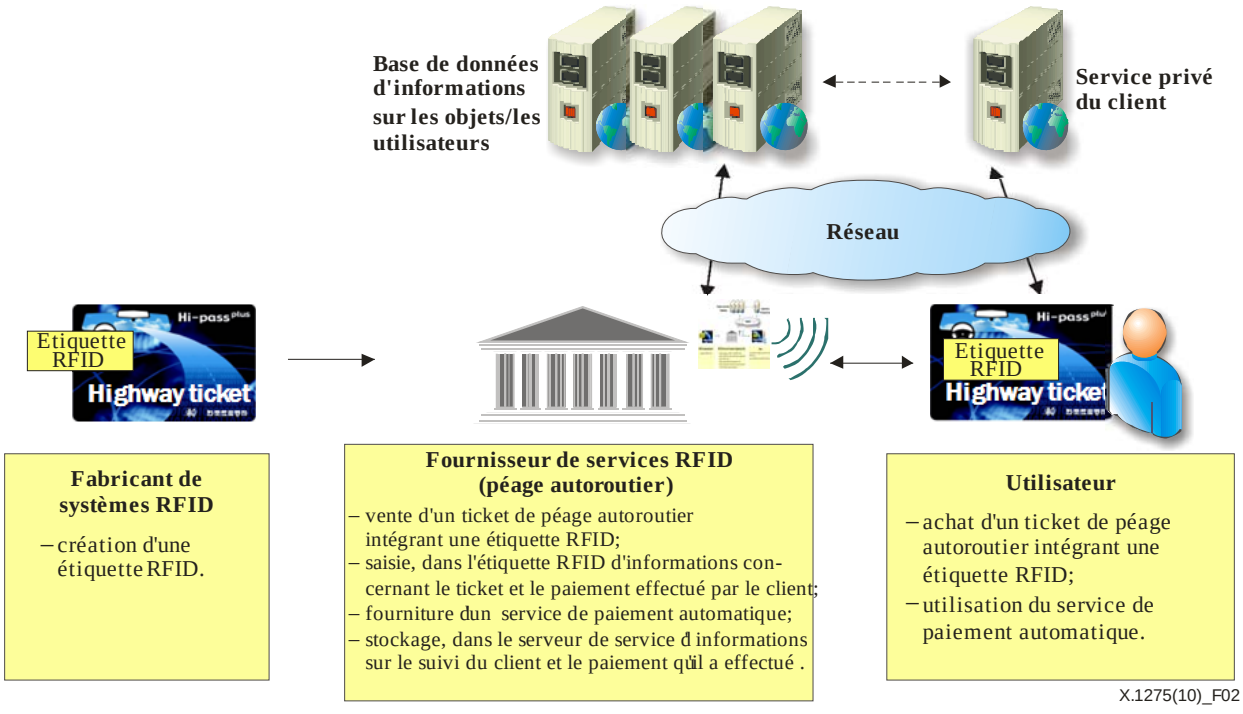


Figure 2 – Exemple d'utilisation de la technologie RFID dans les secteurs du transport et de la logistique

Pour ce qui est des billets de transport public, une carte intelligente "sans contact", équipée d'une puce RFID fonctionnant à 13,56 MHz avec une courte portée de communication, est fréquemment utilisée. Dans le cas d'une étiquette ayant une courte portée de lecture, comme ici, il est possible, tout du moins techniquement, d'utiliser des systèmes cryptographiques conventionnels sécurisés (et même des système asymétriques) – ce qui peut limiter partiellement le risque de divulgation des informations PII de la personne concernée. A noter toutefois que les protocoles actuellement utilisés peuvent uniquement empêcher la copie d'une étiquette (et donc l'usurpation de l'identité de l'utilisateur). Il n'en reste pas moins que l'identificateur d'étiquette apparaît toujours en clair au début de la transaction entre l'étiquette et le lecteur. Il peut dès lors être lu par n'importe qui, d'où un risque d'atteinte aux informations PII associées. Dans tous les cas, les données recueillies dans la base lorsque l'utilisateur interagit avec le système devraient être rendues anonymes dès que possible, de manière à réduire les risques d'atteinte à la vie privée.

8.3 Soins de santé et médecine

La technologie RFID offre plusieurs applications dans le domaine des soins de santé, mais son utilisation peut susciter certaines craintes quant à la confidentialité des informations PII du fait du caractère sensible des données relatives aux soins de santé sur le plan de la vie privée. Parmi les diverses applications de la technologie RFID dans le secteur des soins de santé, on peut citer le traçage des patients pour des raisons de sécurité et de sûreté, ainsi que des médicaments, afin de lutter contre la contrefaçon, le respect de l'ordonnance du patient, ou encore le traçage des échantillons sanguins. Les systèmes RFID sont déjà utilisés dans le secteur pharmaceutique pour faciliter le traçage des médicaments et pour prévenir la contrefaçon et les pertes résultant d'un vol au cours du transport. La Figure 3 donne un exemple d'utilisation de la technologie RFID dans les secteurs des soins de santé et illustre la manière dont une étiquette RFID est employée.

Le fabricant de systèmes RFID pour les applications visant au respect des ordonnances des patients réalise simplement une étiquette RFID et la vend au fournisseur de services RFID. Les fournisseurs de services RFID (les médecins et les infirmières de l'hôpital) peuvent devenir les maîtres de fichiers qui saisissent et gèrent les informations médicales du patient.

Dans l'application présentée dans la Figure 3, les médecins ou les infirmières de l'hôpital peuvent assurer le suivi du traitement du patient et veiller au respect des ordonnances de celui-ci en lisant les informations de l'étiquette RFID associée au patient et, à partir de ces informations, prendre les mesures qui s'imposent. En revanche, pour ce qui est du traçage des médicaments, les informations d'étiquette concernant la personne en possession des médicaments à l'extérieur de l'hôpital ou de la pharmacie peuvent facilement être divulguées. Il serait également possible de déduire directement de quelle maladie souffre le patient à partir des informations de l'étiquette RFID. Ainsi, le risque de divulgation des informations personnelles de la personne concernée dans cette application peut être supérieur à celui concernant l'application décrite dans la Figure 2. Par conséquent, si les informations médicales du patient, telles qu'elles sont stockées dans une étiquette RFID ou dans une base de données principale, ne sont pas correctement gérées et protégées, les informations PII de la personne concernée pourraient être directement menacées.

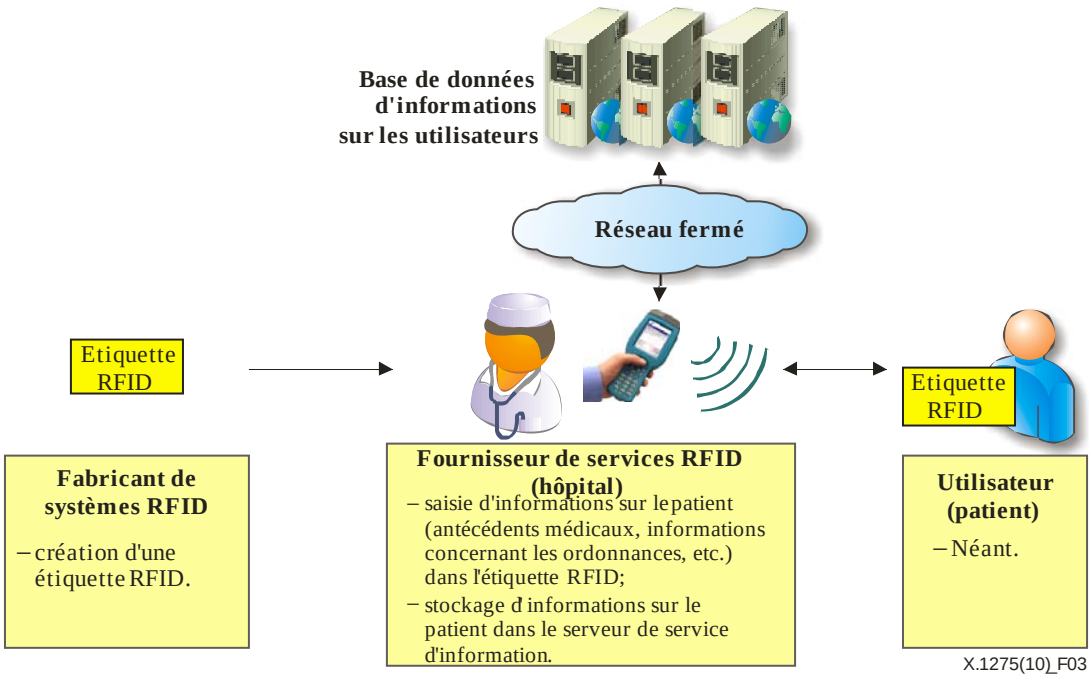


Figure 3 – Exemple d'utilisation de la technologie RFID dans les secteurs de la médecine et des soins de santé

Les étiquettes actives des systèmes RFID utilisés pour les secteurs de la médecine et des soins de santé ont généralement une courte portée de communication. Toutefois, il existe certains cas dans lesquels il peut être préférable d'utiliser des étiquettes actives avec longue portée de communication, par exemple pour les soins à domicile, afin de surveiller l'état de santé d'une personne handicapée.

8.4 Cybergouvernement

Dans le domaine du cybergouvernement, le passeport électronique est l'application la plus courante. La puce RFID intégrée au passeport électronique comporte généralement un grand nombre des informations PII de la personne concernée, telles que le numéro de son passeport, son nom, sa nationalité, sa photographie, ses données biométriques, etc. Les risques potentiels d'atteinte à la confidentialité des informations PII peuvent donc être importants.

Il est indispensable d'intégrer à l'étiquette RFID des mesures de sécurité propres à atténuer les risques d'interception ou de clonage des données contenues dans un passeport électronique, étant donné que celles-ci représentent les informations PII les plus importantes et les plus sensibles. La Figure 4 donne un exemple d'utilisation de la technologie RFID dans le système de passeport électronique et illustre la manière dont une puce RFID est employée.

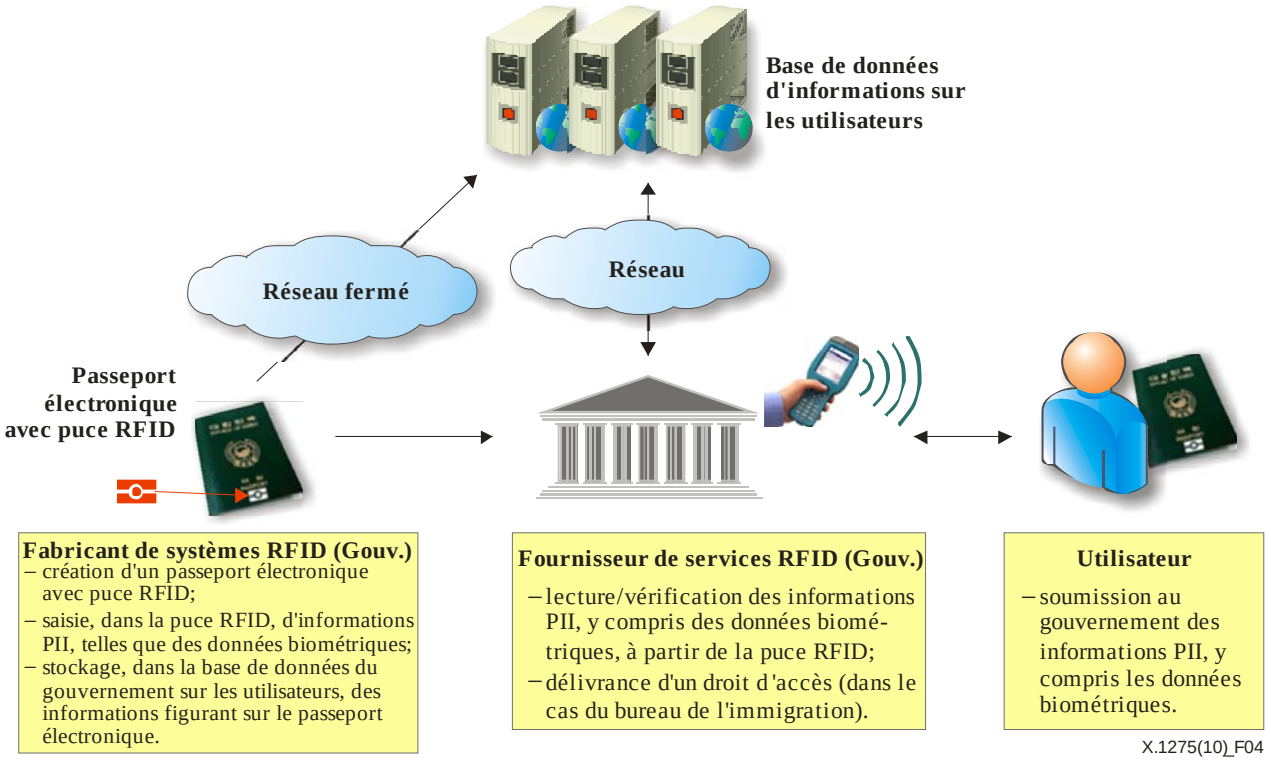


Figure 4 – Exemple d'utilisation de la technologie RFID dans les applications de passeport électronique

Tout utilisateur qui souhaite obtenir un passeport électronique biométrique soumet à l'administration (qui peut être le fabricant des puces RFID utilisées dans les passeports électroniques), des informations PII, notamment des données biométriques. Le passeport électronique est réalisé avec une puce RFID et les informations PII de l'utilisateur, y compris les données biométriques, sont saisies dans la puce RFID. Le fournisseur de services RFID, par exemple le bureau de l'immigration, lit les informations PII à partir de la puce RFID et les vérifie. Les données biométriques stockées dans la puce RFID du passeport électronique comptent parmi les informations PII les plus sensibles, car elles peuvent servir à authentifier ou à identifier l'utilisateur. Si elles sont divulguées ou modifiées, ces données biométriques constitueraient une menace sérieuse pour la vie privée de l'utilisateur. Dans cette application, aussi bien le fabricant de systèmes RFID que le fournisseur de services RFID peuvent être le maître de fichier; l'utilisateur est la personne concernée. Les étiquettes passives à courte portée de communication sont généralement utilisées dans cette application. Le passeport électronique doit pouvoir prendre en charge la cryptographie.

Cela étant, il arrive que les protocoles de sécurité décrits dans les normes telles que [b-OACI] soient parfois facultatifs ou qu'ils soient mal employés. Par conséquent, les applications de passeport électronique suscitent toujours de grandes craintes à l'égard de la vie privée.

8.5 Service d'information

L'affiche intelligente (*smart poster*) est l'une des applications caractéristiques des applications de service d'information. Dans ce cas, un lecteur RFID est généralement intégré à un dispositif mobile, l'étiquette RFID restant en un lieu fixe. La Figure 5 donne un exemple d'utilisation de la technologie RFID dans une application d'affiche intelligente et illustre la manière dont l'étiquette et le lecteur RFID sont employés.

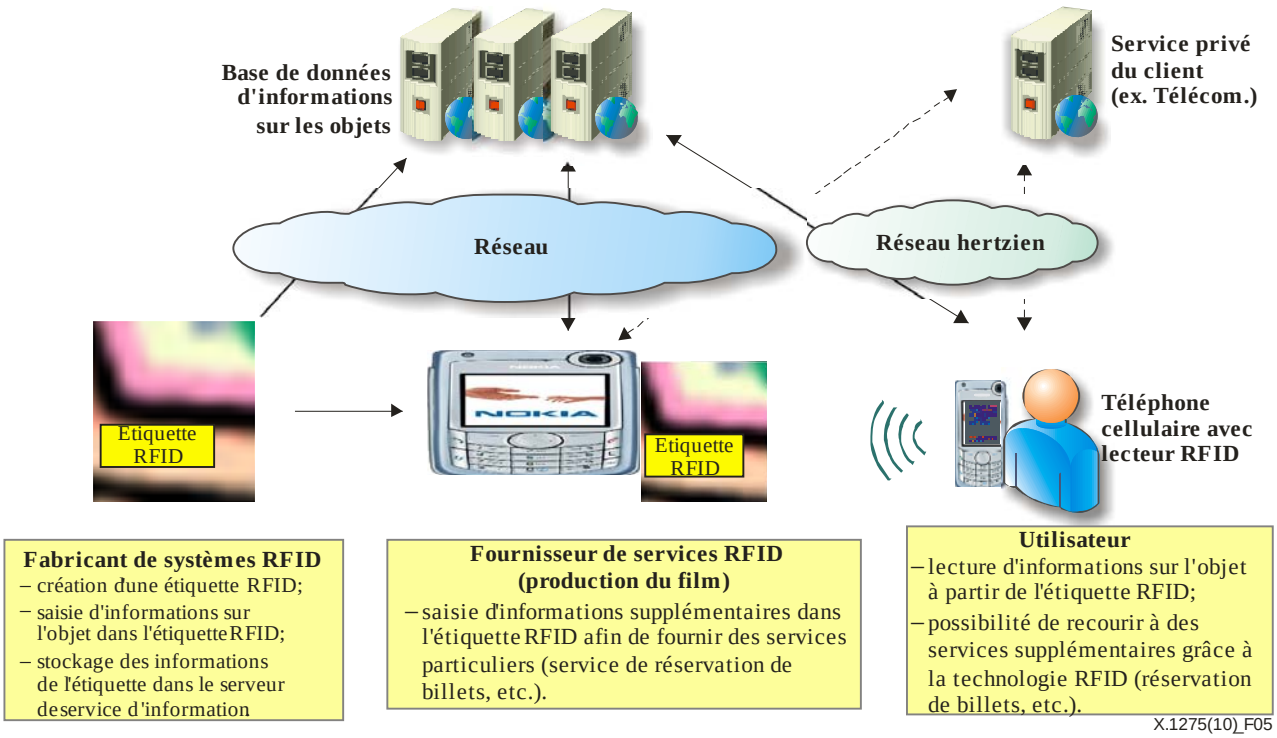


Figure 5 – Exemple d'utilisation de la technologie RFID dans une application d'affiche intelligente

Le fabricant RFID d'une affiche intelligente réalise simplement une puce RFID et la vend au fournisseur de services RFID qui, dans ce cas, est la production du film ou le cinéma projetant ce dernier. Le fournisseur saisit des informations sur le film dans l'étiquette RFID intégrée à l'affiche intelligente. Parmi les autres exemples de service d'information utilisant la technologie RFID, on peut citer le service de guidage routier, qui donne à l'utilisateur des informations sur la manière de calculer facilement un itinéraire. En pratique, ces types d'applications ne suscitent pas de craintes à l'égard de la vie privée, car elles n'utilisent pas d'informations privées ou sensibles. A noter toutefois que la mobilité et la portée de lecture du lecteur RFID intégré à un dispositif mobile sont des facteurs qui peuvent menacer la vie privée des utilisateurs.

9 Lignes directrices relatives à la protection des informations d'identification personnelle

Etant donné que les technologies utilisées pour garantir la vie privée et la sécurité dans les systèmes RFID sont encore à un stade précoce, alors même que leur mise en œuvre est en cours (il n'existe pas de solution "toute faite" car le contexte d'utilisation et les caractéristiques techniques des étiquettes RFID diffèrent grandement d'une application à l'autre), il serait prématuré de les appliquer à l'ensemble du service RFID. Par conséquent, les présentes lignes directrices portent essentiellement sur les mesures de gestion générales visant à protéger les informations PII de la personne concernée, plutôt que sur les mesures techniques. Cela étant, il ne faudrait pas négliger ces dernières: au cours de la conception d'une application reposant sur la technologie RFID, les concepteurs sont encouragés à envisager l'adoption de solutions techniques de pointe susceptibles de renforcer la protection de la vie privée.

9.1 Politiques et procédures

Dans le service RFID, il convient que les maîtres de fichiers définissent des politiques et des procédures régissant le système RFID en question, notamment en ce qui concerne l'utilisation appropriée des informations PII, et qu'ils les publient à l'avance. Ces politiques et procédures

devraient en outre prévoir la répartition des rôles et des responsabilités concernant la gestion et l'utilisation de ces informations. Par ailleurs, le maître de fichier devrait attribuer davantage de responsabilités à la personne chargée directement de la gestion et de l'utilisation des informations PII.

9.2 Restrictions liées à l'enregistrement des informations PII

Les maîtres de fichiers devraient respecter le principe de limitation en matière de collecte. Par conséquent, un maître de fichier ne devrait traiter que les données en rapport avec la finalité pour laquelle le système a été conçu et les informations PII ne devraient pas être conservées plus longtemps que nécessaire.

Plus particulièrement, dans le service RFID, les maîtres de fichiers ne doivent pas, en principe, enregistrer les informations PII dans l'étiquette RFID, à moins que cela ne soit prévu par la loi ou que la personne concernée ait donné son consentement exprès, par écrit.

Si des maîtres de fichiers doivent enregistrer des informations PII dans une étiquette RFID, toutes ces informations doivent être chiffrées. Lorsque les maîtres de fichiers ont besoin de l'accord de la personne concernée, on devrait privilégier la formule de l'acceptation expresse. Les maîtres de fichiers doivent, au préalable, indiquer à la personne concernée à quelle fin les informations PII sont enregistrées et l'usage qu'il pourra être fait de ces informations.

Les maîtres de fichiers dans le service RFID doivent obtenir un consentement distinct et spécifique pour chaque élément d'information PII enregistré et expliquer aux personnes concernées à quelle fin les informations PII sont enregistrées ou utilisées.

9.3 Information, consentement, droit d'accès, rectification, droit d'opposition

Il convient que les maîtres de fichiers respectent le principe de participation individuelle. Par conséquent, dans le service RFID, les maîtres de fichiers doivent faire le nécessaire pour fournir à l'utilisateur des renseignements sur les informations PII enregistrées ainsi que sur le consentement de la personne concernée et son droit d'accès, de rectification et d'opposition en ce qui concerne ses informations PII, sans frais pour l'utilisateur. Cela s'applique aux informations PII codées sur les étiquettes RFID ainsi qu'à celles reliées aux informations enregistrées sur ces étiquettes.

9.3.1 Information

La personne concernée devrait être informée par les maîtres de fichiers des indications de l'étiquette RFID jointe et de l'installation du lecteur RFID, des parties tierces auxquelles les données ont été communiquées et de la modification, de la suppression ou du blocage des données, à moins que cela ne s'avère impossible ou excessivement complexe.

9.3.1.1 Indication de l'étiquette RFID jointe

En cas d'utilisation d'une étiquette RFID intégrée ou jointe, même après que l'utilisateur a acheté ou reçu l'objet en question, les maîtres de fichiers doivent, dans le service RFID, communiquer au préalable à l'utilisateur (avant l'achat de l'objet) les informations qui suivent, les faire figurer sur l'objet, ou encore utiliser un moyen qui soit facilement perceptible:

– la présence d'une étiquette RFID jointe et son emplacement;
– la nature et la fonction de l'étiquette RFID;
– le type d'informations enregistrées dans l'étiquette RFID;
– l'objet ou l'utilisation des informations enregistrées dans l'étiquette RFID;
– les coordonnées du responsable de la protection des données, conformément au § 9.9.

Il est à noter que, si la personne concernée n'est pas censée utiliser l'étiquette après avoir acquis l'objet, celle-ci devrait être désactivée par le service RFID ou les maîtres de fichiers au moment de l'achat par l'utilisateur, à moins que ce dernier ne décide de la laisser en activité.

9.3.1.2 Indication de l'installation du lecteur RFID

Toute personne qui souhaite installer un lecteur capable de lire les informations concernant un objet auquel est intégrée ou jointe une étiquette RFID (ou les informations PII enregistrées dans l'étiquette RFID et diffusées aux personnes concernées) doit indiquer le lieu où est installé le lecteur – par exemple, en caisse – et les raisons de cette installation, de telle sorte que les personnes concernées puissent facilement remarquer sa présence. L'annonce doit au moins faire mention du nom de l'opérateur ainsi que d'un point de contact où obtenir un ensemble d'informations sur le service.

Si un lecteur RFID est intégré à un assistant numérique (PDA) ou à un téléphone cellulaire personnels, sa portée de lecture doit être restreinte afin de limiter l'acquisition d'informations PII à partir de l'étiquette RFID.

9.3.2 Consentement

Les maîtres de fichiers doivent obtenir le consentement préalable de la personne concernée. Dans les domaines de la vente au détail et de la logistique, où l'on applique par défaut le principe de la désactivation, les maîtres de fichiers peuvent obtenir le consentement de la personne concernée par le biais d'un accord écrit spécifique, d'un formulaire d'inscription de l'utilisateur, d'un courrier électronique, etc. Dans les autres cas, notamment pour les passeports électroniques biométriques, il n'est pas nécessaire d'obtenir le consentement de l'utilisateur puisque la loi fait obligation de collecter les informations PII et de les stocker dans l'étiquette.

9.3.3 Droit d'accès, rectification et droit d'opposition

La personne concernée devrait pouvoir obtenir du maître de fichier, à intervalles raisonnables, sans rencontrer d'obstacle et sans que cela ne demande trop de temps ni n'entraîne de dépenses excessives:

– qu'il lui confirme si les données le concernant sont ou non en cours de traitement et lui indique au moins la finalité du traitement, les données concernées et les destinataires ou catégories de destinataires auxquels ces données sont communiquées;

– qu'il lui fournisse des informations intelligibles au sujet du processus en cours ainsi que les informations disponibles concernant l'origine des données;

– qu'il lui explique la logique du traitement automatique des données, s'il y a lieu, au moins dans le cas de décisions automatisées.

En outre, dans le service RFID, les maîtres de fichiers doivent faire le nécessaire pour mettre à la disposition de l'utilisateur une méthode lui permettant de corriger, modifier et détruire les informations PII le concernant, sans frais pour lui.

Cela vaut pour les informations PII codées dans les étiquettes RFID ainsi que pour les informations PII liées à celles stockées dans ces étiquettes.

Plus particulièrement, si l'étiquette n'est d'aucune utilité à la personne concernée (par exemple, dans le secteur de la vente au détail, lorsque l'utilisateur achète un produit étiqueté), les maîtres de fichiers doivent la désactiver, la retirer ou la détruire (voir le § 9.5), à moins que la personne concernée ne demande qu'elle reste activée.

9.4 Restriction de la collecte et de la mise en relation d'informations PII

Les maîtres de fichiers du service RFID devraient informer les personnes concernées lorsqu'ils procèdent à la collecte des informations PII enregistrées dans l'étiquette ou stockées dans une base

de données en les mettant en relation avec les informations d'objet enregistrées dans l'étiquette RFID. Si les fournisseur de services RFID doivent utiliser les informations PII à des fins différentes de celle qui est prévue ou les fournir à un tiers, il leur faut, au préalable, obtenir par écrit le consentement spécifique et éclairé de la personne concernée.

9.4.1 Informations PII enregistrées dans l'étiquette RFID

Dans le service RFID, lorsqu'ils peuvent collecter les informations PII enregistrées dans une étiquette RFID, les maîtres de fichiers doivent le signaler à la personne concernée ou l'indiquer d'une manière facilement perceptible; ils doivent en outre obtenir au préalable le consentement spécifique et éclairé de l'utilisateur.

Lorsqu'ils procèdent à la collecte d'informations PII, les maîtres de fichiers devraient prendre certaines mesures d'authentification pour le lecteur et l'étiquette RFID, telles que l'utilisation d'un protocole d'authentification entre l'étiquette et le lecteur RFID, ainsi qu'entre le lecteur et la base de données principale. Par "mesure d'authentification", on entend dans le présent document le système cryptographique utilisé pour la base de données principale stockant l'identificateur d'étiquette RFID ainsi que les informations PII utilisées pour identifier et authentifier le lecteur RFID et le maître de fichier.

Du point de vue de la protection des informations PII, il convient toutefois de noter que les protocoles d'authentification actuels entre l'étiquette et le lecteur ne sont efficaces que si les informations stockées dans l'étiquette ne se limitent pas à l'identificateur de l'étiquette, étant donné que, avec les protocoles de transmission RFID existants, cet identificateur n'est pas protégé.

9.4.2 Informations d'objet reliées aux informations PII dans l'étiquette RFID

Lorsqu'ils souhaitent relier les informations d'objet enregistrées dans l'étiquette RFID aux informations PII, les maîtres de fichiers devraient normalement, avant de fournir l'étiquette, en informer au préalable la personne concernée, l'indiquer de manière facilement perceptible et obtenir un consentement spécifique et éclairé. Lorsqu'ils relient les informations d'objet contenues dans l'étiquette RFID aux informations PII, les maîtres de fichiers devraient prendre certaines mesures d'authentification pour le lecteur RFID, telles que l'utilisation d'un mot de passe ou d'un protocole d'authentification entre le lecteur RFID et l'étiquette.

Si des informations PII qui n'étaient pas censées être reliées aux informations d'objet au moment de leur collecte doivent l'être ultérieurement, les maîtres de fichiers devraient en donner les raisons à l'utilisateur et obtenir à nouveau son consentement spécifique et éclairé, conformément aux dispositions juridiques.

9.5 Désactivation de l'étiquette RFID une fois son rôle accompli

Les étiquettes RFID intégrées ou jointes sont retirées, détruites ou désactivées définitivement par le fournisseur de services RFID ou le maître de fichier, au moment où l'objet étiqueté est acheté ou reçu par l'utilisateur (au point de vente), sauf si ce dernier décide de ne pas désactiver l'étiquette ou qu'une loi ou un règlement exige qu'elle soit maintenue en fonctionnement. Même lorsque l'utilisateur demande que l'étiquette reste active, les maîtres de fichiers devraient prendre des dispositions pour pouvoir la retirer, la détruire ou la désactiver définitivement si la personne concernée en fait la demande par la suite. L'utilisateur devrait en outre être informé des conséquences de la désactivation.

Si la désactivation devait être la règle générale, cette solution n'est cependant pas adaptée à toutes les applications. Par exemple, si l'on désactive l'étiquette qui est employée, dans l'application de soins de santé, pour accéder à l'historique du traitement du patient et aux informations relatives à ses ordonnances, il est possible que le suivi du traitement s'avère plus difficile. La désactivation des étiquettes peut être obligatoire dans les applications relatives à la chaîne d'approvisionnement, alors qu'elle sera laissée à l'appréciation de l'utilisateur dans les applications relatives au transport et à la

logistique. Dans le cas des applications de soins de santé et de cybergouvernement, il n'y a pas lieu de désactiver l'étiquette, pour des raisons de santé publique ou en vertu de la loi. Dans le service RFID, le fabricant de systèmes RFID ou le maître de fichier peut prendre certaines mesures techniques pour désactiver l'étiquette RFID, en utilisant par exemple un mot de passe "kill" ou un désactivateur d'étiquettes RFID (*zapper*). Au cas où la désactivation d'une étiquette RFID nuirait à l'intérêt de l'utilisateur ou à l'intérêt public, les maîtres de fichiers devraient en donner les raisons à l'utilisateur, ou indiquer ces raisons sur l'objet en question, ou bien utiliser des moyens facilement perceptibles.

9.6 Informations relatives aux fournisseurs de services et aux maîtres de fichiers

Les fournisseurs de services et les maîtres de fichiers devraient élaborer et publier, pour chacune de leurs applications, un ensemble d'informations concises, précises et intelligibles dans lequel ils devraient au moins:

– mentionner l'identité et l'adresse des maîtres de fichiers;

– présenter la finalité du système RFID;

– préciser quelles données seront traitées par le système, en particulier s'il s'agit de données personnelles, et si la localisation des étiquettes fera l'objet d'un suivi;

– donner un résumé de l'évaluation des incidences sur la vie privée et sur la protection des données;

– présenter, le cas échéant, les risques potentiels pour la vie privée découlant de l'utilisation des étiquettes par l'application en question et les mesures que les personnes peuvent prendre pour atténuer ces risques.

9.7 Mesures organisationnelles et techniques pour la protection des informations PII

– Lorsqu'ils utilisent le système RFID pour enregistrer et collecter des informations PII, ou pour relier à celles-ci les informations sur l'objet contenues dans l'étiquette, les maîtres de fichiers devraient prendre des mesures de sécurité, sur le plan organisationnel et technique, visant à protéger les informations PII du système RFID en cas de perte, vol, divulgation, altération ou détérioration. Exemples de mesures organisationnelles et opérationnelles de protection des informations PII:

  • établissement d'un plan de gestion interne de la sécurité;

  • analyse des risques, analyse des menaces à la vie privée et évaluation des incidences sur la vie privée;

  • formation en matière de protection de la vie privée dans le service RFID.

– Exemples de mesures techniques pour la protection des informations PII:

  • contrôle et vérification de l'accès à la base de données principale;

  • contrôle de l'accès pour éviter qu'un lecteur n'accède aux informations stockées dans l'étiquette;

  • chiffrement des informations PII stockées dans l'étiquette et dans la base de données principale;

  • utilisation d'un protocole acceptable entre le lecteur et l'étiquette afin de protéger la transmission des informations PII, par exemple, un protocole de cryptographie ou toute technique pertinente;

  • utilisation d'étiquettes avec un identificateur aléatoire de manière à réduire les risques de traçage;

  • authentification du lecteur RFID valide;

- désactivation de l'étiquette RFID au moyen, par exemple, d'un mot de passe "kill" ou d'un désactivateur d'étiquettes RFID (*zapper*);
- restriction des fonctionnalités du lecteur et de l'étiquette au moyen par exemple d'un brouillage actif (*active jamming*), d'un système de détection des capteurs RFID, d'une étiquette à antenne détachable ("*clipped tag*"), d'une étiquette de blocage ("*blocker tag*"), etc. [b-Juels];
- adoption de mesures de sécurité afin d'atténuer les risques pour la vie privée identifiés par l'évaluation des incidences sur la vie privée (PIA, *privacy impact assessment*).

Il est à noter que les mesures organisationnelles et techniques mentionnées ci-dessus font partie de l'ensemble des mesures destinées à protéger les informations PII. De nouvelles mesures pourraient venir s'y ajouter, à l'avenir, en raison des recherches en cours dans ce domaine.

9.8 Evaluation des incidences du système RFID sur la vie privée

Lorsque des fournisseurs de services RFID ou des maîtres de fichiers utilisent le système RFID pour enregistrer et collecter des informations PII ou pour relier à celles-ci les informations sur l'objet contenues dans l'étiquette RFID, ils devraient s'assurer, avant la mise en œuvre du système RFID, idéalement au moment de sa conception, que la sécurité des informations PII n'est pas compromise, en analysant et évaluant tout risque de divulgation de ces informations ou toute menace à leur égard associé à l'utilisation du système RFID en question.

Compte tenu de la grande diversité de configurations techniques et de scénarios d'utilisation, il n'existe pas de solution "toute faite" applicable aux différentes applications RFID. La réalisation d'une évaluation des incidences des systèmes RFID sur la vie privée pourrait permettre de déterminer les conséquences que ces systèmes sont susceptibles d'avoir sur la vie privée (selon différents critères, notamment juridiques et techniques) et de définir les meilleures stratégies pour les limiter. Sont énoncées ci-après les étapes d'une procédure possible d'évaluation des incidences sur la vie privée (PIA). Cette évaluation devrait couvrir l'ensemble du système RFID:

– Etape 1: Lancement du projet

  Cette étape vise à déterminer le cadre des activités faisant l'objet de l'évaluation PIA, à constituer l'équipe chargée de l'évaluation et à appliquer les outils nécessaires à celle-ci, pour le domaine d'application défini.

– Etape 2: Analyse des flux de données

  Cette étape vise à établir un diagramme ou un graphique des informations d'identification personnelle, de façon à pouvoir vérifier la cible de l'analyse des risques en identifiant les informations d'identification personnelle gérées par le service visé par l'évaluation des incidences, ainsi que les produits d'information contenant ces informations.

  Cette étape consiste en particulier à identifier les informations PII qui sont collectées, utilisées, stockées, détruites ou fournies à un tiers au moyen d'un diagramme ou d'un graphique. Elle consiste également à décrire les rôles et responsabilités de la personne chargée de chaque opération (collecte, utilisation, stockage et destruction) du traitement des informations PII.

– Etape 3: Analyse des facteurs et des risques d'atteinte à la confidentialité des informations d'identification personnelle

  Cette étape vise à identifier les menaces et les vulnérabilités pour les actifs d'informations d'identification personnelle et à soumettre ces derniers à une analyse des risques.

– Etape 4: Plan d'amélioration et planification de la gestion des risques

  Cette étape consiste à déterminer le niveau de risque qu'il faut gérer parmi les divers risques identifiés au cours de l'analyse des risques concernant les informations d'identification personnelle, et à préparer les diverses méthodes de contrôle pour chaque risque devant être limité et géré.

– Etape 5: Communication des résultats de l'évaluation PIA

  Cette étape, l'une des plus importantes de la procédure PIA, consiste à élaborer et à soumettre des rapports sur la procédure PIA exécutée et sur les résultats obtenus.

  Les rapports PIA devraient porter sur les résultats des éléments examinés lors de chaque étape de la procédure PIA allant des résultats de l'évaluation PIA aux méthodes de contrôle et de gestion des risques identifiés pour les informations d'identification personnelle.

Il est à noter que la procédure d'évaluation PIA décrite ci-dessus est donnée à titre d'exemple uniquement et que la procédure d'évaluation PIA proprement dite peut être adaptée en fonction de besoins particuliers ou se baser sur des procédures d'évaluation PIA existant à l'extérieur.

9.9 Désignation d'un responsable de la protection des données

Les maîtres de fichiers devraient désigner un responsable de la protection des données, chargé en particulier de tenir un registre contenant des informations détaillées sur les opérations de traitement qu'ils réalisent, notamment sur les évaluations des incidences sur la vie privée et les mesures de sécurité des applications RFID, et de traiter rapidement les plaintes d'utilisateurs ou les demandes de ces derniers relatives à l'exercice de leurs droits.

Appendice I

Caractéristiques et restrictions des étiquettes RFID

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Classification des étiquettes RFID et caractéristiques de chaque catégorie

Le présent paragraphe vise à expliquer les caractéristiques des différents types d'étiquettes RFID, ainsi que les raisons pour lesquelles certaines techniques de sécurité ne peuvent pas être appliquées facilement aux étiquettes passives. Comme le montre le Tableau I.1 ci-dessous, on distingue généralement deux types d'étiquettes RFID: les étiquettes passives et les étiquettes actives.

Tableau I.1 – Classification des étiquettes RFID et caractéristiques de chaque catégorie

Caractéristiques	Etiquettes passives	Etiquettes actives
Source d'alimentation	Alimentation transférée depuis le lecteur	Batterie interne
Portée de communication	3 m ou moins	100 m ou plus
Durée de vie	Illimitée	Limitée par la durée de vie de la batterie
Stockage des données	Faible capacité – Accès en lecture/écriture (octets)	Grande capacité – Accès en lecture/écriture (kilooctets)
Applications types	Gestion des stocks, commerce de détail, contrôle de bagages/palettes, badges de sécurité, etc.	Applications complexes avec traçage de la personne, etc. (soins de santé ou surveillance de zones, péages autoroutiers, etc.)

Les étiquettes passives ne possèdent pas de source d'alimentation interne; elles utilisent la puissance transférée depuis le lecteur RFID pour envoyer un signal à ce dernier. Leur portée de communication est inférieure ou égale à 3 m environ. Dans le cas d'étiquettes fonctionnant à une fréquence de 13,56 MHz, la portée de communication sera comprise entre 4 et 10 cm environ, mais pourra être étendue à l'aide d'une antenne de grandes dimensions. Les étiquettes fonctionnant en ondes décimétriques ont une portée de communication plus grande (entre 3 et 7 m environ).

Contrairement aux étiquettes passives, les étiquettes actives possèdent leur propre source d'alimentation, qui leur permet d'envoyer elles-mêmes un signal au lecteur. La portée de communication des étiquettes actives est approximativement de 100 m ou plus, mais leur durée de vie est limitée à celle de leur batterie. Par ailleurs, les étiquettes actives sont plus grandes et plus coûteuses que les étiquettes passives.

En règle générale, un système fonctionnant dans la bande des basses fréquences (125/135 kHz) ou des hautes fréquences (13,56 MHz) est un système passif. Les systèmes fonctionnant dans les bandes des ondes décimétriques (433/900 MHz, 2,45 GHz) et des micro-ondes peuvent être soit passifs, soit actifs.

En raison de sa courte portée de balayage, l'étiquette à basses fréquences est essentiellement utilisée pour la sécurité, la gestion des biens et la vérification de l'authenticité d'un produit; l'étiquette à hautes fréquences, quant à elle, est utilisée essentiellement pour les services autoroutiers, la logistique et la distribution, sa portée de balayage étant de 30 m ou plus. En particulier, une étiquette à 13,50 MHz est incorporée et utilisée dans les cartes de crédit ou les cartes de paiement de taxes de transport. Le passeport électronique et les systèmes de communication en champ proche (NFC, *near field communication*) sont d'autres exemples d'applications utilisant une fréquence de 13,56 MHz.

I.2 Restrictions des étiquettes passives

De nombreux experts travaillant dans le secteur des systèmes RFID estiment que le prix d'une étiquette RFID devrait être inférieur à 5 cents afin de promouvoir le marché de cette technologie. Cette exigence limite les ressources pouvant être utilisées par une étiquette, comme la puissance électrique, le temps de traitement, l'espace de stockage ou le nombre de portes.

Une étiquette RFID coûtant moins de 5 cents peut contenir seulement une centaine de bits de données, posséder entre 5 000 et 10 000 portes logiques et avoir une portée de communication maximale de quelques mètres. Parmi les portes logiques, entre 250 et 3 000 portes seulement peuvent être consacrées à des fonctions de sécurité. Il convient en outre de tenir compte de restrictions de puissance, étant donné que la plupart des étiquettes RFID actuellement utilisées sont passives.

La législation limite souvent la puissance rayonnée des lecteurs, ce qui limite la puissance de l'étiquette. Compte tenu de la technologie actuelle, même sans contrainte budgétaire, seules les étiquettes passives de courte portée peuvent être équipées de systèmes cryptographiques standard sécurisés. Dans le cas des étiquettes d'une portée de plusieurs mètres, la puissance rayonnée par le lecteur n'est pas suffisante pour alimenter les nombreuses portes nécessaires pour mettre en œuvre des fonctions cryptographiques sécurisées.

Selon le document [b-CRYPTREC], entre 6 000 et 13 000 portes sont nécessaires pour appliquer un algorithme de chiffrement asymétrique, et un nombre analogue de portes est nécessaire pour implémenter une fonction de hachage. Par exemple, il faut entre 20 000 et 30 000 portes pour une implémentation standard de la norme de chiffrement perfectionné (AES, *advanced encryption standard*). Un algorithme de chiffrement simple destiné à être utilisé dans une étiquette RFID est en cours de développement. Toutefois, la mise en œuvre d'un algorithme de chiffrement dans une étiquette reste imparfaite en raison de ces restrictions liées aux ressources.

Appendice II

Mesures techniques de protection des informations PII dans le système RFID

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Diverses technologies de protection des informations PII sont actuellement mises au point pour limiter les menaces d'atteinte à la vie privée dans les services d'applications RFID. Etant donné que les techniques de chiffrement et d'authentification actuellement disponibles pour protéger la vie privée ne peuvent pas être appliquées aux étiquettes RFID, en raison de leurs ressources limitées, les nouvelles technologies décrites ci-dessous sont en particulier mises en œuvre.

II.1 Désactivation ("*kill*") de l'étiquette au moyen d'un mot de passe

Cette technique, qui est la plus courante pour protéger la vie privée de l'utilisateur, exploite le fait qu'une étiquette RFID peut être soit en phase "inactive" ("*kill*"), soit en phase "active". Lorsque cela est nécessaire, le lecteur envoie une commande de désactivation ("*kill*") comprenant un mot de passe (codé sur 32 bits) pour désactiver l'étiquette. Toutefois, cette fonction ne peut être utilisée que dans certaines applications, étant donné que la fonction d'identification automatique, qui constitue la force de la technologie RFID, ne peut pas être employée une fois que la commande "*kill*" a été appliquée. Par exemple, si la fonction d'étiquette du produit auquel est jointe une étiquette RFID est désactivée après l'achat, un retour ou un remboursement peut être impossible, étant donné que l'on ne pourra pas obtenir l'historique du produit en question. De surcroît, la désactivation d'étiquette n'est pas suffisamment sûre pour protéger les informations PII, car le mot de passe utilisé n'est codé que sur 32 bits et la fonctionnalité de désactivation peut également s'avérer vulnérable à une attaque par déni de service, par laquelle un pirate désactive toutes les étiquettes situées à sa proximité.

II.2 Protection de la vie privée au moyen d'une technique physique

II.2.1 Cage de Faraday

La cage de Faraday est une technologie qui empêche un lecteur RFID illicite de balayer les informations de l'étiquette en perturbant la transmission du signal hertzien du lecteur. Elle utilise pour cela une enceinte faite d'un matériau spécial faisant écran aux émissions radioélectriques. Une bobine métallique permet de bloquer le signal hertzien. Même si elle peut être utile pour certaines applications, la cage de Faraday présente un intérêt relativement limité, dans la mesure où la protection de la vie privée n'est plus assurée lorsque l'article en question est retiré de l'enceinte.

X.1275(10)_FII.1

Figure II.1 – Portefeuille doté d'une cage de Faraday

II.2.2 Etiquette de blocage

L'étiquette de blocage ("*blocker tag*") est une technologie qui a été développée en 2003 par la société RSA. Cette étiquette RFID spéciale empêche, par l'émission d'un signal dépourvu de sens, la divulgation des informations de l'étiquette par un lecteur illicite qui tente de perturber la communication des étiquettes voisines. Par exemple, une étiquette RFID peut contenir un bit spécial paramétré pour une utilisation "publique" ou "privée". Dans le cas d'un article médical comportant cette étiquette, le bit spécial est positionné sur la valeur correspondant à un statut "public" avant que l'article soit vendu, puis sur la valeur correspondant à un statut "privé" au moment de son achat. Au moment de mettre l'article médical dont l'étiquette est positionnée sur "privé" dans un conteneur en y appliquant une étiquette de blocage, les informations d'étiquette paramétrées sur "privé" par l'étiquette de blocage ne peuvent pas être lues par un tiers, garantissant ainsi la protection de la vie privée de l'acheteur.

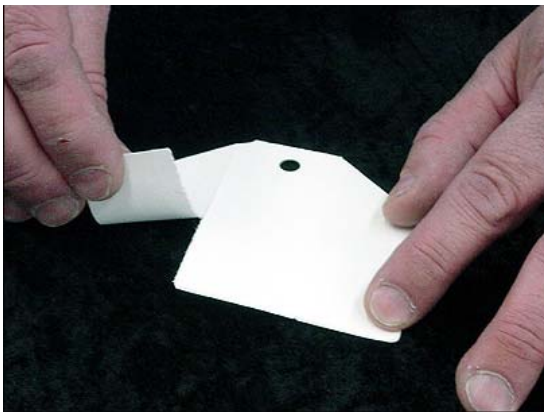
II.2.3 Brouillage actif

Le brouillage actif ("*active jamming*") perturbe le fonctionnement de tous les lecteurs RFID situés à proximité d'un dispositif émettant une forte onde brouilleuse. Cette technologie empêche ainsi la divulgation d'informations personnelles en bloquant les informations de l'étiquette RFID.

Il est à noter que l'étiquette de blocage et le brouillage actif sont des techniques simples qui peuvent facilement être utilisées pour mener des attaques par déni de service. De plus, ces solutions ne sont applicables qu'au niveau de l'utilisateur et ne peuvent être intégrées au service RFID.

II.2.4 Etiquette à antenne détachable

L'étiquette à antenne détachable (*clipped tag*) a été développée par la société IBM pour remédier aux inconvénients de la commande "*kill*". Elle consiste à réduire la distance de communication d'une étiquette en ôtant une partie de la ligne de connexion de l'antenne associée. Cette technique limite les risques d'atteinte à la vie privée par un traçage de la localisation à partir d'un site distant, en réduisant considérablement la distance d'information, tout en maintenant inchangée la fonction de stockage d'informations de l'étiquette.



X.1275(10)_FII.2

Figure II.2 – Etiquette à antenne détachable

II.2.5 Désactivateur d'étiquettes RFID

Le désactivateur d'étiquettes RFID (*RFID zapper*) a été présenté au Chaos Communication Congress, en 2005. Il s'agit d'un système électronique permettant de désactiver définitivement les étiquettes RFID passives. Le désactivateur d'étiquettes est conçu pour ne causer aucun dommage au dispositif auquel une étiquette peut être jointe, contrairement à d'autres solutions telles que le brouillage actif ou l'étiquette à antenne détachable.

II.3 Protection de la vie privée au moyen de la technologie cryptographique

On trouvera ci-après des solutions fondées sur des protocoles de cryptographie simples pour renforcer la sécurité et la protection de la vie privée au niveau de l'étiquette. Ces solutions ne sont pas encore suffisamment éprouvées pour être utilisées efficacement dans les applications existantes mais de nombreux travaux de recherches universitaires leur sont consacrés à l'heure actuelle. Bien qu'elles ne soient pas applicables pour le moment, elles donnent un bon aperçu de la solution fiable à laquelle on pourrait parvenir un jour. Il est à noter que ces protocoles nécessiteront très probablement d'apporter des changements aux protocoles radioélectriques actuellement normalisés (voir [b-ISO/CEI 14443], [ISO/CEI 18000] ou les études menées dans le cadre de EPCGlobal).

II.3.1 Verrouillage par hachage

Méthode faisant appel à la technologie cryptographique, le verrouillage par hachage consiste à transmettre au lecteur autorisé et à la base de données principale les informations stockées dans une étiquette, en calculant seulement une fonction inverse d'une fonction de hachage unilatérale. Comme il est détaillé dans la Figure II.3, seul le méta-identificateur (*metaID*) est fourni en réponse à la demande d'informations d'étiquette formulée par le lecteur, demande qui est ensuite transmise à un lecteur après vérification des informations d'authentification légalement obtenues de la base de données principale par le lecteur. Toutefois, l'inconvénient de cette méthode réside dans le fait que l'utilisateur peut être tracé, étant donné qu'un méta-identificateur a une valeur statique et pourrait avoir été utilisé comme identificateur d'étiquette.

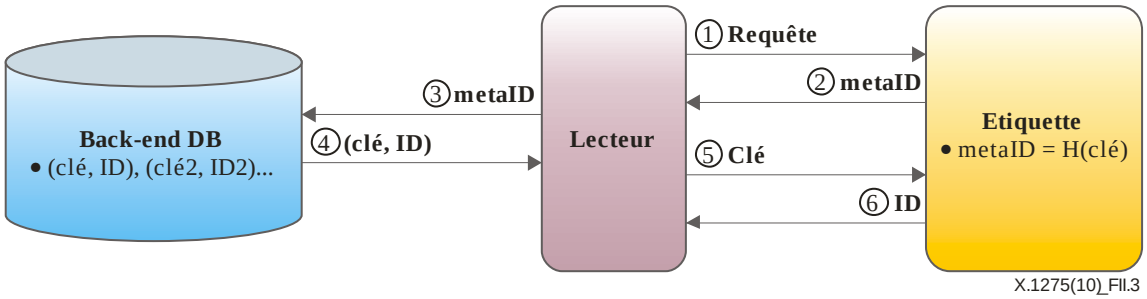


Figure II.3 – Verrouillage par hachage

La technique de verrouillage par hachage randomisé est l'une des méthodes proposées pour résoudre le problème de la traçabilité de l'utilisateur dans la technique actuelle de verrouillage par hachage. Comme il est détaillé dans la Figure II.4, la technique de verrouillage par hachage randomisé peut empêcher le traçage de l'utilisateur en permettant à une étiquette de générer une valeur différente chaque fois que l'on accède aux informations de l'étiquette, à l'aide d'un générateur de nombres aléatoires doté d'une fonction de hachage. Diverses autres techniques fondées sur une fonction de hachage, par exemple la chaîne de hachage, ont été proposées, mais se sont révélées peu pratiques [b-Weis].

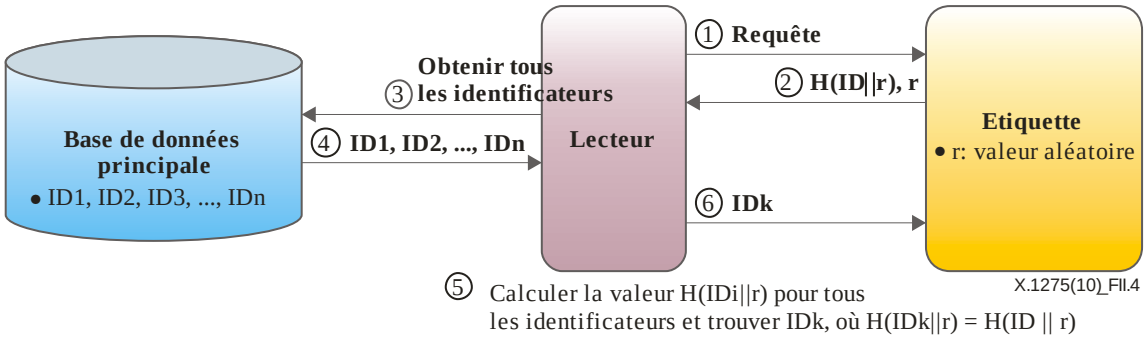


Figure II.4 – Verrouillage par hachage randomisé

II.3.2 Rechiffrement

La méthode de rechiffrement consiste à autoriser seulement la base de données principale ou le lecteur détenant la clé publique de la base de données principale à collecter les informations d'étiquette, la base de données principale licite ou le lecteur chiffrant périodiquement l'identificateur d'étiquette à l'aide de la clé publique et sauvegardant les informations générées dans l'étiquette. Le protocole de rechiffrement repose sur le système ElGamal et se décompose en deux étapes. D'abord, la base de données principale génère C, à l'aide de sa clé publique et d'un nombre aléatoire, et l'enregistre dans l'étiquette. La deuxième étape est décrite en détails dans la Figure II.5.

Cette méthode peut être appliquée à de grosses coupures. Le chiffrement périodique empêche le traçage des informations d'étiquette RFID. Néanmoins, étant donné qu'une méthode de chiffrement de clé publique est utilisée, il existe une menace de divulgation d'informations par branchement clandestin au cours de la transmission de la clé publique. En outre, les méthodes fondées sur le chiffrement de clé publique, telles que le rechiffrement, ne peuvent pas être appliquées à une étiquette passive bon marché à l'aide de la technologie actuellement disponible.

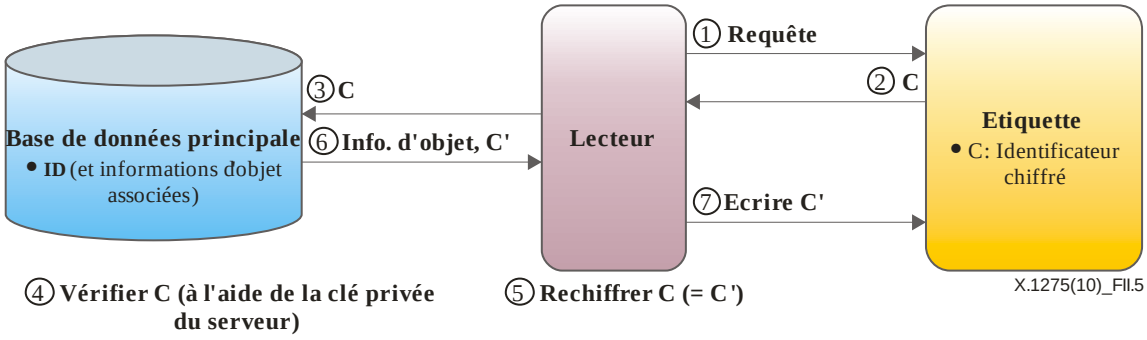


Figure II.5 – Rechiffrement

Bibliographie

[b-Conseil de l'Europe] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 1981, http://conventions.coe.int/treaty/fr/Treaties/html/108.htm.

[b-CRYPTREC] Telecommunications Advancement Organization of Japan, "*CRYPTREC Report 2002*", mars 2003, Information-technology Promotion Agency, Japan.

[b-DSTI/ICCP] "*RFID, identification par radiofréquence, Orientations de l'OCDE, sécurité de l'information et protection de la vie privée, applications, impacts et initiatives nationales*", Réunion ministérielle de l'OCDE sur le futur de l'économie Internet, 17-18 juin 2008.

[b-CE1] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal Officiel L 281, 1995, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_fr.pdf.

[b-CE2] Directive 2002/58/CE du Parlement européen et du Conseil 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 (directive vie privée et communications électroniques) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FR:HTML.

[b-EPIC] Electronic Privacy Information Center, "Guidelines on Commercial Use of RFID Technology", juillet 2004.

[b-E-Zpass] http://www.ezpass.com/static/info/howit.shtml.

[b-OACI] OACI, Doc 9303, Documents de voyage lisibles à la machine, Partie 1, Volume 2, 6ème édition, 2006.

[b-IPC] Ontario, Commissaire à l'information et à la protection de la vie privée, "*Lignes directrices régissant la protection de la vie privée pour les systèmes d'identification par radiofréquence*", juin 2006.

[b-Isamu Y] Isamu Y., Shinichi S., Akira I. and Satoshi I., "Secure Active RFID Tag System", 7th International Conference on Ubiquitous Computing, septembre 2005.

[b-ISO 22307] ISO 22307:2008, "*Services financiers – Evaluation de l'impact privé*", août 2008.

[b-ISO/CEI 14443] ISO/CEI 14443:2008, "*Cartes d'identification – Cartes à circuit(s) intégré(s) sans contact – Cartes de proximité*".

[b-Japon] MIC (Ministry of Internal Affairs and Communications), METI (Ministry of Economy, Trade and Industry) Gouvernement du Japon, "*Guidelines for Privacy Protection with Regard to RFID Tags*", juillet 2004.

[b-Juels] Juels, A., Rivest, R.L., and Szydlo, M., "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*", ACM Conference on Computer and Communications Security, 2003.

[b-Junichiro] Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai, "*Enhancing privacy of Universal Re-encryption scheme for RFID tags*", Embedded and Ubiquitous Computing 2004.

[b-Corée] MIC (Ministry of Information and Communication), Corée, "*RFID Privacy Protection Guideline*", juillet 2005.

[b-NIST] NIST SP 800-98, "*Guidance for Securing Radio Frequency Identification (RFID) Systems*", septembre 2007.

[b-OCDE] OCDE, "*Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*", 1980.

[b-Peris-Lopez] Pedro Peris-Lopez et al, "*M2 AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*", 3rd International Conference on Ubiquitous Intelligence and Computing, septembre 2006.

[b-PIA Canada] Secrétariat du Conseil du Trésor du Canada, "*Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée – Cadre de gestion des risques d'entrave à la vie privée*", 2002, http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-fra.asp.

[b-PIA Corée] MIC (Ministry of Information and Communication), Corée, "*Privacy Impact Assessment Guideline for Private Sector*", décembre 2005.

[b-Simon L1] Simson L., Garfinkel, Ari Juels and Ravi Pappu, "*RFID Privacy: An Overview of Problems and Proposed Solutions*", IEEE Security and Privacy, 2005.

[b-Simon L2] Simson L., Garfinkel and Beth Rosenberg, "*RFID: Applications, Security, and Privacy*", Addison-Wesley Professional, juillet 2005.

[b-HCNUR] Assemblée générale des Nations Unies, "*Guidelines for the Regulation of Computerized Personal Data Files*" (Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel), 1990, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08, PDF/G9010708-pdf.

[b-Weis] Weis S. et al., "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*", Security and Pervasive Computing 2003.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2011