4 ANALYSE DE LA SÉCURITÉ

Note (temporaire) : ce fichier est la source de la section "Analyse de la sécurité" du document SP 1.2. (étude prospective des besoins dans un réseau RFID communautaire) du projet PAC-ID GD.

Participants : IBM (responsable), EURECOM, *Carrefour*, *Orange Labs*, *GS1 France*
Auteurs de ce document : Dr. Philippe Martin - Pr. Refik Molva
{Philippe.Martin, Refik.Molva}@eurecom.fr
Adresse sur le Web : http://www.eurecom.fr/~martinph/PAC-ID/SP1_2secur.html

Plan

Note : une section "4.5 Scénarii d'attaque dans la grande distribution, selon le type d'attaquant" avait été prévue juste avant les annexes et références mais elle a été supprimée faute de contenu suffisant ; les quelques informations initialement collectées pour cette section ont été inclues dans la section 4.1.2.

4.1 Besoins généraux en sécurité

Résumé. Par ses caractéristiques et en devenant populaire, la technologie RFID va créer de multiples problèmes de sécurité, en particulier pour la protection de la vie privée, avec l'avènement de "l'internet des choses". Même si les risques pour la grande distribution sont plus limités, pour satisfaire les besoins de sécurité (confidentialité, intégrité, accessibilité, imputabilité) et respecter les lois européennes à ce sujet, différents principes de sécurité doivent être appliqués, notamment en assurant la transparence et le caractère minimal des collections, stockages et exploitations des données sensibles.

4.1.1 Importance particulière des besoins en sécurité

La vie des entreprises et les individus dépend de plus en plus de technologies informatiques, et donc de la confidentialité, intégrité et accessibilité des données et processus utilisés par ces technologies. Les "systèmes RFID" (i.e., les systèmes liés à l'exploitation d'étiquettes RFIDs) sont exposés aux menaces classiques sur les systèmes informatiques qu'ils incluent, e.g., des virus, erreurs logicielles et intrusions non-autorisées dans leurs réseaux et bases de données. Par ailleurs, si elles ne sont pas sécurisées, les étiquettes RFID et leurs connexions sans-fil avec des lecteurs RFID offrent de multiples possibilités de lectures et modifications non-autorisées de données ou, plus simplement, de détection ou localisation de certains objets et personnes. Plus généralement, de par leurs caractéristiques listées dans les deux points suivants, les systèmes RFIDs ont des besoins de sécurité particuliers.

Quelques faits. Les *étiquettes RFID sont de plus en plus bon marché*, *sophistiquées* (multiple senseurs, puissance de calcul), *versatiles* (i.e., utilisables et utiles dans de très nombreux contextes) et *petites* (donc invisibles ; certaines étiquettes passives peuvent avoir la taille d'un grain de sable et certaines contenant un microphone ou un appareil photo peuvent avoir la taille d'une mouche ; même si la miniaturisation des antennes d'étiquettes rencontre des limites physiques, il est possible de les dissimuler, par exemple en tissant les antennes dans le tissu les accueillant). Les étiquettes RFID ont donc le potentiel d'être très nombreuses (e.g., au Japon, plus de 50 millions de téléphones portables porteurs de d'étiquettes RFID ont été vendus en 2007 et permettaient des paiements dans plus de 50,000 points de vente [ASP 08]). Les étiquettes peuvent ne pas être vues et leurs fonctions peuvent être inconnues ou incontrôlables par les personnes directement ou indirectement liés à ces étiquettes. La plupart des étiquettes passives (celles qui n'ont pas de batterie et qui sont donc généralement peu sophistiquées mais bon marché et qui sont/seront donc répandues) offrent peu ou pas de mesures de sécurité : pas d'encodage des données, pas de mesures d'authentification avant transmission, fonction de désactivation de l'étiquette pas entièrement fiable (note : les étiquettes utilisées dans PAC-ID GD sont passives mais ont quelques fonctions de sécurité). Les *lecteurs RFID sont également petits, relativement bon marché et ont la possibilité de lire (et parfois d'écrire sur) la plupart des étiquettes du marché* ou encore d'écouter des transmissions de requêtes ou de données entre un autre lecteur et des étiquettes [BSI 04]. En 2004, des experts en RFID interrogés par [BSI 04] prédisaient que les *facteurs technologiques essentiels empêchant la diffusion et utilisation à grande échelle des étiquettes seraient résolus d'ici 2010*. Les étiquettes RFID peuvent transmettre *leurs identités et diverses données*, en particulier leurs positions spatiales et temporelles, jusqu'à plusieurs fois par seconde, à tout lecteur "proche" (quelques mètres au plus pour les étiquettes passives, plusieurs dizaines de mètres pour les étiquettes actives ou semi-actives). Ceci permet la collection d'un grand nombre de données, y compris sur des personnes si elles sont souvent proches d'une ou plusieurs étiquettes RFID (par exemple celles

placées dans un badge, un sac, ou des chaussures), sans que ces personnes soient averties. De par leur nombre, ces données peuvent permettre - par déduction ou via des techniques purement statistiques - de créer des profils personnalisés, par exemple des mouvements d'une personne ou des interactions entre entreprises, même lorsque les données ont été rendus anonymes par exemple via l'usage de pseudonymes [BSI 04]. Avec le prochain avènement de "l'Internet des Choses" (Internet of Things) il y aura de nombreux lecteurs RFID qui seront compatibles entre eux ou qui stockeront des données complémentaires sur des objets/personnes dans diverses bases de données.

Conclusions à partir des faits précédents. Les étiquettes RFID permettront de plus en plus de stocker de nombreuses données sur des personnes (consommateurs, employés) - ou des entreprises - sans qu'elles le sachent ou sans qu'elles aient autorisé ce stockage. La multiplicité des données stockées par différents organismes dans différentes bases offrira la possibilité (si ces données sont croisées) de déduire des informations confidentielles et incitera donc de tels croisements par des entreprises, organisations gouvernementales ou individus malveillants. Ces deux conclusions tendent à laisser penser qu'à l'avenir les interdictions légales (e.g., les lois de protections de données privées) ne pourront être efficacement appliquées. Ceci conduit, ou pourra conduire, à une méfiance de consommateurs vis à vis des produits porteurs d'étiquettes RFID. Ceci peut aussi conduire un consommateur à intenter un procès à une entreprise lui ayant vendu un produit étiqueté sans lui avoir dévoilé l'existence de l'étiquette, permis de rectifier les informations collectées, et permis de désactiver chacune des fonctions de l'étiquette. Une solution majeure est donc (i) de limiter au maximum le stockage de données à risque (e.g., données identifiantes ou personnelles) et leur association aux autres données stockées, et (ii) de permettre et d'encourager un contrôle aussi fin qu'économiquement possible par les utilisateurs des étiquettes RFID (entreprises, employés, consommateurs et individus en général) de ces informations et fonctions. C'est la conclusion du projet ASPIRE [ASP 08], compte-tenu de son analyse des différentes alternatives (cf. annexe "ASP-2.4"). Plus précisément, le but du projet ASPIRE [ASP 08] est de développer et disséminer les éléments suivants :
- des méthodes et recommandations pour, dans le cadre de systèmes RFID, effectuer des *collections, stockages et exploitations (logicielles, opérationnelles, etc.) transparentes et minimales* de données, et ainsi respecter les lois et recommandations européennes (cf. annexes "ASP-2.5" et "ASP-2.6" pour une analyse de ces lois ; l'annexe "ASP-8" donne une liste de "méthodes" proposées par ASPIRE ; la section 4.2 fournit également une synthèse),
- une architecture logicielle (ou système d'exploitation) pour le développement et l'exploitation de logiciels liés aux RFIDs, dont le code et ses modifications seront librement accessibles et seront conformes aux bonnes méthodes citées ci-dessus,
- des programmes d'audit et de certification (cf. annexe "ASP-7") de la bonne utilisation de cette architecture logicielle, et des programmes d'éducation des consommateurs.
ASPIRE incitera également ISO à adopter un standard (et donc un emblème) qui forcera les marchandises portant une étiquette RFID à être marquées pour expliciter ce fait. Les organisations AIM et EPCglobal ont déjà leurs propres standards et emblèmes pour cela et proposent donc aussi des recommandations pour le respect de la confidentialité des informations.

Toutefois, ***le risque actuel semble peu élevé***, en particulier pour les systèmes RFID liés à la ***grande distribution***. [BSI 04] note par exemple que "l'Internet des Choses" n'est pas encore développé et que peu de problèmes de protection de données privée, ou même de sécurité en général, ne semblent être posés ni par des applications impliquant des mécanismes d'encodage et d'authentification pour tous leurs accès aux données (y compris pour les accès aux étiquettes donc), ni par les applications peu

sécurisés exploitant des étiquettes RFID pour identifier - et en particulier de manière temporaire - (i) des palettes de produits (donc sans identifier le contenu de ces palettes) ou (ii) des produits communs et bon marché comme des cannettes de soda. Dans la grande distribution, le premier cas n'est pas rare, le second l'est encore vu les prix actuels des étiquettes RFID. Dans le sondage effectué pour [BSI 04] les experts interrogés pensaient que (i) pour la plupart des applications, les problèmes de sécurité posés par les systèmes RFID étaient mineurs en comparaison des problèmes pour mettre en œuvre ces systèmes, (ii) la protection des données était moins menacée par les attaques sur ces systèmes que par le fonctionnement normal de ces systèmes, et (iii) les avantages apportés par l'usage des étiquettes RFID au consommateurs seront privilégiés par ces derniers sur la possible exploitation de leurs données personnelles (exemple d'avantages dans le domaine de la distribution : meilleur service après-vente et transparence de la chaine d'approvisionnement en ce qui concerne la fabrication des produits et leurs contextes sociaux ou écologiques). Pour ce qui est des risques accrus que l'utilisation ou prochaine de ces systèmes pourrait faire peser sur des individus en complétant les données déjà collectées par d'autres systèmes (cartes de crédit, cartes de consommateurs, téléphones portables, etc.), les avis de ces experts étaient partagés. Ils notaient que compte-tenu des prix des étiquettes et de la fragmentation des données il serait difficile et très couteux de dériver le mouvement de personnes avec des systèmes RFID, que les informations venant des étiquettes n'ajouteraient pas grand chose d'important par rapport à ce qui est déjà stocké via les systèmes existants, et que la plupart des données existantes collectées par les systèmes existants ne sont jamais utilisées car dresser des "profils de consommateurs" n'a souvent pas assez d'intérêt commercial. L'annexe "BSI-7.8", et en particulier sa dernière section, fournit plus de détails sur l'évaluation par ces experts des menaces que posent les systèmes RFID.

Dans les pilotes de PAC-ID GD, les produits étiquetés (électroménager, Hi-Fi, téléphones portables, etc.) ont des prix relativement importants mais sont néanmoins communs et ne semblent donc pas soulever de problèmes de respect de vie privée, à moins que les étiquettes servent à localiser leurs acheteurs ou compléter leurs "profils d'acheteur" sans les avertir ; ces deux derniers points sont à l'heure actuelle extrêmement improbables entre autres parce que (i) les étiquettes utilisées sont passives et ont donc une portée de transmission d'au plus quelques mètres, (ii) il n'y a pas encore "d'Internet des Choses", donc pas de réseau de lecteurs RFID pour surveiller les gens, (iii) à part dans le cas des baladeurs et téléphones mobiles, les étiquettes ne sont pas portées par les consommateurs (et, pour un téléphone mobile, le risque de localisation n'est accru par la présence de l'étiquette que lorsque le téléphone est débranché), et (iv) comme pour des raisons de couts, Carrefour n'aura pas de lecteur RFID à ses caisses de vente, la vente du produit étiqueté se fera par un vendeur et l'acheteur devra donner son accord écrit pour la désactivation ou non de l'étiquette ainsi que pour l'association entre ses données personnelles et l'identifiant du produit (i.e., le numéro de l'étiquette ou bien le numéro de série). Les informations associées aux étiquettes seront des informations peu sensibles relatives aux objets, par exemple les numéros de série, les numéros de commande ainsi que les quantités, lieux et dates de fabrication, livraison, contrôle, stockage et vente du produit. Si des informations sont stockées dans l'étiquette elle-même, ce ne sera qu'un sous-ensemble de ces informations ou des informations peu sensibles et temporaires (i.e., à usage interne dans un entrepôt). Toutefois, la non-désactivation des étiquettes pose, à long terme, le problème de la localisation des personnes, problème qui ne peut être résolu qu'en permettant une désactivation aisée et fiable de l'étiquette par l'acheteur. Une telle fonction n'existe pas encore. Enfin, comme résumé dans [BRIDGE-EconomicRelevanceOfSecure-RFIDsyst 07], il sera tôt ou tard intéressant d'adopter de fortes mesures de sécurité. Il faudra alors utiliser les possibilités en mémoire, calcul et mesures de sécurité de l'étiquette XRAG2K qui est compatible avec le standard EPCGlobal Class1 Gen2 UHF et a été choisie pour les pilotes de PAC-ID GD.

4.1.2 Problèmes et critères généraux de sécurité (confidentialité, intégrité, accessibilité, …)

Rapide typologie. Les ***besoins de sécurité*** sont classiquement classés suivant les ***critères*** suivants :
- la *confidentialité* (la garantie que seules des personnes autorisées ont accès à - et donc connaissent ou utilisent - des objets considérés : données, messages ou contenu de messages, services ou fonctionnalités),
- l'*intégrité* (la garantie que les objets considérés sont exacts et complets, ce qui inclut la garantie que seules des personnes autorisées ont pu modifier ces objets),
- l'*accessibilité* (la garantie que les objets considérés sont accessibles - i.e., disponibles, mais aussi opérables avec des interfaces standards - au moment voulu par les personnes autorisées ; ceci implique, entre autres, que l'infrastructure et les techniques employées passent à l'échelle en nombre d'utilisateurs), et
- l'*imputabilité* (la garantie que l'auteur d'un objet ne puisse prétendre ensuite qu'il n'en est pas l'auteur, ou bien la garantie que le destinataire d'un message ne puisse prétendre qu'il ne l'a pas reçu ; ceci peut donc nécessiter l'intégrité, l'accessibilité et la *traçabilité* des objets, c'est à dire la garantie que les accès et tentatives d'accès aux objets considérés sont tracés et que ces traces sont conservées, exploitables et accessibles ; un critère connexe à ceux de traçabilité et d'accessibilité est celui de *transparence*).

Les directives européennes de ***protection des données et de la vie privée*** (cf. annexe "ASP-2.5") impliquent qu'une base de données (i) ne peut stocker, communiquer et utiliser des données personnelles sur un individu qu'avec son accord, et seulement celles utiles pour un but bien défini, (ii) doit offrir à cet individu la possibilité de modifier ou détruire ces données et de contrôler leur usage, et (iii) doit signaler la présence d'étiquettes RFID dans des produits et les moyens de les désactiver. Ainsi, la protection de la vie privée implique le respect de tous les critères précédemment cités et, de par le premier point listé, le *non-stockage de données permettant d'identifier l'individu* (e.g., son nom et son adresse ; en anglais, ce critère est nommé "unlinkability"), lorsque ceci est possible. Pour ceci, différentes techniques, comme l'usage des pseudonymes, peuvent être utilisés (cf. annexe "ASP-8.1"). Il est prudent de la part des individus de protéger eux-mêmes leur vie privée et donc d'utiliser des pseudonymes ou de choisir des fournisseurs de services leur permettant d'utiliser des "logiciels de protection de la vie privée" comme par exemple PRIME [PRIME-whitePaper_08]. Un ***problème de sécurité***, c'est à dire l'atteinte à un besoin de sécurité, peut affecter ou bien être causé (directement ou via un programme, volontairement ou par insouciance) par tout ***agent*** : consommateur, organisation, espion industriel, voleur, cyber-terroriste, fournisseur de réseau, etc. Les sinistres (e.g., vol, incendie, dégât des eaux) peuvent également être vus comme des agents puisqu'ils peuvent entraîner une perte de matériel et/ou de données. A part dans le cas d'un sinistre, tout agent peut être auteur de *diverses* ***attaques*** (et donc de problèmes), utiliser *diverses* ***techniques*** pour chaque attaque, attaquer *divers* ***composants*** ou ***fonctionnalités*** d'un système, et avoir *divers* ***buts*** pour chaque attaque. Enfin, pour chaque composant ou fonctionnalité, *diverses* ***mesures de sécurité*** peuvent être adoptées pour prévenir *divers* problèmes de sécurité. Les ***risques de sécurité*** peuvent être évalués avec *diverses* ***méthodes d'analyse de risque***, comme par exemple les méthodes Ebios, Mehari et Octave. Ces évaluations impliquent d'identifier les ***informations critiques*** à protéger. L'annexe "EPC-IS-BRIDGE-criticalInfo" donne des exemples pour les systèmes RFID dans la grande distribution malgré le fait que la plupart des informations stockées ne semblent pas confidentielles (l'annexe "EPC-IS-FAQ-23-31" résume les possibilités et limitations du stockage et de la recherche d'informations dans les bases de données RFID des adhérents au réseau EPCglobal).

Les relations référées ci-dessus par l'usage répété du mot "divers" sont le plus souvent des relations N-N, non des relations 1-N. Il serait trop long (voire illusoire) et peu intéressant de représenter ou classer

toutes ces relations, notamment celles entre agents, buts et techniques. Toutefois, nous avons pu effectuer quelques classements d'éléments en fonction des critères généraux de sécurité : le classement de quelques exemples d'attaques ou problèmes généraux (cf. les trois paragraphes suivants), celui de "techniques *générales* de sécurité" (cf. section 4.2) et celui de "problèmes et techniques de sécurité par grand type de composant ou fonctionnalité" (cf. sections 4.3 et 4.4). Ceci permet de mieux cerner les diverses relations entre les divers éléments cités ci-dessus.

Exemples de problèmes généraux pour la confidentialité : l'espionnage industriel (e.g., par la surveillance de produits d'un compétiteur dans un réseau/entrepôt commun), la détection d'objets confidentiels (e.g., certains livres politiques ou religieux) ou intéressants à voler (e.g., des objets chers dans un sac ou derrière une cloison) et donc la mise à jour de conditions médicales ou de comportements embarrassants (e.g., via la détection de certain médicaments sur une personne). De manière plus générale, la détection d'une étiquette RFID (i.e., la détection de sa présence à certaines places et certains temps, et via son numéro d'identification la détection du type de produit auquel l'étiquette est associée) permet parfois de déduire (i) une action prochaine par une personne ou une entreprise, (ii) le produit exact et/ou la personne auxquels l'étiquette est associée, (iii) l'emplacement et la trajectoire d'un produit ou d'une personne (identifiée ou non), (iv) des préférences d'une personne, (vi) des réseaux sociaux (via la transmission d'objets étiquetés entre personnes). Des déductions erronées peuvent parfois aussi être détrimentales, par exemple si l'arme d'un crime est attribuée à une personne alors qu'on lui a volé cette arme avant le crime. Les informations recueillies peuvent être utilisées de multiples manières, i.e, pour de nombreux buts : marketing, ajustement dynamique de prix en fonction de la richesse présumée du consommateur, vol d'identité, traçage des déplacements d'une personne, etc.

Exemples de problèmes généraux pour l'intégrité : la destruction de données et la contrefaçon (e.g., par clonage d'étiquette ou simple transplantation d'une étiquette sur un autre produit). Comme de telles attaques requiert une atteinte préalable à la confidentialité (e.g., l'obtention d'un identifiant et d'un mot de passe), les techniques utiles pour sauvegarder la confidentialité sont également utiles pour l'intégrité. L'*intégrité d'un système* sous-entend que le traitement effectué par le système doit être complet, exact, autorisé et rapide (pour ce dernier cas, le critère d'*accessibilité* semble être aussi requis). L'*intégrité des données* comporte quatre sous-critères : l'intégralité, la précision, l'exactitude/authenticité et la validité pour maintenir la cohérence interne (la fiabilité des données) et la cohérence externe (l'adéquation des données avec la réalité et les besoins).

Exemples de problèmes généraux pour l'accessibilité : la surcharge d'un réseau, le transfert de risques techniques de l'entreprise vers le consommateur (e.g., l'usage d'étiquettes RFID permet d'offrir plus de services à des clients mais ceux-ci en deviennent dépendants et doivent alors pouvoir en payer le cout technique et financier à tout moment), la fidélisation forcée (e.g., une machine à laver acceptant seulement des dosettes de détergents portant une certaine étiquette RFID et donc venant d'un fournisseur prédéterminé) et autres abus liés à des décisions automatiques. Inversement, un consommateur peut décider d'attaquer un système RFID (e.g., des étiquettes ou un réseau), et notamment son accessibilité, pour protéger sa vie privée. Ainsi, les techniques utiles pour sauvegarder la confidentialité et l'intégrité peuvent aussi être utiles pour sauvegarder l'accessibilité.

Exemples de problèmes généraux pour l'imputabilité : le clonage d'étiquettes RFID, la manipulation des traces RFID, les attaques de "l'homme du milieu" (dans lesquels l'agent attaquant retransmet et modifie les transmissions entre deux agents). De manière générale, le problème est d'assurer la non-répudiation de *l'origine* d'un objet (un agent ayant créé, envoyé ou utilisé un objet ne doit pas pouvoir nier l'avoir fait)

ou de sa *réception* (un agent ne doit pas pouvoir nier avoir lu, reçu ou utilisé l'objet). Ceci nécessite donc d'assurer l'intégrité, l'accessibilité et la traçabilité des objets.

Les attaques les plus simples sont de détruire ou de changer de place des étiquettes, ou encore de lire des identifiants d'étiquettes avec un lecteur RFID dans la poche. Ces attaques peuvent être effectuées par tout consommateur ou employé de la chaine de distribution. Des identifiants d'étiquettes, i.e., des numéros d'identification de produits, peuvent également se trouver dans des bases de données. Avec ces identifiants, il est possible de trouver plus d'informations sur les produits (fabricants, destinataires, prix, nombre d'unités, etc.) en interrogeant des services de découvertes, lesquels exploitent les bases de données RFID - ou "services d'informations RFID" - des fabricants, distributeurs ou transporteurs de produits. D'autres bases de données peuvent bien sûr aussi être utilisées en complément. Normalement, afin d'obtenir des informations "sensibles" dans une base de données, il faut être un agent connu et autorisé à le faire par cette base. Toutefois, en croisant les informations de plusieurs bases, il est parfois possible d'inférer des informations confidentielles. Pour éviter cela, c'est à chaque propriétaire d'informations de veiller à (faire) ajuster les droits d'accès à ces informations et, plus généralement, de veiller à ce que de bonnes mesures de sécurité soient prises pour les protéger, y compris contre des experts comme des "administrateurs de sécurité" ou les "fournisseurs du réseau". Le reste de ce document liste des mesures à prendre pour que ces informations soient protégées. Dans le cadre de la grande distribution, les informations échangées via les réseaux RFID ou stockées dans les bases de données RFID ne semblent peu confidentielles (cf. [EPC-IS 07] [GS1-128-barcodeForSupplyChain 08] [GS1-GPC 07]) mais peuvent être protégées, par exemple pour permettre à une entreprise de ne pas dévoiler "en temps réel" certains produits qu'elle achète - et à quels fournisseurs - à ses compétiteurs.

4.2 Mesures ou techniques générales de sécurité

Résumé. Pour satisfaire les besoins de sécurité, il faut permettre aux propriétaires d'informations de leur associer des politiques de contrôle d'accès et d'utilisation, puis faire respecter ces politiques. Ceci implique (i) la mise à disposition et l'exploitation de langage de spécifications versatiles et intuitifs, (ii) l'authentification des utilisateurs et des processus, (iii) le stockage des traces des processus, (iv) l'utilisation de techniques de validation syntaxique, structurelle, sémantique et statistique pour la détection d'informations incorrectes, obsolètes, incomplètes ou non-pertinentes vis à vis des contraintes ou buts fixés, (v) l'encodage et la limitation du stockage des informations sensibles, en particulier sur les étiquettes et réseaux RFID, (vi) la transparence, l'accès et l'interopérabilité des processus, et (vii) la sauvegarde des informations et le maintien de leur accès par les personnes autorisées.

Il existe de très nombreuses techniques contribuant à accroître la sécurité des données. Les sections suivantes sont destinées à permettre une vision d'ensemble. Les techniques cryptographiques ne sont donc que rapidement évoquées. Celles actuellement employées dans les systèmes RFID seront citées soit dans la section 4.3, soit dans cette section en référençant les annexes "BSI-7.7" et "EPCarchi-11". La protection des données nécessite l'utilisation d'une infrastructure supportant l'usage de multiples de techniques complémentaires et passant à l'échelle en nombre d'utilisateurs.

4.2.1 Contrôle des accès et usages (pour plus de confidentialité, intégrité, accessibilité, …)

Idéalement, le propriétaire d'une information, d'un support d'information ou d'un logiciel doit pouvoir restreindre son accès (lecture, écriture, réception, utilisation) et ses usages (citations, inférences, etc.) et à tels ou tels agents (personnes ou logiciels) en fonction de leurs identités ou de leurs caractéristiques (fonctions, buts, etc.). Par exemple, dans l'idéal, une personne devrait pouvoir spécifier de manière simple et *formelle* (i.e., automatiquement interprétable) via une politique d'usage qu'elle autorise ou non l'utilisation de certaines données la concernant (e.g., son identité et/ou son poids, certaines de ses maladies, etc.) à des traitements statistiques et anonymes par une industrie pharmaceutique.

Pour cela, un propriétaire d'objets (informations, supports, logiciels) doit pouvoir définir une **politique de contrôle d'accès et d'utilisation** sur un ou plusieurs objets, et divers mécanismes doivent être mis en place pour que cette politique soit respectée. L'annexe "PRIME-policies" donne quelques exemples de politiques et de mécanismes. Une politique peut couvrir tout ce qui est associé à un objet, y compris les résultats des-dits mécanismes (e.g., les traces des utilisations) ou les descriptions de cette politique. Une politique permet de définir pour chaque (type d')objet les droits d'accès de chaque (type d')agents en listant les *modes d'accès* auquel il a droit (e.g., none, read only, read&write, execute, call, use, open, close, send, receive, exit, enter, insert, delete, append, sample, etc.). Une politique discrétionnaire permet à chaque propriétaire de définir lui-même les droits d'accès pour chaque agent selon ses caractéristiques (e.g., son identité ou ses rôles). Une politique de sécurité peut aussi être globale (donc définie par un administrateur) et, par exemple, être basée sur des rôles ou être "obligatoire", c'est à dire constituée de règles basée sur la position de chaque objet et de chaque agent dans une hiérarchie de sécurité (ou "clearance"). Par exemple, Biba (un modèle formel de contrôle d'accès destiné à assurer l'intégrité des données) est basé sur le principe suivant : "pas d'écriture dans un niveau supérieur, pas de lecture d'un niveau inférieur".

A la base des mécanismes de contrôle des accès et usages se trouve (i) l'identification des agents et des objets, (ii) leur **authentification** (c'est à dire la vérification de leur identité) et (iii) l'autorisation, c'est à dire la vérification que l'agent dispose des droits nécessaires pour accéder à l'objet. Une "authentification forte" repose sur la communication de plusieurs facteurs d'identification, par exemple un mot de passe et le temps ou bien une variable aléatoire préalablement échangée. Il est bien-sur préférable que tous les échanges soient uncodés, qu'un secret partagé par les deux parties ne soit pas transmis, même encodé (et donc que le secret serve plutôt à encoder un autre facteur), et que les deux parties s'authentifient mutuellement. L'authentification basée sur un secret partagé a le désavantage de ne pas également pouvoir garantir l'imputabilité (puisqu'au moins deux parties peuvent accéder à l'objet) et celui de devoir impliquer une distribution préalable de ce secret (e.g., la distribution du mot de passe pour chaque application ou pour chaque étiquette RFID). Les techniques d'encodage à clés publiques permettent d'éviter ce problème. Comme elles sont plus lentes que les techniques d'encodage symétriques, elles sont souvent utilisées pour l'authentification et l'échange de secrets partagés générés dynamiquement. Cela peut se faire soit directement soit via un "serveur de clés" qui génère et distribue des clés (secrets partagés) et certificats électroniques aux deux parties. Cette procédure permet donc à un utilisateur d'accéder à différentes applications sécurisées en ne commençant qu'une seule session sur sa machine, ou en d'autres termes, d'accéder à un ou plusieurs serveurs de clé ("Single Sign-On"). [EPC-certif 08] définit un profil de certificat pour serveurs à clés publiques X.509 dans le réseau RFID EPCglobal (cf. section 11.3.6 de l'annexe "EPCarchi-11.3"). L'annexe "EPCarchi-11.3.1" (ou, plus exactement, la section 1 de l'annexe "EPCarchi-11.3") liste les mesures d'authentification et d'encodage dans le réseau EPCglobal, entre lecteurs et/ou services d'informations EPCglobal (via TLS ou AS2) ainsi qu'entre

lecteurs et étiquettes EPCGlobal Class1 Gen2 (via l'usage de mots de passe). L'annexe "BSI-7.7.1" liste les mesures générales d'authentification au niveau des étiquettes et lecteurs RFID. [BRIDGE-AuthRFID 07] fournit un état de l'art plus commercial que technique sur les mesures d'anti-contrefaçon (et donc les mesures d'authentification), y compris dans les systèmes RFID. Le projet européen SToP (www.stop-project.eu) contre la contrefaçon fournit un état de l'art technique [AuthRFIDsyst 07], en particulier pour les possibles extensions d'EPCglobal. Des algorithmes de détection de contrefaçons dans le cadre de la grande distribution sont également proposés [RFID-GD-auth 07].

Toutes les attaques ne peuvent être évitées, ne serait-ce que parce que certains sous-systèmes (e.g., sous-réseaux) sont vulnérables. Pour contrôler *a posteriori* les accès et usages et ainsi détecter (puis, si possible, réparer) les attaques, il faut **conserver une trace de tout accès** aux objets sensibles (agent, action effectuée, date, etc.). Ceci assure aussi l'imputabilité et peut décourager certains attaquants.

Les techniques authentifiant l'**intégrité d'un bloc d'information** utilisent une fonction non-réversible de hachage pour calculer un code de vérification et l'encode à l'intérieur du bloc pour éviter des modifications non-autorisées. Cette technique est réutilisée dans le contrôle d'accès "obligatoire" (au moins lors de transmissions d'informations) puisque ce contrôle nécessite d'associer à chaque agent et chaque bloc d'information sa position dans une hiérarchie de sécurité. Ces techniques peuvent aussi servir à garantir l'imputabilité lorsqu'elles sont basées sur des techniques d'encodage à clés publiques.

4.2.2 Contrôle automatique de la pertinence des données (pour plus d'intégrité)

Assurer l'intégrité des informations implique au moins deux types de sous-tâches. Une première est **d'éviter ou de détecter des modifications non autorisées** d'informations grâce aux techniques décrites dans la section précédente. Une seconde sous-tâche est **de vérifier que l'intégrité syntaxique ou sémantique** des informations recueillies, c'est à dire de vérifier qu'elles soient "vraies", à jour, complètes et pertinentes (e.g., leur existence doit être conforme aux buts de l'application et aux politiques d'usage relatives à ces données). Les erreurs détectées dans des informations non encore stockées doivent être rejetées. Les erreurs détectées dans des informations déjà stockées peuvent indiquer des attaques et doivent être réparées lorsque cela est possible. La détection d'erreur doit employer des systèmes complémentaires de validation, typiquement (i) des systèmes "syntaxico-sémantiques" (i.e., vérifiant que des règles/contraintes syntaxiques, sémantiques ou méthodologiques soient respectées, ou bien utilisant des règles pour détecter des attaques) **et** (ii) des systèmes "statistiques". Citons par exemple le système Deckard, développé par Auto-ID Labs, qui effectue des statistiques sur des traces de processus pour détecter des anomalies dues à des changements d'appartenance d'une étiquette à un produit.

4.2.3 Nécessité de représentations explicites pour permettre les contrôles

Plus les données sont sémantiquement structurées, plus des **inférences logiques** peuvent être effectuées pour détecter des erreurs. Les validations syntaxiques, structurelles ou sémantiques citées dans la section précédente doivent souvent être effectuées par les applications car souvent elles-seules connaissent la syntaxe, structure **ou** sémantique des données transmises.

Cependant, XML étant maintenant une syntaxe standard pour transmettre et spécifier la structure de données, des **validations structurelles** peuvent être faites par certains éléments du réseau. EPCglobal définit de nombreux modèles XML, par exemple pour (i) les EPC-IS (bases/services d'informations dans EPCglobal) [EPC-IS 07] et (ii) les documents de transactions relatives à un produit dans la chaine de distribution pharmaceutique [EPC-Pedigree 07] (annexe "EPCarchi-11.3.7"). Comme résumé dans l'annexe "EPC-IS-FAQ-23-31", le modèle d'information utilisé par les EPC-IS propose des types d'information (e.g., Objet, Agrégation, Quantité, Transaction) avec quelques sous-types et un certain nombre d'attributs pour permettre d'expliciter, ou au moins de structurer, les catégories d'informations (quoi, pourquoi, quand et où) relatives aux évènements RFID. Ce modèle permet également d'effectuer des requêtes : addition, destruction, recherche et filtrage de données.

De manière similaire, (une partie de) la **sémantique** des données pourrait être décrite dans des **ontologies** (dictionnaire sémantique plus règles sémantiques) par les applications ou les créateurs des informations. Le standard de-facto pour cela est actuellement le modèle RDF+OWL avec la notation "RDF/XML". Les éléments du réseau pourraient alors utiliser des moteurs d'inférences pour valider les modifications et donc éviter certaines erreurs ou attaques. Ce n'est pas encore le cas. Le modèle d'information des EPC-IS accepte certaines certaines extensions de ses propres schémas XML par les applications, et accepte l'utilisation par des agents de mots clés non-définis, mais ne prend pas en compte des ontologies fournies par des agents, i.e., n'accepte pas l'extension dynamique de ses modèles de données par des agents. A part PRIME, les grand projets dans le domaine des systèmes RFID, comme EPCglobal, BRIDGE ou ASPIRE, ne semblent pas encore envisager l'utilisation d'ontologies complétables par les agents ou bien fournies par eux. Laisser les agents compléter une seule ontologie initiale est une solution plus simple à mettre en place et exploiter que celle consistant à utiliser des ontologies fournie par les agents. De nombreuses avancées dans cette direction ont été effectuées, et implémentées dans le serveur de connaissances WebKB [Martin 01] [Martin 05] par l'un des auteurs de ce document (e.g., WebKB permet d'éviter ou de résoudre les conflits entre les diverses extensions créées par les agents). Ces avancées pourraient être appliquées dans le domaine des RFID, tout d'abord en permettant une extension par les agents des schémas ou ontologies liés à EPCglobal. Ceci inclurait GPC (Global Product Classification) [GS1-GPC 07], une large taxonomie à cinq niveaux de types de produits, créée par GS1 (la société fondatrice de EPCglobal), et dont les identifiants sont inclus dans les identifiants de produits que stockent les étiquettes RFID faisant partie du réseau EPCglobal.

Il faut également noter qu'un agent ne peut définir une **politique de contrôle d'accès ou d'usage de manière précise, libre** (i.e., sans être restreint à combiner quelques critères simples et prédéfinis) **et réutilisable** par toute application ou service de réseau que si l'agent dispose d'un moyen de décrire des objets, des agents et des actions (i) dans une ontologie *réutilisable* (i.e., dont les catégories conceptuelles sont connectées à de nombreuses autres catégories de nombreuses autres ontologies et en particulier à des ontologies sur la sécurité), et (ii) avec un *langage de représentation de connaissances puissant et intuitif*. Ceci est un idéal, il n'existe pas encore d'ontologie *générale* sur la sécurité dont les concepts soient utilisés par des langages ou des systèmes permettant le contrôle d'accès ou d'usage. Il existe des langages destinés à des administrateurs de systèmes, procéduraux (e.g., Ponder, IPDL) ou déclaratifs (e.g., Rei qui est basé sur une logique déontique et permet de définir des "droits", "interdits" et "obligations") qui offrent des fonctions ou concepts spéciaux pour permettre de spécifier et d'exécuter certain contrôles d'accès ou d'usage. Ceci peut également se faire en utilisant des schémas XML (et donc des langages XML), e.g. P3P (Platform for Privacy Preferences) XACML (eXtensible Access Control Markup Language) (cf. [W3CWorshopOnPrivacyPolicy 06] pour un état de

l'art). Enfin, certain systèmes proposent également de tels concepts via des ontologies RDF+OWL et permettent leur utilisation et/ou spécialisation via l'écriture d'ontologies RDF+OWL. Citons par exemple PRIME (cf. annexe "PRIME-policies"), PAW, KAoS, Rei 2.0 [Toninelli 05] et ACCENT [CallControl 07] (ACCENT utilise le langage APPEL qui utilise P3P et qui peut être spécialisé via des ontologies pour définir des connaissances du domaine et résoudre des conflits dans le cadre d'applications de téléphonie). Les ontologies de ces systèmes pourraient être intégrées et spécialisées dans un serveur de connaissances tel que WebKB, ce qui permettrait une réutilisation de ces ontologies par plusieurs systèmes. Les utilisateurs pourraient alors également éditer et intégrer leurs ontologies via WebKB, et donc facilement accéder et réutiliser des politiques et autres connaissances déjà stockées (dont une ontologie générale incluant 90,000 concepts reliés à 120,000 mots de la langue anglaise). Nous avons débuté la conception d'une ontologie sur la sécurité dans WebKB [OntologyOfRFIDsecurity 08].

[BSI 04], tout comme [ASP 08], insiste sur l'importance de la **transparence** dans les mécanismes de gestion des informations liées aux étiquettes RFID, et sur l'importance de laisser aux agents la possibilité de contrôler l'existence et l'usage qui est fait de leurs données. Bien que non mentionné par [BSI 04] et [ASP 08], le fait que des services RFID suivent des politiques d'usage rend ces services plus transparents pour les agents. Le fait que ces services utilisent des données représentées de manière formelle et organisée apporte également plus de transparence car cela permet aux agents de mieux retrouver (dans les bases d'informations de ces services) leurs données ainsi que les informations générées à partir de ces données - normalement, ce lien *doit* être conservé lorsque cela ne pose pas de problème de confidentialité. Les agents peuvent alors contrôler l'usage fait de leurs données et exercer leur droit de rectification. Ce contrôle peut bien sûr être automatique (via les systèmes cités dans le paragraphe précédent) ou semi-automatique : une personne lance des processus vérifiant l'existence ou l'usage ce certaines informations et, si un problème potentiel est détecté, cette personne est alertée pour vérifier. Pour cela, les politiques doivent bien-sûr être facilement retrouvables à partir des données ; elles peuvent par exemple être inclues dans ces données ("sticky policies").

Enfin, [BSI 04] et [ASP 08] insistent sur l'importance d'**éduquer** les utilisateurs présents ou futurs d'étiquettes RFID, de leur permettre une recherche aisée des techniques et autres informations relatives aux étiquettes RFID, de leur permettre de discuter sur ces sujets et d'enregistrer leurs "informations en retour". Tout ceci implique une organisation conceptuelle et flexible des informations, et serait donc facilité par l'usage d'un serveur de connaissances.

Les suggestions mentionnées dans cette section sont originales dans le domaine des RFID et ont un rapport "effort à investir / résultats prévus" intéressant.

4.2.4 Réduction et encodage des informations sensibles (pour plus de confidentialité, d'intégrité)

Un des principes de base des projets ASPIRE et PRIME est de limiter la transmission ou le stockage d'informations potentiellement "sensibles", et donc aussi de limiter l'association de données et d'identifiants de personnes. L'annexe "ASP-8.1" donne une liste de techniques pour cela. Cette liste inclue l'encodage systématique des données ainsi que, lors d'une transmission de données (pour éviter de laisser deviner le volume des données échangées ou l'identité des agents échangeant les données), l'encodage des "silences" entre les transmissions et la distribution aléatoire du routage des transmissions. [PRIME-whitePaper 08] et [PRIME-architecture] précisent pourquoi et comment un

utilisateur peut (i) indiquer ses données sensibles (et politiques d'accès/usage associées) à son logiciel PRIME, (ii) lors d'une transaction avec un fournisseur de services ayant également un logiciel PRIME, laisser son logiciel envoyer sous une forme anonyme et codée le nombre minimal de données que requiert le fournisseur de services, puis plus tard, (iii) laisser son logiciel périodiquement vérifier que les politiques d'usage définies par l'utilisateur sont respectées. Lorsque cela est possible, ce logiciel génère des identités temporaires (des pseudonymes) pour masquer l'identité réelle de l'utilisateur.

Pour les étiquettes RFID, une mesure élémentaire est de ne stocker les informations sensibles que dans des bases de données, jamais sur les étiquettes elles même. Cela simplifie également la gestion des données. Les propriétaire des bases de données doivent alors toutefois veiller à ce que les individus concernés par ces informations puissent les accéder, les rectifier et contrôler leurs usages dans les bases de données, sinon ces individus ont moins de contrôle sur leurs informations que lorsqu'elles sont uniquement stockées sur une étiquette leur appartenant. Permettre ceci n'est pas simple et est donc couteux. Les fonctionnalités d'EPCglobal ne prennent pas en compte les informations stockées sur des étiquettes (seul le numéro d'identification du produit est pris en compte) mais cela n'empêche pas une entreprise de stocker ou d'accéder des informations sur des étiquettes conformes au standard EPCGlobal Class1 Gen2. Il faut par ailleurs noter que le choix par un consommateur de détruire une étiquette RFID sur un produit lui appartenant ne doit pas le désavantager : les services proposés avant un usage systématique d'étiquettes RFID (e.g, les services après-vente) doivent demeurer accessibles sans étiquettes RFID. Cela signifie souvent que l'utilisation du numéro de série d'un produit doit demeurer une alternative à l'usage d'un numéro d'étiquette RFID.

L'annexe "EPCarchi-11.3.1" liste les techniques d'authentification et d'encodage utilisés dans le réseau EPCglobal entre lecteurs et/ou services d'informations EPCglobal (via TLS ou AS2) ainsi qu'entre lecteurs et étiquettes EPCGlobal Class1 Gen2 : usage de pseudonymes (section 11.3.1.1), encodage (section 11.3.1.2), commandes de blocage en lecture/écriture de zones de mémoire (section 11.3.1.3) et commande de désactivation permanente de l'étiquette (section 11.3.1.4). Il n'existe toutefois que deux mots de passe stockés dans l'étiquette : un pour le blocage et un pour la désactivation. Ils doivent donc être partagés par tous les utilisateurs.

L'annexe "BSI-7.7" inclut des descriptions de techniques pour le respect de la confidentialité au niveau des étiquettes et lecteurs RFID: encodage (section 7.7.2), protocoles d'anticollision non sensibles aux écoutes non autorisées (section 7.7.3), l'utilisation de pseudonymes (section 7.7.4), la prévention d'écoutes non autorisées via l'usage d'étiquettes bloquantes (section 7.7.5), et la destruction ou désactivation permanente des étiquettes (section 7.7.6). La seconde moitié de la section "BSI-7.8" liste d'autres techniques pour détruire des étiquettes ou bloquer totalement les écoutes autour d'une étiquette ; ces techniques sont présentées comme des techniques d'attaques mais, comme toute technique d'attaque, elles peuvent également être utilisées (légitimement ou pas) comme des techniques de protection de la vie privée.

4.3 Sécurité au niveau des étiquettes et lecteurs RFID

Résumé. Les informations inscrites sur une étiquette ou un lecteur d'étiquettes, ou encore transmises à/par une étiquette, peuvent être lues/écoutées, détruites/brouillées, ou mises à jour par des personnes non autorisées. Des étiquettes peuvent aussi être contrefaites ou clonées. Cette section liste les contremesures principales à ces problèmes.

Cette section résume, réorganise et complète les informations de l'annexe "BSI-7.8". En ce qui concerne cette réorganisation, les sous-sous-sections (i.e., les sections non-numérotées) de l'annexe "BSI-7.8" - qui liste des techniques d'attaques - sont ici directement reprises (quoique parfois regroupées) en tant que "paragraphes titrés", alors que le groupement en sous-sections est basé sur les critères généraux de sécurité mis à mal par ces techniques d'attaques. Cette correspondance ayant maintenant été explicitée, l'annexe "BSI-7.8" ne sera plus référencée et le lecteur est implicitement invité à se reporter à cette annexe pour plus de détails. La mesure de sécurité consistant à ne pas stocker d'information sur une étiquette s'applique à toutes les attaques et ne sera donc pas répétée.

Les documents [BRIDGE-TagSecurity 07] [BRIDGE-TagAntiCloning 07] et [BRIDGE-ReaderSecurity 07] donnent (i) une description des composants électroniques, protocoles et fonctionnalités relatifs à la sécurité et actuellement disponibles dans les étiquettes EPCGlobal Class1 Gen2 et les lecteurs RFID, et (ii) une description des extensions souhaitables de ces composants, protocoles et fonctionnalités. Les sous-sections suivantes ne descendent pas à ce niveau de détail. [XRAG2K 08] liste des composants et fonctionnalités de l'étiquette XRAG2K qui a été choisie pour les pilotes de PAC-ID GD et qui est compatible avec le standard EPCGlobal Class1 Gen2 UHF.
`//Problème : [XRAG2K 08] est une liste de transparents de STU actuellement marqués "à usage interne" (donc non actuellement accessibles sur le Web).`

4.3.1 Confidentialité au niveau des étiquettes et lecteurs RFID

Écoute non-autorisée de messages entre lecteurs et étiquettes. En théorie, pour les étiquettes du projet PAC-ID, le risque d'écoute de l'envoi d'une requête par un lecteur existe jusqu'à 100 ou 200 mètres autour du lecteur, voire jusqu'à 500 ou 1000 mètres avec une antenne directionnelle. La distance maximale de réception de la réponse de l'étiquette est de 3 à 5 mètres autour de celle-ci. Pour de longues distances, de telles écoutes, ainsi que la localisation d'étiquette, sont difficiles à réaliser. Pour de courtes distances, des lecteurs normaux peuvent être réutilisés. Des *contremesures* sont (i) de protéger contre les radiations électromagnétiques les zones où des lecteurs sont utilisés, par exemple en tapissant les murs avec du papier métallisé, et (ii) d'encoder les données transférées autant que les possibilités de calcul de l'étiquette le permettent. L'encodage et l'usage de pseudonymes ne sont pas des mesures contre la localisation et le suivi d'étiquettes.

Lecture non-autorisée d'une étiquette. Une lecture est aisée dans les 3 à 5 mètres autour de l'étiquette (donc par exemple par quelqu'un se promenant dans un supermarché avec un lecteur dans sa poche), difficile et facilement détectable sinon. Des *contremesures* contre les lectures non-autorisées sont (i) d'installer des détecteurs reconnaissant les champs magnétiques de lecteurs, et (ii) d'utiliser des méthodes d'authentification (cf. annexes "BSI-7.7.1" et "EPCarchi-11.3.1"). Toutefois, dans les étiquettes EPCGlobal Class1 Gen2 le mot de passe contrôlant l'accès à des zones mémoire est partagé par tous

les utilisateurs et n'est donc intéressant que pour le stockage temporaire de données sensibles à l'intérieur d'une entreprise, i.e., pour éviter à certains des employés d'accéder à ces informations. Dans le cas général, si un lecteur stocke une liste des mots de passe, celle-ci doit être encodée et/ou maintenue dans une partie protégée de la mémoire de ce lecteur.

Suivi de personnes porteuses d'étiquettes RFID. Comme indiqué dans la section 4.1.1, ceci ne deviendra un danger que lorsqu'il y aura un "Internet des Choses". A l'intérieur d'une entreprise, il peut déjà y avoir un danger de suivi des employés quoique cela soit souvent légal. Une *contremesure* peut être la génération automatique d'identités temporaires comme indiqué dans l'annexe "BSI-7.7.4".

4.3.2 Intégrité et imputabilité au niveau des étiquettes et lecteurs RFID

Émulation d'étiquette ou de lecteur ; écriture non-autorisée sur une étiquette ou un lecteur. Les données d'une étiquette ou d'un lecteur peuvent être modifiées physiquement, quoique cela soit difficile. Les données d'un lecteur peuvent également être lues ou modifiées via un accès réseau, et donc par exemple par un virus. L'identité et les mots de passe d'un lecteur peuvent aussi être volés par écoute non-autorisée des transmissions de lecteur sur le réseau ou vers des étiquettes. Un simulateur d'étiquette ou de lecteur peut aussi être approché d'un lecteur ou d'une étiquette, ou même être positionné entre les deux et relayer leurs transmissions, afin de lire ou écrire sur l'étiquette ou le lecteur (dans ce dernier cas, "écrire sur le lecteur" signifie lui faire enregistrer une fausse information de la part d'une étiquette, e.g., un nouvel emplacement). Des *contremesures* sont (i) des protections physiques des étiquettes et des lecteurs, et (ii) un contrôle d'accès sur les lecteurs ainsi que, si possible, les étiquettes. Ceci implique l'encodage et l'authentification mutuelle de toutes les transmissions, avec si possible l'imputabilité de celles-ci (e.g., si un lecteur modifie des données sur une étiquette, celle-ci peut associer dans sa mémoire l'identité du lecteur à chacune des données qu'il a modifié).

Clonage d'étiquette. Le numéro d'identification d'une étiquette peut être inscrit sur une autre étiquette ou utilisé dans un réseau pour injecter de fausses données dans une base d'informations. Des *contremesures* sont (i) d'éviter que les numéros d'identification soient connus d'agents non autorisés en évitant des écoutes ou lectures non-autorisées sur l'étiquette ou le réseau, (ii) de créer sur l'étiquette des fonctions d'authentification de celle-ci qui soient très difficiles à reproduire, via des fonctions de hachage ou des "circuits logiques non reproductibles" (cf. [BRIDGE-TagAntiCloning 07] pour des exemples), et (iii) de détecter les duplications (de numéros) d'étiquettes, qu'elles soient d'origine malveillante ou dues à des erreurs, en détectant des anomalies dans les données associées à un numéro d'étiquette, par exemple qu'elle est située dans deux endroits différents en même temps ou deux endroits éloignés dans un laps de temps court. [AuthRFID-GD 07] propose des algorithmes pour de telles détections dans le cadre de la grande distribution. Comme noté plus haut, le système Deckard effectue des statistiques sur des traces de processus pour détecter des anomalies dues à des changements d'appartenance d'une étiquette à un produit.

4.3.3 Accessibilité des informations au niveau des étiquettes et lecteurs RFID

Les étiquettes et lecteurs ne doivent pas pouvoir être facilement mis hors service par erreur ou par malveillance, et doivent être accessibles via des standards de facto (comme EPCglobal) ainsi que, au moins partiellement, via des protocoles peu sécurisés (comme ceux d'EPCglobal en 2008). Ce dernier point peut être atteint en permettant (i) une restriction adaptée des accès (donc *pas* de mot de passe pour les accès aux parties *publiques* d'un lecteur ou d'une étiquette), et (ii) la génération automatique d'identifiants temporaires lorsque l'étiquette ou le lecteur requiert un identifiant pour toute lecture. Un lecteur doit pouvoir appliquer différentes politiques de lecture d'étiquettes.

Détachement d'une étiquette d'un produit. C'est une attaque facile qui peut créer d'importantes confusions. Elle permet par exemple d'échanger les étiquettes de produits. Des *contremesures* sont (i) de faire en sorte que l'étiquette se brise et endommage le produit si elle est détachée, (ii) d'associer d'autres identifiants au produit (e.g., un code barre, des marques invisibles ou des étiquettes mieux cachées), et (iii) de permettre à l'étiquette de déceler son détachement et donc de l'enregistrer puis, tôt ou tard, de le communiquer.

Destruction mécanique ou chimique d'une étiquette. Des *contremesures* sont d'inclure l'étiquette dans un endroit difficile à trouver ou atteindre, et d'inclure plusieurs étiquettes.

Destruction d'une étiquette via un champ électromagnétique. A courte distance, des étiquettes anti-vol peuvent ainsi être aisément désactivées. Pour d'autres étiquettes, cela peut parfois endommager le produit. L'usage de court-circuits auto-réparant est une *contremesure* potentielle.

Destruction d'une étiquette via une commande de désactivation. Une *contremesure* est une procédure d'authentification propre à cette commande. C'est le cas pour les étiquettes EPCGlobal Class1 Gen2.

Destruction d'une étiquette active par décharge de sa batterie, via une série de lectures. Une *contremesure* est de limiter le nombre d'interactions par seconde. Les étiquettes EPCGlobal Class1 Gen2 sont passives.

Blocage ou brouillage de transmissions entre lecteurs et étiquettes par émetteurs de brouillage, des des "étiquettes bloquantes", du papier métal, de l'eau, une main, etc. Des *contremesures* potentielles sont (i) de détecter les émetteurs ou les blocages, et (ii) de permettre aux lecteurs d'utiliser différents protocoles ou fréquences.

4.4 Sécurité au niveau du réseau de communication et des applications

Résumé. Rappel de services à fournir, ou de mesures principales à prendre, à ce niveau et en particulier ceux pris ou étudiés par EPCglobal et BRIDGE : (i) interopérabilité et authentification unique des utilisateurs pour l'exploitation différents réseaux ou applications, (ii) vérification, authentification, traçage et localisation des produits, et (iii) utilisation de SNMP, AS2, SOAP, X.509, SAML, etc.

Les besoins en sécurité des réseaux et applications liées aux RFID sont plus communs que les besoins en sécurité des étiquettes et lecteurs RFID. Plus le nombre de techniques *complémentaires* utilisées sera grand, plus la sécurité sera bonne. Nous ne répèterons pas ici les types de techniques listés dans la section 4.2 mais nous rappellerons les méthodes utilisées dans EPCglobal pour son réseau et ses applications. Comme le projet européen BRIDGE étudie des extensions ou des compléments à ces méthodes, nous introduirons ces recherches [BRIDGE-AnalysisOfRFIDsecurity 07] [BRIDGE-NetworkConfidentiality 07] [BRIDGE-NetworkSecurity 07] [BRIDGE-IntegrityOfSupplyChain 07].

4.4.1 Confidentialité et contrôle d'accès dans le réseau de communication et les applications

Idéalement, toute communication avec ou à l'intérieur du réseau doit être signée et n'être effectuée qu'après mutuelle authentification. Tout stockage d'information et accès à cette information dans un élément du réseau (et donc sa communication par cet élément) doit respecter les politiques de contrôle d'accès et d'utilisation définies par le propriétaire de cette information (ceci inclut la possibilité pour le propriétaire de corriger ou supprimer cette information). Pour cela, les mécanismes d'authentification et de contrôle d'accès du réseau EPC Global doivent être étendus. L'utilisation de "mécanismes d'autorité" permettant à certaines sociétés de valider (et donc signer) certaines informations doit être possible. Toutes les données, requêtes et traces contenues dans les applications et les éléments du réseau doivent être protégées conformément aux politiques d'accès et d'utilisation définies par les propriétaires des informations stockées ou transmises. Avant de répondre à une requête, la trace des requêtes précédentes de la part du même utilisateur doit être exploitée pour éviter de communiquer à cet utilisateur des informations qui, par recoupement avec des informations préalablement communiquées, pourraient dévoiler des informations confidentielles. Les mécanismes d'authentification et de contrôle d'accès doivent permettre de ne pas associer l'identité d'un utilisateur à ses transactions : des "transactions anonymes" doivent être possibles [BRIDGE-AnalysisOfRFIDsecurity 07]. Les applications doivent détecter et résoudre les problèmes de contrôle d'accès et de confidentialité, (i) en interne, (ii) au niveau de leurs interfaces, et (iii) en externe (i.e., au niveau des éléments du réseau, des lecteurs et des étiquettes).

Dans le réseau EPCglobal, comme le souligne l'annexe "EPCarchi-11.3", différentes techniques de transport, d'authentification et d'encodage sont déjà utilisées, pour les transmissions en général (TLS, HTTPS), pour l'ALE (l'interface de filtrage d'évènements destinés aux applications ; section 11.3.1.1 ; utilisation de SOAP), pour les communications avec les lecteurs RFID (sections 11.3.1.2 et 11.3.1.3 ; utilisation de SNMP) et pour les services d'informations (section 11.3.1.4 ; utilisation de AS2 et de SOAP/HTTP). L'ONS (le service qui, compte tenu du numéro d'identification de produit contenu dans une étiquette RFID, renvoie l'adresse internet des services d'informations de l'entreprise ayant créé ce produit) n'offre aucune protection pour la confidentialité car les informations fournies sont publiques (section 11.3.2.1). Les demandes d'ajouts à ONS s'effectuent par interface Web, et ces demandes sont

protégées par ACL (Access Control List) et secret partagé (mot de passe). L'ONS est actuellement basé sur DNS. L'application de DNSSec (cf. www.dnssec.net) à l'ONS pourrait mieux protéger son intégrité.

Le projet BRIDGE espère offrir une plateforme permettant de fédérer différents réseaux RFID autonomes, dont EPCglobal. La fonction spécifiée (mais non encore implémentée) par EPCglobal pour authentifier ses adhérents est donc insuffisante pour BRIDGE puisque nombre des opérateurs et utilisateurs des composants de l'architecture de BRIDGE ne seront pas adhérents à EPCglobal. BRIDGE étudie donc des moyens d'assurer un système d'authentification permettant d'accéder à différent services, RFID ou non, avec une seule procédure d'identification pour chaque utilisateur ("Single Sign-On"), par exemple en utilisant SAML (Security Assertion Markup Language) un langage XML conçu pour permettre une telle authentification unique. La spécification des EPC-IS (services d'informations dans EPCglobal) ne détaille pas comment une telle authentification unique peut être assurée ; actuellement, pour accéder aux informations non-publiques d'un EPC-IS, par exemple à l'historique d'un produit, il faut être un utilisateur connu de cet EPC-IS. La spécification des EPC-IS ne détaille pas non plus comment des politiques de sécurité peuvent être construites et relayées. Pour permettre cela, BRIDGE considère l'utilisation de méthodes standards pour décrire des politiques de contrôle d'accès, typiquement XACML (eXtensible Access Control Markup Language) qui étend SAML, ou des langages plus "sémantiques". Rappelons que XACML n'est qu'un schéma XML, donc non flexible et non prévu pour permettre l'utilisation d'ontologies, lesquelles sont indispensables pour de meilleures spécifications, exploitations et réutilisations des politiques d'accès (cf. section 4.2.3). BRIDGE considère le contrôle d'accès comme le problème le plus important pour les "services de découverte d'informations" à cause des conflits entrainés par (i) l'actuelle importante granularité des spécifications d'accès, et (donc) (ii) l'appartenance des données à différents agents. BRIDGE considère les politiques d'accès comme un sous-ensemble de la politique des EPC-IS.

4.4.2 Intégrité et imputabilité au niveau du réseau de communication et des applications

Idéalement, l'inscription des agents pour l'accès au réseau doit être précise et complète. Les mises à jour d'informations doivent être régulières. Chaque agent ou nœud du réseau doit enregistrer les processus auquel il prend part. Les transactions doivent être bien-formées. Toutes les validations sur le contenu des informations qui peuvent être faites dans un élément de réseau doivent être faites.
Les applications doivent (i) authentifier chaque utilisateur et identifier ses rôles ainsi que ses droits vis à vis de la gestion des informations et des éléments du réseau, (ii) s'assurer qu'une politique de contrôle d'accès et d'utilisation est définie pour chaque information, et (iii) chiffrer l'information et mettre en place des mécanismes pour assurer des fonctions de contrôle d'accès et d'utilisation et plus généralement effectuer des validations structurelles et sémantiques non couvertes par les éléments du réseau (e.g., les applications doivent mettre en place des mécanismes de détection d'erreurs ou d'intrusions sur les étiquettes RFID ou les éléments du réseau, dont par exemple le système Deckard cité plus haut).
Que les propriétaires ou fournisseurs d'information aient créé ou non des politiques d'accès et d'usage pour leurs informations, afin d'assurer l'intégrité des informations, les applications doivent s'assurer (i) que les données collectées sont adéquates, pertinentes, non excessives et sont utilisées pour un but précis (e.g., une fouille de données avec un but légal), (ii) que les données ne sont pas gardées plus longtemps que nécessaire, et (iii) que les agents (entreprises, clients, etc.) peuvent accéder les données à leur sujet.

Le projet BRIDGE étudie diverses applications pour améliorer le partage, la recherche et la sécurité des informations [BRIDGE-IntegrityOfSupplyChain 07]. Ces applications utilisent les "services de découverte d'informations" et les EPC-IS d'EPCglobal. Les principales applications sont la vérification des produits, l'authentification des produits, le pédigrée électronique, et le traçage des produits. Pour ce dernier cas, les principaux problèmes sont (i) d'estimer l'emplacement des produits dans la chaine de distribution, et (ii) d'analyser les retards ou les déviations par rapport aux routes prévues, (iii) de prédire où les produits vont bientôt être vus. Pour cela, des algorithmes probabilistes et des règles sont utilisées (e.g., "si un produit est empaqueté, il faut traquer l'identificateur du paquet"). Comme les EPC-IS ne permettent pas aux utilisateurs qu'ils ne connaissent pas d'accéder à l'historique d'un produit, [AuthRFIDsyst 07] propose que l'application de traçage (ou, plus précisément, d'analyse de traces de produit) soit une application interne à EPCglobal à qui les EPC-IS autoriseraient l'accès aux historiques de produits ainsi que certaines autres informations potentiellement sensibles (par exemple les passages autorisées des étiquettes ou le fait qu'à cause d'un incident certaines étiquettes suivent un parcours exceptionnel mais autorisé) pour permettre à cette application d'effectuer certaines analyses comme par exemple la détection d'étiquettes clonées. Ceci permettrait donc à des consommateurs de savoir si leurs étiquettes sont clonées, sans que les informations nécessaires pour arriver à cette conclusion leur soient dévoilées.

4.4.3 Accessibilité des informations au niveau du réseau de communication et des applications

L'accès à tout objet (information ou support) doit être constamment maintenu. Ceci implique par exemple (i) d'éviter des mises hors service injustifiées, (ii) d'empêcher des monopolisations de ressources (e.g., des attaques par déni de services), et (iii) d'assurer la résilience des objets (e.g., via des copies de sauvegarde ou des serveurs miroirs).

L'inter-opérabilité entre objets doit être possible même lorsque certains objets ne sont pas sécurisés. Pour cela, if faut par exemple permettre (i) l'utilisation d'identifiants alloués temporairement, (ii) une restriction adaptée des accès, et (iii) l'utilisation de protocoles d'échanges ou de contrôle d'accès standards. C'est un des buts du projet BRIDGE.

4.6 Références

Les références débutant par le mot "Source" sont celles utilisées par les annexes "BSI-7.7" et "BSI-7.8".

[ASP 08] WP2 D2.5 (Privacy Specifications - ASPIRE FP7 215417) of the FP7 collaborative project ASPIRE (Advanced Sensors and lightweight Programmable middleware for Innovative Rfid Enterprise applications). June 13, 2008, http://fp7-aspire.eu/fileadmin/aspire/docs/D25final.pdf

[AuthRFIDsyst 07] Lehtonen, M., Michahelles, F., Fleisch, E.: Trust and Security in RFID-based Product Authentication Systems. IEEE Systems Journal, Volume 1, Issue 2, pp. 129-144, December 2007, http://www.systemsjournal.org/

[AuthRFID-GD 07] Dada, A., Magerkurth C.: Anti-Counterfeiting Based on Supply Chain Proximity. Proceedings of the 4th European Workshop on RFID Systems and Technology (RFID Sys-tech), 2008, http://www.alexandria.unisg.ch/Publikationen/44284/L-fr

[BRIDGE-AuthRFID 07] WP5 - Anti-Counterfeiting Business Application. July 11, 2007, http://www.bridge-project.eu/index.php/workpackage5/en/

[BRIDGE-AnalysisOfRFIDsecurity 07] WP04 - Security Analysis Report. July 11, 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-EconomicRelevanceOfSecureRFIDsyst 07] WP04 - The Economic Relevance of Secure RFID Solutions - a Qualitative Perspective (D4.1.3). December 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-IntegrityOfSupplyChain 07] WP04 - Supply Chain Integrity (D4.6.1). December 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-NetworkConfidentiality 07] WP04 - RFID Network Confidentiality (D 4.5.1). December 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-NetworkSecurity 07] WP04 - A Threat Model Analysis of EPC-based Information Sharing Networks. June 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-ReaderSecurity 07] WP04 - Trusted Networks: Design of an RFID Trusted Reader (D4.4.1). December 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-TagAntiCloning 07] WP04 - Report on first part of the security WP: Anti-Cloning Tag (D4.3.1). February 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BRIDGE-TagSecurity 07] WP04 - Report on first part of the security WP: Tag security (D4.2.1). July 11, 2007, http://www.bridge-project.eu/index.php/workpackage4/en/

[BSI 04] Security Aspects and Prospective Applications of RFID Systems. Study prepared for, and in cooperation with, the German Federal Office for Information Security (BSI) in an interdisciplinary collaborative arrangement between IZT - Institute for Futures Studies and Technology Assessment and the Swiss Federal Laboratories for Materials Testing and Research (EMPA). October 2004, http://www.bsi.bund.de/fachthem/rfid/RIKCHA_englisch.pdf

[CallControl 07] Campbell, G.A., Turner, K.J.: Ontologies to Support Call Control Policies. Telecommunications, 2007. AICT 2007. The Third Advanced International Conference on May 2007 Page(s):18 – 18
http://ieeexplore.ieee.org/iel5/4215214/4215215/04215239.pdf?tp=&arnumber=4215239&isnumber=4215215

[EPCarchi 07] The EPCglobal Architecture Framework, EPCglobal Final Version 1.2, approved 10 September 2007, http://www.epcglobalinc.org/standards/architecture/

[EPC-certif 08] EPCglobal Certificate Profile. May 14, 2008, http://www.epcglobalinc.org/standards/cert

[EPC-IS 07] EPC Information Services Standard (EPCIS) Version 1.0.1 Specification. September 21, 2007, http://www.epcglobalinc.org/standards/epcis/

[EPC-IS-FAQ 07] EPCIS (Electronic Product Code Information Service) - Frequently Asked Questions. April 27, 2007, http://www.epcglobalinc.org/standards/epcis/epcis_1_0-faq-20070427.pdf

[EPC-Pedigree 07] Pedigree Ratified Standard. January 5, 2007, http://www.epcglobalinc.org/standards/pedigree/

[GS1-GPC 07] Global Product Classification (GPC). Published GPC Standards, 10 December 2007, http://www.gs1.org/services/gsmp/kc/gpc/index.html

[GS1-128-barcodeForSupplyChain 08] http://en.wikipedia.org/wiki/GS1-128 and http://www.gs1.fr/gs1_fr/assistance_technique/les_codes_a_barres_gs1/le_code_a_barres_gs1_128

[Martin 05] Martin, P., Blumenstein, M., Deer, P.: Toward cooperatively-built knowledge repositories. Proceedings of ICCS 2005, 13th International Conference on Conceptual Structures (Springer, LNAI 3596, pp. 411-424), Kassel, Germany, July 18-22, 2005, http://www.webkb.org/doc/papers/iccs05/

[Martin 01] Martin, P., Eklund, P.: Large-scale cooperatively-built heterogeneous KBs. Proceedings of ICCS 2001, 9th International Conference on Conceptual Structures (Springer, LNAI 2120, pp. 231-244; electronically published on 21/1/2008), Stanford University, California, USA, July 30 to August 3, 2001, http://www.webkb.org/doc/papers/iccs01/

[OntologyOfRFIDsecurity 08] Martin, P.: Semantic classification of security requirements about RFID-related entities or processes. http://www.eurecom.fr/~martinph/PAC-ID/secure_rfid_management.html

[PRIME-whitePaper 08] Leenes, R, Schallaböck, J, Hansen, M.: PRIME white paper. Third and final version, 15 May 2008, https://www.prime-project.eu/prime_products/whitepaper/

[PRIME-architecture 08] Sommer, D., Casassa, M., Pearson, S.: PRIME Architecture. Version 3, July 9, 2008, https://www.prime-project.eu/prime_products/reports/arch/

[Source: Booz 04] Booz A. H. (in Kooperation mit der UNIVERSITÄT ST. GALLEN): RFID-Technologie: Neuer Innovationsmotor für Logistik und Industrie?. July 19, 2004, http://www.boozallen.de/content/downloads/5h_rfid.pdf

[Source: Comp 04c] Schinken an Zentrale: "Bin reif". In: Computerwoche Online: CW-EXTRA Nr. 01, February 15, 2002 & Seite 12-13, July 4, 2004, http://www1.computerwoche.de/heftarchiv/ 2002/20020215/a80106467.html

[Source: EC 95] EUROPEAN COMMISSION: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.

[Source: EPC 04] EPCGLOBAL INC. July 19, 2004, http://www.epcglobalinc.org

[Source: FiKe 04] FINKE, T., KELTER, H.: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. BSI, October 12, 2004, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

[Source: FSL 04] FLOERKEMEIER, C., SCHNEIDER, R., LANGHEINRICH, M.: Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004, http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf

[Source: Hilt 04] HILTY, LORENZ: Verselbständigt sich der Computer? Pervasive Computing könnte den Menschen schrittweise entmündigen. Electrosuisse Bulletin SEV/AES, September 2004

[Source: Klaß 04] KLAß, C.: Einkaufsbetrug mit RFID-Umprogrammierung. In: Networld, July 29, 2004 http://www.golem.de/0407/32666.html

[Source: LLS 00] LAW, C., LEE, K., SIU, K.Y.: Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Boston, MA, USA. 75-84, July 16, 2004, http://portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal

[Source: Weis 03] Weis, S.A.: Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, July 16, 2004, Massachusetts Institute of Technology, Cambridge, MA, USA, http://theory.lcs.mit.edu/~sweis

[XRAG2K 08] XRAG2K - Features and requirements, May 6, 2008, http://www.eurecom.fr/~martinph/PAC-ID/slides/XRAG2K/

[W3CWorshopOnPrivacyPolicy 06] W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement. October 17-18, 2006, Ispra/Italy. Actes du Workshop et résumés des discussions à http://www.w3.org/2006/07/privacy-ws/report

[Toninelli 05] Toninelli A., Kagal L., Bradshaw J.M., Montanari R.: Rule-based and Ontology-based Policies: Toward a Hybrid Approach to Control Agents in Pervasive Environments. Proceedings of the Semantic Web and Policy Workshop (SWPW), in conjunction with ISWC 2005, Galway, Ireland, November 7, 2005, http://www.cs.umbc.edu/swpw/papers/toninelli.pdf