Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1171

(02/2009)

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

Applications et services sécurisés – Sécurité des identificateurs en réseau

Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette

Recommandation UIT-T X.1171

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	X.1000–
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	X.1200–X.1299
APPLICATIONS ET SERVICES SÉCURISÉS	X.1300–X.1399

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

Recommandation UIT-T X.1171

Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette

Résumé

Le déploiement généralisé des étiquettes d'identification, notamment des étiquettes d'identification par radiofréquence (RFID), peut poser des problèmes d'atteinte à la vie privée, étant donné que les technologies RFID permettent de collecter (et de traiter) automatiquement des données, avec le risque que ces données soient divulguées (délibérément ou accidentellement).

S'agissant des applications utilisant l'identification par étiquette et fondées sur une étiquette d'identification personnalisée dans les applications de gestion après-vente personnalisées, les applications liées aux soins de santé, etc., la question de la confidentialité pose des problèmes de plus en plus graves. La présente Recommandation décrit plusieurs atteintes aux informations d'identification personnelle (PII) pour les applications utilisant l'identification par étiquette ainsi que les spécifications de protection des informations PII. En outre, elle présente une structure de base de la protection des informations PII fondée sur le profil des politiques PII.

Source

La Recommandation UIT-T X.1171 a été approuvée le 20 février 2009 par la Commission d'études 17 (2009-2012) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

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
1	Domaine d'application	1
2	Références	1
3	Définitions	2
	3.1 Termes définis ailleurs	2
	3.2 Termes définis dans la présente Recommandation	3
4	Abréviations et acronymes	3
5	Conventions	4
6	Considérations générales	4
7	Applications B2C utilisant l'identification par étiquette	4
8	Modèle de référence pour les applications B2C utilisant l'identification par étiquette	5
9	Atteintes aux informations PII dans les applications B2C utilisant l'identification par étiquette	6
	9.1 Divulgation d'informations associées à l'identificateur	6
	9.2 Divulgation des données relatives au contexte historique	7
	9.3 Relation entre des atteintes aux informations PII et le modèle de référence	8
10	Spécifications de protection des informations PII pour des applications B2C utilisant l'identification par étiquette	9
	10.1 Gestion des informations PII par l'utilisateur d'étiquette ID et/ou par l'utilisateur de terminal ID	9
	10.2 Authentification pour un utilisateur d'étiquette ID et/ou un utilisateur de terminal ID	9
	10.3 Contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application	9
	10.4 Confidentialité des informations associées à une étiquette ID	9
	10.5 Accord en vue de la collecte d'informations PII	9
	10.6 Garanties techniques pour les serveurs d'application	10
	10.7 Relation entre les spécifications et les atteintes aux informations PII	10
Annexe A – Principes fondamentaux applicables au plan national		11
Annexe B – Principes fondamentaux applicables au plan international: Libre circulation et restrictions légitimes		12
Appendice I – Localisation par l'identificateur dans les services RFID		13

Page

Appendice II – Service de protection des informations PII (PPS) pour les applications utilisant l'identification par étiquette 14
II.1 Service de protection des informations PII (PPS) pour les applications utilisant l'identification par étiquette 14
II.2 Entités de service du PPS pour les applications utilisant l'identification par étiquette 14
II.3 Scénario de service général pour le PPS 15
II.4 Fonctions du PPS 15
Bibliographie 19

Recommandation UIT-T X.1171[1]

Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette

1 Domaine d'application

Le domaine d'application de la présente Recommandation couvre les objectifs ci-dessous, en particulier les menaces et la protection requise pour les informations d'identification personnelle (PII) dans les applications utilisant l'identification par étiquette, décrites ci-après:

– décrire les menaces pour les informations PII dans un environnement entreprise-client (B2C) d'applications utilisant l'identification par étiquette;

– définir les spécifications de protection des informations PII dans un environnement entreprise-client d'applications utilisant l'identification par étiquette.

Les objectifs suivants n'entrent pas dans le cadre de la présente Recommandation:

– analyser les menaces à la sécurité générale et les spécifications applicables aux applications utilisant l'identification par étiquette;

– analyser les menaces pour les informations PII et les spécifications applicables entre une étiquette d'identification (ID) et un terminal ID;

– analyser les menaces aux informations PII et les spécifications applicables selon l'étiquetage ID spécifique et la méthode de lecture, par exemple une étiquette d'identification par radiofréquence (RFID) et un terminal ID;

– définir et développer les formats des messages et un mécanisme de protection des informations PII en fonction du profil des politiques PII des utilisateurs d'une application utilisant l'identification par étiquette.

NOTE 1 – Il conviendrait ultérieurement de définir ces formats, qui pourraient ne pas se limiter à la seule protection des informations PII utilisées aux fins d'identification par étiquette, mais peut-être moyennant une approche plus générale (respect de la vie privée).

Dans le cadre de la présente Recommandation, l'utilisateur d'une étiquette ID peut directement la contrôler de sorte qu'il est réputé être responsable de ce qui est fait de l'étiquette ID.

NOTE 2 – Dans certains cas, l'utilisateur d'une étiquette ID ne peut en aucun cas la contrôler. Par exemple, quelqu'un achète un produit étiqueté dont le fabriquant souhaite que l'étiquette ID reste active pour des raisons de garantie; dans ce scénario, l'utilisateur de l'étiquette ID peut donc être quiconque détient et utilise le produit étiqueté. La présente Recommandation ne saurait être appliquée pour résoudre le problème évoqué ci-dessus, le scénario en question soulevant des questions politiques et juridiques (voir [b-OCDE]). La problématique pourra être examinée dans une autre Recommandation.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'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 de Recommandation.

---

[1] La présente Recommandation peut ne pas être applicable en Allemagne à cause de la législation nationale.

[UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [b-UIT-T X.800]: Précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 serveur d'application [UIT-T X.1121]: Entité connectée à un réseau ouvert pour la transmission de données à des terminaux mobiles.

3.1.3 fournisseur de services d'application (ASP, *application service provider*) [UIT-T X.1121]: Entité (personne ou groupe) fournissant des services d'application aux utilisateurs mobiles par l'intermédiaire d'un serveur d'application.

3.1.4 authentification [b-UIT-T X.811]: Attestation de l'identité revendiquée par une entité.

NOTE – Le mot "identité" est utilisé sachant que, dans le domaine des télécommunications, il s'agit d'un identificateur ou ensemble d'identificateurs de confiance, c'est-à-dire considéré comme fiable dans une situation particulière pour représenter un élément de réseau, un équipement terminal de réseau ou un utilisateur, au terme d'un processus de validation. Au sens où le terme est utilisé ici, il n'est pas possible de conclure que les identificateurs de confiance constituent une validation positive d'une personne.

3.1.5 identificateur [b-UIT-T F.771]: Série de chiffres, caractères et symboles, ou de toute autre forme de données, utilisée pour identifier une identité du monde réel. Est utilisé pour représenter la relation entre l'entité du monde réel et ses informations/attributs informatisés. Cette relation permet aux utilisateurs d'accéder aux informations/attributs de l'entité stockés et informatisés via des terminaux ID d'utilisateurs.

3.1.6 étiquette ID [b-UIT-T F.771]: Petit objet physique stockant une petite quantité d'informations qui est un identificateur ou comprend un identificateur, avec d'autres données d'application additionnelles telles qu'un nom, un titre, un prix ou une adresse.

3.1.7 terminal ID [b-UIT-T F.771]: Dispositif pourvu d'une fonctionnalité de saisie de données à partir d'étiquettes ID, ainsi que d'autres fonctionnalités telles qu'une fonctionnalité de communication et une fonctionnalité de présentation d'informations multimédias. La fonctionnalité de saisie de données peut comprendre une fonction permettant d'obtenir un identificateur à partir d'étiquettes ID même sans fonctionnalité de communication, comme des codes barres et des codes barres 2D. Des exemples d'équipements utilisant des techniques de saisie de données sont les caméras numériques, les scanners optiques, les répéteurs RF, les systèmes IrDA, les lignes filaires galvaniques, etc.

3.1.8 réseau mobile [UIT-T X.1121]: Réseau fournissant des points d'accès sans fil à des terminaux mobiles.

3.1.9 terminal mobile [UIT-T X.1121]: Entité dotée d'une fonction d'accès sans fil et qui peut être connectée à un réseau mobile pour des communications de données avec des serveurs d'application ou d'autres terminaux mobiles.

3.1.10 utilisateur mobile [UIT-T X.1121]: Entité (personne) utilisant et exploitant un terminal mobile pour la réception de divers services assurés par des fournisseurs de services d'application.

3.1.11 informations d'identification personnelle (PII) [b-UIT-T Y.2720] : 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).

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 applications utilisant l'identification par étiquette: Applications mettant en œuvre au moins les éléments suivants: identificateur, terminal ID, étiquette ID et réseau(x). Dans cette application, l'identificateur est mémorisé sur une étiquette ID, et toutes les informations qui lui sont associées sont fournies du côté réseau.

NOTE – L'identificateur est mémorisé sur une étiquette ID (ou dans une étiquette ID, selon le type d'étiquette ID) et un terminal ID procède à la lecture ou à l'écriture de l'identificateur à partir/à destination de l'étiquette ID via un scanner optique (lecture uniquement), une caméra (lecture uniquement), un système IrDA (lecture/écriture), une technique RF (lecture/écriture) ou d'autres méthodes similaires.

3.2.2 entreprise-client (B2C, business-to-consumer): Relations commerciales entre des entreprises et des clients, où les clients de services fournissent aux consommateurs des services utiles et précieux, que les consommateurs utilisent.

3.2.3 profil des politiques PII par défaut: Ensemble formaté des règles et politiques de protection des informations PII d'une application utilisant l'identification par étiquette.

3.2.4 identification (ID): Procédure permettant d'identifier spécifiquement un objet à partir d'une classe importante d'objets par la lecture d'identificateurs d'étiquettes ID.

3.2.5 utilisateur d'étiquette ID: Personne qui achète et détient ou utilise un objet muni d'une étiquette ID.

3.2.6 utilisateur de terminal ID: Personne qui utilise et exploite un terminal ID. Un exemple type d'utilisateur de terminal ID pourrait être un utilisateur mobile équipé d'un terminal ID.

3.2.7 étiquette ID personnalisée: Etiquette ID contenant un identificateur permettant l'identification d'un individu plutôt que d'un objet anonyme.

3.2.8 service de protection des informations PII (PPS): Service de sécurité assurant la protection des informations PII pour les utilisateurs d'étiquettes ID et/ou de terminaux ID d'une application utilisant l'identification par étiquette. Le service PPS gère (c'est-à-dire crée/actualise/ supprime/applique) un profil des politiques PII d'utilisateur (d'étiquette ID et/ou de terminal ID) sur le réseau dans lequel tourne une application utilisant l'identification par étiquette.

3.2.9 profil des politiques PII: Ensemble formaté des règles et des politiques de protection des informations PII.

3.2.10 profil des politiques PII défini par l'utilisateur: Ensemble formaté des règles et des politiques de protection des informations PII défini par l'utilisateur (d'une étiquette ID et/ou d'un terminal ID).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASP Fournisseur de services d'application (*application service provider*)

B2C Entreprise-client (*business-to-customer*)

ID Identification

IrDA Infrared data association

OCDE Organisation de coopération et de développement économiques

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

PPS Service de protection des informations PII (*PII protection service*)

RF Fréquence radioélectrique (*radio frequency*)

RFID Identification par radiofréquence (*radio frequency identification*)

SCM Gestion de la chaîne d'approvisionnement (*supply chain management*)

5 Conventions

Sans objet.

6 Considérations générales

Le déploiement généralisé des étiquettes d'identification (notamment des étiquettes RFID) peut poser des problèmes d'atteinte à la vie privée, étant donné que les technologies RFID permettent de collecter (et de traiter) automatiquement des données, avec le risque que ces données soient divulguées (délibérément ou accidentellement).

S'agissant des applications utilisant l'identification par étiquette et fondées sur une étiquette d'identification personnalisée dans les applications de gestion après vente personnalisées, les applications liées aux soins de santé, etc., la question de la confidentialité pose des problèmes de plus en plus graves.

Au niveau des universités et de l'industrie, la plupart des efforts pour élaborer des mécanismes de protection des informations PII ont porté sur l'élaboration de protocoles d'authentification entre l'étiquette ID et le terminal ID. On observera toutefois que ces efforts ne peuvent s'appliquer à l'environnement effectif, en particulier aux applications utilisant l'identification par étiquette, environnement où des informations utiles de l'identificateur existent sur le serveur dans le domaine du réseau; il est donc essentiel d'élaborer un mécanisme de protection des informations PII qui soit adapté à l'environnement des applications utilisant une identification par étiquette. A cet égard, une des nombreuses solutions possibles pourrait être un mécanisme de protection des informations PII qui soit fonction du profil.

La présente Recommandation décrit les atteintes aux informations PII dans l'environnement d'applications utilisant l'identification par étiquette, les spécifications de protection des informations PII et la structure de base de la protection des informations PII fondées sur le profil des politiques PII défini par l'utilisateur.

7 Applications B2C utilisant l'identification par étiquette

Une application utilisant l'identification par étiquette se définit comme une application d'identification élargie et plus générale utilisée pour communiquer avec une série de réseaux, entre des réseaux et des systèmes d'application globalement distribués. En d'autres termes, une application utilisant l'identification par étiquette est une application basée sur le réseau mondial, déclenchée par une étiquette ID (y compris une étiquette RFID).

Des applications de ce type ont déjà fait l'objet d'une adoption généralisée dans des secteurs industriels, comme par exemple la gestion de la chaîne d'approvisionnement et la gestion d'entrepôts, mais également dans le cadre de mesures de lutte anticontrefaçons dans la chaîne d'approvisionnement de médicaments. L'application d'identification par étiquette est maintenant étendue au niveau des utilisateurs finals (par exemple fourniture de contenu d'informations de produits déclenchées par une étiquette ID, gestion après-vente de l'objet physique, dossiers des patients, gestion des péages, etc.) tout en progressant dans le domaine industriel.

Les applications B2C utilisant l'identification par étiquette peuvent se classer en trois types, comme suit:

a) L'utilisateur du terminal ID est le client: Par exemple, dans le service de fourniture de contenu d'informations, le client extrait les informations au moyen de son terminal ID. Dans ce type de service, la plupart des fournisseurs de services d'application peuvent supposer que le terminal ID a une fonctionnalité de télécommunication mobile doublée d'une fonctionnalité de présentation des informations multimédias. La Figure 1 montre un modèle de base de ce type d'application utilisant l'identification par étiquette, se composant de deux opérations de base sur le réseau: la résolution ID et l'extraction du contenu. La résolution ID est la procédure consistant à traduire ou à "réduire" un identificateur en une adresse [b-UIT-T Y.2213]. Le terminal mobile pourvu d'un terminal ID commence par réduire un identificateur, qu'il a reçu en provenance de l'étiquette ID via le service d'annuaire, avant d'exécuter une opération d'extraction du contenu.

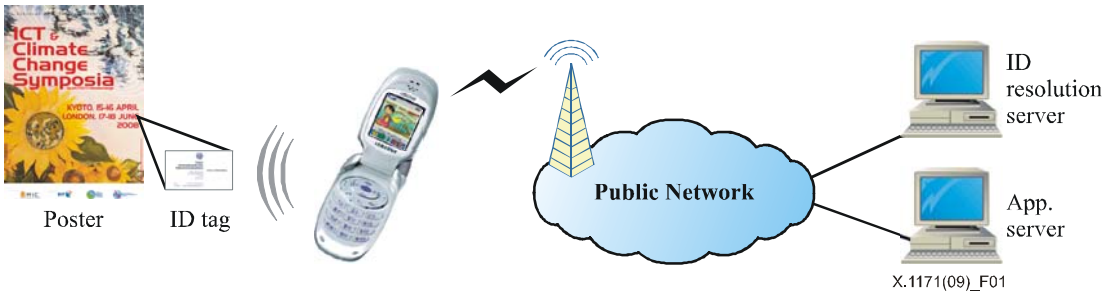

Figure 1 – Modèle de base d'une application B2C utilisant l'identification par étiquette

b) L'utilisateur de l'étiquette ID est le client: Un exemple type de cette application B2C utilisant l'identification par étiquette concerne le contrôle d'accès et/ou l'authentification, par exemple le contrôle des entrées, les passeports, les permis, le service de gestion après-vente, etc. Dans ce type de modèle d'application, les terminaux ID sont des terminaux fixes et/ou des terminaux mobiles; le client n'a pas besoin de posséder son propre terminal ID.

c) Le client est à la fois utilisateur de l'étiquette ID et du terminal ID: Dans le service d'extraction des informations relatives à des produits (type de base de l'application B2C utilisant l'identification par étiquette), le client devient à son tour utilisateur de l'étiquette dès qu'il achète le produit étiqueté après avoir lu les informations relatives au produit avec son terminal mobile. Un autre exemple peut être un service dans le domaine des soins de santé déclenché par une carte de patient dotée d'une étiquette ID; dans cette application, les types de "clients" sont nombreux: par exemple le patient, le médecin, l'infirmière, etc., qui peuvent utiliser l'étiquette ID. L'utilisateur de l'étiquette ID peut consulter son propre dossier médical grâce au terminal mobile pourvu d'un terminal ID en lisant sa carte de patient qui est dotée d'une étiquette ID.

De nombreuses applications avec l'identification par étiquette étant transformées en applications B2C, les consommateurs sont très préoccupés par le risque de divulgation des informations PII via les étiquettes ID. La présente Recommandation porte pour l'essentiel sur le modèle d'application B2C utilisant l'identification par étiquette.

8 Modèle de référence pour les applications B2C utilisant l'identification par étiquette

La Figure 2 illustre un modèle de référence pour les applications B2C utilisant l'identification par étiquette.

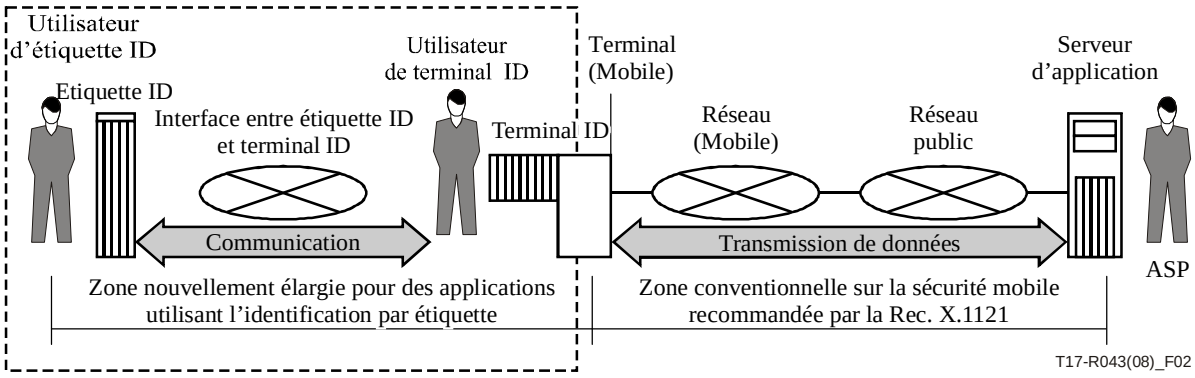

Figure 2 – Modèle de référence pour les applications B2C utilisant l'identification par étiquette

Ce modèle de référence est un modèle augmenté de la transmission de données mobile de bout en bout exposé dans [UIT-T X.1121]. Parmi les entités nouvellement ajoutées figurent une étiquette ID, un utilisateur d'étiquette ID, une interface entre l'étiquette ID et le terminal ID, et un terminal ID. Dans ce modèle, le terminal (mobile) peut être un terminal fixe, câblé, mais aussi un terminal mobile sans fil, et peut être considéré comme un terminal ID.

9 Atteintes aux informations PII dans les applications B2C utilisant l'identification par étiquette

Dans l'environnement des applications utilisant l'identification par étiquette, de sérieux problèmes d'atteinte aux informations PII se posent dans les cas où la propriété d'un produit ou d'un document pourvu d'une étiquette ID est transférée à un particulier.

Dans l'environnement des applications utilisant l'identification par étiquette, il existe plusieurs méthodes de stockage/lecture de l'identificateur, par exemple un code barre (bidimensionnel) et un lecteur optique (ou caméra), une étiquette RFID passive et un lecteur dans le champ proche, une étiquette RFID passive et un lecteur dans le champ lointain. La présente section ne concerne que les fuites génériques d'informations PII dans un environnement B2C d'application utilisant l'identification par étiquette. Plus précisément, la présente Recommandation ne traite pas des menaces suivantes:

– Menaces à la sécurité générale dans les applications utilisant l'identification par étiquette: la présente section ne s'attache qu'aux menaces pour les informations PII dans les applications utilisant l'identification par étiquette.

– Menaces propres aux méthodes de stockage/lecture de l'identificateur: par exemple, dans le cas d'une étiquette RFID, un "pirate" peut réussir à situer l'utilisateur de l'étiquette ID du produit étiqueté par une RFID grâce à l'identificateur de cette étiquette RFID. L'Appendice I explique en détail cette possibilité de situer avec précision un utilisateur dans l'environnement RFID.

– Menaces entre une étiquette ID et un terminal ID: la présente section ne concerne que les menaces pour les informations PII du côté réseau.

9.1 Divulgation d'informations associées à l'identificateur

Le pirate peut lire des informations de l'étiquette ID sans qu'en soit conscient l'utilisateur de l'étiquette ID du produit étiqueté. D'abord, le pirate lit un identificateur émis par l'étiquette ID que porte l'utilisateur; ensuite, il réduit l'identificateur et demande au service d'annuaire la localisation des informations; enfin, il demande des informations associées à l'étiquette ID. En outre, si les informations concernent des PII, telles que des informations sur une carte de crédit ou un dossier

médical, etc., il peut s'ensuivre une atteinte beaucoup plus grave aux informations PII de l'utilisateur de l'étiquette ID. La Figure 3 illustre une atteinte aux informations PII par suite de la divulgation de renseignements; dans cette hypothèse, le pirate peut collecter des informations dynamiques (heure et lieu de l'achat du produit étiqueté, informations de suivi du produit, etc.) ainsi que des informations statiques (par exemple nom et description du produit).

Pour éviter ce type d'atteinte aux informations PII, l'étiquette ID doit être retirée ou désactivée. Dans de nombreuses applications utilisant l'identification par étiquette, comme les services de gestion après-vente personnalisés, les services de soins de santé, etc., il est toutefois essentiel de préserver l'étiquette ID et sa fonctionnalité.

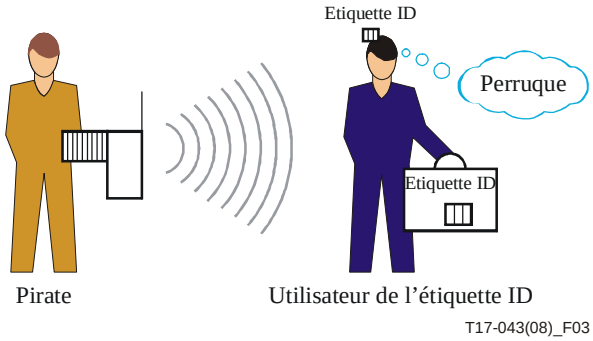

Figure 3 – Atteinte aux informations PII par suite d'une divulgation de renseignements

9.2 Divulgation des données relatives au contexte historique

Le pirate peut extraire des données significatives sur l'utilisateur (préférences, habitudes, centres d'intérêt, etc.), des données relatives au contexte historique associées à l'étiquette ID. En outre, il peut utiliser ce type de données à des fins illicites ou commerciales sans l'accord de l'utilisateur. Dans ce type d'atteinte, on entend par utilisateur celui du terminal ID; ce dernier lit l'identificateur des produits ou documents étiquetés à l'aide de son terminal ID et obtient d'utiles informations à partir du serveur d'applications dans le cas d'une application utilisant l'identification par étiquette. A ce moment, les diverses données en mémoire concernant le contexte (date de location d'un DVD, date et lieu d'achat d'un objet, lieu où a été lue l'affiche d'un film, etc.) peuvent être collectées par le réseau d'applications utilisant l'identification par étiquette; ces données peuvent être liées à l'utilisateur (voir la Figure 4).

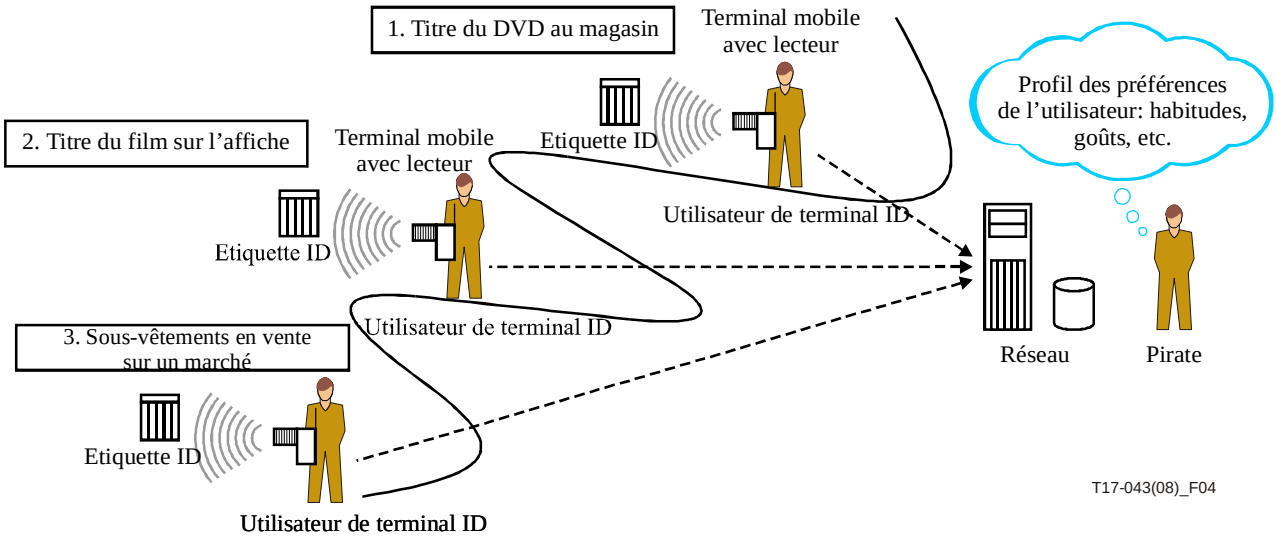

Figure 4 – Atteinte aux informations PII liée à la collecte de données relatives au contexte historique

9.3 Relation entre des atteintes aux informations PII et le modèle de référence

La relation entre des atteintes aux informations PII et les entités du modèle illustré à la Figure 2 est résumée au Tableau 1, dans lequel les cases signalées par un "X" indiquent qu'une atteinte aux informations PII visée dans la ligne est liée à une entité ou à une relation entre des entités figurant dans la colonne.

Tableau 1 – Relation entre des atteintes aux informations PII et le modèle de référence

Entités et relations entre entités	Atteintes	
	Divulgation d'informations fournies par une/des application(s) utilisant l'identification par étiquette	**Divulgation de données relatives au contexte historique stocké dans un/des serveur(s) d'application**
Relation entre l'utilisateur de l'étiquette ID et l'utilisateur du terminal ID		X
Relation entre le terminal (mobile) et le serveur d'application	X	X
Relation entre l'utilisateur de l'étiquette ID et le serveur d'application	X	
Relation entre l'étiquette ID et le serveur d'application	X	
Serveur d'application	X	X

10 Spécifications de protection des informations PII pour des applications B2C utilisant l'identification par étiquette

La présente section traite pour l'essentiel des spécifications techniques contre deux des atteintes aux informations PII analysées à la section 9. Des lignes directrices plus générales pour les utilisateurs et les fabricants d'étiquettes RFID concernant la protection des informations PII dans le contexte de la technologie RFID sont exposées dans d'autres Recommandations. Ces spécifications reposent en partie sur les principes tirés des Lignes directrices de l'OCDE régissant la protection de la vie privée [b-OCDE]. Les principes énoncés dans ce document ([b-OCDE]) et étudiés dans la présente section sont présentés dans l'Annexe A; d'autres principes tirés de ces lignes directrices sont exposés dans l'Annexe B. Les spécifications ci-dessous découlent des atteintes aux informations PII dans des applications B2C utilisant l'identification par étiquette:

– gestion des informations PII par un utilisateur d'étiquette ID et/ou par un utilisateur de terminal ID;
– authentification pour un utilisateur d'étiquette ID et/ou un utilisateur de terminal ID;
– contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application;
– confidentialité des informations associées à une étiquette ID;
– accord en vue de la collecte d'informations PII;
– garanties techniques pour les serveurs d'application.

10.1 Gestion des informations PII par l'utilisateur d'étiquette ID et/ou par l'utilisateur de terminal ID

Les utilisateurs d'étiquettes ID et/ou les utilisateurs de terminaux ID doivent être à même de gérer ou d'actualiser les informations PII associées à leurs étiquettes ID et/ou à leurs terminaux ID sur le réseau. Les utilisateurs peuvent ainsi déterminer quelles informations PII devraient être supprimées ou conservées dans l'application utilisant l'identification par étiquette. De plus, les utilisateurs peuvent fixer une limite de temps pour leurs informations PII dans l'application utilisant l'identification par étiquette.

10.2 Authentification pour un utilisateur d'étiquette ID et/ou un utilisateur de terminal ID

Le serveur d'application d'une application utilisant l'identification par étiquette est tenu d'offrir une procédure d'authentification destinée à l'utilisateur d'étiquette ID, et il peut au besoin offrir une procédure d'authentification de l'utilisateur de terminal ID (certaines applications utilisant l'identification par étiquette n'ont pas à authentifier l'utilisateur).

10.3 Contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application

Il conviendrait que l'accès aux informations PII d'utilisateurs d'étiquettes ID mémorisées par un serveur d'application soit sécurisé et limité aux personnes autorisées à demander de telles informations et aux informations pertinentes dont a besoin chacune de ces personnes.

10.4 Confidentialité des informations associées à une étiquette ID

Le serveur d'application pour une application utilisant l'identification par étiquette est tenu d'assurer la confidentialité des données pour faire en sorte que les informations associées à une étiquette ID ne puissent pas être lues par des utilisateurs non autorisés.

10.5 Accord en vue de la collecte d'informations PII

Le serveur d'application pour une application utilisant l'identification par étiquette est tenu d'offrir une procédure d'accord en vue de la collecte d'informations PII, y compris des données archivées

relatives à l'utilisateur de terminal ID. L'application utilisant l'identification par étiquette constitue une solution technique qui permet de garder des informations PII aussi précises et récentes que l'exigent les fins déterminées et de les limiter aux informations pertinentes nécessaires. Il conviendrait que l'application indique les finalités de la collecte des informations PII lors de la procédure d'accord. Un accord supplémentaire de l'utilisateur est nécessaire pour pouvoir utiliser les informations PII collectées précédemment à des fins autres que celles prévues initialement.

10.6 Garanties techniques pour les serveurs d'application

Le fournisseur ASP d'une application utilisant l'identification par étiquette qui traite des informations PII est tenu d'adopter des mesures de sécurité technique pour les serveurs d'application, et notamment pour les informations PII.

10.7 Relation entre les spécifications et les atteintes aux informations PII

Le Tableau 2 résume la relation existant entre les spécifications de protection des informations PII et les atteintes à ces mêmes informations. Dans le tableau, les cases signalées par un "X" indiquent qu'une atteinte aux informations PII visée dans la colonne se rapporte à une spécification de protection des informations PII figurant sur la ligne.

Tableau 2 – Relation entre les spécifications et les atteintes aux informations PII

Spécifications	**Atteintes**	
	Divulgation d'informations associées à l'identificateur	**Divulgation de données relatives au contexte historique**
Gestion des informations PII par l'utilisateur d'étiquette ID et/ou par l'utilisateur de terminal ID	X	
Authentification pour un utilisateur d'étiquette ID et/ou de terminal ID	X	X
Contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application	X	
Confidentialité des informations associées à une étiquette ID	X	X
Accord en vue de la collecte d'informations PII		X
Garanties techniques pour les serveurs d'application	X	X

Annexe A

Principes fondamentaux applicables au plan national[2]

(Cette annexe fait partie intégrante de la présente Recommandation)

- Limitation en matière de collecte: Il conviendrait d'assigner des limites à la collecte des données de 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 de 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 de 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 de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées.
- Garanties de sécurité: Il conviendrait de protéger les données de 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 de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de 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.

---

[2] Ces principes sont extraits de la Partie II des "Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel", OCDE, 1980.

Annexe B[3]

Principes fondamentaux applicables au plan international: Libre circulation et restrictions légitimes

(Cette annexe fait partie intégrante de la présente Recommandation)

– Les pays Membres devraient prendre en considération les conséquences pour d'autres pays Membres d'un traitement effectué sur leur propre territoire et de la réexportation des données de caractère personnel.

– Les pays Membres devraient prendre toutes les mesures raisonnables et appropriées pour assurer que les flux transfrontières de données de caractère personnel, et notamment le transit par un pays Membre, aient lieu sans interruption et en toute sécurité.

– Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, sauf lorsqu'un ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de protection équivalente.

– Les pays Membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-delà des exigences propres à cette protection.

---

[3] Ces principes sont extraits de la Partie III des "Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel", OCDE, 1980.

Appendice I

Localisation par l'identificateur dans les services RFID

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

Le pirate peut localiser l'utilisateur de l'étiquette ID du produit étiqueté grâce à l'identificateur de l'étiquette RFID; ce type de violation des règles de sécurité permet de pister ou de surveiller un identificateur d'étiquette donné à l'aide d'un lecteur RFID invisible et illicite. Etant donné que le pirate peut utiliser l'identificateur de l'étiquette comme identificateur personnel, il peut facilement localiser l'utilisateur, comme il est indiqué à la Figure I.1.

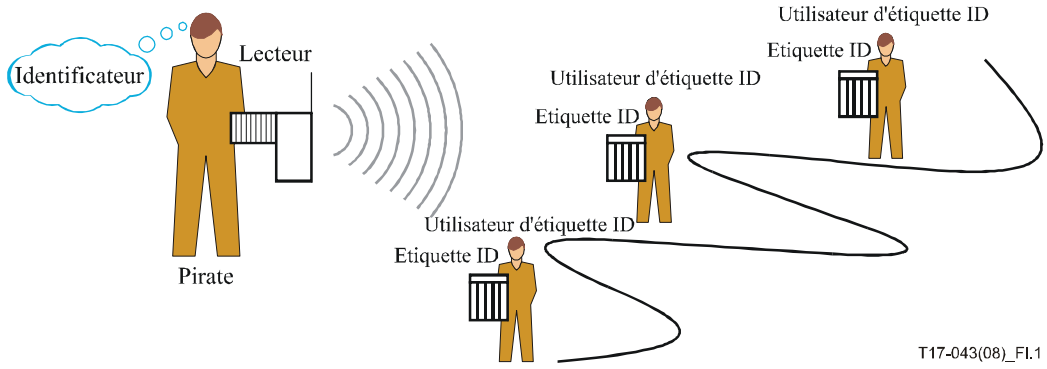

Figure I.1 – Menace pour les règles de sécurité par la localisation d'une personne

Afin de protéger la traçabilité de l'identificateur, on peut utiliser une méthode d'authentification entre l'étiquette RFID et le lecteur: l'étiquette RFID donne au lecteur son identificateur uniquement si le lecteur est authentifié par l'étiquette RFID; en d'autres termes, le pirate ne peut pas obtenir l'identificateur de l'étiquette sans effectuer la procédure d'authentification. Toutefois, si l'étiquette RFID n'est pas suffisamment puissante pour effectuer des opérations nécessitant des calculs importants, tels que des calculs cryptographiques, cette méthode d'authentification peut ne pas être une solution réaliste.

Une autre solution peut être la technique de recodage de l'identificateur, qui consiste à recoder l'identificateur de l'étiquette RFID périodiquement avec un pseudo-identificateur (ou méta-identificateur) et donc de réduire la connectivité de l'identificateur de l'étiquette RFID à son utilisateur. On observera toutefois que cette méthode de recodage n'est pas applicable si l'étiquette RFID n'a pas de fonctionnalité d'accessibilité en écriture, ou si l'étiquette ID utilise un format d'identificateur particulier (comme le code EPC ([b-EPCglobal])). En outre, l'utilité de cette technique se limite aux services qui exigent une lecture fréquente de l'étiquette RFID, ce qui peut donner une grande complexité du côté du serveur.

Appendice II

Service de protection des informations PII (PPS) pour les applications utilisant l'identification par étiquette

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

II.1 Service de protection des informations PII (PPS) pour les applications utilisant l'identification par étiquette

Le service PPS est un exemple de service de protection des informations PII basé sur le profil des politiques PII de l'utilisateur.

La section II.3 illustre un scénario de service général du PPS pour une application utilisant l'identification par étiquette. Pour le PPS, l'utilisateur de l'étiquette ID ou du terminal ID demandant une application spécifique utilisant l'identification par étiquette crée ses propres politiques de protection PII pour ce type d'application et les communique à un système tiers de confiance (système PPS); ce dernier crée alors le profil des politiques PII de l'utilisateur et l'envoie aux serveurs d'application (systèmes côté service). A ce moment, les serveurs d'application peuvent contrôler l'accès aux informations PII associées à l'utilisateur d'étiquette ID et/ou de terminal ID.

II.2 Entités de service du PPS pour les applications utilisant l'identification par étiquette

Le PPS a trois entités de service qui sont (voir la Figure II.1):

– Système PPS: en tant qu'entité chargée de la fonction de gestion des politiques PII de l'utilisateur, cette entité crée le profil des politiques PII défini par l'utilisateur pour les politiques PII de l'utilisateur et fournit ce profil au(x) système(s) côté service.

  NOTE – Dans le cas d'un système PPS centralisé qui est responsable de nombreuses applications utilisant l'identification par étiquette, il conviendrait de prévoir des contremesures appropriées face à un seul cas de dysfonctionnement; toutefois, selon l'utilisation, il peut n'y avoir qu'un seul système PPS pour une application utilisant l'identification par étiquette.

– Système côté service: entité qui fournit des informations relatives à l'identificateur d'une étiquette ID, c'est-à-dire qu'elle peut être considérée comme un serveur d'application dans une application utilisant l'identification par étiquette. Il peut en conséquence exister de nombreux systèmes côté service pour une application utilisant l'identification par étiquette. Cette entité assure une fonction de contrôle d'accès en utilisant le profil des politiques PII défini par l'utilisateur ou le profil des politiques PII par défaut.

– Système côté utilisateur: entité chargée de la fonction d'accès réseau sans fil (ou filaire) et, au besoin, d'une fonction de saisie de l'identificateur, cette entité pourrait être un terminal mobile pourvu d'un terminal ID. L'utilisateur d'étiquette ID et/ou du terminal ID peut accéder aux systèmes côté service et au système PPS grâce à un système côté utilisateur de ce type. Utilisant le système côté utilisateur, l'utilisateur vérifie sa politique de protection des informations PII pour une application spécifique utilisant l'identification par étiquette.

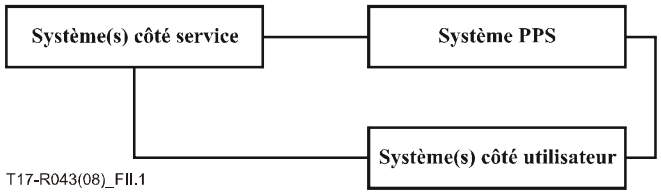

Figure II.1 – Entités de service du PPS pour les applications utilisant l'identification par étiquette

II.3 Scénario de service général pour le PPS

Le scénario de service pour le PPS correspond en général à une procédure de personnalisation par étiquette, comme dans le cas de l'achat d'un produit étiqueté. La Figure II.2 illustre le flux PPS général pour l'application utilisant l'identification par étiquette.

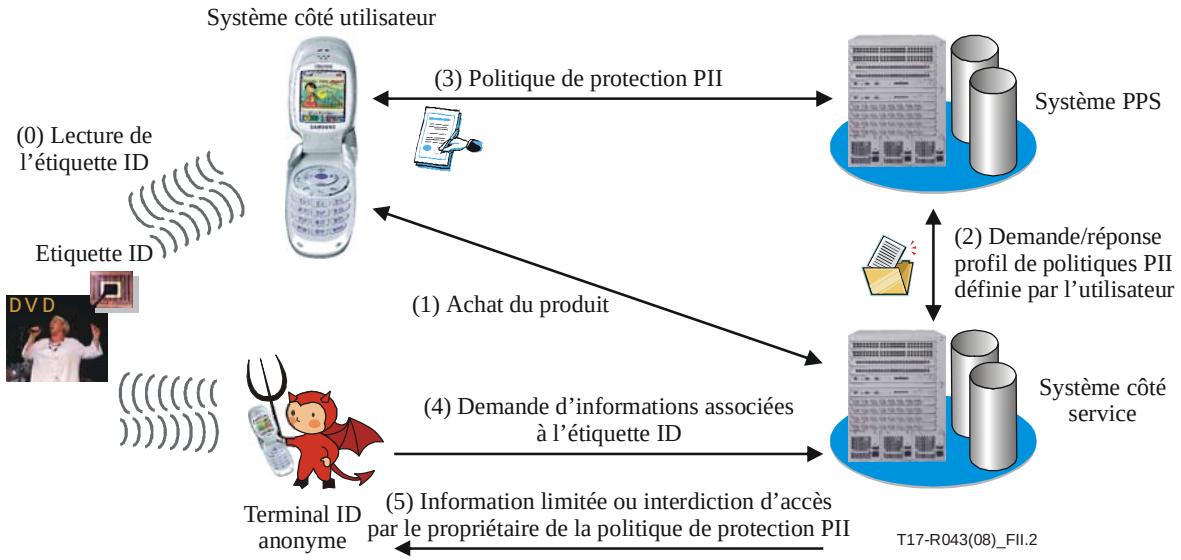

Figure II.2 – Flux PPS général

0) Un consommateur lit l'identificateur du produit étiqueté à l'aide de son terminal mobile équipé d'un terminal ID.

1) Le consommateur consulte les informations sur le produit à partir du réseau de services d'application, puis achète le produit en utilisant l'une des diverses méthodes de paiement. A ce moment, le consommateur devient l'utilisateur de l'étiquette ID.

2) L'application utilisant l'identification par étiquette demande ensuite au système PPS de lui fournir le profil des politiques PII définies par l'utilisateur, le système fournissant alors à l'application le profil PII en question.

3) Le système PPS reçoit la politique de protection des informations PII de l'utilisateur pour cette application.

4) N'importe qui peut demander les informations associées à cette étiquette ID depuis le système côté service.

5) Le demandeur peut consulter toutes les informations fournies par le système côté service s'il est l'utilisateur de l'étiquette ID. Sinon, soit le demandeur obtient des informations limitées, soit il ne peut pas accéder à une quelconque information.

NOTE – Un travail complémentaire devra être fait pour étudier les différents scénarios de cas d'utilisation du PPS pour des applications utilisant l'identification par étiquette, pouvant décrire les avantages du PPS.

II.4 Fonctions du PPS

Pour satisfaire aux spécifications de protection des informations PII des applications utilisant l'identification par étiquette, le PPS doit avoir les fonctions suivantes:

– Gestion du profil des politiques PII.

– Contrôle d'accès.

– Enregistrement.

– Transmission du profil des politiques PII.

– Actualisation du profil des politiques PII.

II.4.1 Gestion du profil des politiques PII

La gestion du profil des politiques PII est une fonction essentielle du PPS. Le système PPS gère deux types de profils des politiques PII, à savoir:

– Un profil des politiques PII par défaut: il s'agit d'un ensemble formaté des règles et des politiques de protection des informations PII d'une application utilisant l'identification par étiquette. Ces règles peuvent être basées sur des pratiques d'information équitables, telles que celles décrites dans les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ([b-OCDE]).

– Un profil des politiques PII défini par l'utilisateur: il s'agit d'un ensemble formaté des règles et politiques de protection PII définies par l'utilisateur de l'étiquette ID et/ou du terminal ID.

Le système PPS établit et gère le profil des politiques PII défini par l'utilisateur (ou par défaut). En particulier, il devrait créer et gérer le profil des politiques PII par défaut pour une application utilisant l'identification par étiquette et le profil des politiques PII défini par l'utilisateur à partir des politiques de protection des informations PII de l'utilisateur déterminées lors de la procédure d'enregistrement. Ce profil des politiques PII peut donc être envoyé au(x) système(s) côté service; d'une façon générale, il peut contenir les éléments suivants:

– Politique de divulgation pour les ressources d'information (y compris les informations PII).

– Politique d'expiration pour les ressources d'information.

– Politique de collecte des registres d'événements.

Le système côté service contrôle ensuite l'accès aux ressources d'information à l'aide de ce profil des politiques PII pour chaque demandeur d'information.

II.4.2 Contrôle d'accès

La fonction de contrôle d'accès du système PPS sert à authentifier l'identité de l'utilisateur, ou de l'ASP, et à autoriser l'accès aux ressources d'information de l'utilisateur, qui correspondent principalement aux politiques de protection des informations PII du titulaire.

NOTE – Le terme identité est utilisé sachant que, dans le domaine des télécommunications, il s'agit d'un identificateur ou d'un ensemble d'identificateurs de confiance, c'est-à-dire considéré comme étant de confiance aux fins d'une situation particulière pour représenter un élément de réseau, un équipement terminal de réseau, ou un utilisateur, au terme d'un processus de validation. Etant donné la manière dont ce terme est utilisé ici, il ne peut être conclu que des identificateurs de confiance constituent la validation positive d'une personne.

D'un autre côté, la fonction de contrôle d'accès du système côté service est un élément essentiel du PPS, étant donné que le système côté service devrait contrôler l'accès à toutes les ressources d'information, et fournir des informations PII compte tenu du profil des politiques PII défini par l'utilisateur (ou le profil par défaut en l'absence de profil défini par l'utilisateur). Le système côté service doit être à même de déterminer si un demandeur a accès à certaines informations PII de l'utilisateur compte tenu du profil des politiques PII défini par le titulaire.

II.4.3 Enregistrement

Le système côté service et le système côté utilisateur ont une procédure d'enregistrement avec le système PPS. Dans la procédure d'enregistrement, les informations d'enregistrement fournies par les systèmes côté service et côté utilisateur se présentent comme suit:

– Système côté service: des informations d'identité (y compris des informations d'authentification telles qu'un mot de passe) et un type d'informations (c'est-à-dire des informations de prix, la méthode d'achat, etc.) fournis à un système côté utilisateur par le serveur d'application utilisant l'identification par étiquette.

– Système côté utilisateur: des informations d'identité (y compris des informations d'authentification telles qu'un mot de passe) et les propres politiques de protection PII de l'utilisateur ainsi que l'accord de ce dernier pour l'application utilisant l'identification par étiquette.

Le système PPS devrait créer le profil des politiques PII par défaut pour le système côté service et le lui fournir (voir la Figure II.3). Le profil des politiques PII par défaut peut être créé par l'intermédiaire de la fonctionnalité de gestion du profil PII.

Par ailleurs, le système PPS devrait créer le profil des politiques PII défini par l'utilisateur en fonction des politiques de protection PII de l'utilisateur. La Figure II.3 illustre la procédure d'enregistrement du PPS.

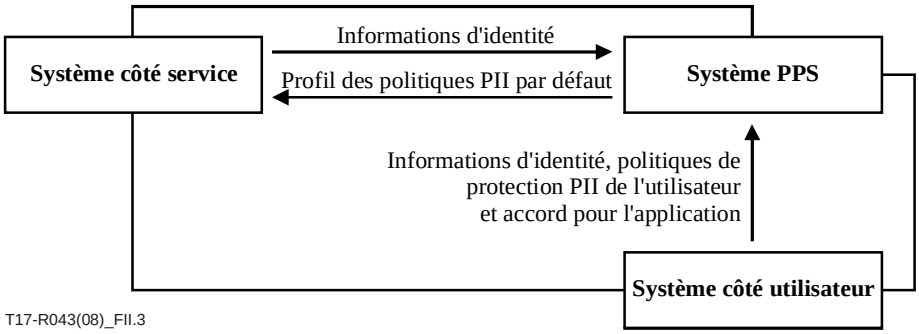

Figure II.3 – Procédure d'enregistrement

II.4.4 Transmission du profil des politiques PII

La procédure de transmission du profil des politiques PII est déclenchée par le système côté service. La Figure II.4 illustre cette procédure.

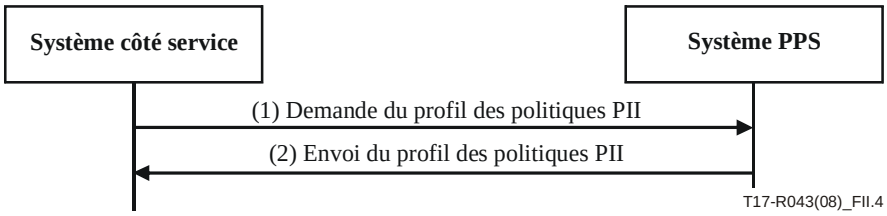

Figure II.4 – Procédure de transmission du profil des politiques PII

1) Demande de profil des politiques PII: le système côté service demande le profil des politiques PII défini par l'utilisateur avec l'identité de ce dernier.
2) Envoi du profil des politiques PII: le système PPS vérifie le profil des politiques PII défini par l'utilisateur pour cet utilisateur et l'envoie.

NOTE – Le terme identité est utilisé sachant que, dans le domaine des télécommunications, il s'agit d'un identificateur ou d'un ensemble d'identificateurs de confiance, c'est-à-dire considéré comme étant de confiance aux fins d'une situation particulière pour représenter un élément de réseau, un équipement terminal de réseau, ou un utilisateur, au terme d'un processus de validation. Etant donné la manière dont ce terme est utilisé ici, il ne peut pas être conclu que des identificateurs de confiance constituent la validation positive d'une personne.

II.4.5 Actualisation du profil des politiques PII

La procédure d'actualisation du profil des politiques PII est déclenchée par le système PPS. Lorsque l'utilisateur change ses politiques de protection PII, le système PPS régénère le profil des politiques PII défini par l'utilisateur. Il envoie ensuite le message d'actualisation du profil à tous les systèmes côté service enregistrés dans le système PPS. Chaque système côté service actualise ensuite le profil des politiques PII défini par l'utilisateur et envoie le message de réponse d'actualisation de ce profil. La Figure II.5 illustre la procédure d'actualisation du profil des politiques PII.

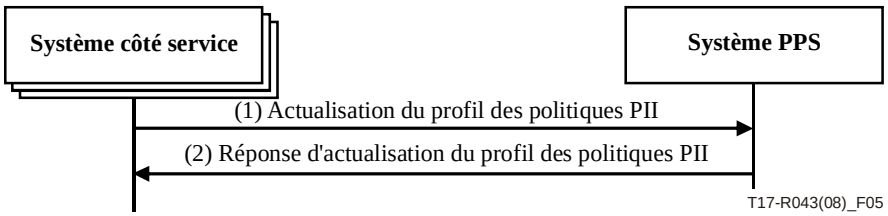

Figure II.5 – Procédure d'actualisation du profil des politiques PII

1) Actualisation du profil des politiques PII: le système PPS envoie la version actualisée du profil des politiques PII défini par l'utilisateur à chaque système côté service.
2) Réponse d'actualisation du profil des politiques PPI: chaque système côté service envoie le message de réponse d'actualisation au système PPS.

Bibliographie

[b-UIT-T F.771] Recommandation UIT-T F.771 (2008), *Description et spécifications du service d'accès à des informations multimédias déclenché par une identification basée sur une étiquette*.

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[b-UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2: 1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour systèmes ouverts: cadre d'authentification*.

[b-UIT-T Y.2091] Recommandation UIT-T Y.2091 (2008), *Termes et définitions pour les réseaux de prochaine génération*.

[b-UIT-T Y.2213] Recommandation UIT-T Y.2213 (2008), *Exigences et capacités liées aux services NGN concernant les aspects réseau des applications et services utilisant une identification par étiquette*.

[b-UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN*.

[b-EPCglobal] EPCglobal standard (2008), *EPCglobal Tag Data Standards Version 1.4*. <http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf>

[b-OCDE] OCDE (1980), *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*. <http://www.oecdbookshop.org/oecd/display.asp?CID=&LANG=EN&SF1=DI&ST1=5LMQCR2K94S8l>

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, 2009