Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1363

(05/2020)

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

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Cadre technique applicable au traitement des informations d'identification personnelle dans l'environnement de l'Internet des objets

Recommandation UIT-T X.1363

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
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 (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1363

Cadre technique applicable au traitement des informations d'identification personnelle dans l'environnement de l'Internet des objets

Résumé

Les dispositifs de l'Internet des objets (IoT) peuvent recueillir des données très diverses, notamment des informations d'identification personnelle (PII). Dans la mesure où les données PII sont utiles pour différents types de services, elles peuvent être partagées entre de multiples fournisseurs de services.

Il est préférable, pour les utilisateurs, de pouvoir gérer comme ils le souhaitent leurs propres données, notamment leurs informations d'identification personnelle, dans l'environnement IoT. L'utilisation des données dans l'environnement IoT avec de multiples fournisseurs de services étant complexe, il convient de s'adapter de façon souple aux souhaits des utilisateurs concernant l'utilisation des données. À titre d'exemple, si un fournisseur de services IoT propose les fonctions ci-après, il est souhaitable, pour les utilisateurs, que le fournisseur de services collecte des données (y compris des données PII) et les contrôle de manière appropriée:

- Les utilisateurs peuvent configurer leurs propres préférences PII, notamment en définissant la liste des données qu'il est permis de partager avec d'autres fournisseurs de services.
- La collecte et le partage des données sont soumis à un contrôle d'accès fondé sur les préférences PII. Les données non autorisées ne peuvent pas être stockées dans une mémoire de données, ni partagées avec d'autres fournisseurs de services.
- Les utilisateurs peuvent consulter le journal contenant l'historique du partage de données entre les fournisseurs de services. Ils peuvent aussi vérifier à quel moment leurs données ont été partagées.

La Recommandation UIT-T X.1363 définit un cadre technique applicable au traitement des informations PII dans un environnement de l'Internet des objets avec un ou plusieurs fournisseurs de services.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1363	29-05-2020	17	11.1002/1000/14087

Mots clés

IoT, PII, informations d'identification personnelle.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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 on 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 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

Recommandation UIT-T X.1363

Cadre technique applicable au traitement des informations d'identification personnelle dans l'environnement de l'Internet des objets

1 Domaine d'application

La présente Recommandation définit un cadre technique applicable au traitement des informations d'identification personnelle (PII) dans l'environnement de l'Internet des objets (IoT).

Dans l'environnement de l'Internet des objets, certains dispositifs IoT ont la capacité de collecter des données PII. Dans la mesure où les données PII sont utiles pour différents types de services, elles peuvent être partagées entre de multiples fournisseurs de services. Le cadre technique défini dans la présente Recommandation prévoit un mécanisme de protection des données PII des utilisateurs de l'IoT lorsque ces données sont collectées, partagées et utilisées par un ou plusieurs fournisseurs de services IoT.

2 Références

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

[UIT-T X.1058] Recommandation UIT-T X.1058 (2017) | ISO/CEI 29151:2017, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle*.

[ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [b-ISO/CEI 27000]: méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte.

3.1.2 contrôle d'accès [b-ISO/CEI 10027]: capacité de restreindre l'utilisation des services accédant aux données pour les utilisateurs ayant été préalablement autorisés.

3.1.3 mesure de sécurité [b-ISO/CEI 27000]: mesure qui modifie un **risque** (3.1.16).

NOTE 1 – Les mesures de sécurité comprennent tous les **processus** (3.1.15), **politiques** (3.1.14), dispositifs, pratiques ou autres actions qui modifient un **risque** (3.1.16).

NOTE 2 – Il est possible que les mesures de sécurité ne puissent pas toujours aboutir à la modification voulue ou supposée.

3.1.4 dispositif [b-UIT-T Y.4000]: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

3.1.5 Internet des objets (IoT) [b-UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

NOTE 1 – En exploitant les capacités d'identification, d'acquisition de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en garantissant le respect des exigences de sécurité et de confidentialité.

NOTE 2 – Dans une optique plus large, l'IoT peut être considéré comme un concept ayant des répercussions sur les technologies et la société.

3.1.6 système de management/gestion [b-ISO/CEI 27000]: ensemble d'éléments corrélés ou interactifs d'un **organisme** (3.1.10) visant à établir des **politiques** (3.1.14), des **objectifs** (3.1.7) et des **processus** (3.1.15) permettant d'atteindre ces objectifs.

NOTE 1 – Un système de management peut recouvrir une ou plusieurs disciplines.

NOTE 2 – Les éléments du système comprennent la structure de l'organisme, les rôles et responsabilités, la planification et les opérations.

NOTE 3 – Le domaine d'un système de management peut comprendre l'organisme dans son ensemble, certaines de ses fonctions spécifiques et identifiées, certaines de ses sections spécifiques et identifiées, ou une ou plusieurs fonctions au sein d'un groupe d'organismes.

3.1.7 objectif [b-ISO/CEI 27000]: résultat à atteindre.

NOTE 1 – Un objectif peut être stratégique, tactique ou opérationnel.

NOTE 2 – Les objectifs peuvent concerner différentes disciplines (par exemple: finance, santé, sécurité ou environnement) et différents niveaux [par exemple: au niveau stratégique, à l'échelle de l'organisme, au niveau d'un projet, d'un produit et d'un **processus** (3.1.15)].

NOTE 3 – Un objectif peut être exprimé de différentes manières, par exemple comme un résultat recherché, un but, un critère opérationnel, un objectif de sécurité de l'information, ou en utilisant d'autres mots de sens similaire (par exemple: intention ou cible).

NOTE 4 – Dans le contexte des systèmes de management de la sécurité de l'information, les objectifs de sécurité de l'information sont définis par l'organisme, conformément à la politique de sécurité de l'information, afin d'obtenir des résultats spécifiques.

3.1.8 consentement [b-ISO/TS 17975]: processus ou type de politique en vertu duquel le sujet des données doit effectuer une action distincte pour donner une autorisation spécifique, explicite ou préalable en vue d'un type de traitement donné.

3.1.9 opposition [b-ISO/TS 17975]: processus ou type de politique en vertu duquel le sujet des données doit effectuer une action distincte pour indiquer son refus ou le retrait de son autorisation en vue d'un type de traitement donné.

NOTE – L'opposition comprend le concept d'autorisation implicite, qui permet à l'organisme qui collecte les données de traiter les informations personnelles, sauf si l'individu indique explicitement son refus ou le retrait de son autorisation. L'opposition est aussi une action proposée par l'organisme qui collecte les données pour permettre à un sujet de données d'indiquer son refus ou de retirer son autorisation pour un type de traitement donné.

3.1.10 organisme [b-ISO/CEI 27000]: personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses **objectifs** (3.1.7).

NOTE – Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

3.1.11 information d'identification personnelle PII [ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte; ou b) est ou peut être directement ou indirectement liée à une personne.

NOTE – Pour déterminer si la personne à laquelle les informations PII se rapportent peut être identifiée, il convient de tenir compte de tous les moyens qui peuvent être raisonnablement utilisés par la partie intervenant dans la protection de la vie privée et détenant les données ou par toute autre partie pour identifier cette personne.

3.1.12 préférences PII [ISO/CEI 29100]: choix particuliers effectués par le titulaire des informations d'identification personnelle (PII) sur la manière dont ses informations PII devraient être traitées à des fins spécifiques.

3.1.13 titulaire des informations d'identification personnelle [ISO/CEI 29100]: personne physique à laquelle les informations d'identification personnelle (PII) se rapportent.

NOTE – Suivant le pays et la législation en matière de protection des données et de respect de la vie privée, on peut aussi employer le terme "sujet des données" comme synonyme du terme "titulaire des informations PII".

3.1.14 politique [b-ISO/CEI 27000]: intentions et orientation d'un **organisme** (3.1.10) telles que formalisées par sa **direction** (3.1.18).

3.1.15 processus [b-ISO/CEI 27000]: ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.

3.1.16 risque [b-ISO/CEI 27000]: effet de l'incertitude sur les **objectifs** (3.1.7).

3.1.17 objet [b-UIT-T Y.4000]: dans l'Internet des objets, objet du monde physique (objet physique) ou du monde de l'information (objet virtuel), pouvant être identifié et intégré dans des réseaux de communication.

3.1.18 direction [b-ISO/CEI 27000]: personne ou groupe de personnes qui dirige et contrôle un **organisme** (3.1.10) au plus haut niveau.

NOTE 1 – La direction a le pouvoir de déléguer l'autorité et de fournir des ressources au sein de l'organisme.

NOTE 2 – Si le domaine du système de management (3.1.6) ne s'étend qu'à une partie de l'organisme, la direction en réfère à l'équipe qui dirige et contrôle cette partie de l'organisme.

NOTE 3 – La direction est parfois appelée le management exécutif. Elle peut comprendre les présidents directeurs généraux, les directeurs financiers, les directeurs des systèmes d'information et autres fonctions similaires.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACT table de contrôle d'accès (*access control table*)

IoT Internet des objets (*Internet of things*)

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

T&C conditions générales d'utilisation (*terms and conditions*)

5 Conventions

Aucune.

6 Aperçu général

Il existe de nombreux types de dispositifs IoT, et certains d'entre eux sont capables de collecter des données PII. Dans la mesure où les données PII sont utiles pour différents types de services, les

fournisseurs de services ont tendance à collecter de nombreux types de données PII auprès des utilisateurs. De plus, les données PII collectées peuvent être partagées par un fournisseur de services avec d'autres en vue de fournir collectivement des services qui sont plus utiles aux utilisateurs. Dans ce cas, deux types de fournisseurs de services interviennent: un fournisseur qui collecte les données (PII) auprès des utilisateurs et un autre qui fournit divers services au moyen des données collectées par d'autres fournisseurs de services.

Du point de vue des utilisateurs, les données PII devraient être traitées de manière appropriée par ces fournisseurs de services. Il est recommandé que les utilisateurs précisent leurs souhaits concernant la manière dont leurs données, notamment leurs données PII, devraient être traitées dans l'environnement IoT. L'utilisation des données dans l'environnement IoT avec de multiples fournisseurs de services étant complexe, il convient de s'adapter de façon souple aux souhaits des utilisateurs concernant l'utilisation des données. À titre d'exemple, si un fournisseur de services IoT propose les fonctions ci-après, il est souhaitable, pour les utilisateurs, que ce fournisseur collecte des données et traite les données PII de manière appropriée:

– Les utilisateurs peuvent configurer leurs propres préférences PII, notamment en définissant la liste des données qu'il est permis de partager avec d'autres fournisseurs de services.
– La collecte et le partage des données sont soumis à un contrôle d'accès fondé sur les préférences PII. Les données non autorisées ne peuvent pas être stockées dans une mémoire de données, ni partagées avec d'autres fournisseurs de services.
– Les utilisateurs peuvent consulter le journal contenant l'historique du partage de données entre les fournisseurs de services. Ils peuvent aussi vérifier à quel moment leurs données ont été partagées.

7 Modèle de service IoT avec un ou plusieurs fournisseurs de services

La Figure 1 correspond à un modèle de service IoT pour un service assuré par un fournisseur unique. Dans ce cas, le fournisseur de services collecte plusieurs types de données (y compris des données PII) et conserve les informations dans une mémoire de données gérée par le fournisseur lui-même. Il fournit diverses applications aux utilisateurs qui lui confient leurs données (y compris leurs données PII).

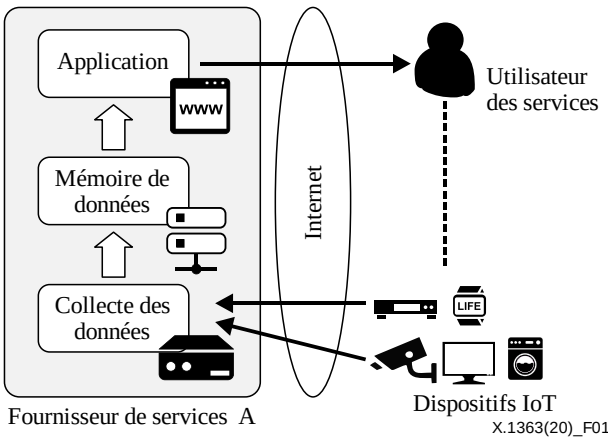

Figure 1 – Modèle pour un fournisseur de services unique

Dans ce modèle de service IoT, le fournisseur de services unique traite les données collectées, et les utilisateurs utilisent l'application ou les applications selon les conditions générales d'utilisation approuvées.

La Figure 2 correspond à un modèle dans lequel plusieurs fournisseurs de services partagent les données collectées auprès de dispositifs IoT. Dans ce cas, deux types de fournisseurs de services

interviennent: un "fournisseur de services de données" et un "fournisseur de services d'application". Dans la Figure 2, le fournisseur de services A collecte des données (y compris des données PII) auprès des dispositifs IoT et les partage avec d'autres fournisseurs de services (le fournisseur de services B et le fournisseur de services C). Le fournisseur de services A relève de la catégorie "fournisseur de services de données", et les fournisseurs B et C, de la catégorie "fournisseur de services d'application". Un fournisseur de services peut appartenir à ces deux catégories à la fois.

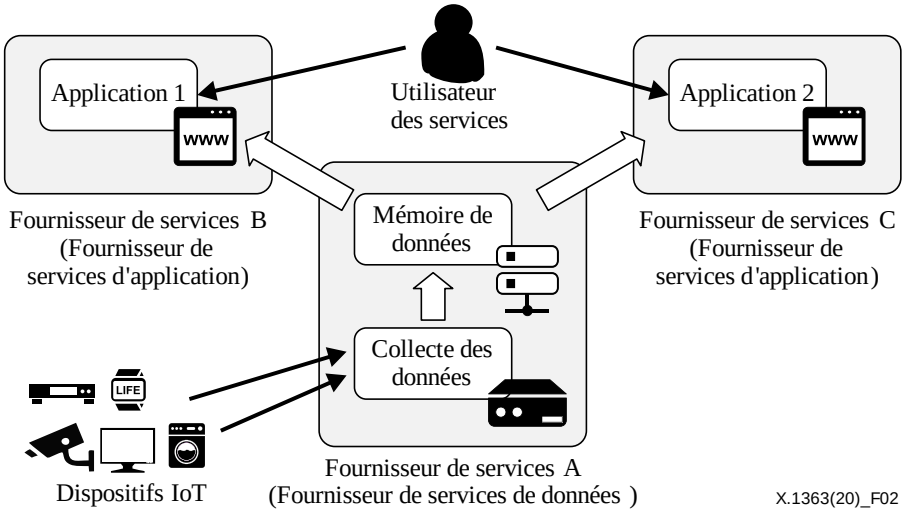

Figure 2 – Modèle pour plusieurs fournisseurs de services

La liste des données partagées avec d'autres fournisseurs de services figure normalement dans les conditions générales d'utilisation d'un fournisseur de services de données, et les utilisateurs doivent les accepter avant de pouvoir utiliser les services du fournisseur.

La principale différence entre le modèle pour un fournisseur unique et le modèle pour plusieurs fournisseurs tient à la question de savoir si les données collectées par les dispositifs IoT sont partagées avec d'autres fournisseurs de services d'application ou non. Dans le cas du modèle correspondant à plusieurs fournisseurs de services, les données collectées par les dispositifs IoT sont transférées à d'autres fournisseurs de services d'application.

8 Aspects concernant le traitement des données PII par les services IoT

Les fournisseurs de services IoT devraient tenir compte des aspects suivants lorsqu'ils traitent des données PII:

– Finalité de la collecte de données PII

Afin d'éviter toute collecte de données inutile du point de vue des utilisateurs, ceux-ci doivent connaître la finalité de la collecte de données et la nature des données collectées pour un service IoT.

– Autorisation obligatoire pour la collecte de données PII

Lorsque des utilisateurs souscrivent à un service IoT, le fournisseur de services de données doit obtenir leur autorisation concernant la collecte de différents types de données PII. En règle générale, ces informations figurent dans les conditions générales d'utilisation du fournisseur de services de données, et les utilisateurs doivent donner leur autorisation avant de pouvoir souscrire au service.

– Transfert des données PII vers des tierces parties

Les données collectées auprès des dispositifs IoT peuvent être partagées avec des tierces parties, c'est-à-dire d'autres fournisseurs de services. Dans ce cas, le fournisseur de services de données doit obtenir l'accord exprès des utilisateurs concernant le transfert de leurs données PII à des tierces parties avant

de pouvoir envoyer ces données PII à d'autres fournisseurs de services. Dans la plupart des cas, les utilisateurs ne peuvent pas contrôler le transfert des données PII. À titre d'exemple, les utilisateurs ne peuvent pas sélectionner les tierces parties vers lesquelles ils autorisent le transfert de leurs données PII, ni configurer les types de données PII qui peuvent être partagées. De plus, les utilisateurs n'ont aucun moyen de savoir quels types de données PII sont envoyées à des tierces parties.

– Consentement et opposition concernant la collecte et le transfert de données PII

Lorsqu'un service utilise les données PII des utilisateurs, le fournisseur de services de données doit obtenir l'autorisation de l'utilisateur, aussi bien pour collecter des données PII auprès de l'utilisateur que pour les transférer à une tierce partie. Le moment auquel l'autorisation est obtenue a autant d'importance que la méthode utilisée pour l'obtenir (consentement ou opposition).

9 Principes applicables au traitement des données PII par les services IoT

Les principes et les mesures de sécurité applicables à la protection des données PII sont définis dans les normes [ISO/CEI 29100] et [UIT-T X.1058], sur la base des principes existants en la matière dans un certain nombre de pays, d'États et d'organisations internationales, comme l'Organisation pour la coopération et le développement économiques (OCDE) et la Coopération économique Asie-Pacifique (APEC).

Les paragraphes 9.1 et 9.2 dressent la liste des principes à respecter dans le cadre du traitement des données PII par les services IoT en vue de satisfaire les principes définis dans les normes [ISO/CEI 29100] et [UIT-T X.1058].

9.1 Principes généraux applicables au traitement des données PII par les services IoT

Les informations PII peuvent être utilisées pour identifier, contacter ou localiser une personne en particulier. La divulgation de ces informations peut donner lieu à une usurpation d'identité ou à d'autres utilisations frauduleuses, ce qui peut, dans une large mesure, porter préjudice aux individus, les mettre dans l'embarras ou leur causer des désagréments [b-GAO-08-343]. En conséquence, le traitement des données PII par un service IoT devrait respecter les principes généraux suivants:

1) Chiffrement des données PII

Toutes les données PII stockées dans les dispositifs IoT ou dans les bases de données de service doivent être chiffrées. De plus, toutes les données PII doivent être chiffrées pendant la transmission au sein de toutes les composantes du service IoT et entre ces composantes (dispositif IoT, mémoire de données et application, par exemple).

2) Contrôle d'accès et authentification

Si les données PII sont stockées sur des dispositifs IoT ou dans des bases de données de service (mémoire de données), il convient d'appliquer des contrôles d'accès appropriés. L'autorisation concernant l'accès aux données PII est strictement limitée aux fins de l'utilisation pour laquelle une demande d'autorisation a été faite par le fournisseur de services. La finalité de cette utilisation doit figurer dans les conditions générales d'utilisation pour lesquelles le fournisseur de services a obtenu l'autorisation de l'utilisateur. L'accès est également limité lorsqu'il existe une possibilité de relier des ensembles de données stockés entre eux entraînant l'identification ou la déduction non autorisée de données PII supplémentaires.

3) Journalisation

La création d'extraits de données lisibles par ordinateur comprenant des données PII doit être répertoriée dans un journal officiel, avec des renseignements concernant le créateur de l'entrée, la date, le type d'informations, la finalité de l'extraction et l'utilisateur. Les éventuelles données PII inscrites dans ces journaux (par exemple le nom de l'utilisateur) doivent être chiffrées et assujetties à des contrôles d'accès.

4) Chiffrement pour les communications

Les données PII doivent être chiffrées ou masquées si elles sont partagées entre plusieurs fournisseurs de services.

5) Notification en cas d'atteinte aux données

S'il est porté atteinte aux données PII en raison d'une violation, d'une fuite, d'une utilisation abusive ou d'une mauvaise utilisation des données, à tout moment dans le cadre d'un service IoT, le fournisseur de services en informe les utilisateurs et les fournisseurs de services concernés, immédiatement après la découverte de l'incident.

6) Procédure de réduction des données au minimum en vue de la conservation

Le stockage de données PII, qu'elles soient collectées ou produites dans le cadre du traitement de données effectué par un fournisseur de services, est exclusivement limité aux fins spécifiées pour lesquelles le fournisseur de services a obtenu une autorisation explicite. Le fournisseur de services fixe une période maximale pour la conservation des données PII, limitée en fonction de la finalité précisée pour l'utilisation de ces données, de la possibilité de relier des ensembles de données stockés entre eux entraînant l'identification ou la déduction de données PII supplémentaires, ainsi que de la législation ou de la réglementation nationale applicable.

9.2 Principes applicables au traitement des données PII

Les fournisseurs de services de données qui recueillent des données PII auprès de dispositifs IoT devraient traiter ces données de façon appropriée. En particulier, si les données sont utilisées par des services et partagées avec d'autres fournisseurs de services, le traitement de ces données doit être conforme aux souhaits de l'utilisateur. En conséquence, le traitement des données PII par les fournisseurs de services IoT devrait respecter les principes suivants:

1) Explication de la finalité de la collecte de données PII

Afin de recueillir les données PII minimales requises auprès des utilisateurs pour fournir un service IoT, un fournisseur de services doit expliquer, dans les conditions générales d'utilisation, la finalité de la collecte des données PII ainsi que la période de conservation de toute donnée PII collectée.

2) Accord exprès pour la collecte et le partage des données PII des utilisateurs

Lorsqu'un fournisseur de services offre des services qui collectent des données PII auprès des utilisateurs, il doit obtenir l'accord exprès des utilisateurs pour la collecte et le partage des données. En particulier, le fournisseur de services doit mettre en œuvre un modèle d'obtention du consentement à chaque fois que cela est possible afin de recueillir l'autorisation de l'utilisateur.

3) Transparence de l'utilisation des données PII

Lorsque les données PII, y compris celles produites dans le cadre du traitement de données par un fournisseur de services, sont partagées avec d'autres fournisseurs de services, le fournisseur de services veille à la transparence du mécanisme de gestion des données PII, afin de permettre aux utilisateurs de vérifier l'utilisation qui est faite de leurs propres données PII. Le service IoT doit également fournir un mécanisme de recours que les utilisateurs peuvent utiliser en cas de mauvaise attribution des données.

4) Contrôle des préférences personnelles

Les données PII doivent être traitées sur la base des préférences PII configurées par les utilisateurs.

10 Traitement des données PII dans l'environnement IoT

10.1 Cadre de base pour le traitement des données PII dans un environnement IoT

La Figure 3 présente un cadre de base pour le traitement des données PII dans un environnement IoT.

Tout d'abord, les utilisateurs déterminent leurs souhaits concernant le traitement des données PII et les reflètent en définissant leurs préférences PII dans le gestionnaire de préférences PII. Les données (y compris les données PII) fournies par les utilisateurs sont gérées selon les préférences PII.

Les préférences PII peuvent comprendre les éléments ci-après:

– Le type de données collectées par les dispositifs IoT – Les dispositifs IoT devraient collecter uniquement les données PII pour lesquelles les utilisateurs ont donné leur autorisation explicite dans les préférences PII.

– Le moment de la collecte des données par les dispositifs IoT (par exemple les jours ouvrés, de 9 h 00 à 17 h 30) – Les utilisateurs ne veulent pas envoyer leurs données PII à n'importe quel moment, c'est pourquoi leurs souhaits en la matière doivent être configurés dans les préférences PII.

– Les fournisseurs de services avec lesquels le partage de données PII est autorisé – Les utilisateurs peuvent choisir quels fournisseurs de services d'application peuvent accéder à leurs données PII. Les utilisateurs peuvent également choisir les types de données PII auxquelles les fournisseurs de services d'application peuvent avoir accès, y compris les données qui sont collectées auprès des dispositifs IoT ou produites dans le cadre du traitement de données effectué par le fournisseur de services principal.

Lorsque les composantes du service IoT (dispositif IoT, mémoire de données, application, etc.) commencent à collecter et à utiliser les données, il convient de vérifier les préférences PII et de traiter les données en conséquence.

Ensuite, des informations de contrôle d'accès sont créées sur la base des préférences PII, et la table de contrôle d'accès (ACT) est mise à jour avec ces informations.

Enfin, chaque composante consulte cette table de contrôle d'accès dès lors qu'elle collecte ou transfère des données PII. Les informations de contrôle d'accès figurant dans la table sont utilisées pour contrôler quel type de données PII peuvent être transférées entre les composantes du service IoT.

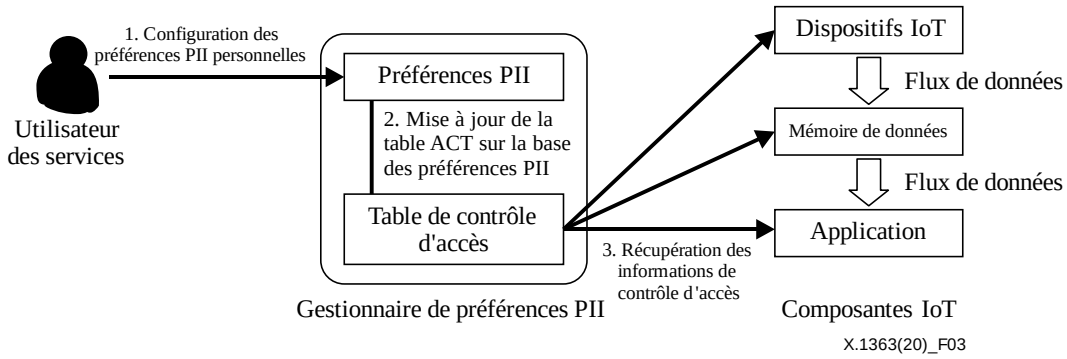

Figure 3 – Cadre de base pour le traitement des données PII

10.2 Principes applicables à une interface utilisateur pour la configuration des préférences PII

Afin de mettre en œuvre ce cadre de base, les fournisseurs de services devraient mettre à disposition une interface utilisateur, afin de permettre aux utilisateurs de configurer leurs préférences PII. Cette interface utilisateur devrait respecter les principes suivants:

1) Facilité d'accès pour tous les utilisateurs

Tous les utilisateurs doivent pouvoir accéder facilement à l'interface utilisateur. La page d'accueil des services fournis devrait comporter un lien vers cette interface utilisateur, par exemple.

2) Contrôle d'accès à l'interface utilisateur approprié

Chaque utilisateur de services a ses propres préférences PII. Par conséquent, chaque utilisateur doit posséder un compte utilisateur unique et doit pouvoir s'authentifier de façon sécurisée, par exemple au moyen d'une authentification à deux facteurs, avant de pouvoir accéder à son compte utilisateur.

3) Exhaustivité

L'interface utilisateur doit permettre de gérer toutes les préférences PII d'un utilisateur au même endroit, tant en ce qui concerne la collecte que le partage de données PII.

4) Facilité d'utilisation

L'interface utilisateur doit être simple d'utilisation pour permettre aux utilisateurs de configurer facilement leurs préférences PII.

11 Cadre technique pour le traitement des données PII dans un environnement IoT

Cette section indique comment appliquer le cadre de base défini dans la section 10 pour le traitement des données PII dans des environnements avec un et plusieurs fournisseurs de services.

11.1 Traitement des données PII pour des services IoT fournis par un fournisseur de services unique

11.1.1 Modèle de référence pour des services IoT fournis par un fournisseur de services unique

La Figure 4 correspond à un modèle de référence pour des services IoT fournis par un fournisseur de services unique. Dans ce cas, un fournisseur de services prend en charge toutes les fonctions des services IoT. Il collecte des données (y compris des données PII) auprès des dispositifs IoT et stocke ces données en mémoire. Des services d'application peuvent être fournis aux utilisateurs au moyen des données collectées.

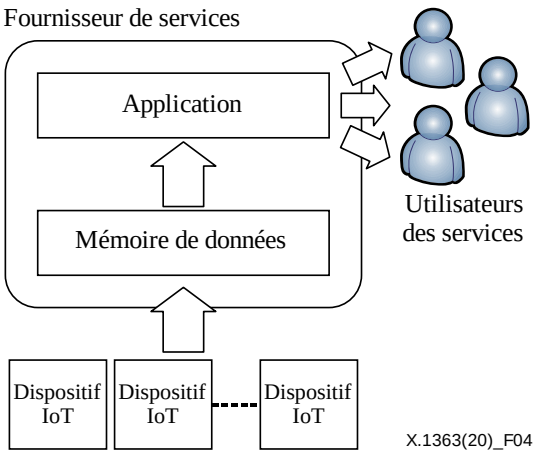

Figure 4 – Modèle de référence pour des services IoT fournis par un fournisseur de services unique

11.1.2 Cadre technique applicable au traitement des données PII par un fournisseur de services unique

La Figure 5 correspond à un cadre technique pour un fournisseur de services disposant d'un gestionnaire de préférences PII qui gère les préférences PII des utilisateurs. Les utilisateurs peuvent configurer leurs préférences PII au moyen de ce gestionnaire, et les composantes des services IoT (dispositif IoT, mémoire de données et application, par exemple), traitent les données PII en fonction de cette configuration. À titre d'exemple, si un utilisateur souhaite limiter la collecte de données PII

spécifiques auprès de dispositifs IoT, ces dispositifs ne devraient pas envoyer ces données PII dans la mémoire de données.

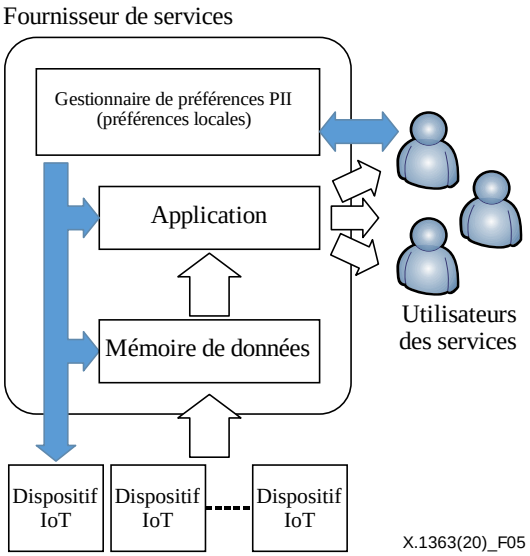

Figure 5 – Cadre technique applicable au traitement des données PII par un fournisseur de services unique

11.1.3 Cadre technique applicable au traitement des données PII par un fournisseur unique, avec un portail de gestion des préférences PII communes

Lorsque des services IoT sont fournis à un utilisateur par un fournisseur unique, les données collectées par les dispositifs IoT ne sont pas partagées avec d'autres fournisseurs de services dont les services IoT ne sont pas utilisés par cet utilisateur. Toutefois, il pourrait être nécessaire de partager certains éléments de base communs liés aux préférences PII entre les fournisseurs de services, dans la mesure où il peut être trop long, pour les utilisateurs, de configurer leurs préférences PII pour chaque service IoT. Si les utilisateurs ont la possibilité de définir des préférences PII communes pour tous types de services IoT, la configuration des préférences PII pour chaque service sera plus simple et plus efficace. Pour ce faire, on a recours deux types de gestionnaire de préférences PII.

La Figure 6 correspond à un cadre technique dans lequel on trouve deux composantes pour le gestionnaire de préférences PII: la première correspond au gestionnaire de préférences PII du fournisseur de services, la seconde, à un portail de gestion des préférences PII qui est utilisé pour gérer les préférences communes pour l'ensemble des services IoT, ainsi que pour l'accès des autres fournisseurs de services.

Dans ce cas, les préférences communes d'un utilisateur pour tous les services sont stockées sur le portail de gestion des préférences PII, tandis que ses préférences pour chaque service en particulier sont stockées dans le gestionnaire de préférences PII géré par chaque fournisseur de services. Lorsqu'un utilisateur commence à souscrire à un nouveau service, le gestionnaire de préférences PII locales du fournisseur de services de données récupère ses préférences communes dans le portail de gestion des préférences PII, qui peuvent être gérées par une tierce partie et configurées à l'avance par l'utilisateur. Même si les utilisateurs doivent toujours configurer leurs préférences PII au moyen du gestionnaire de préférences PII locales pour ce service en particulier, ils n'ont pas à configurer à chaque fois leurs préférences communes stockées dans le portail de gestion des préférences PII. Les composantes des services IoT (dispositif IoT, mémoire de données et application, par exemple), traitent les données PII sur la base des préférences locales contenues dans le gestionnaire de préférences PII.

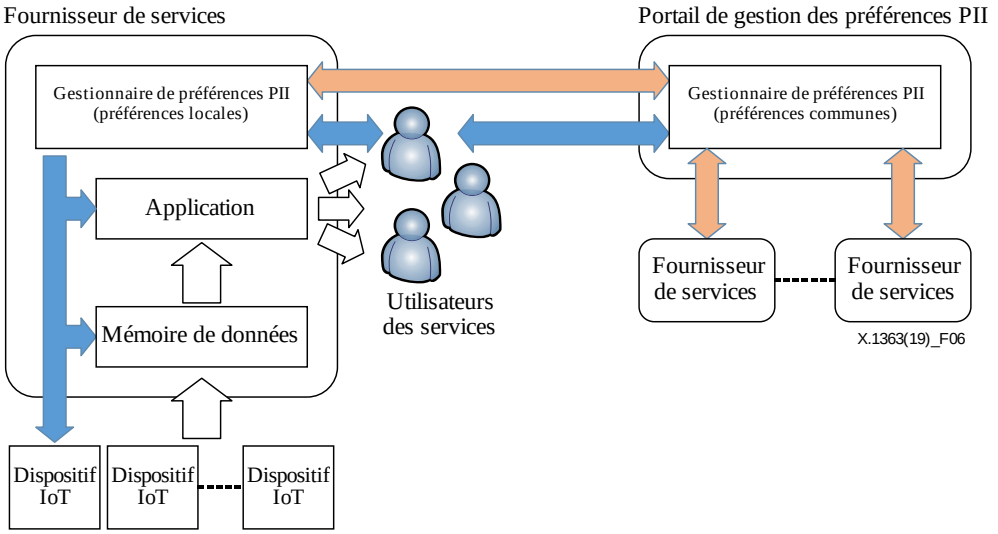

Figure 6 – Cadre technique applicable au traitement des données PII dans le cadre de services IoT fournis par un fournisseur unique, avec un portail de gestion des préférences PII communes

11.2 Traitement des données PII pour un service IoT fourni par plusieurs fournisseurs de services

11.2.1 Modèle de référence pour les services IoT fournis par plusieurs fournisseurs de services

La Figure 7 correspond à un modèle de référence pour des services IoT fournis par plusieurs fournisseurs de services. Dans ce cas, un service IoT fait intervenir plusieurs fournisseurs de services (fournisseur de services d'application et fournisseur de services de données) et chaque fournisseur de services d'application fournit ses propres services aux utilisateurs grâce aux données collectées par le fournisseur de services de données. Ainsi, les fournisseurs de services qui collectent des données (y compris des données PII) auprès de dispositifs IoT (fournisseurs de services de données) peuvent être différents de ceux qui fournissent uniquement des services aux utilisateurs (fournisseurs de services d'application). Dans la Figure 7, deux types de fournisseurs de services interviennent: l'un est un "fournisseur de services de données" qui collecte des données (y compris des données PII) auprès des dispositifs IoT, et l'autre est un "fournisseur de services d'application" qui fournit des services d'application aux utilisateurs en utilisant les données collectées.

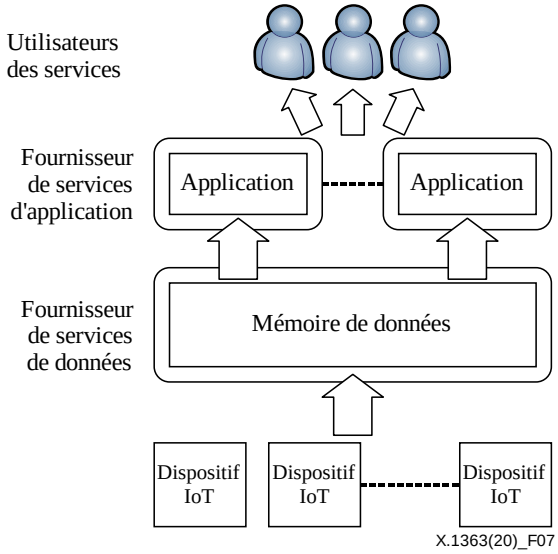

Figure 7 – Modèle de référence pour les services IoT fournis par plusieurs fournisseurs de services

11.2.2 Cadre technique applicable au traitement des données PII par plusieurs fournisseurs de services

La Figure 8 correspond à un cadre technique pour un fournisseur de services de données disposant d'un gestionnaire de préférences PII dans lequel toutes les préférences des utilisateurs pour le traitement des données PII sont gérées au niveau de ce composant de gestion local. Les utilisateurs configurent leurs préférences locales dans le gestionnaire de préférences PII. Les composantes des services IoT (y compris les applications fournies par les autres fournisseurs de services d'application) traitent les données PII sur la base des préférences locales figurant dans le gestionnaire de préférences PII du fournisseur de services de données.

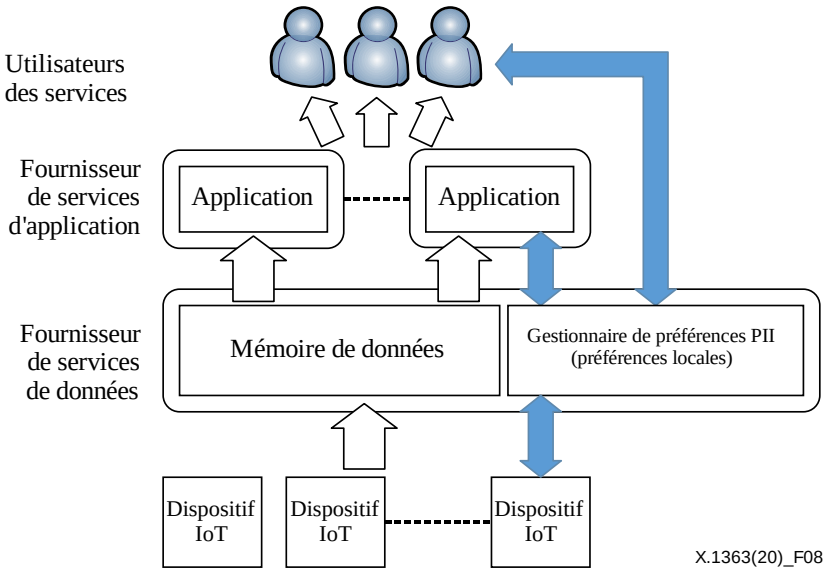

Figure 8 – Cadre technique applicable au traitement des données PII pour des services IoT fournis par plusieurs fournisseurs de services

11.2.3 Cadre technique applicable au traitement des données PII pour des services IoT fournis par plusieurs fournisseurs de services, avec un portail de gestion des préférences PII communes

La Figure 9 correspond à un cadre technique dans lequel plusieurs fournisseurs de services utilisent les préférences PII stockées dans un portail de gestion des préférences PII communes et dans les gestionnaires de préférences PII locales des fournisseurs de services de données.

Dans ce cas, les préférences communes pour l'ensemble des services sont stockées dans le portail de gestion des préférences PII communes, tandis que les préférences particulières pour chaque service sont stockées dans un gestionnaire de préférences PII locales géré par chaque fournisseur de services de données. Lorsqu'un utilisateur commence à souscrire à un nouveau service, le gestionnaire de préférences PII locales du fournisseur de services récupère les préférences communes dans le portail de gestion des préférences PII. Même si l'utilisateur doit toujours configurer ses préférences PII dans le gestionnaire de préférences PII locales, il n'a pas à configurer les préférences PII communes stockées dans le portail de gestion des préférences PII à chaque fois. Les composantes des services IoT traitent les données PII sur la base des préférences locales contenues dans le gestionnaire de préférences PII.

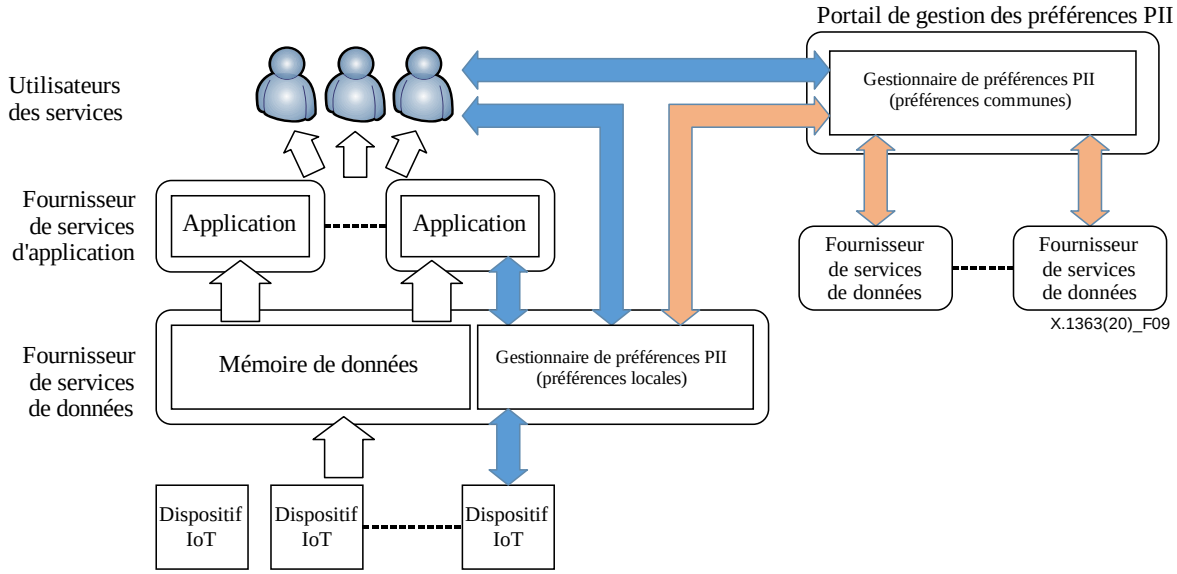

Figure 9 – Cadre technique applicable au traitement des données PII pour des services IoT fournis par plusieurs fournisseurs de services, avec un portail de gestion des préférences PII communes

Bibliographie

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets*.

[b-ISO/CEI 10027] ISO/CEI 10027:1990, *Technologies de l'information – Cadre pour le gestionnaire de ressources du système d'information (IRDS)*.

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/TS 17975] ISO/TS 17975:2015, *Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information.*

[b-GAO-08-343] GAO-08-343 (2008). *Information security: Protecting personally identifiable information*. Washington, DC: United States Government Accountability Office. 34 p.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020