Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.4805

(08/2017)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

Internet des objets et villes et communautés intelligentes – Identification et sécurité

Exigences applicables aux services d'identification pour l'interopérabilité des applications des villes intelligentes

Recommandation UIT-T Y.4805

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999
INTERNET DES OBJETS ET VILLES ET COMMUNAUTÉS INTELLIGENTES	
Considérations générales	Y.4000–Y.4049
Termes et définitions	Y.4050–Y.4099
Exigences et cas d'utilisation	Y.4100–Y.4249
Infrastructure, connectivité et réseaux	Y.4250–Y.4399
Cadres, architectures et protocoles	Y.4400–Y.4549
Services, applications, calcul et traitement des données	Y.4550–Y.4699
Gestion, commande et qualité de fonctionnement	Y.4700–Y.4799
Identification et sécurité	**Y.4800–Y.4899**
Evaluation et analyse	Y.4900-Y.4999

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

Recommandation UIT-T Y.4805

Exigences applicables aux services d'identification pour l'interopérabilité des applications des villes intelligentes

Résumé

La Recommandation UIT-T Y.4805 décrit un ensemble d'exigences applicables aux services d'identification des applications des villes intelligentes afin de garantir l'interopérabilité et la sécurité des systèmes correspondants. Ces exigences peuvent en outre tenir lieu de lignes directrices pour l'élaboration de nouveaux services d'identification destinés aux villes intelligentes. Elles contiennent notamment des mesures relatives à la sécurité afin d'assurer l'intégrité des services et la confidentialité des données. Cette Recommandation comprend une liste exhaustive des exigences applicables aux services d'identification, notamment en matière de sécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.4805	2017-08-22	20	11.1002/1000/13267

Mots clés

Confidentialité des données, identifiant, intégrité des services, ville intelligente.

* 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 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 Y.4805

Exigences applicables aux services d'identification pour l'interopérabilité des applications des villes intelligentes

1 Domaine d'application

La présente Recommandation décrit un ensemble d'exigences applicables aux services d'identification des applications des villes intelligentes afin de garantir l'interopérabilité et la sécurité des systèmes correspondants. Ces exigences peuvent en outre tenir lieu de lignes directrices pour l'élaboration de nouveaux services d'identification destinés aux villes intelligentes. Elles contiennent notamment des mesures relatives à la sécurité afin d'assurer l'intégrité des services et la confidentialité des données. La présente Recommandation comprend une liste exhaustive des exigences applicables aux services d'identification, notamment en matière de sécurité.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 application [b-UIT-T Y.2261]: ensemble structuré de capacités, qui constituent une fonctionnalité à valeur ajoutée acceptée par un ou plusieurs services, pouvant être pris en charge par une interface API.

3.1.2 identifiant, identificateur [b-UIT-T Y.2091]: suite de chiffres, de caractères, de symboles ou de toute autre forme de données, utilisée pour identifier un ou plusieurs abonnés, utilisateurs, éléments de réseau, fonctions, entités de réseau fournissant des services ou des applications, ou d'autres entités (par exemple des objets physiques ou logiques). Les identifiants peuvent être utilisés pour l'enregistrement ou l'autorisation. Ils peuvent être publics (totalité des réseaux), partagés (nombre limité de réseaux) ou privés (un seul réseau donné) (les identifiants privés ne sont normalement pas divulgués à des tiers).

3.1.3 résolution d'identifiant [b-UIT-T Y.4108]: fonction permettant de passer d'un identifiant aux informations associées et inversement.

3.1.4 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, de saisie 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.

3.1.5 interopérabilité [b-UIT-T Y.101]: capacité, pour deux systèmes ou applications ou plus, d'échanger des informations et de les utiliser mutuellement.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 administration des identifiants: capacité d'assurer des fonctions d'aide à la gestion des identifiants et de leurs attributs au cours de leur cycle de vie, dont l'enregistrement des nouveaux identifiants, la suppression d'identifiants existants, la modification et la mise à jour de toute information associée aux identifiants et toute autre fonction administrative afférente, dans le cadre d'un système d'identification particulier, tel que défini au point 3.1.2 ci-dessus.

3.2.2 service d'identification: service d'informations relatives au réseau, qui est exploité sur l'Internet et assure la résolution d'identifiant et l'administration des identifiants telles que définies respectivement aux points 3.1.3 et 3.2.1 ci-dessus.

3.2.3 service racine d'un service d'identification: composante essentielle au sommet d'un service d'identification ou de nommage de type hiérarchique. Par exemple, dans le système DNS, le service racine renvoie à l'ensemble des serveurs de noms racine et aux données au sommet du système de nommage sur l'Internet.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ID identifiant (*identifier*)

IoT Internet des objets (*Internet of things*)

TTL durée de vie (*time-to-live*)

UTF-8 format de transformation unicode à 8 bits (*8-bit unicode transformation format*)

5 Conventions

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**peut, à titre d'option,**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps de la présente Recommandation et dans ses annexes, on trouve parfois les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est obligatoire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Services d'identification pour les applications des villes intelligentes

Les services d'identification pour les applications des villes intelligentes s'articulent selon des modèles de services, de données et d'exploitation. Le modèle de services est la structure des services fournis par les services d'identification, qui permet de mieux prendre en charge les applications des villes intelligentes, notamment les composantes de service et les relations entre elles. Le modèle de données définit la structure de données idoine essentielle à la prise en charge des attributs

d'identification des applications des villes intelligentes, ainsi que les opérations relatives à la sécurité et la gestion des identifiants et de leurs attributs. Le modèle d'exploitation renvoie aux opérations essentielles que les services d'identification devraient réaliser, ainsi qu'aux principes de base permettant d'assurer la cohérence, la transparence et la fiabilité des opérations entre les différentes composantes du service d'identification, selon qu'il convient.

6.1 Modèle de services

Les services d'identification pour les applications des villes intelligentes doivent prendre en charge les applications exploitées dans différentes villes et gérées par différents organismes ou prestataires de services. Un modèle de services répartis convient aux services d'identification de ce type.

Le modèle de services d'un service d'identification fait référence à sa structure de services, à savoir ses composantes, dans un environnement de réseau réparti.

Les services d'identification pour les applications des villes intelligentes peuvent être constitués de plusieurs composantes de service, chacune étant gérée par un organisme ou un prestataire différent. Chaque composante est responsable d'un domaine local d'identification utilisé par les applications des villes intelligentes, et doit coopérer avec les autres composantes afin d'identifier n'importe quelle entité d'une ville intelligente à l'aide d'un identifiant unique à l'échelle mondiale, et de résoudre et de mettre à jour en temps réel les informations associées à cet identifiant.

En outre, une composante de service d'un service d'identification peut être exploitée et gérée par des organismes individuels, indépendamment des autres. Toute interruption d'une composante ne devrait pas avoir de répercussions sur les services assurés par d'autres composantes. L'administration des identifiants et des informations afférentes peut être assurée par une seule composante d'un service d'identification, sans qu'il soit nécessaire de faire appel aux autres.

6.2 Modèle de données

Le modèle de données d'un service d'identification est la structure de données essentielle à la prise en charge de la résolution et de l'administration des identifiants. Cette structure devrait être suffisamment souple pour prendre en charge les applications des villes intelligentes existantes et permettre une rétrocomptabilité.

Dans un service d'identification, un identifiant permet non seulement d'identifier une entité d'une ville intelligente, mais également de disposer d'informations associées au sujet identifié. Le modèle de données devrait définir une structure permettant d'associer tout type de données à l'identifiant. Il devrait également définir des mécanismes communs qui permettent d'établir la confiance concernant les informations associées à l'identifiant ou de les certifier, afin que les utilisateurs puissent les valider, selon qu'il convient.

6.3 Modèle d'exploitation

Le modèle d'exploitation renvoie aux opérations essentielles que les services d'identification devraient réaliser afin de prendre en charge les applications des villes intelligentes, ainsi qu'à la manière dont ils devraient le faire. Ce modèle devrait également définir des principes de base afin d'assurer la cohérence des opérations entre les différentes composantes du service d'identification.

De plus, les services d'identification pour les applications des villes intelligentes devraient fournir des services de sécurité clairement définis et intégrés pour chacune des opérations assurées. Les services de sécurité devraient eux-mêmes inclure des options visant à garantir l'intégrité des services et la confidentialité des données, ainsi qu'une option de non-répudiation des services selon qu'il convient.

7 Exigences applicables aux services d'identification pour les applications des villes intelligentes

7.1 Exigences générales applicables aux services d'identification

7.1.1 Compatibilité avec les pratiques existantes relatives aux villes intelligentes

Un service d'identification pour les villes intelligentes doit tenir compte des pratiques existantes en matière d'applications. Il doit veiller à ce que les applications existantes continuent de fonctionner et doit fournir des mécanismes permettant d'établir une interface avec les autres applications des villes intelligentes. Il doit être suffisamment souple pour prendre en charge toute convention de nommage utilisée par les applications existantes.

7.1.2 Possibilité d'extension

Toutes les applications pour les villes intelligentes ne font pas appel aux mêmes données associées aux identifiants. Les services d'identification doivent prendre en charge la structure de données et de métadonnées définies pour chaque application, et permettre aux applications d'enregistrer leur propre structure de données et de métadonnées. Le système de résolution et d'administration des identifiants doit pouvoir traiter tout type de données associées aux identifiants.

7.1.3 Efficacité de la résolution

Les services d'identification des villes intelligentes doivent être efficaces en terme de temps, en particulier pour ce qui est de la résolution d'identifiant. S'ils prennent également en charge l'administration des identifiants, il est recommandé qu'ils disposent d'une interface distincte à cette fin.

Le service de résolution peut, à titre d'option, utiliser plusieurs techniques pour améliorer son efficacité, dont la mesure du délai de réponse à d'autres services d'identification, la mise en mémoire cache, la réduction ou l'optimisation du nombre de demandes, et la gestion des serveurs d'identification défectueux ou qui ne répondent pas.

Afin de gagner en efficacité, les services d'identification peuvent également mettre en place des mécanismes de mise en mémoire cache afin de réduire le trafic sur le réseau, qui est induit par les demandes de résolution.

7.1.4 Modulabilité

Les services d'identification doivent être modulables pour prendre en charge le nombre croissant d'identifiants et d'applications pour les villes intelligentes. Il est obligatoire de mettre en place un modèle de services répartis pour prendre en charge ce degré de modulabilité. Dans un modèle de services répartis, les services peuvent être gérés de manière à ce que des organismes individuels puissent gérer et exploiter leur propre service d'identification de manière indépendante. Chaque opération du service d'identification peut, à titre d'option, établir plusieurs copies du service (duplication) afin de veiller à la redondance des services et à la répartition de la charge. On peut également, à titre d'option, définir des mécanismes prenant en charge le concept de groupes de services, d'identifiants ou de demandes de service.

7.1.5 Prise en charge à l'échelle internationale

Les services d'identification des villes intelligentes doivent prendre en charge Unicode, qui comprend la plupart des caractères actuellement utilisés dans le monde. Il y a plusieurs manières de coder les caractères Unicode en vue de la transmission par le réseau. Pour parvenir à une efficacité et une compatibilité maximales, il est recommandé que les services d'identification des villes intelligentes utilisent la méthode de codage au format de transformation Unicode à 8 bits (UTF-8).

7.2 Exigences générales en matière de sécurité

7.2.1 Résolution sécurisée

Les services d'identification doivent avoir un niveau de sécurité approprié en matière de résolution d'identifiant. Ils doivent garantir l'intégrité des services fournis afin que les clients puissent valider toute information reçue du service d'identification. Ils devraient également proposer, à titre d'option, un niveau adéquat de confidentialité des données échangées dans le cadre de la résolution lors de la transmission par le réseau.

7.2.2 Contrôle d'accès discrétionnaire

De nombreuses applications des villes intelligentes requièrent un contrôle d'accès discrétionnaire aux informations identifiées. Le service d'identification d'une ville intelligente a l'obligation de mettre en place un contrôle d'accès pour les informations associées à son identifiant. Ce contrôle doit être mis en place indépendamment de l'administrateur du serveur afin de garantir la plus grande souplesse possible. Pour ce faire, le service d'identification doit mettre en place une interface d'authentification et d'autorisation du client.

7.2.3 Interface d'administration et de gestion réparties

Concernant les applications des villes intelligentes utilisées pour le contrôle et la gestion en temps réel de dispositifs de l'IoT, il peut également être nécessaire de modifier ou de mettre à jour les données de statut associées à leur identifiant. Le service d'identification d'une ville intelligente doit fournir une interface administrative sécurisée afin que les applications puissent gérer et mettre à jour les attributs des identifiants en temps voulu.

7.3 Exigences relatives au modèle de services

7.3.1 Interopérabilité: modèle de services répartis

Les services d'identification pour les applications des villes intelligentes doivent prendre en charge un modèle de services répartis et être constitués de composantes de service réparties, avec une répartition des services de type homologue ou hiérarchique.

Le modèle de répartition des services de type homologue est indispensable à une gestion répartie des services d'identification de plusieurs applications de villes intelligentes, que ce soit à l'intérieur ou à l'extérieur des limites d'une ville donnée. Ce modèle permet à chaque application de fournir son propre service d'identification de manière indépendante, tout en coopérant avec ses homologues (voir la Figure 1).

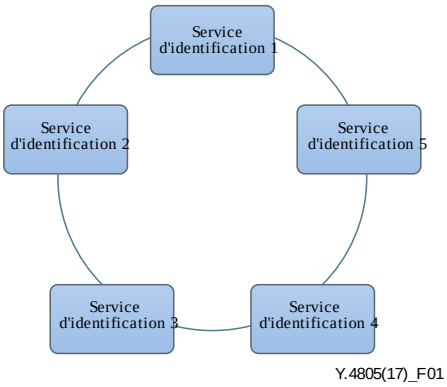

Figure 1 – Modèle de répartition des services de type homologue

Le modèle de répartition des services de type hiérarchique convient aux applications des villes intelligentes qui ont une structure de gestion hiérarchique. Il permet à tout organisme de fournir un service d'identification partagé entre les différents domaines de ses filiales, tout en laissant à ces dernières la possibilité de fournir leur propre service d'identification lorsque nécessaire (voir la Figure 2).

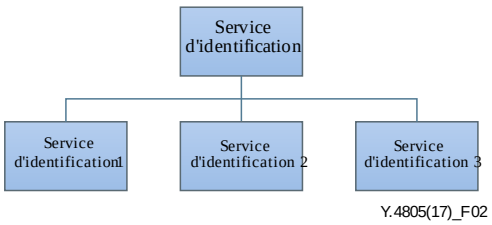

Figure 2 – Modèle de répartition des services de type hiérarchique

7.3.2 Interopérabilité: service racine réparti

Tous les services de type hiérarchique ont besoin d'un service racine sur lequel ancrer leur hiérarchie de services. Le service racine du système DNS en est un exemple. Les services d'identification pour les applications des villes intelligentes doivent fournir un service racine qui sert de point de départ à l'enregistrement de toute composante de service dans le cadre de la hiérarchie des services. Ils doivent également fournir un justificatif de la fiabilité des services à toutes les composantes de service lorsque nécessaire. Ce service racine est également obligatoire pour tous les services d'identification des villes intelligentes de type hiérarchique. Il doit être réparti de manière à ne connaître aucun point de défaillance isolé. Il doit également permettre une gestion multipartite de type homologue par les différentes parties prenantes, de manière à ne pas être contrôlé par une seule entité. Si différents Etats ou organismes exploitent leurs propres instances d'un serveur racine pour un service d'identification, ils doivent prendre les mesures nécessaires pour prévenir tout point de défaillance isolé.

7.3.3 Sécurité: racine de confiance

Le service racine est la base essentielle sur laquelle repose la confiance accordée à un service d'identification de type hiérarchique. Dans le cadre d'un système hiérarchique, le service d'identification doit délivrer un justificatif aux services d'identification dérivés. Il est recommandé de le délivrer sous la forme d'une clé publique signée par le service d'identification de niveau supérieur, qui doit être un gage de l'intégrité du service pour les clients qui en font la demande. A partir de ce justificatif, tout client utilisant un service d'identification doit pouvoir remonter au service racine afin de vérifier l'authenticité du service d'identification.

7.3.4 Sécurité: copie et duplication

Tout service d'identification d'un service d'identification réparti peut, à titre d'option, créer plusieurs copies des services fournis afin d'éviter tout point de défaillance isolé. Il est nécessaire d'avoir plusieurs services d'identification de type homologue sur les sites de copie afin de permettre des opérations simultanées d'administration des identifiants. Dans ce cas, il est obligatoire de mettre en place des mécanismes pour éviter des conditions de concurrence, c'est à dire que plusieurs sites de copie essayent de mettre à jour le fichier d'un même identifiant au même moment.

7.3.5 Interopérabilité: service de mise en mémoire cache

Les services d'identification doivent prendre en charge la mise en mémoire cache afin d'aider à réduire le trafic superflu sur le réseau. Il est recommandé d'inclure un champ standard de durée de vie (TTL) dans les résultats de la résolution d'identifiant afin d'indiquer la durée de validité des données. Un service de mise en mémoire cache spécifique peut, à titre d'option, être déployé pour une communauté d'utilisateurs particulière.

7.3.6 Interopérabilité: prise en charge du service de résolution en mode itératif et récursif

Il est recommandé qu'un service d'identification envoie des demandes de manière itérative ou récursive à une autre instance de service d'identification de la part d'un client final. Le service d'identification qui envoie ces demandes peut placer les réponses reçues en mémoire cache.

7.4 Exigences relatives au modèle de données

7.4.1 Sécurité: dispositif commun de contrôle d'accès aux attributs des identifiants

De nombreuses applications des villes intelligentes exigent un contrôle d'accès aux attributs des identifiants. Il est possible que seul un sous-ensemble des attributs soit ouvert au grand public, tandis que les autres ne sont accessibles que pour quelques parties autorisées grâce à la résolution d'identifiant.

Le modèle de données des services d'identification pour les applications des villes intelligentes doit comprendre un mécanisme commun de contrôle d'accès aux attributs des identifiants. Il doit en particulier permettre de mettre en place un contrôle d'accès fondé sur la fonction ou la catégorie pour tout sous-ensemble d'attributs.

7.4.2 Sécurité: prise en charge de la validation des justificatifs

Dans un système informatique réparti, l'intégrité des services ne sert qu'à prouver que les données proviennent d'un service autorisé. Mais elle n'est pas nécessairement un gage de la fiabilité des données. Les services d'identification pour les applications des villes intelligentes doivent garantir l'intégrité des services fournis, conformément à ce qui a été dit plus haut dans la présente Recommandation, et également proposer, à titre d'option, une validation des justificatifs. Il est recommandé de valider les justificatifs soit au moyen de la signature numérique d'une tierce partie associée aux attributs de l'identifiant, soit en faisant appel au service de validation d'une tierce partie qui pourra être utilisé pour valider l'authenticité ou la crédibilité des attributs de l'identifiant.

7.4.3 Sécurité: prise en charge de l'administration discrétionnaire et propriété des identifiants

Le modèle de données d'un service d'identification doit proposer à l'administrateur d'un identifiant donné des options indépendantes du service d'hébergement et permettre l'administration discrétionnaire de l'identifiant et de ses attributs. Lors de sa mise en oeuvre, un service d'identification doit fournir des moyens de protéger les identifiants et leurs attributs, de manière à ce que seules des modifications autorisées leur soient apportées.

Il est important de prévoir une administration discrétionnaire pour les applications des villes intelligentes afin que chaque sujet identifié puisse interagir directement avec le service d'identification pour mettre à jour ses attributs en temps réel, sans avoir à passer par l'administrateur d'un serveur centralisé. Cela permet également de minimiser les risques liés à la sécurité en empêchant que des modifications non autorisées soient apportées aux identifiants hébergés par le service d'identification.

7.4.4 Interopérabilité: possibilité d'étendre le modèle de données

Les identifiants pour les applications des villes intelligentes sont utilisés pour associer différents types d'informations concernant le sujet identifié. Le modèle de données utilisé par le service d'identification doit être suffisamment souple pour prendre en charge de nouveaux types de données qui seront définis pour les attributs des identifiants utilisés dans les applications des villes intelligentes. Ce type d'application doit avoir la possibilité de définir son propre type de données et de l'enregistrer auprès du service d'identification.

7.4.5 Interopérabilité: dispositif de nommage adaptable

De nombreuses applications des villes intelligentes disposent de leur propre système d'identification. D'un point de vue pratique, il est difficile de changer les dispositifs de nommage de ces applications. Les services d'identification pour les applications des villes intelligentes doivent mettre en place un dispositif de nommage souple afin de prendre en charge la modification des noms utilisés par les applications des villes intelligentes existantes.

7.5 Exigences relatives au modèle d'exploitation

7.5.1 Sécurité: opérations sécurisées

Les services d'identification des villes intelligentes doivent prendre en charge un vaste ensemble d'opérations sécurisées relatives aux identifiants, notamment:

1) la création ou l'enregistrement d'un nouvel identifiant et son association à un ensemble d'attributs;
2) la résolution ou la demande des attributs associés à tout identifiant enregistré;
3) la mise à jour et la modification sécurisées des attributs associés à un identifiant existant;
4) la suppression d'un identifiant ou le retrait de tout attribut associé à lui.

Le service d'identification devrait fournir des interfaces de protocole normalisées afin de prendre en charge toutes ces opérations. Il devrait également fournir des mécanismes d'authentification et d'autorisation adéquats afin de renforcer la sécurité de ces opérations.

7.5.2 Interopérabilité: exploitation cohérente d'un service d'identification dans un environnement réparti

Chaque service d'identification dans la hiérarchie des services doit fonctionner de manière cohérente dans un environnement réparti. Lorsqu'il reçoit une demande de service, il doit la traiter de manière récursive ou itérative. En mode récursif, le service d'identification doit transmettre la demande au service d'identification responsable, obtenir de lui une réponse et la communiquer au client. En mode itératif, le service d'identification doit rediriger le client vers le service d'identification responsable, et le client doit renvoyer sa demande au service d'identification responsable.

7.5.3 Sécurité: confiance au sein de la hiérarchie des services d'identification

Chaque service d'identification dans la hiérarchie des services doit recevoir son justificatif du service d'identification de niveau supérieur. Il est recommandé de le délivrer sous la forme d'une clé publique signée ou d'un certificat de clé publique. Ce type de justificatif est nécessaire pour garantir l'intégrité des services dans un environnement réparti. Il doit également servir à garantir la non-répudiation des services sous certaines conditions. Un client qui interagit avec un service d'identification doit pouvoir, à partir d'un justificatif, remonter au service d'identification racine, afin de valider son authenticité. Il est recommandé de placer ces informations de validation en mémoire cache afin d'éviter de répéter inutilement des opérations, à condition que la mise en mémoire cache ait une durée limitée ou expire d'une manière ou d'une autre.

Bibliographie

[b-UIT-T Y.101] Recommandation UIT-T Y.101 (2000), *Infrastructure mondiale de l'information: termes et définitions*.

[b-UIT-T Y.2091] Recommandation UIT-T Y.2091 (2011), *Réseaux de prochaine génération: Termes et définitions*.

[b-UIT-T Y.2261] Recommandation UIT-T Y.2261 (2006), *Evolution des RTPC/RNIS vers les réseaux de prochaine génération*.

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

[b-UIT-T Y.4108] Recommandation UIT-T Y.4108/Y.2213 (2008), *Exigences et capacités liées aux services NGN concernant les aspects réseau des applications et services utilisant une identification par étiquette.*

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	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, 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, 2017