|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Assemblée mondiale de normalisation  des télécommunications (AMNT-16) Hammamet, 25 octobre - 3 novembre 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| **SÉANCE PLÉNIÈRE** | | **Addendum 32 au Document 43-F** | |
|  | | **11 octobre 2016** | |
|  | | **Original: anglais** | |
|  | | | |
| Administrations des Etats arabes | | | |
| Propositions et avis sur la strucTUre de la commission d'Etudes 20 de l'UIT-T | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| **Résumé:** | Les Administrations des Etats arabes proposent d'adopter deux nouvelles Questions et de revoir la structure de la Commission d'études 20 de l'UIT-T, afin de renforcer le rôle de cette dernière compte tenu des Documents 22 et 21 soumis à l'Assemblée, en particulier de la partie "Observations concernant les futurs travaux". |

Discussion

– A sa réunion de juin 2015, le Groupe consultatif de la normalisation des télécommunications (GCNT) a décidé de créer une nouvelle Commission d'études 20 de l'UIT-T intitulée: "L'Internet des objets et ses applications, y compris les villes et les communautés intelligentes". Le mandat et la structure de la CE 20, ainsi que le texte des Questions qui lui sont confiées ont été approuvés par le GCNT à sa réunion de juin 2015 et font l'objet du Document [TD322Rév3](http://www.itu.int/md/T13-TSAG-150602-TD-GEN-0322/en).

– La structure de la CE 20 a été approuvée par le GCNT à sa réunion de juin 2015, puis modifiée par la CE 20 à sa première réunion, qui a eu lieu du 19 au 23 octobre 2015. La CE 20 a approuvé la structure figurant dans le Document [TD 003 Rév.5(GEN/20)](http://www.itu.int/md/T13-SG20-151019-TD-GEN-0003/en), qui a été présenté au GCNT en février 2016.

A sa réunion de février 2016, le GCNT a décidé de ce qui suit, comme indiqué dans le rapport de réunion correspondant:

– attribution à la CE 20 de l'UIT-T de la fonction de commission d'études directrice pour l'Internet des objets (IoT) et ses applications et pour les villes et les communautés intelligentes;

– texte actualisé des six Questions confiées à la CE 20 (Annexe C de la Pièce jointe 1 de la note de liaison de la CE 20 de l'UIT-T ([TD368](http://www.itu.int/md/T13-TSAG-160201-TD-GEN-0368/en));

– modifications apportées au mandat et au domaine de compétence de la JCA-IoT et SC&C, étant entendu que le premier objectif de la JCA est modifié comme suit: "… et d'établir une liaison avec l'UIT-R…".

On trouvera dans la présente contribution une proposition concernant l'adoption de deux nouvelles Questions et une proposition de modification de la structure de la CE 20, afin de renforcer et de consolider le rôle de cette Commission pour lui permettre de mener à bien sa mission.

# 1 Proposition de deux nouvelles Question

ARB/43A32/1

Nouvelle Question 2/20 intitulée "Evaluation des villes et des communautés intelligentes"

Conformément au mandat confié par le GCNT à la CE 20 en tant que commission d'études directrice pour les villes et les communautés intelligentes, et compte tenu des travaux transférés de la Commission d'études 5 de l'UIT-T à la CE 20, les auteurs de la présente contribution proposent d'adopter une nouvelle Question intitulée "Evaluation des villes et des communautés intelligentes".

Question 2/20

Evaluation des villes et des communautés intelligentes

# 1 Motifs

Des stratégies très détaillées visant à mettre en place des villes et des communautés intelligentes sont adoptées à travers le monde pour répondre aux enjeux de l'urbanisation rapide. Ces stratégies prévoient l'intégration des technologies de l'information et de la communication (TIC) dans tous les aspects de l'urbanisme et de la gestion des villes. Pour ce faire, les TIC, en particulier l'Internet des objets, peuvent améliorer l'efficacité de la gestion urbaine en facilitant la collecte des informations pertinentes et l'interconnexion d'une multitude de domaines différents. Ainsi, les municipalités concernées, les communautés et les citoyens pourront prendre des décisions plus avisées, ce qui facilitera l'intégration des services urbains et la coopération entre les différents secteurs.

A ce stade, il est important de pouvoir mesurer les résultats des diverses initiatives relatives aux villes et communautés intelligentes. L'une des approches consistent à utiliser des indicateurs fondamentaux de performance (IFP) qui facilitent le suivi des progrès accomplis dans la mise en place de villes et communautés intelligentes, ainsi que dans les différents secteurs comme l'environnement, la santé, l'éducation ou les services collectifs.

Il est souhaitable que les villes puissent quantifier les progrès qu'elles ont accomplis par rapport à leurs objectifs. Par conséquent, l'utilisation de ces indicateurs permet aux villes et à leurs parties prenantes d'évaluer de manière objective dans quelle mesure elles peuvent être perçues comme plus intelligentes et plus durables.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quels sont les principes généraux à utiliser pour établir la méthodologie d'évaluation de l'utilisation des TIC et de leurs incidences dans le caractère durable des villes?

– Quelles sont les formules qui permettraient de calculer un indice des villes intelligentes et durables à utiliser partout dans le monde?

– Comment collecter des données fiables, en particulier les données ayant une grande incidence sur les résultats? Comment tenir compte de l'évolution des données au fil du temps?

– Comment évaluer la méthodologie (mesure, échantillonnage statistique, études de cas, etc.), y compris les différents aspects régionaux ou nationaux?

– Comment évaluer la réalisation des Objectifs de développement durable (ODD) dans une ville intelligente?

– Comment évaluer les différentes performances d'une ville selon des indicateurs définis par secteur, par exemple données ouvertes, cybersanté, services collectifs, etc.?

– Comment évaluer la qualité des services de cybersanté? Comment améliorer les systèmes de cybersanté afin qu'ils s'adaptent aux technologies futures sur la base des résultats des évaluations?

– Quelle collaboration faudra-t-il instaurer avec les organisations de normalisation pour exploiter au mieux les synergies et harmoniser les normes existantes relatives à l'évaluation des villes et des communautés intelligentes?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Elaborer des Recommandations sur la méthodologie d'évaluation de la réalisation des ODD dans les villes, compte tenu des principes et de critères généraux d'évaluation des incidences des TIC.

– Elaborer des Recommandations sur la collecte et l'obtention de données brutes fiables à injecter dans le modèle d'évaluation.

– Elaborer des Recommandations sur la méthodologie permettant de mesurer les différentes performances d'une ville selon des indicateurs définis par secteur.

– Elaborer, si nécessaire, des manuels faisant référence aux bases de données disponibles relatives aux profils courants des villes et des communautés intelligentes.

– Elaborer des manuels concernant la présentation de l'indice mondial des villes intelligentes et durables.

– Elaborer des lignes directrices des bonnes pratiques concernant l'élaboration de rapports sur les performances d'une ville, afin d'aider les villes à atteindre les ODD.

– Assurer à intervalles réguliers la coordination avec les autres commissions d'études et d'autres organisations de normalisation, ainsi qu'avec les autres institutions des Nations Unies, afin de permettre une collaboration efficace.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 20 (<http://www.itu.int/ITU-T/workprog/wp_search.aspx?Q=xx/20>).

# 4 Relations

Recommandations:

• Recommandations UIT-T de la série Y.4000 y compris Y.4900/L.1600, Y.4901/L.1601, Y.4902/L.1602 et Y.4903/L.1603

Questions:

• Toutes les Questions confiées à la CE 20

Commissions d'études:

• Commissions d'études de l'UIT‑T (par exemple compte tenu de leurs rôles en tant que commissions d'études directrices), commissions d'études de l'UIT‑D et de l'UIT‑R, le cas échéant

Organismes de normalisation:

• Groupe de coordination CEN-CENELEC-ETSI "Villes et communautés intelligentes et durables" (SSCC-CG)

• ETSI TC EE

• ETSI TC Smart M2M

• IEC SEG1

• IEC TC 111

• OneM2M

• Communauté des villes intelligentes de l'IEEE

• ISO/CEI JTC 1/WG11

• ISO TC 268 SC1

• ISO SAGIIC (Industrial Internet Consortium)

ARB/43A32/2

**Nouvelle Question 3/20 intitulée "Sécurité, confidentialité, confiance et identification"**

Conformément au mandat confié par le GCNT à la CE 20 en ce qui concerne l'étude de la sécurité, de la confidentialité, de la confiance et de l'identification pour les systèmes, les services et les applications de l'Internet des objets (IoT) et des villes et des communautés intelligentes (SC&C), compte tenu des travaux et des études menés au titre des Questions 1/20, 4/20, 5/20 et 6/20, les auteurs de la présente contribution proposent d'adopter une question autonome intitulée "Sécurité, confidentialité, confiance et identification" pour les services et les applications compte tenu des travaux et des études menés au titre des Questions 4/20, 5/20 et 6/20.

Question 3/20

Sécurité, confidentialité, confiance et identification

# 1 Motifs

A l'ère de la société de l'information, le nombre de cyberattaques et de cyberdélits augmente et la perte de crédibilité ou de confiance s'accentue. L'infrastructure des TIC évoluera pour fournir les services et les applications de demain issus de la convergence en prenant en charge un grand nombre de capteurs de l'Internet des objets (IoT) et de systèmes liés à l'Internet des objets. En outre, les villes intelligentes évoluent elles aussi partout dans le monde. Les services convergents et intelligents de demain qui seront déployés grâce à l'infrastructure des TIC font intervenir un grand nombre de parties prenantes de divers secteurs. Bien qu'il augure de progrès considérables concernant les modalités de fourniture des services et des applications et les modalités de gestion, d'administration et de maintenance des systèmes, cet environnement hétérogène n'en est pas moins associé à de très nombreux risques propres aux secteurs et à de très nombreux vecteurs de menace. Les répercussions pour la sécurité, la confidentialité et la confiance en général dans l'utilisation, l'adoption et la multiplication des dispositifs, des systèmes, des services, des applications et des plates-formes de l'Internet des objets et des villes intelligentes pourraient nuire au développement du marché correspondant dans son ensemble. Par conséquent, il est important d'appliquer le principe de "l'intégration de la confidentialité et de la sécurité dès la conception", selon lequel les mécanismes de protection doivent être intégrés dans les technologies de l'information, les pratiques commerciales, les systèmes, les processus, la conception physique et l'infrastructure en réseau.

Le respect des exigences relatives à la sécurité et à la confidentialité joue un rôle primordial dans l'environnement de l'Internet des objets (IoT) et dans les villes et les communautés intelligentes (SC&C). Ces exigences sont la confidentialité et l'authentification des données, le contrôle d'accès au sein des réseaux IoT, la disponibilité, l'intégrité des données, la protection de la vie privée et la confiance entre les utilisateurs et les objets, ainsi que la non-répudiation. Les contre-mesures classiques de sécurité ne peuvent être appliquées directement aux technologies IOT, à cause des différentes normes et des piles relatives aux communications utilisées, en plus des différentes compétences spécialisées propres aux domaines de connaissance requise. En outre, le nombre élevé de dispositifs interconnectés pose des problèmes de modularité; par conséquent, il est nécessaire de disposer d'une infrastructure souple, capable de faire face aux menaces de sécurité dans cet environnement dynamique. L'infrastructure des TIC de demain devrait être fiable et sûr et garantir la confidentialité et la confiance. Par conséquent, l'instauration de la sécurité et de la confiance dans l'Internet des objets est l'une des principales questions de normalisation que la CE 20 de l'UIT-T devra traiter.

Par ailleurs, les technologies d'identification ont toujours été considérées comme véritablement indispensables à la mise en oeuvre de l'Internet des objets. On pourrait attribuer aux dispositifs physiques (par exemple, articles et produits avec étiquette, capteurs) et aux entités virtuelles (par exemple, processus informatiques, logiciels) un identificateur qui permettrait leur identification et leur distinction. Etant donné qu'un objet est lui-même composé d'autres objets, chaque objet doit impérativement être adressable et identifiable si l'on veut résoudre les problèmes de confidentialité, de sécurité, de confiance et d'accessibilité du réseau dans le cadre du déploiement de l'Internet des objets.

# 2 Question

Cette Question concerne la sécurité, la confidentialité, l'instauration de la confiance, le nommage, l'adressage et l'identification des systèmes, des services, des applications et des protocoles IoT.

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

– Quelles sont les possibles menaces pouvant mettre à mal l'authenticité, la confidentialité, l'intégrité, la non-répudiation et la disponibilité des dispositifs, des systèmes, des applications, des protocoles, des plates-formes et des services IoT, quels que soient la difficulté et le coût de la mise en oeuvre d'une attaque concrétisant une menace particulière?

– Quelles sont les probabilités estimées associées aux diverses attaques contre un système IoT ou SC&C et quel est le gain potentiel pour l'attaquant? Quels sont les dégâts estimés pour le système visé?

– Quelles sont les exigences à respecter pour atténuer et contrer les risques et les menaces identifiés pour les dispositifs, les systèmes, les applications, les protocoles, les plates‑formes et les services IoT et SC&C?

– Quels sont les systèmes d'identification requis pour satisfaire aux exigences de l'Internet des objets, y compris en ce qui concerne la sécurité, la confidentialité et la confiance?

– Quelles sont les exigences et les mécanismes permettant de protéger les informations relatives aux objets et d'éviter leur divulgation?

– Comment intégrer la gestion sécurisée des justificatifs dans les systèmes d'identification?

– Comment intégrer les technologies d'authentification dans les systèmes d'identification?

– Comment peut-on appliquer les mesures traditionnelles visant à garantir l'intégrité, la disponibilité, l'authenticité et la non‑répudiation dans les dispositifs IoT, afin de protéger l'identité, la confidentialité et la sécurité des systèmes, compte tenu des ressources limitées des dispositifs en termes d'énergie, de place, de mémoire, de bande passante et de connectivité?

– Quels sont les mesures techniques, les protocoles et les systèmes nécessaires pour garantir la protection de la confidentialité dans les applications, les services et les plates‑formes SC&C? Comment peut-on maintenir et garantir la confiance dans l'utilisation de ces systèmes?

– Comment peut-on empêcher le pistage illicite, le profilage et le traitement illicite des systèmes, des applications, des plates-formes et des services IoT?

– Quelles mesures peut-on élaborer afin de garantir en permanence la disponibilité et la portabilité des données dans les plates-formes, les systèmes et les services IoT et SC&C?

– Comment peut-on traiter les objets connectés n'utilisant pas le protocole IP et/ou le web dans un système IoT hétérogène mixte?

– De quelle manière l'interopérabilité sémantique peut-elle être utilisée en tant que mécanisme pour identifier un objet? Quels sont les risques d'identification erronée associés?

– Comment les noms de IoT sont-ils enregistrés et gérés?

– Quelles sont les mesures techniques nécessaires pour la découverte d'identité? De quels attributs un registre d'identités aurait-il besoin pour permettre l'identification des objets et l'intégration des systèmes?

– Comment les dispositifs empêcheront-t-il l'usurpation d'identité des autres dispositifs avec lesquels ils échangent des données? De quelle manière les dispositifs procéderont‑ils pour générer, traiter, stocker ou extraire des données privées, sensibles, confidentielles ou secrètes afin de pouvoir repérer et empêcher les utilisations frauduleuses?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

– Elaborer des Recommandations sur les manières d'assurer l'authenticité, la confidentialité, l'intégrité, la non-répudiation et la disponibilité pour les dispositifs, les systèmes, les applications, les protocoles, les plates-formes et les services IoT.

– Elaborer des Recommandations sur l'instauration de la sécurité et de la confiance dans l'Internet des objets, à la fois au niveau de l'infrastructure des TIC (par exemple, dans la couche infrastructure) et au niveau des futurs environnements de services convergents hétérogènes (par exemple, la couche service).

– Elaborer des Recommandations sur l'instauration de la sécurité et de la confiance dans les services et les applications IoT pour les environnements issus de la convergence entre de nombreuses parties prenantes d'autres secteurs (par exemple, utilisation de l'infrastructure TIC pour le réseau d'énergie).

– Elaborer des Recommandations sur les exigences à respecter pour atténuer les risques et les menaces identifiés pour les dispositifs, les systèmes, les applications, les protocoles, les plates-formes et les services IoT et SC&C.

– Elaborer des Recommandations sur l'utilisation des constructions traditionnelles visant à assurer l'intégrité, la disponibilité, l'authenticité et la non-répudiation dans les systèmes IoT afin de protéger l'identité, la confidentialité et la sécurité des systèmes.

– Elaborer des Recommandations sur les mesures techniques propres à empêcher le pistage illicite, le profilage et le traitement illicite des systèmes, des applications, des plates-formes et des services IoT.

– Elaborer des Recommandations sur les mesures techniques, les protocoles et les systèmes nécessaires pour garantir la protection de la confidentialité dans les applications, les services et les plates-formes SC&C.

– Elaborer des lignes directrices sur l'identification des risques potentiels associés aux différentes opérations de gestion, d'administration, de maintenance et de fourniture des services dans les villes et les communautés intelligentes.

– Elaborer des lignes directrices sur la manière d'atténuer les risques associés aux différentes opérations de gestion, d'administration, de maintenance et de fourniture des services dans les villes et les communautés intelligentes.

– Elaborer des Recommandations sur les solutions permettant de garantir la disponibilité et la portabilité des données dans les plates-formes, les systèmes et les services IoT et SC&C.

– Elaborer des Recommandations sur l'utilisation du nommage et de l'identification dans le cadre du déploiement de l'Internet des objets et des villes et des communautés intelligentes.

– Elaborer des Recommandations sur la découverte d'identité dans l'Internet des objets.

– Elaborer des Recommandations sur la gestion de l'identité dans l'Internet des objets.

– Elaborer des Recommandations sur le nommage et l'adressage dans les applications et les services IoT/SC&C.

– Assurer à intervalles réguliers la coordination avec les autres commissions d'études et des autres organisations de normalisation, ainsi qu'avec d'autres institutions des Nations Unies, afin de permettre une collaboration efficace.

# 4 ****Relations****

Recommandations:

– Recommandations UIT-T de la série Y et autre Recommandations relatives à la sécurité, à la confidentialité, à la confiance et à l'identification.

Questions:

– Toutes les Questions confiées à la CE 20

Commissions d'études:

– Commissions d'études de l'UIT‑T (par exemple compte tenu de leur rôle en tant que commissions d'études directrices), commissions d'études de l'UIT‑D et de l'UIT‑R, le cas échéant

Other bodies:

– ISO/CEI JCT 1

– Fondation DONA

– ETF

– OASIS

– OneM2M

# 2 Proposition de modification de la structure de la CE 20

ARB/43A32/3

Au cours de la période d'études, la CE 20 a tenu trois réunions, qui ont rassemblé de nombreux participants. Les travaux menés par la Commission ont abouti à de nombreux résultats; 314 contributions ont été reçues, plusieurs thèmes de travail ont été définis et un certain nombre de Recommandations ont été approuvées.

Par ailleurs, en raison du risque de chevauchement entre les travaux des GT 1/20 (Internet des objets) et 2/20 (Villes et communautés intelligentes) de la CE 20, un certain nombre de réunions conjointes ont été organisées, étant donné que les thèmes abordés et/ou les contributions se rapportaient à plusieurs Questions. Par conséquent, les auteurs de la présente contribution proposent de revoir et de réorganiser la structure de la CE 20, étant donné que la CE 20 conservera ses attributions et poursuivra les travaux entamés au cours de la période d'études précédente, comme indiqué dans le tableau suivant.

Proposition de modification de la structure de la Commission d'études 20 de l'UIT-T

|  |  |
| --- | --- |
| Questions confiées à la CE 20 | Titre |
| PLEN |  |
| Groupe de travail 1 |  |
| Question 1/20 | Travaux de recherche et technologies émergentes, y compris la terminologie et les définitions |
| Question 2/20 | Evaluation des villes et des communautés intelligentes |
| Question 3/20 | Sécurité, confidentialité, confiance et identification |
| Groupe de travail 2 |  |
| Question 4/20 | Exigences, capacités, secteurs verticaux et cas d'utilisation |
| Question 5/20 | Cadres, architecture et protocoles |
| Question 6/20 | Services, applications, calcul et traitement des données |
| Groupe de travail 3 |  |
| Question 7/20 | Infrastructure, connectivité, réseaux et interopérabilité |
| Question 8/20 | Gestion, commande et qualité de fonctionnement |

# 3 Résumés des propositions

1) Adopter une nouvelle Question 2/20 intitulée "Evaluation des villes et des communautés intelligentes".

2) Adopter une nouvelle Question 3/20 intitulée "Sécurité, confidentialité, confiance et identification".

3) Modifier la structure de la CE 20 comme indiqué dans la proposition ARB/043A32/3 afin de créer davantage de synergies entre les Questions confiées à la CE 20, de limiter les risques de chevauchement entre les Questions et de disposer d'une structure plus fiable, plus ciblée et mieux organisée.

4) Demander à l'AMNT-16 d'examiner et d'envisager la structure générale proposée et d'approuver les nouvelles Questions proposées.

5) Demander à l'AMNT-16 de charger la CE 20, à la première réunion qu'elle tiendra après l'AMNT-16, d'établir la version définitive de sa structure et d'élaborer les textes appropriés des autres Questions (Questions 1/20, 4/20, 5/20, 6/20, 7/20 et 8/20) compte tenu des résultats de l'Assemblée.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_