|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Assemblée mondiale de normalisation  des télécommunications (AMNT-16) Hammamet, 25 octobre - 3 novembre 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| **SÉANCE PLÉNIÈRE** | | **Document 20-F** | |
|  | | **Juin 2016** | |
|  | | **Original: anglais** | |
|  | | | |
| Commission d'études 17 de l'UIT-T | | | |
| Sécurité | | | |
| rapport de la CE 17 de l'UIT-T à l'assemblÉe mondiale de normalisation des tÉlÉcommunications (AMNT‑16), partie iI:  QUESTIONS qu'il est proposÉ d'étudier pendant  la prochaine pÉriode d'études (2017-2020) | | | |
| \_ | | | |

|  |  |
| --- | --- |
| **Résumé:** | La présente contribution de la Commission d'études 17 de l'UIT-T à l'AMNT‑16 contient les Questions qu'il est proposé d'étudier pendant la prochaine période d'études (2017-2020). |

Note du TSB:

Le rapport de la Commission d'études 17 à l'AMNT‑16 est présenté dans les documents suivants:

Partie I: **Document 19** – Considérations générales; y compris des propositions de modification de la Résolution 2 de l'AMNT (Annexe 2)

Partie II: **Document 20** – Questions qu'il est proposé d'étudier pendant la période d'études 2017‑2020

# 1 Liste des Questions proposées par la Commission d'études 17

| Numéro de la Question | Titre de la Question | Statut |
| --- | --- | --- |
| A/17 | Coordination en matière de sécurité des télécommunications/TIC | Suite de la Question 1/17 |
| B/17 | Architecture et cadre de sécurité | Suite de la Question 2/17 |
| C/17 | Gestion de la sécurité des informations de télécommunication | Suite de la Question 3/17 |
| D/17 | Cybersécurité | Suite de la Question 4/17 |
| E/17 | Lutte contre le spam par des moyens techniques | Suite de la Question 5/17 |
| F/17 | Aspects relatifs à la sécurité des services et des réseaux de télécommunication | Suite de la Question 6/17 |
| G/17 | Services applicatifs sécurisés | Suite de la Question 7/17 |
| H/17 | Sécurité de l'informatique en nuage | Suite de la Question 8/17 |
| I/17 | Télébiométrie | Suite de la Question 9/17 |
| J/17 | Architecture et mécanismes de gestion d'identité | Suite de la Question 10/17 |
| K/17 | Technologies génériques (annuaire, infrastructure de clé publique (PKI), infrastructure de gestion des privilèges (PMI), notation de syntaxe abstraite numéro un (ASN.1), identificateurs d'objet (OID)) utilisées pour les applications sécurisées | Suite de la Question 11/17 |
| L/17 | Langages formels pour les logiciels de télécommunication et les tests | Suite de la Question 12/17 |

# 2 Libellé des Questions

projet de QUESTION A/17

Coordination en matière de sécurité des télécommunications/TIC

(Suite de la Question 1/17)

# 1 Motifs

Les menaces contre la sécurité de l'infrastructure des télécommunications et des technologies de l'information et de la communication (TIC) sont en augmentation – tant par leur nombre que par leur complexité. Les efforts déployés au fil des années pour sécuriser l'infrastructure ont été quelque peu fragmentés et ponctuels et n'ont pas réussi jusqu'ici à assurer le degré souhaité de protection contre ces menaces. Par ailleurs, compte tenu du grand nombre d'organisations qui travaillent sur divers aspects de la sécurité, la coordination, la collaboration et la coopération sont extrêmement difficiles.

Etant donné qu'une grande partie des transactions commerciales dans le monde entier sont réalisées par le biais de liaisons de télécommunication, il est essentiel de pouvoir utiliser cette cyberinfrastructure en toute sécurité pour garantir le bon fonctionnement des entreprises, le bien‑être des citoyens et le fonctionnement efficace des administrations. Des millions d'ordinateurs et des réseaux de télécommunication du monde entier ont subi les attaques de vers, de virus et d'autres codes malveillants. L'impact économique de ces attaques a été considérable. Des efforts intenses, permanents et ciblés sont essentiels pour combattre ces menaces.

Le domaine de la sécurité est vaste. Les questions relatives à la sécurité concernent la quasi-totalité des aspects des télécommunications et de l'informatique. Pour traiter les exigences de sécurité, il existe diverses méthodes, à savoir:

• Une méthode ascendante, dans laquelle les experts conçoivent des mesures de sécurité pour renforcer et protéger un domaine particulier du réseau en utilisant des contre‑mesures et des techniques spécifiques telles que la biométrie et la cryptographie. Quoique relativement courante, c'est une méthode fragmentée qui conduit souvent à des inégalités dans la détermination et l'application des mesures de sécurité.

• Une méthode descendante, qui est une méthode stratégique et de haut niveau pour traiter les questions relatives à la sécurité. Cette méthode, pour laquelle il faut avoir un aperçu global de la situation, est généralement plus difficile à appliquer. En effet, il est plus difficile de trouver des experts qui connaissent de façon complète chaque partie du réseau et ses exigences de sécurité, que de trouver des experts qui connaissent en détail un ou deux domaines particuliers.

• Une combinaison de la méthode ascendante et de la méthode descendante, des efforts de coordination devant être déployés pour assembler les différents éléments. Il s'est avéré que cette méthode pose souvent de nombreux problèmes lorsque les intérêts et les agendas diffèrent.

Lors de la précédente période d'études, la présente Question a conduit à l'élaboration de nombreux documents que l'UIT‑T considère comme utiles pour promouvoir ses travaux et ses résultats, par exemple la feuille de route relative aux normes de sécurité des TIC, le Manuel sur la sécurité et les recueils relatifs à la sécurité. L'objectif de la présente Question sera toujours de coordonner et d'organiser toutes les activités relatives à la sécurité des télécommunications/TIC au sein de l'UIT‑T ainsi que d'élaborer et de mettre à jour des documents pour faciliter la coordination et la diffusion externe. Une méthode descendante relative à la sécurité sera utilisée en collaboration et en coordination avec d'autres Commissions d'études et d'autres organismes de normalisation. Cette activité vise à cibler davantage les efforts déployés au niveau des projets et des stratégies à la fois à l'intérieur et à l'extérieur de la CE 17.

Les travaux de la CE 17 sur la sécurité sont fondés sur les Résolutions 7, 11, 40, 50, 52, 58, 64, 65, 67, 70, 73, 75, 76 et 78 de l'AMNT, les Résolutions 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200 et 201 de la Conférence de plénipotentiaires et les Résolutions 23, 30, 34, 45, 47, 54, 63, 67, 69 et 80 de la CMDT.

La CE 17 contribue en outre à la réalisation de la grande orientation C5 du SMSI "Etablir la confiance et la sécurité dans l'utilisation des TIC" et à la réalisation de l'Objectif 3 du Plan d'action de Dubaï adopté à la Conférence mondiale de développement des télécommunications de 2014 sur le renforcement de la sécurité et de la confiance dans l'utilisation des applications TIC.

Rapports techniques relevant de la présente Question au 23 mars 2016: Rapport technique sur la sécurité dans les télécommunications et les technologies de l'information.

Textes en cours d'élaboration: Rapport technique sur l'utilisation efficace des normes de sécurité (X.TRsuss).

# 2 Question

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

a) Quels sont les résultats attendus pour la présente Question?

b) Quels sont les processus, sujets d'étude, méthodes de travail et délai à prévoir pour obtenir les résultats attendus dans le cadre de la Question?

c) Quels documents de diffusion externe (feuille de route, recueils sur la sécurité, rapports techniques, dépliants, pages web, etc.) devront être élaborés et mis à jour par l'UIT?

d) Quels ateliers sur la sécurité sont nécessaires et comment peut-on les organiser?

e) Quelles mesures faut-il prendre pour nouer des relations efficaces avec d'autres organismes de normalisation afin d'avancer les travaux dans le domaine de la sécurité?

f) Quels sont les principales étapes et les principaux critères de réussite?

g) Comment peut-on stimuler l'intérêt des Membres du Secteur et des administrations pour les travaux réalisés dans le domaine de la sécurité et comment peut-on maintenir la dynamique?

h) Comment faire en sorte que les fonctions de sécurité des télécommunications/TIC soient plus attrayantes sur le marché?

i) Comment bien faire comprendre au secteur public et au secteur privé l'importance capitale de la sécurité et la nécessité urgente de protéger les intérêts économiques au niveau mondial, qui dépendent d'une infrastructure des télécommunications/TIC robuste et sécurisée?

j) Quelles activités relatives à la sécurité sont actuellement menées dans d'autres commissions d'études de l'UIT et dans d'autres organismes de normalisation?

# 3 Tâches

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

a) Faire office de contact principal de la CE 17 pour les questions de coordination en matière de sécurité des télécommunications/TIC.

b) Tenir à jour la feuille de route relative aux normes de sécurité des TIC.

c) Tenir à jour les recueils de l'UIT-T relatifs à la sécurité.

d) Fournir une assistance et des contributions au TSB pour la mise à jour du manuel sur la sécurité, publié en tant que rapport technique sur la sécurité dans les télécommunications et les technologies de l'information.

e) Poursuivre l'élaboration du rapport technique sur l'utilisation efficace des normes de sécurité.

f) Faciliter l'identification des lacunes qui existent dans les normes relatives à la sécurité des télécommunications/TIC et faire en sorte de remédier à ces lacunes.

g) Fournir des orientations pour la mise en œuvre des normes de sécurité des télécommunications/TIC.

h) Encourager la coopération et la collaboration entre les groupes travaillant à la normalisation de la sécurité des télécommunications/TIC.

i) Examiner comme il se doit les Recommandations et les notes de liaison des autres Commissions d'études et des autres organismes de normalisation pour évaluer les conséquences sur la coordination en matière de sécurité.

j) Fournir une assistance concernant les efforts déployés pour garantir une coordination efficace en matière de sécurité en cas de besoin.

k) Faciliter les liaisons directes entre des groupes externes et les Commissions d'études appropriées de l'UIT-T.

l) Prendre l'initiative à l'UIT-T d'organiser et de planifier des ateliers et des séminaires sur la sécurité en tant que de besoin.

m) Veiller à participer de manière efficace et efficiente aux efforts de coordination en matière de sécurité déployés avec d'autres organismes.

n) Aider la CE 17 à améliorer l'efficacité de ses travaux (par exemple en créant des gabarits, des outils ou des procédures).

o) Encourager les autorités nationales et les opérateurs des pays en développement à collaborer au niveau régional afin de mieux contribuer aux activités de la CE 17 de l'UIT‑T conformément au mandat de ladite commission d'études et pour ce qui est de la mise en œuvre des Recommandations de la CE 17 sur la sécurité, par exemple au sein du Groupe régional de la CE 17 pour l'Afrique établi officiellement.

p) Aider la CE 17 à réduire l'écart en matière de normalisation conformément à la Rés. 44 de l'AMNT, à la Rés. 123 de la PP et à la Rés. 47 de la CMDT.

q) Assurer une participation efficace et efficiente aux efforts de coordination déployés par la CE 17 en matière de sécurité pour que les activités menées actuellement par la CE 17 dans le domaine de la sécurité soient prises en compte dans le programme de travail de la CE 17 et que des réponses puissent être apportées aux préoccupations des membres de l'UIT‑T.

# 4 Relations

Recommandations:

• Série X et autres Recommandations se rapportant à la sécurité des télécommunications/TIC.

Questions:

• Questions B/17, C/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 et L/17 de l'UIT‑T.

Commissions d'études:

• UIT‑D, UIT‑R, CE 2, 5, 9, 11, 13, 15, 16 et 20 de l'UIT‑T; GCNT, ainsi que les JCA et groupes spécialisés concernés.

Organismes de normalisation:

• Alliance for Telecommunications Industry Solutions (ATIS); Cloud Security Alliance (CSA); Institut européen des normes de télécommunication (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 6 et SC 27, ISO TC 292, ISO TMB; Organization for the Advancement of Structured Information Standards (OASIS); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2).

Autres organismes:

• Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); National Institute of Standards and Technology (NIST); Regional Asia Information Security Exchange (RAISE) Forum.

Projet de QUESTION B/17

Architecture et cadre de sécurité

(Suite de la Question 2/17)

# 1 Motifs

Les Recommandations UIT‑T X.800, X.802 et X.803 traitent de la sécurité dans le contexte des systèmes ouverts. L'architecture de sécurité des systèmes offrant des communications de bout en bout est décrite dans la Recommandation UIT‑T X.805. Un ensemble complet de cadres de sécurité détaillés, couvrant des aspects tels que l'authentification, le contrôle d'accès, la non-répudiation, la confidentialité, l'intégrité, l'audit et les alarmes de sécurité, a été établi (X.810, X.811, X.812, X.813, X.814, X.815 et X.816). Pour offrir une sécurité générique des couches supérieures (GULS), les Recommandations UIT‑T X.830, X.831, X.832, X.833, X.834 et X.835 ont été élaborées. En coopération avec l'ISO/CEI JTC 1/SC 27, les Recommandations UIT‑T X.841, X.842 et X.843 relatives aux objets informationnels de sécurité et aux services de tiers de confiance ont été également établies.

Il est nécessaire de poursuivre les efforts de mise à jour et d'amélioration de ces Recommandations relatives à la sécurité pour répondre aux besoins des nouvelles technologies (par exemple les réseaux de prochaine génération (NGN), les aspects relatifs à la sécurité des réseaux pilotés par logiciel (SDN)/de la virtualisation des fonctions de réseau (NFV), l'évolution à long terme/l'évolution de l'architecture système (LTE/SAE), les orientations pour la mise en œuvre technique des systèmes assurant des communications de bout en bout et les réseaux IP) et des nouveaux services. Les Recommandations X.1035 et X.1036, qui présentent en détail les protocoles d'échange de clé avec authentification par mot de passe et la distribution et l'application des politiques, rendent compte de ces efforts.

Du fait de la convergence et de la mobilité, les réseaux des opérateurs de télécommunication et les systèmes d'information associés sont exposés à de nouveaux types de menaces de sécurité. Les attaquants ont besoin de moins de compétences pour aller plus en profondeur dans les réseaux et ont tendance à causer des dégâts plus importants. Les attaques par virus, piratage et déni de service se généralisent et ont des effets négatifs sur les éléments de réseau comme sur les systèmes d'appui.

Les secteurs des télécommunications et de l'informatique sont à la recherche de solutions sécuritaires complètes et rentables qui soient indépendantes de la technologie et protègent une grande variété de services et d'applications. Pour parvenir à de telles solutions dans un environnement multifournisseur, la sécurité du réseau doit s'articuler sur des architectures et des technologies de sécurité normalisées. Compte tenu des menaces contre la sécurité de l'environnement des télécommunications et des progrès réalisés dans le domaine des contre-mesures de protection, il convient d'étudier les nouvelles exigences et solutions de sécurité. Il faut élaborer de nouvelles Recommandations qui indiquent comment combiner les normes sur les technologies et les cadres de sécurité afin de mettre en place des solutions de sécurité complètes pour les nouveaux réseaux et services.

Recommandations et Suppléments relevant de la présente Question au 29 avril 2016: Recommandations X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036 et X.1037 et Suppléments X.Suppl.2, X.Suppl.3, X.Suppl.15, X.Suppl.16 et X.Suppl.23.

Textes en cours d'élaboration: X.salcm, X.sdnsec-2, X.sgmvno, X.tigsc et X.voLTEsec-1.

# 2 Question

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

a) Comment une solution de sécurité des télécommunications complète et cohérente doit‑elle être définie?

b) Quelle est l'architecture d'une solution de sécurité des télécommunications complète et cohérente?

c) Quel est le cadre d'application de l'architecture de sécurité pour élaborer une nouvelle solution de sécurité?

d) Quel est le cadre d'application de l'architecture de sécurité pour évaluer (et donc améliorer) une solution de sécurité existante?

e) Quelles sont les bases architecturales de la sécurité?

i) Quelle est l'architecture pour la sécurité de bout en bout?

ii) Quelle est l'architecture de sécurité pour les systèmes ouverts?

iii) Quelle est l'architecture de sécurité pour l'environnement mobile?

iv) Quelle est l'architecture de sécurité pour les réseaux en évolution?

v) Quelle est l'architecture de sécurité pour les services applicatifs, en collaboration avec les travaux menés au titre de la Question G/17?

f) Quelles nouvelles Recommandations relatives aux architectures et cadres de sécurité sont nécessaires pour définir des solutions de sécurité dans l'environnement en évolution?

g) Comment convient-il de structurer les normes architecturales par rapport aux Recommandations existantes sur la sécurité?

h) Comment convient-il de structurer les normes architecturales par rapport aux technologies de sécurité avancées existantes?

i) Comment convient-il de modifier les Recommandations relatives aux cadres de sécurité pour les adapter aux nouvelles technologies et quelles nouvelles Recommandations sont nécessaires?

j) Comment sont appliqués les services de sécurité pour définir des solutions de sécurité?

k) Comment est appliqué le contrôle de l'infrastructure des télécommunications/TIC pour définir des solutions de sécurité?

# 3 Tâches

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

a) Elaborer un ensemble complet de Recommandations relatives aux architectures et cadres de sécurité pour définir des solutions de sécurité normalisées pour les télécommunications, en collaboration avec d'autres organismes de normalisation et Commissions d'études de l'UIT-T.

b) Réaliser des études et élaborer des Recommandations relatives à une architecture de réseau de télécommunication fiable qui intègre les technologies de sécurité avancées.

c) Mettre à jour et améliorer les Recommandations et Suppléments des séries X.800 et X.103x.

# 4 Relations

Recommandations:

• Série X et autres Recommandations se rapportant à la sécurité.

Questions:

• Questions A/17, C/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17 et K/17 de l'UIT‑T.

Commissions d'études:

• CE 2 de l'UIT‑D; GT 6B de l'UIT‑R; CE 2, 9, 11, 13, 16 et 20 de l'UIT-T.

Organismes de normalisation:

• Alliance for Telecommunications Industry Solutions (ATIS); Institut européen des normes de télécommunication (ETSI); Forum for International Irregular Network Access (FIINA); ISO/CEI JTC 1/SC 27 et SC 37; CEI TC 25; ISO TC 12; Internet Engineering Task Force (IETF); Projet de partenariat pour la troisième génération (3GPP), Projet 2 de partenariat pour la troisième génération (3GPP2).

projet de QUESTION C/17

Gestion de la sécurité des informations de télécommunication

(Suite de la Question 3/17)

# 1 Motifs

Pour les organisations de télécommunication, les informations et les processus d'appui, les installations de télécommunication, les réseaux et les supports de transmission constituent des actifs d'entreprise de télécommunication importants. Pour que les organisations de télécommunication gèrent comme il convient ces actifs d'entreprise et continuent de mener à bien leurs activités dans des conditions satisfaisantes, il est indispensable de gérer la sécurité des informations. C'est la raison pour laquelle on a élaboré la Recommandation UIT‑T X.1051, qui énonce des lignes directrices applicables à la gestion de la sécurité des informations pour les organisations de télécommunication.

Compte tenu de ces lignes directrices, des aspects détaillés et spécifiques relatifs à la gestion (gouvernance, cadre de gestion, risques, incidents et actifs) ont également été examinés. Il convient d'étudier plus avant de nouveaux aspects en lien avec la Recommandation UIT‑T X.1051. Dans le même temps, les séries de Recommandations doivent être tenues à jour afin de traiter des questions les plus récentes relatives à la gestion de la sécurité des informations. L'objectif est d'élaborer un ensemble de Recommandations UIT-T relatives à la gestion de la sécurité pour les télécommunications sur la base de la Recommandation UIT-T X.1051.

Parallèlement à l'élaboration de Recommandations sur des aspects détaillés et spécifiques relatifs à la gestion sur la base de la Recommandation UIT‑T X.1051, il convient d'examiner les nouveaux domaines relatifs aux télécommunications/TIC que sont l'informatique en nuage, le passage d'IPv4 à IPv6 et la protection des informations d'identification personnelle et pour lesquels des mesures nouvelles et globales sont nécessaires. Il convient donc de mener des études portant tout particulièrement sur les aspects de gestion dans les nouveaux domaines précités.

Durant ces études, la collaboration étroite entre l'UIT-T et le JTC 1 de l'ISO/CEI sera maintenue afin d'assurer la compatibilité la plus large possible des solutions de sécurité. Il faut en outre tenir compte de la performance des solutions que de nombreux pays ont élaborées sous la forme de normes nationales.

La présente Question diffère des Questions de la Commissions d'études 2 en ce sens que la Commission d'études 2 s'occupe de l'échange des informations de gestion de réseau entre éléments de réseau et systèmes de gestion ainsi qu'entre systèmes de gestion dans l'environnement du RGT. La présente Question porte essentiellement sur la protection des actifs d'entreprise, y compris les informations et les processus, en vue de la gestion de la sécurité des informations.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations E.409 (conjointement avec la CE 2), X.1051, X.1052, X.1054, X.1055, X.1056 et X.1057 et Supplément X.Suppl.13.

Textes en cours d'élaboration: X.gpim, X.sgsm, X.sup-gisb et X.sup-gpim.

# 2 Question

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

a) Comment identifier les questions spécifiques de gestion de la sécurité pour les organisations de télécommunication?

b) Comment mettre en place une gestion de la sécurité spécifique pour les petites et moyennes organisations de télécommunication (SMTO)?

c) Comment mettre en place correctement une gestion de la sécurité des informations pour les organisations de télécommunication, en utilisant les normes existantes (UIT‑T, ISO/CEI, etc.)?

d) Comment identifier et gérer la mesure de la gestion de la sécurité des informations dans les télécommunications?

e) Comment mettre en place une gestion appropriée de la sécurité des informations dans l'environnement de l'informatique en nuage?

f) Comment protéger convenablement les informations d'identification personnelle?

g) Comment mettre en place une gestion de la sécurité des informations dans l'environnement IP, en particulier lors du passage du protocole IPv4 au protocole IPv6?

h) Quelles améliorations convient-il d'apporter aux Recommandations existantes en cours de révision ou aux nouvelles Recommandations en cours d'élaboration pour réduire directement ou indirectement l'impact sur le changement climatique (par exemple économies d'énergie, réduction des émissions de gaz à effet de serre, mise en œuvre de systèmes de surveillance) dans le secteur des télécommunications/TIC ou dans les autres secteurs?

# 3 Tâches

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

a) Etudier et définir un cadre pour les fonctions de gestion de la sécurité des informations décrites dans la Recommandation UIT‑T X.1051.

b) Etudier et définir une méthodologie de mise en place d'une gestion de la sécurité des informations pour les organisations de télécommunication compte tenu des normes existantes (UIT‑T, ISO/CEI, etc.).

c) Etudier et définir des orientations pour la mise en place d'une gestion de la sécurité des informations pour les petites et moyennes organisations de télécommunication (SMTO).

d) Etudier et définir des lignes directrices pour la mise en place d'une gestion de la sécurité des informations pour l'informatique en nuage.

e) Etudier et définir des lignes directrices ou un cadre pour la mise en place d'une gestion de la sécurité des informations dans l'environnement IPv6.

f) Etudier, et définir dans des Recommandations, des lignes directrices relatives à la protection des informations d'identification personnelle.

g) Proposer le plan général de nouvelles Recommandations.

h) Evaluer les résultats des activités ci-dessus par rapport aux possibilités d'utilisation pour les installations et services de télécommunication.

i) Elaborer des projets de Recommandation.

j) Mettre à jour et améliorer les Recommandations de la série X.105x.

# 4 Relations

Recommandations:

• Séries X.800, X.1000, X.1100, X.1200 et X.1300.

Questions:

• Questions A/17, B/17, D/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 et 14/15 de l'UIT‑T.

Commissions d'études:

• UIT‑D; UIT‑R; CE 2, 9, 11, 13, 15 et 16 de l'UIT‑T.

Organismes de normalisation:

• Cloud Security Alliance (CSA); Institut européen des normes de télécommunication (ETSI); ISO/CEI JTC 1/SC 27; ISO/TC 68, ISO/TC 215; National Institute of Standards and Technology (NIST); Telecommunication Technology Committee (TTC); Projet de partenariat pour la troisième génération (3GPP).

projet de QUESTION D/17

Cybersécurité

(Suite de la Question 4/17)

# 1 Motifs

Le paysage des télécommunications évolue constamment, tout comme les exigences associées relatives à la sécurité des télécommunications/TIC*.* Dans le cyberenvironnement, il existe un fort besoin de sécurisation des protocoles, infrastructures et applications qui sont utilisés pour nos communications quotidiennes.

La cybersécurité repose sur la sécurisation et la protection des services et des informations personnelles, sur la protection des informations d'identification personnelle et sur la fourniture d'une garantie des informations entre les entités en interaction.

Les cyberattaques sont toujours très nombreuses; elles causent un large éventail de problèmes aux utilisateurs, fournisseurs de services, opérateurs et réseaux. Pour pouvoir lutter contre ce fléau par des moyens techniques, il faut définir des cadres et des exigences applicables aux cyberattaques: détection et protection, atténuation des effets et retour à la normale, et échange d'informations sur la cybersécurité.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1544, X.1546, X.1570, X.1580, X.1581 et X.1582 et Suppléments X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.18 et X.Suppl.20.

Textes en cours d'élaboration: X.1542 (X.simef), X.cogent, X.metric, X.nessa, X.samtn et X.sbb.

# 2 Question

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

a) Comment les fournisseurs de télécommunications/TIC doivent-ils sécuriser leur infrastructure, maintenir un fonctionnement fiable et utiliser des mécanismes de garantie de la sécurité dans les réseaux de télécommunications/TIC?

b) Quelles sont les exigences de sécurité que les concepteurs et fabricants de logiciels, de protocoles de télécommunication et de systèmes de communication doivent prendre en considération pour concevoir, élaborer et partager des bonnes pratiques dans le cyberenvironnement?

c) Comment partager efficacement les informations sur les vulnérabilités pour faciliter le traitement de ces vulnérabilités?

d) Quelles exigences et solutions sont nécessaires pour garantir la résilience, la sécurité et l'intégrité des systèmes composables dans le domaine des télécommunications/TIC?

e) Quelles exigences et solutions sont nécessaires pour la responsabilisation, l'intervention en cas d'incident, le suivi des menaces et la communication des risques dans le domaine des télécommunications/TIC?

f) Quels mécanismes sont nécessaires pour le partage d'informations relatives à la garantie de la sécurité des systèmes dans le cyberenvironnement, en particulier des systèmes en nuage, imbriqués et composables?

g) Comment peut-on utiliser les réseaux pour assurer des services critiques (par exemple, utilisation du protocole d'alerte commun) de façon sécurisée pendant une situation d'urgence nationale?

h) Quelles sont les lignes directrices et bonnes pratiques nécessaires en matière de sécurité afin d'identifier et d'atténuer les cybermenaces et de réduire leur impact, en particulier pour ce qui est des logiciels malveillants, du déni de service réparti et de l'ingénierie sociale?

i) Quelles améliorations convient-il d'apporter aux Recommandations existantes en cours de révision ou aux nouvelles Recommandations en cours d'élaboration pour réduire directement ou indirectement l'impact sur le changement climatique (par exemple économies d'énergie, réduction des émissions de gaz à effet de serre, mise en œuvre de systèmes de surveillance) dans le secteur des télécommunications/TIC ou dans les autres secteurs?

# 3 Tâches

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

a) Collaborer avec les Commissions d'études de l'UIT‑T, l'ETSI, les FIRST, l'IETF, l'IEEE, l'ISO/CEI JTC 1, l'OASIS, l'OMA, le TCG, le 3GPP, le 3GPP2, et d'autres organismes de normalisation concernant la cybersécurité.

b) Réfléchir à des cadres et à des Recommandations pour spécifier comment les fournisseurs de télécommunications/TIC peuvent sécuriser leur infrastructure et maintenir un fonctionnement fiable, et échanger des informations sur la cybersécurité.

c) Elaborer un ensemble de Recommandations définissant des solutions de sécurité pour la responsabilisation, la garantie et l'intervention en cas d'incident dans le domaine des télécommunications/TIC.

d) Etudier et spécifier les techniques et capacités de sécurité permettant aux fournisseurs de services de coordonner et d'échanger des informations sur les vulnérabilités, les plates-formes, les cyberattaques, etc.

e) Spécifier comment appliquer des mécanismes de responsabilisation, de garantie et d'intervention en cas d'incident dans les réseaux de télécommunication/TIC.

f) Elaborer des lignes directrices et des techniques de protection des informations personnelles et des informations d'identification personnelle (PII) sur la base de techniques CYBEX.

g) Aider les autres Commissions d'études de l'UIT‑T à appliquer les Recommandations relatives à la cybersécurité pour définir des solutions de sécurité spécifiques.

h) Elaborer des bonnes pratiques et des lignes directrices concernant le partage d'informations sur les vulnérabilités ainsi que des solutions pour faciliter le traitement des vulnérabilités.

# 4 Relations

Recommandations:

• Série X et autres Recommandations se rapportant à la sécurité.

Questions:

• Questions A/17, B/17, C/17, E/17, F/17, G/17, H/17, I/17, J/17, K/17 et 7/11 de l'UIT‑T

Commissions d'études:

• CE 2 de l'UIT‑D (Question 3/2); CE 2, 9, 11, 13 (Question 7/13) et 16 de l'UIT‑T.

Organismes de normalisation:

• Institut européen des normes de télécommunication (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); CEI TC 57, CEI TC 65/WG10; ISO/CEI JTC 1/SC 27; National Institute of Standards and Technology (NIST); Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); Open Group; Object Management Group (OMG); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2); Trusted Computing Group (TCG).

Autres organismes:

• Anti-Phishing Working Group (APWG); CERT/CC; CIRT; Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); GSM Association (GSMA); Forum for Incident Response and Security Teams (FIRST); International Multilateral Partnership Against Cyber Threats (IMPACT); Organisation de coopération et de développement économiques (OCDE).

projet de QUESTION E/17

Lutte contre le spam par des moyens techniques

(Suite de la Question 5/17)

# 1 Motifs

Le spam est devenu un problème de grande ampleur, susceptible d'entraîner des pertes de recettes pour les fournisseurs d'accès Internet, opérateurs de télécommunications, opérateurs de télécommunications mobiles et entreprises dans le monde entier. Utilisé entre autres pour l'hameçonnage et la diffusion de virus, de vers, de logiciels-espions et d'autres formes de logiciels malveillants, le spam crée en outre des problèmes au niveau de la sécurité des informations et des réseaux de télécommunication. Par conséquent, par sa Résolution 52, l'AMNT-08 a chargé les commissions d'études compétentes de continuer à fournir un appui aux travaux en cours, en particulier à ceux de la Commission d'études 17, concernant la lutte contre le spam et d'accélérer leurs travaux sur le spam afin de traiter le problème des menaces actuelles et futures, dans les domaines de compétence de l'UIT-T, selon qu'il conviendra. Elle les a aussi chargées de poursuivre la collaboration avec les organisations concernées afin de continuer à élaborer, d'urgence, des Recommandations techniques en vue d'échanger de bonnes pratiques et à diffuser des informations dans le cadre d'ateliers organisés conjointement, de séances de formation, etc., et a en outre chargé la Commission d'études 17 de rendre compte régulièrement au Groupe consultatif de la normalisation des télécommunications de la mise en œuvre de cette Résolution.

Il a été admis que la lutte contre le spam est un problème de portée mondiale qui appelle une approche tous azimuts et exhaustive. En tant que Commission d'études directrice pour la sécurité des télécommunications et dans le cadre des activités déployées au titre de la Résolution 52 de l'AMNT, la Commission d'études 17 est bien placée pour étudier les diverses mesures techniques susceptibles de faciliter la lutte contre le spam afin d'assurer la stabilité et la fiabilité du réseau de télécommunication. La structure technique des Recommandations existantes et potentielles relatives à la lutte contre le spam par des moyens techniques a notamment été établie afin de faciliter la production de Recommandations. Par ailleurs, il convient de publier de nouvelles Recommandations relatives à la lutte contre les nouvelles formes de spam.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations X.1231, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246 et X.1247 et Suppléments X.Suppl.6, X.Suppl.11, X.Suppl.12, X.Suppl.14 et X.Suppl.25.

Textes en cours d'élaboration: X.cspim, X.gcspi, X.tfcma et X.ticsc.

# 2 Question

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

a) Comment comprendre et identifier le spam?

b) Quelles sont les nouvelles formes de spam dans les réseaux existants et futurs?

c) Quelles sont les graves conséquences du spam?

d) Quels sont les facteurs techniques qui contribuent à rendre difficile l'identification des sources de spam?

e) En quoi les nouvelles technologies, les nouveaux services et les nouvelles applications (messagerie instantanée, réseaux sociaux, applications mobiles, téléphonie LTE (évolution à long terme)/RCS (suite de communications riches), etc.) rendent-ils possibles la création et la diffusion de spams?

f) Quelles sont les études techniques déjà entreprises dans le cadre des activités de l'IETF, du 3GPP, de la GSMA, du M3AAWG, et d'autres forums, ainsi que par des entités du secteur privé, pour traiter le problème du spam?

g) Quel travail de normalisation du réseau de télécommunication est-il éventuellement nécessaire de réaliser pour lutter efficacement contre le spam et assurer la stabilité et la fiabilité du réseau de télécommunication?

h) Quelles sont les solutions efficaces et efficientes de lutte contre le spam?

i) Comment définir des exigences génériques et spécifiques pour le partage d'informations sur la lutte contre le spam?

j) Quelles sont les bonnes pratiques de lutte contre le spam?

# 3 Tâches

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

a) Coordonner à l'UIT-T l'étude des moyens techniques permettant de lutter contre le spam, au sens donné par la Commission d'études 2.

b) Cerner et étudier les risques résultant, au niveau de la sécurité du réseau de télécommunication (aux bords et dans l'infrastructure centrale), de l'évolution constante de la nature du spam.

c) Etablir une liste complète et actualisée des ressources et moyens techniques permettant de lutter contre le spam dans un réseau de télécommunication (ressources et moyens déjà disponibles ou en cours d'élaboration).

d) Elaborer de nouvelles Recommandations relatives à la lutte contre les formes existantes ou nouvelles de spam.

e) Définir des exigences génériques et spécifiques pour le partage d'informations sur la lutte contre le spam.

f) Etablir si de nouvelles Recommandations ou des améliorations apportées à des Recommandations existantes – notamment en ce qui concerne les méthodes permettant de lutter contre la diffusion de courriels non sollicités, de logiciels malveillants et d'autres types de contenus malveillants, et de lutter contre les équipements de réseau compromis, en particulier les botnets – pourraient être utiles dans les efforts déployés pour lutter efficacement contre le spam et assurer la stabilité et la fiabilité du réseau de télécommunication.

g) Fournir régulièrement au Groupe consultatif de la normalisation des télécommunications et au Directeur du Bureau de la normalisation des télécommunications des éléments actualisés, destinés à être incorporés dans le rapport annuel au Conseil.

# 4 Relations

Recommandations

• Série X.

Questions:

• Questions A/17, B/17, C/17, D/17, F/17, G/17, H/17, I/17 et J/17 de l'UIT-T.

Commissions d'études:

• CE 1 et 2 de l'UIT-D; CE 2, 11, 13 et 16 de l'UIT‑T.

Organismes de normalisation:

• ISO/CEI JTC 1; Internet Engineering Task Force (IETF); Institut européen des normes de télécommunication (ETSI); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2); Open Mobile Alliance (OMA) et autres organismes nationaux et internationaux de normalisation concernés.

Autres organismes:

• GSM Association (GSMA); Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG); Forum for Incident Response and Security Teams (FIRST); National Institute of Standards and Technology (NIST); Organisation de coopération et de développement économiques (OCDE).

projet de QUESTION F/17

Aspects relatifs à la sécurité des services et des réseaux de télécommunication

(Suite de la Question 6/17)

# 1 Motifs

La Recommandation UIT‑T X.1101 décrit les exigences de sécurité et le cadre applicables aux communications en multidiffusion. Les Recommandations UIT‑T X.1111, X.1112, X.1113 et X.1114 décrivent le cadre de sécurité, le profil de certificat de dispositif, les mécanismes d'authentification et le cadre d'autorisation pour les réseaux domestiques. Les Recommandations UIT‑T X.1121, X.1122, X.1123, X.1124 et X.1125 spécifient en détail la sécurité pour les réseaux mobiles. Les Recommandations UIT‑T X.1171, X.1311 et X.1312 spécifient respectivement le cadre de confidentialité pour les services NID mobiles, le cadre de sécurité des réseaux de capteurs ubiquitaires, les lignes directrices sur la sécurité des intergiciels des réseaux de capteurs ubiquitaires et les exigences de sécurité pour le routage dans les réseaux de capteurs sans fil. Les Recommandations UIT‑T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 et X.1198 décrivent un ensemble complet d'exigences, mécanismes et cadre pour la sécurité des services de TVIP. Les Suppléments UIT‑T X.Suppl.19 et X.Suppl.24 portent sur les aspects de sécurité des téléphones mobiles. Il faut poursuivre les efforts pour mettre à jour et améliorer ces Recommandations et Suppléments relatifs à la sécurité afin de répondre aux besoins des nouvelles technologies et des nouveaux services.

Les services et les réseaux de télécommunication permettent à n'importe qui d'accéder à n'importe quelle information souhaitée de façon conviviale, à tout moment, en tout lieu et en utilisant n'importe quel dispositif. Le secteur des télécommunications connaît une croissance exponentielle dans le domaine des services de télécommunication basés sur la technologie mobile. En particulier, la sécurité des services et des réseaux de télécommunication propres à un domaine entre des dispositifs hétérogènes utilisant des technologies au niveau application telles que les réseaux de capteurs ubiquitaires (y compris l'Internet des objets (IoT), les communications de machine à machine (M2M), les systèmes de transport intelligents et les réseaux de cinquième génération), les réseaux domestiques, les aspects de sécurité lors de l'utilisation de réseaux pilotés par logiciel (SDN)/de la virtualisation des fonctions de réseau (NFV), les réseaux électriques intelligents, les réseaux mobiles (y compris les communications en champ proche (NFC), le module d'identité d'abonné incorporé (eSIM) et les smartphones), les réseaux de multidiffusion, les réseaux de TVIP, etc. est indispensable pour le développement futur du secteur, des opérateurs de réseau et des fournisseurs de services.

La normalisation de solutions de sécurité complètes optimales est essentielle pour les opérateurs de réseau et les fournisseurs de services qui travaillent dans un environnement de télécommunication international multifournisseur. En raison de certaines caractéristiques particulières des télécommunications mobiles (par exemple transmission par voie hertzienne, puissance de calcul et taille de mémoire limitées des petits dispositifs mobiles), assurer la sécurité est une tâche particulièrement difficile qui mérite une attention et une étude particulières.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313 et X.1314 et Suppléments X.Suppl.19, X.Suppl.24 et X.Suppl.26.

Textes en cours d'élaboration: X.iotsec-1, X.iotsec-2, X.itsec-1, X.itssec-2, X.msec-9, X.msec-11, X.sdnsec-1, X.sgsec-2 et X.sotavsu.

# 2 Question

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

a) Comment identifier et définir les aspects relatifs à la sécurité des services et des réseaux de télécommunication dans le domaine des télécommunications mobiles?

b) Comment identifier et traiter les menaces qui pèsent sur les services et les réseaux de télécommunication?

c) Quelles technologies de sécurité peuvent être utilisées pour les services et les réseaux de télécommunication?

d) Comment assurer et maintenir une interconnectivité sécurisée entre les services et les réseaux de télécommunication?

e) Quelles techniques, quels mécanismes et quels protocoles de sécurité sont nécessaires pour les nouveaux services et réseaux de télécommunication, en particulier les nouveaux services de protection du contenu numérique?

f) Quelles sont les solutions de sécurité globales pour les services et les réseaux de télécommunication (par exemple les services utilisés pour les réseaux électriques intelligents et les systèmes de transport intelligents qui sont fondés sur les réseaux de télécommunication/TIC)?

g) Quelles sont les bonnes pratiques ou lignes directrices applicables aux services et aux réseaux de télécommunication sécurisés?

h) Quelles améliorations convient-il d'apporter aux Recommandations existantes en cours de révision ou aux nouvelles Recommandations en cours d'élaboration pour réduire, directement ou indirectement, l'impact sur le changement climatique (par exemple économies d'énergie, réduction des émissions de gaz à effet de serre, mise en œuvre de systèmes de surveillance) dans le secteur des télécommunications/TIC ou dans les autres secteurs?

i) Quels mécanismes de protection et de gestion des informations d'identification personnelle (PII) sont nécessaires pour les services et les réseaux de télécommunication sécurisés?

# 3 Tâches

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

a) En collaboration avec d'autres commissions d'études de l'UIT‑T et d'autres organismes de normalisation, notamment l'IETF, l'ISO/CEI JTC 1/SC 6, 25, 27 et 31, élaborer un ensemble de Recommandations définissant des solutions de sécurité complètes pour les services et les réseaux de télécommunication sécurisés.

b) Examiner les Recommandations/normes existantes de l'UIT-T, de l'ISO/CEI et d'autres organismes de normalisation dans le domaine des réseaux domestiques, des réseaux électriques intelligents, des réseaux mobiles (y compris la sécurité des smartphones), des services IoT mobiles et des réseaux de capteurs ubiquitaires pour identifier les services et les réseaux de télécommunication sécurisés.

c) Poursuivre les études afin de définir les aspects relatifs à la sécurité des services et des réseaux de télécommunication pour un environnement de télécommunication international multifournisseur, et pour les nouveaux services (par exemple les services utilisés pour les systèmes de transport intelligents et les réseaux électriques intelligents qui sont fondés sur les réseaux de télécommunication/TIC).

d) Etudier et recenser les problèmes et menaces de sécurité dans les services et les réseaux de télécommunication sécurisés.

e) Etudier et définir les mécanismes de sécurité pour les services et les réseaux de télécommunication sécurisés.

f) Etudier et définir les mécanismes d'interconnectivité pour les services et les réseaux de télécommunication sécurisés dans un environnement de télécommunication comportant un seul ou plusieurs fournisseurs.

g) Etudier et recenser les problèmes de protection des informations PII et les menaces associées dans les services et les réseaux de télécommunication sécurisés.

h) Etudier et définir les mécanismes de protection et de gestion des informations PII pour les services et les réseaux de télécommunication sécurisés.

# 4 Relations

Recommandations:

• Série X et autres Recommandations se rapportant à la sécurité.

Questions:

• Questions A/17, B/17, C/17, D/17, E/17, G/17, H/17, I/17, J/17, K/17, 7/13, 13/16 et 21/16 de l'UIT‑T.

Commissions d'études:

• UIT‑R; CE 9, 11, 13, 15, 16 et 20 de l'UIT‑T, JCA-IoT, JCA-IPTV; Collaboration sur les normes de communication pour les systèmes ITS (CITS).

Organismes de normalisation:

• GSM Association (GSMA); Internet Engineering Task Force (IETF); CEI SEG 6 (micro-réseaux électriques), CEI SMB WG3, CEI TC 57 et 65; ISO/CEI JTC 1/SC 6, 25, 27 et 31; ISO TC 204, Open Mobile Alliance (OMA); Projet de partenariat pour la troisième génération (3GPP), Projet 2 de partenariat pour la troisième génération (3GPP2).

Autres organismes:

• Alliance for Telecommunications Industry Solutions (ATIS); China Communications Standards Association (CCSA); Institut européen des normes de télécommunication (ETSI) (TC CYBER, TC ITS), M2M Alliance; NFC Forum; National Institute of Standards and Technology (NIST); oneM2M; Telecommunication Technology Committee (TTC); Telecommunications Technology Association (TTA); Universal Plug and Play (UPnP).

projet de QUESTION G/17

Services applicatifs sécurisés

(Suite de la Question 7/17)

# 1 Motifs

Les Recommandations UIT‑T X.1141, X.1142, X.1143 et X.1144 constituent un ensemble de Recommandations sur les jetons de sécurité pour l'authentification/autorisation et les architectures de sécurité pour les messages des services de réseau. Les Recommandations UIT‑T X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158 et X.1159 spécifient les lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés et divers services de tiers de confiance (TTP). Les Recommandations UIT‑T X.1161, X.1162, X.1163 et X.1164 spécifient un cadre complet et des mécanismes pour la sécurité des services P2P. Il faut poursuivre les efforts pour mettre à jour et améliorer ces Recommandations relatives à la sécurité afin de répondre aux besoins des nouvelles technologies et des nouveaux services.

Le secteur des télécommunications connaît une croissance exponentielle des services de tiers de confiance (TTP). La sécurité des services applicatifs basés sur les télécommunications (par exemple services de réseaux sociaux, services P2P et services TTP) est indispensable pour le développement futur du secteur. Les protocoles applicatifs sécurisés jouent un rôle très important dans la fourniture de services applicatifs sécurisés. La normalisation de solutions de sécurité complètes optimales est essentielle pour les entreprises et les opérateurs de réseau qui travaillent dans un environnement international multifournisseur. De plus, il faut aussi étudier et définir d'autres types de services applicatifs sécurisés comme les services d'horodatage, les services notariaux sécurisés, les services financiers numériques sécurisés (paiement en ligne, services bancaires en ligne, commerce électronique), les services d'analyse de données et les services de détection des logiciels malveillants, d'intervention et d'analyse du comportement des logiciels malveillants dans des environnements contrôlés; l'utilisation d'assertions de sécurité au lieu d'utiliser des certificats dans les protocoles fondés sur l'infrastructure PKI et les services applicatifs PKI, etc. Les technologies de sécurité comme l'assertion de sécurité et l'assertion de contrôle d'accès deviennent très importantes dans les réseaux de communication.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations X.1141, X.1142, X.1143, X.1144, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163 et X.1164 et Suppléments X.Suppl.17, X.Suppl.21 et X.Suppl.22.

Textes en cours d'élaboration: X.websec-6, X.websec-7 et X.websec-8.

# 2 Question

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

a) Comment identifier et traiter les menaces qui pèsent sur les services applicatifs sécurisés?

b) Quelles sont les technologies de sécurité à utiliser pour la fourniture de services applicatifs sécurisés?

c) Comment assurer et maintenir une interconnectivité sécurisée entre les services applicatifs?

d) Quels protocoles ou techniques de sécurité sont nécessaires pour les services applicatifs sécurisés?

e) Quels protocoles ou techniques de sécurité sont nécessaires pour les nouveaux services applicatifs sécurisés?

f) Quelles sont les solutions de sécurité globales pour les services applicatifs sécurisés et pour leurs applications?

# 3 Tâches

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

a) En collaboration avec d'autres Commissions d'études de l'UIT‑T et d'autres organismes de normalisation, notamment l'ISO/CEI JTC 1/SC 27, élaborer un ensemble complet de Recommandations définissant des solutions de sécurité complètes pour les services applicatifs sécurisés.

b) Examiner les Recommandations/normes existantes de l'UIT‑T et de l'ISO/CEI dans le domaine des services applicatifs sécurisés.

c) Mener des études complémentaires pour définir les aspects de sécurité des services applicatifs sécurisés existants ou nouveaux.

d) Etudier et définir les problèmes et menaces de sécurité dans les services applicatifs sécurisés.

e) Etudier et définir les mécanismes de sécurité pour les services applicatifs sécurisés.

# 4 Relations

Recommandations:

• Série X.800 et autres Recommandations se rapportant à la sécurité.

Questions:

• Questions A/17, B/17, C/17, D/17, E/17, F/17, H/17, I/17, J/17, K/17, 7/13 et 13/16 de l'UIT‑T.

Commissions d'études:

• CE 2, 9, 11, 13, 16 et 20 de l'UIT‑T.

Organismes de normalisation:

• Internet Engineering Task Force (IETF); Institut européen des normes de télécommunication (ETSI); GSM Association (GSMA); ISO/CEI JTC 1/SC 27, ISO/TC 68; Kantara Initiative; Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); World Wide Web Consortium (W3C).

Autres organismes:

• Conseil de l'Europe; Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); Fast Identity Online (FIDO) Alliance; International Multilateral Partnership Against Cyber Threats (IMPACT).

projet de QUESTION H/17

**Sécurité de l'informatique en nuage**

(Suite de la Question 8/17)

# 1 Motifs

L'informatique dématérialisée, ou informatique en nuage, est un modèle permettant d'offrir à un utilisateur de services un accès ubiquitaire, pratique, à la demande et via le réseau à un ensemble mutualisé de ressources informatiques configurables (par exemple réseaux, serveurs, mémoires, applications et services), qui peuvent être rapidement mobilisées et mises à disposition moyennant un minimum de gestion ou d'interaction avec le fournisseur de services. Le modèle de l'informatique en nuage comporte cinq caractéristiques essentielles (à la demande, accès universel via le réseau, mutualisation des ressources, élasticité rapide, libre-service avec facturation à l'utilisation), cinq catégories de services (à savoir logiciel en tant que service (SaaS, *software as a service*), communication en tant que service (CaaS, *communication as a service*), plate‑forme en tant que service (PaaS, *platform as a service*), infrastructure en tant que service (IaaS, *infrastructure as a service*) et réseau en tant que service (NaaS, *network as a service*)) et différents modèles de déploiement (public, privé, hybride …). L'informatique en nuage est devenue le support privilégié pour la découverte, l'externalisation, la composition et la réutilisation des services dans des flux de travail, des applications et des applications fondées sur les communications, de sorte que l'exigence de sécurité revêt une importance accrue.

L'informatique en nuage devrait offrir divers avantages tels que la fourniture de ressources souple et dynamique et une simplification ainsi qu'une automatisation de l'administration des infrastructures informatiques. La dématérialisation permet de partager une quantité quasi illimitée de ressources et permet d'améliorer l'évolutivité et de réduire massivement les coûts liés à la gestion des infrastructures. Toutefois, les systèmes ouverts et les ressources partagées de l'informatique en nuage soulèvent bon nombre de problèmes de sécurité, ce qui constitue peut-être l'obstacle le plus important à leur adoption. Le passage à l'informatique en nuage signifie que les systèmes informatiques internes sécurisés classiques seront supplantés par des infrastructures ouvertes, non sécurisées et "mises en nuage", d'où la nécessité de "repenser" radicalement le concept de sécurité.

L'informatique en nuage a été considérée pendant plusieurs années comme étant centrée sur les services informatiques et contrôlée par les acteurs de l'Internet. Toutefois les acteurs des télécommunications ont un rôle important à jouer sur le marché et dans l'écosystème émergents de l'informatique en nuage. Les services en nuage étant fournis par l'intermédiaire des réseaux de télécommunication, les acteurs des télécommunications devraient assurer un niveau de garantie élevé. Une protection de la sécurité efficace et offrant la souplesse voulue sera un élément déterminant du marché et de l'écosystème de l'informatique en nuage dans leur ensemble.

En outre, la souplesse d'utilisation de ressources précieuses dans les environnements informatiques en nuage permettra de fournir de nouveaux services de sécurité que les dispositifs de protection actuels ne peuvent assurer (par exemple les services de lutte contre les logiciels malveillants en tant que service en nuage). En conséquence, il faut examiner quels types de mesures de sécurité l'informatique en nuage pourra assurer à brève échéance.

Les Recommandations UIT-T X.1601, X.1602 et X.1631 constituent un ensemble de Recommandations relatives aux services de sécurité pour l'aperçu général, l'architecture et le cadre de sécurité de l'informatique en nuage, la sécurité en nuage transcouche et la sécurité propre aux services de réseau. A l'heure actuelle, il est essentiel de sécuriser les services (services critiques vocaux, multimédias, d'identité, assurance des informations, services d'identité et de données et services d'urgence) rendus possibles par l'informatique en nuage. La présente Question a pour objet d'élaborer de nouvelles Recommandations, à partir du rapport technique (Partie 5) du Groupe spécialisé sur l'informatique dématérialisée, sur les thèmes suivants:

• bonnes pratiques et lignes directrices à élaborer pour donner des orientations sur la manière d'assurer la sécurité dans un environnement utilisant l'informatique en nuage;

• clarification des responsabilités et définition des exigences de sécurité ainsi que des menaces qui pèsent sur la sécurité pour les principaux acteurs et rôles correspondants dans l'écosystème de l'informatique en nuage;

• architecture de sécurité fondée sur l'architecture de référence décrite au titre de la Question 18/13;

• gestion de la sécurité et technologies d'audit pour la gestion de la confiance.

Les responsables de la Question H/17 collaboreront avec les responsables des Questions connexes, par exemple les Questions B/17, C/17, D/17, G/17, J/17 et K/17, en vue d'élaborer des Recommandations relatives à la sécurité de l'informatique en nuage.

Recommandations relevant de la présente Question au 23 mars 2016: X.1601, X.1602, X.1631 et X.1642.

Textes en cours d'élaboration: X.1641 (X.CSCDataSec), X.dsms et X.SRIaaS.

# 2 Question

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

a) Quelles nouvelles Recommandations ou autres types de documents convient-il d'élaborer à l'intention des principaux acteurs – fournisseurs et utilisateurs de services et partenaires – ainsi que des autres principaux acteurs concernés, pour promouvoir la sécurité de l'informatique en nuage?

b) Quelles nouvelles Recommandations convient-il d'élaborer concernant l'architecture de la sécurité et l'organisation des fonctionnalités de la sécurité conformément à l'architecture de référence?

c) Quelles nouvelles Recommandations convient-il d'élaborer concernant les mécanismes de garantie, les technologies d'audit et l'évaluation des risques associés pour instaurer la confiance entre les différents acteurs?

d) Quelle collaboration faut-il établir avec d'autres Questions, commissions d'études et organismes de normalisation pour éviter autant que possible toute répétition des tâches?

e) Comment la sécurité en tant que service doit-elle être mise au point pour protéger les systèmes de télécommunication/TIC?

# 3 Tâches

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

a) Elaborer des Recommandations ou d'autres types de documents pour promouvoir la sécurité de l'informatique en nuage.

b) Elaborer des Recommandations pour définir les exigences de sécurité et les menaces qui pèsent sur la sécurité, afin de sécuriser les services liés à l'informatique en nuage sur la base des exigences générales définies par la Commission d'études 13 de l'UIT‑T en matière d'informatique en nuage.

c) Elaborer des Recommandations pour définir l'architecture de sécurité et organiser les fonctions de sécurité sur la base de l'architecture de référence définie par la Commission d'études 13 de l'UIT‑T.

d) Elaborer des Recommandations pour définir une architecture et une mise en œuvre de la sécurité efficaces, souples et élastiques pour les systèmes informatiques en nuage.

e) Elaborer des Recommandations pour déterminer des mécanismes de garantie, des technologies d'audit et une évaluation des risques, l'objectif étant d'établir des relations de confiance dans l'écosystème de l'informatique en nuage.

f) Assumer la responsabilité de toutes les activités liées à la sécurité de l'informatique en nuage au sein de la Commission d'études 17.

g) Représenter la Commission d'études 17, pour ce qui est des travaux relatifs à la sécurité de l'informatique en nuage, au sein de l'activité conjointe de coordination sur l'informatique en nuage.

# 4 Relations

**Recommandations:**

• Recommandations de la série Y relatives à l'informatique en nuage.

**Questions:**

• Questions A/17, B/17, C/17, D/17, G/17, J/17 et K/17 de l'UIT‑T.

**Commissions d'études:**

• CE 2, 13, 16 et 20 de l'UIT‑T.

**Organismes de normalisation:**

• Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 27 et SC 38; Organization for the Advancement of Structured Information Standards (OASIS) et autres organismes concernés identifiés.

**Autres organismes:**

• Cloud Security Alliance (CSA); Distributed Management Task Force (DMTF).

projet de QUESTION I/17

Télébiométrie

(Suite de la Question 9/17)

# 1 Motifs

Pendant la période d'études précédente, les travaux menés au titre de la Question 9/17 ont préparé le terrain pour l'utilisation de la biométrie dans les applications de télécommunication et les Recommandations nécessaires ont été élaborées. À mesure que la biométrie s'est généralisée pour la vérification d'identité dans des applications comme le commerce électronique et la cybersanté, les systèmes biométriques ont posé divers problèmes liés à la protection de la vie privée, à la fiabilité et à la sécurité des données biométriques pour les applications de biosûreté et de biosécurité. Ces problèmes deviennent plus complexes et plus sévères lorsque l'authentification biométrique est adoptée dans un environnement de réseau ouvert.

Actuellement, les applications de télécommunication sur les terminaux mobiles et les services Internet exigent des méthodes d'authentification qui non seulement offrent une sécurité élevée mais aussi sont pratiques pour les utilisateurs. Les services bancaires en ligne sur téléphone mobile et la vidéosurveillance au moyen de caméras en réseau ou d'un système de télévision en circuit fermé sont des exemples de ces applications émergentes, pour lesquelles l'authentification télébiométrique devrait satisfaire à ces exigences. Il est donc nécessaire de spécifier des exigences concernant l'utilisation des Recommandations relatives à la sécurité, à la sûreté et à la protection de la vie privée. De plus, il est nécessaire de s'intéresser aussi aux tests de conformité et d'interopérabilité pour les Recommandations ainsi qu'au remplissage de la base de données télébiométriques.

Recommandations relevant de la présente Question au 23 mars 2016: X.1080.1, X.1081, X.1082, X.1083, X.1084, X.1086, X.1088, X.1089, X.1090, X.1091 et X.1092.

Textes en cours d'élaboration: X.bhsm, X.pbact, X.tam, X.th2, X.th3, X.th4, X.th5, X.th6 et X.th13.

# 2 Question

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

a) Comment améliorer encore ou réviser les Recommandations actuelles pour qu'elles soient largement déployées et utilisées?

b) Quelles sont les exigences de l'authentification biométrique dans un réseau comportant de nombreuses fonctionnalités comme le NGN?

c) Comment évaluer les contre‑mesures de sécurité pour des applications particulières de télébiométrie?

d) Comment définir les systèmes et opérations biométriques pour qu'ils soient conformes aux exigences de sécurité de n'importe quelle application de télébiométrie, y compris les services informatiques en nuage?

e) Comment peut-on améliorer l'identification et l'authentification des utilisateurs en termes de sécurité et de sûreté en utilisant des modèles télébiométriques interopérables?

f) Quels mécanismes faut-il prendre en charge pour garantir la sûreté et la sécurité de manipulation des données biométriques dans les applications de télébiométrie tant existantes qu'émergentes, par exemple la cybersanté, la télémédecine, le commerce électronique, les services bancaires en ligne ou la vidéosurveillance?

# 3 Tâches

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

a) Améliorer et réviser les Recommandations actuelles sur l'authentification télébiométrique et remplir la base de données télébiométriques.

b) Examiner les similitudes et les différences entre les Recommandations UIT-T et les normes de l'ISO/CEI existantes relatives à la télébiométrie.

c) Etudier et définir les exigences et lignes directrices relatives à la sécurité de n'importe quelle application de télébiométrie sur la base des architectures et des cadres tels que ceux définis au titre de la Question B/17.

d) Etudier et définir les exigences pour évaluer la sécurité, la conformité et l'interopérabilité avec les techniques de protection de la vie privée pour n'importe quelle application de télébiométrie.

e) Etudier et définir les exigences des applications télébiométriques dans un réseau comportant de nombreuses fonctionnalités.

f) Etudier et définir les exigences et cadres intégrés relatifs aux architectures télébiométriques pour les environnements de l'informatique en nuage et du stockage des données.

g) Etudier et définir les exigences d'authentification télébiométrique pour un cadre d'identité sécurisé.

h) Etudier et définir les exigences des protocoles génériques appropriés concernant la sûreté, la sécurité, la protection de la vie privée et l'accord "pour la manipulation de données biométriques" dans n'importe quelle application de télébiométrie, par exemple la cybersanté, la télémédecine, le commerce électronique, les services bancaires en ligne, le paiement en ligne ou la vidéosurveillance.

i) Etudier et définir des protocoles biologie-machine (B2M) de transmission de métriques biologiques qui soient compatibles avec les protocoles machine-machine (M2M).

j) Etudier et définir des applications télébiométriques utilisant des bio-signaux pour des applications d'authentification, d'identification, de suivi de l'état de santé, etc.

k) Etudier et définir un protocole de télécommunication holosphérique.

# 4 Relations

Recommandations:

• X.200, X.273, X.274, X.509, X.680, X.805 et X.1051.

Questions:

• Questions A/17, B/17, C/17, D/17, E/17, F/17, G/17, H/17, J/17, K/17, 7/13 et 14/15 de l'UIT‑T.

Commissions d'études:

• CE 2/2 de l'UIT‑D; CE 7 de l'UIT‑R; CE 2, 5, 9, 11, 13, 15 et 16 de l'UIT‑T.

Organismes de normalisation:

• CEI/TC 25, CEI/TC 25/JWG 1; Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 17, 27 et 37; ISO/TC 12, 68 et 215; ISO/TC 12/JWG 20.

Autres organismes:

• Bureau international des poids et mesures (BIPM); Commission internationale des unités et mesures radiologiques (ICRU); Fast Identity Online (FIDO) Alliance; Bureau international du travail (BIT); Organisation mondiale de la santé (OMS).

projet de QUESTION J/17

Architecture et mécanismes de gestion d'identité

(Suite de la Question 10/17)

# 1 Motifs

La gestion d'identité (IdM) est la gestion du cycle de vie et de l'utilisation (création, tenue à jour, utilisation, configuration et révocation) des justificatifs, identificateurs, attributs, authentification, attestation et profils au moyen desquels les entités (par exemple fournisseurs de services, utilisateurs finals, réseaux sociaux, organisations, dispositifs de réseau, applications et services) sont connues avec un certain degré de confiance. Suivant le contexte, de multiples identités peuvent exister pour une même entité en des endroits multiples et pour répondre à différentes exigences de sécurité. Dans le nuage et les réseaux publics, l'IdM permet un échange sécurisé d'informations entre entités autorisées basé sur la validation et la confirmation des identités à travers des systèmes répartis. L'IdM permet de protéger les informations et de garantir que seules les informations autorisées sont diffusées. L'IdM est un élément essentiel au bon fonctionnement des réseaux de télécommunication/TIC (par exemple l'Internet des objets (IoT), l'informatique en nuage et l'informatique mobile, les services et les produits), car elle permet d'établir et de maintenir des communications fiables. Elle permet non seulement l'authentification de l'identité d'une entité, mais aussi l'autorisation de privilèges, la modification aisée des privilèges lorsqu'une entité change de rôle, la délégation, la nomadicité et d'autres services importants basés sur l'identité.

L'IdM est un élément critique pour la gestion de la sécurité de réseau et pour permettre un accès nomade à la demande aux réseaux et aux services électroniques, accès attendu par les utilisateurs finals actuels. Conjointement avec d'autres mécanismes de défense, l'IdM contribue à prévenir les fraudes et les vols d'identité et ainsi à augmenter la confiance des utilisateurs dans la sécurité et la fiabilité des transactions électroniques (par exemple dans l'IoT et dans les systèmes informatiques en nuage ou mobiles qui ne sont pas contrôlés directement par l'organisation utilisatrice).

Il existera différentes spécifications et solutions IdM nationales ou régionales, qui continueront à évoluer. Du point de vue des communications à l'échelle mondiale, il est très important d'harmoniser les différentes approches, spécifications et solutions IdM nationales ou régionales. Pour pouvoir atteindre cet objectif, des normes IdM qui reposent sur des environnements adaptés aux besoins des développeurs et qui encouragent le développement à grande échelle d'applications et d'outils utilisant diverses technologies web (HTTP, JSON, OAUTH et OpenID Connect) sont nécessaires.

La présente Question vise à définir la vision ainsi qu'à coordonner et à organiser toutes les activités relatives à l'IdM au sein de l'UIT-T. Une méthode descendante relative à l'IdM sera utilisée en collaboration avec d'autres Commissions d'études, d'autres organismes de normalisation et des consortiums. Il est admis que certains aspects de l'IdM (protocoles, exigences et identifiants de dispositif de réseau) relèveront d'autres Questions.

Recommandations et Suppléments relevant de la présente Question au 23 mars 2016: Recommandations X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257 et X.1275 et Supplément X.Suppl.7.

Textes en cours d'élaboration: X.1258 (X.eaaa) et X.te.

# 2 Question

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

a) Quels sont les concepts fonctionnels d'une infrastructure commune de gestion d'identité (IdM)?

b) Comment définir un modèle IdM approprié qui soit indépendant des technologies de réseau, qui soit centré sur l'utilisateur, qui représente les informations IdM et qui permette un échange sécurisé des informations IdM entre les entités concernées (par exemple utilisateurs, parties utilisatrices et fournisseurs d'identité)?

c) Quels sont les éléments nécessaires pour rassembler les systèmes IdM sociaux, mobiles et d'entreprise de manière à sécuriser davantage les transactions numériques?

d) Quels sont les aspects fonctionnels des modèles IdM?

e) Quelles sont les exigences IdM propres aux fournisseurs de services et aux consommateurs de services?

f) Quels sont les attributs des identités qui peuvent être partagés par les fournisseurs d'identités dans les cadres de confiance?

g) Quelles sont les exigences, les capacités et les stratégies possibles pour parvenir à une interopérabilité entre différents systèmes IdM (par exemple garantie d'identité, interfonctionnement)?

h) Quels sont les mécanismes envisageables en matière d'interopérabilité des systèmes IdM, par exemple l'identification et la définition de profils applicables, pour réduire au minimum les problèmes liés à l'interopérabilité?

i) Quelles sont les exigences et les mécanismes permettant de protéger les informations d'identification personnelle (PII) et d'éviter leur divulgation?

j) Quelles sont les exigences applicables à la protection des systèmes IdM contre les cyberattaques?

k) Quelles capacités IdM peuvent être utilisées contre les cyberattaques?

l) Comment doit-on intégrer l'IdM avec les technologies de sécurité avancées?

m) Quelles sont les exigences IdM propres à l'informatique en nuage?

n) Quelles sont les exigences IdM propres à l'informatique mobile?

o) Quelles sont les exigences IdM propres à divers environnements répartis comme l'IoT et le nuage?

p) Comment intégrer le contrôle d'identité dans les systèmes IdM?

q) Comment intégrer la gestion sécurisée des justificatifs dans les systèmes IdM?

r) Comment intégrer les technologies d'authentification dans les systèmes IdM?

# 3 Tâches

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

a) Spécifier un cadre IdM qui prenne en charge un modèle de découverte, de politique et de confiance, l'authentification et l'autorisation, les assertions et la gestion du cycle de vie des justificatifs nécessaires pour la gestion d'identité dans les environnements en évolution.

b) Définir les concepts fonctionnels de l'architecture IdM afin d'assurer un relais IdM parmi les réseaux et parmi les systèmes IdM compte tenu des technologies de sécurité avancées.

c) Définir les exigences et proposer des mécanismes concernant la garantie d'identité. Etablir des critères pour la mise en correspondance/l'interfonctionnement de différentes méthodes de garantie d'identité qui pourraient être adoptées dans divers réseaux. Dans ce contexte, la garantie d'identité recouvre les profils d'identité et la réputation.

d) Proposer des lignes directrices pour l'interopérabilité des systèmes IdM.

e) Définir les exigences (et proposer des mécanismes) concernant la protection des systèmes IdM, y compris l'utilisation par les fournisseurs de services de capacités IdM pour assurer une coordination et échanger des informations concernant les cyberattaques.

f) Mettre à jour et coordonner une liste ouverte de termes et définitions concernant l'IdM et poursuivre les travaux en cours.

g) Etudier et définir les risques et menaces de sécurité liés à l'IdM.

# 4 Relations

Recommandations:

• Séries X et Y.

Questions:

• Questions A/17, C/17, D/17, F/17, G/17, et H/17 de l'UIT‑T

Commissions d'études:

• CE 1 et 2 de l'UIT‑D; CE 2, 3, 11, 13, 16 et 20 de l'UIT‑T; GCNT

Organismes de normalisation:

• Internet Engineering Task Force (IETF); Institut européen des normes de télécommunication (ETSI); ISO/CEI JTC 1 SC 6, 27 et 37.

Autres organismes:

• National Institute of Standards and Technology (NIST); Organization for the Advancement of Structured Information Standards (OASIS); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2).

projet de QUESTION K/17

Technologies génériques (par exemple annuaire, PKI, ASN.1, identificateurs d'objet) utilisées pour les applications sécurisées

(Suite de la Question 11/17)

# 1 Motifs

La présente Question vise à encourager la poursuite du développement de diverses technologies génériques qui sont largement utilisées pour les applications sécurisées, à savoir:

• Services d'annuaire (série X.500).

• Infrastructures de clés publiques (PKI – X.509).

• Infrastructure de gestion des privilèges (PMI – X.509).

• ASN.1 (séries X.680 et X.690), identificateurs d'objet et leurs autorités d'enregistrement (séries X.660 et X.670).

• Services web rapides et Fast Infoset (série X.890).

• OSI et ODP.

## 1.1 Motifs pour les travaux sur les annuaires et les infrastructures PKI et PMI

La série X.500 de Recommandations UIT-T a une grande incidence dans les entreprises. Ces Recommandations, sur lesquelles reposent en grande partie des technologies largement déployées telles que l'infrastructure de clé publique (PKI) et le protocole simple d'accès à l'annuaire (LDAP), sont utilisées dans de nombreux domaines, par exemple financier, médical et juridique. Lorsque des services d'annuaire présentant une grande sécurité sont nécessaires, par exemple dans le domaine militaire, la série X.500 est la seule solution.

La Recommandation UIT‑T X.500 définit des mécanismes détaillés de contrôle d'accès et de protection de la confidentialité des données. Il s'agit d'une spécification ouverte qui peut être adaptée à de nombreuses applications différentes. Elle peut être étendue afin de répondre aux exigences futures. Le protocole LDAP largement utilisé est fondé sur le modèle d'annuaire UIT‑T X.500. La Recommandation UIT‑T X.500 comporte des fonctionnalités permettant un interfonctionnement avec le protocole LDAP. La gestion d'identité (IdM) repose en grande partie sur les solutions d'annuaire UIT‑T X.500 et LDAP. Les fournisseurs de solutions d'annuaire les commercialisent comme des systèmes IdM. Plusieurs exigences liées à la gestion d'identité et aux réseaux NGN (par exemple pour les applications basées sur des étiquettes) peuvent être satisfaites grâce au service d'annuaire.

La Recommandation UIT‑T X.509 est importante. Les certificats de clés publiques sont largement utilisés. Dans chaque session de navigation sécurisée utilisant le protocole TLS (sécurité de la couche transport), un certificat est utilisé pour authentifier le serveur web et déterminer la clé de chiffrement qui sera utilisée pour protéger les informations échangées durant la session. Le certificat de clé publique sert aussi à authentifier et à protéger le courrier électronique. Pour leurs travaux, le groupe de travail PKIX de l'IETF, le CA Browser Forum, Electronic Signatures and Infrastructure (ESI) de l'ETSI, etc., se fondent sur la Recommandation UIT‑T X.509.

Les certificats d'attributs constituent une méthode sûre pour transmettre des privilèges, notamment dans les systèmes fédérés de gestion d'identité. Les spécifications SAML OASIS sont fondées sur les certificats d'attribut UIT‑T X.509. Les certificats d'attribut sont utiles en particulier lorsque des privilèges sont assignés par des autorités autres que celles qui ont délivré les certificats de clé publique et lorsque des privilèges de longue durée et révocables sont nécessaires, par exemple pour les membres d'un groupe.

La série X.500 de Recommandations UIT‑T doit être actualisée afin de tenir compte des nouvelles exigences relatives à la gestion d'identité, aux réseaux NGN et aux communications en champ proche.

En collaboration avec d'autres groupes, il faut actualiser la Recommandation UIT‑T X.509 afin de tenir compte et de tirer parti des expériences acquises dans le domaine de l'infrastructure de clés publiques (PKI) et dans celui de l'infrastructure de gestion des privilèges (PMI). Des améliorations doivent être apportées à la Recommandation UIT-T X.509 afin de tenir compte des nouvelles exigences relatives aux communications machine-machine, à la sécurité des réseaux électriques intelligents et à la sécurité de l'Internet des objets.

Recommandations relevant de la présente Question au 23 mars 2016: E.104 (conjointement avec la CE 2), E.115 (conjointement avec la CE 2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525 et X.1341.

Textes en cours d'élaboration: X.pki-em (Infrastructure de clé publique: Etablissement et maintenance) et X.pki-prof (Infrastructure de clé publique: Profil).

## 1.2 Motifs pour les travaux sur l'ASN.1, les identificateurs d'objet et leurs autorités d'enregistrement

De nouvelles Recommandations seront élaborées selon qu'il sera nécessaire pour tenir compte des progrès technologiques et des besoins supplémentaires des utilisateurs concernant la notation ASN.1 et ses règles de codage ainsi que des besoins supplémentaires des utilisateurs et des fournisseurs concernant les autorités d'enregistrement et les identificateurs d'objet internationaux.

L'ASN.1 s'est révélée être la notation de prédilection pour de nombreux groupes de normalisation de l'UIT-T, dont un grand nombre continue de demander que des corrections soient apportées aux adjonctions et amendements les plus récents à ces Recommandations pour résoudre des problèmes d'ambiguïté ou de manque de clarté.

Les identificateurs d'objet (OID) se sont avérés être un espace de noms très apprécié, basé essentiellement sur une structure arborescente d'autorités d'enregistrement hiérarchiques identifiées par un entier. L'extension récente de cet espace de noms aux identificateurs d'objet internationaux permettant d'identifier les arcs par des étiquettes Unicode est également appréciée pour diverses applications, et une nouvelle extension sera probablement nécessaire, pour de nouvelles attributions.

Les autres Commissions d'études, les organismes de normalisation externes et les pays demandent régulièrement des conseils et une assistance non seulement sur des questions liées à la notation ASN.1 mais aussi et de plus en plus sur la gestion de l'espace de noms des identificateurs d'objet. Les besoins d'aide et de conseils devraient augmenter avec la mise en place des identificateurs d'objet internationaux et l'utilisation croissante d'autorités d'enregistrement nationales par les pays en développement. Il est donc nécessaire de poursuivre le "Projet OID" de l'UIT‑T placé sous la responsabilité d'un chef de projet afin de répondre à ces besoins.

Toute utilisation innovante des identificateurs d'objet doit être mise au point conjointement avec la Commission d'études 2 de l'UIT‑T.

Recommandations relevant de la présente Question au 23 mars 2016: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.891, X.892 et X.893.

Textes en cours d'élaboration: X.894 (X.cms), X.jsoner, X.oid-iot (Lignes directrices relatives à l'utilisation d'identificateurs d'objet pour l'Internet des objets), X.oiddev (Technologies de l'information – Utilisation d'identificateurs d'objet pour identifier les dispositifs dans l'Internet des objets) et X.cms (Syntaxe de message cryptographique).

## 1.3 Motifs pour la tenue à jour des Recommandations OSI

Les systèmes fondés sur les Recommandations OSI peuvent être mis en œuvre pendant relativement longtemps. Lors de l'exploitation des systèmes mis en œuvre sur la base de ces Recommandations, on peut constater qu'il existe des erreurs techniques ou qu'il est souhaitable d'apporter des améliorations à ces Recommandations. Il est donc nécessaire de tenir à jour en permanence les Recommandations OSI de la série X.

Le travail consacré aux Recommandations de base relatives à l'interconnexion des systèmes ouverts (OSI) a été achevé.

Recommandations relevant de la présente Question au 23 mars 2016: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217bis, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227bis, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237bis, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881 et X.882.

Textes en cours d'élaboration: Aucun.

## 1.4 Motifs pour la tenue à jour des Recommandations ODP

Dans un système de télécommunication, la disponibilité de logiciels permettant un traitement réparti ouvert (ODP) revêt une importance fondamentale. Pour pouvoir assurer un traitement réparti ouvert, il faut normaliser des modèles de référence, des architectures, des fonctions, des interfaces et des langages (série UIT‑T X.900).

Recommandations relevant de la présente Question au 23 mars 2016: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 et X.960.

# 2 Question

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

## 2.1 Sujets à étudier concernant les travaux sur les annuaires et les infrastructures PKI et PMI

Concernant les services d'annuaire*:*

a) Quelles nouvelles définitions de services ou quelles modifications dans la série F sont nécessaires pour déterminer comment les capacités actuelles peuvent être utilisées et quelles sont les nouvelles exigences concernant la Recommandation UIT‑T X.500?

b) Quelles améliorations faut-il apporter à la série E de Recommandations pour satisfaire aux nouvelles exigences des services?

c) Quelles améliorations faut-il apporter à l'annuaire pour satisfaire aux nouvelles exigences liées à l'infrastructure PKI?

d) Quelles sont les nouvelles exigences en matière de sécurité et de confidentialité des informations d'annuaire?

e) Quelles autres règles de codage pour la Recommandation UIT‑T X.500 (XML par exemple) peuvent être nécessaires pour améliorer encore l'utilité de la Recommandation UIT‑T X.500?

f) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour permettre leur utilisation dans divers environnements, par exemple les environnements à ressources limitées, les environnements de machine à machine et les grands réseaux?

g) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour accroître leur utilité dans des domaines tels que la biométrie, l'authentification, le contrôle d'accès et le commerce électronique?

h) Quelles modifications faut-il apporter à la Recommandation UIT‑T X.509 pour définir des améliorations et corriger les erreurs?

Cette étude sera réalisée en collaboration avec l'ISO/CEI JTC 1/SC 6 dans le cadre du travail qu'il consacre à l'extension de la norme ISO/CEI 9594. Une coopération sera maintenue avec l'IETF, en particulier concernant le protocole LDAP et l'infrastructure PKI*.*

## 2.2 Sujets à étudier concernant les travaux sur l'ASN.1, les identificateurs d'objet et leurs autorités d'enregistrement

a) Quelles améliorations faut-il apporter à la notation de syntaxe abstraite numéro un (ASN.1) et à ses règles de codage pour répondre aux besoins des futures applications?

b) Quels tutoriels sont nécessaires pour faciliter l'utilisation d'identificateurs d'objet dans divers environnements?

c) Quelles autorités d'enregistrement supplémentaires ou quelles procédures sont nécessaires pour faciliter les travaux effectués au titre de la présente Question et d'autres Questions?

d) Quelle collaboration, en dehors des accords en vigueur, faut-il établir avec d'autres organismes élaborant des normes de droit ou de fait pour que le travail de l'UIT-T sur l'ASN.1 et les identificateurs d'objet continue d'occuper une place prééminente dans le domaine de la fourniture de notations pour la définition de protocoles et pour l'établissement de noms non ambigus?

## 2.3 Sujets à étudier concernant la tenue à jour des Recommandations OSI

a) Mise à jour permanente des Recommandations sur l'architecture OSI et sur les différentes couches pour leur apporter les éventuelles améliorations nécessaires et pour corriger les erreurs signalées.

b) Mise à jour permanente du service et des systèmes de traitement des messages, du transfert fiable, des opérations distantes, du service CCR et du traitement transactionnel OSI pour leur apporter les éventuelles améliorations nécessaires et pour corriger les erreurs signalées.

Il est hautement souhaitable de maintenir une collaboration et une liaison étroites avec les autres Commissions d'études et les autres groupes internationaux mettant en œuvre l'OSI pour garantir l'applicabilité la plus large possible des Recommandations correspondantes.

Le travail doit être effectué en collaboration avec l'ISO/CEI JTC 1 et ses sous-comités.

## 2.4 Sujets à étudier concernant la tenue à jour des Recommandations ODP

Mise à jour permanente des Recommandations ODP.

Il est hautement souhaitable de maintenir une collaboration et une liaison étroites avec les autres Commissions d'études et les autres groupes internationaux mettant en œuvre l'ODP pour garantir l'applicabilité la plus large possible des Recommandations correspondantes.

Le travail doit être effectué en collaboration avec l'ISO/CEI JTC 1/SC 7/WG 19.

# 3 Tâches

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

## 3.1 Tâches concernant les travaux sur les annuaires et les infrastructures PKI et PMI

a) Mettre à jour l'annuaire en élaborant des rapports d'erreurs et des corrigenda techniques.

b) Déterminer les nouvelles exigences relatives à l'annuaire découlant des technologies existantes ou nouvelles.

c) Elaborer la neuvième édition de la série X.500 de Recommandations UIT‑T.

d) Définir les améliorations à apporter aux Recommandations UIT‑T X.509, X.pki-prof et X.pki-em pour satisfaire aux nouvelles exigences.

## 3.2 Tâches concernant les travaux sur l'ASN.1, les identificateurs d'objet et leurs autorités d'enregistrement

a) Assurer le suivi de tous les travaux en cours à la fin de la dernière période d'études en vue de la publication des textes correspondants.

b) Collaborer avec l'ISO/CEI JTC 1/SC 6 dans les domaines d'intérêt commun.

c) Mettre à jour les Recommandations UIT‑T des séries X.660, X.670, X.680, X.690 et X.890 au cours de la période d'études pour répondre aux besoins des utilisateurs et élaborer de nouvelles versions si nécessaire.

d) Lorsqu'il est nécessaire d'améliorer le transfert de données, aider toutes les Commissions d'études à fournir des modules ASN.1 équivalents aux schémas XML définis dans les Recommandations UIT‑T (en vigueur ou en cours d'élaboration), notamment dans les cas où la largeur de bande est étroite.

e) Assurer le suivi des Recommandations | Normes internationales et corrigenda techniques approuvés en vue d'en faciliter la publication.

f) Traiter tous les rapports d'erreur présents au début de la période d'études (et les nouveaux rapports soumis pendant la période d'études) et élaborer des corrigenda techniques si nécessaire.

g) Faire en sorte que toutes les notes de liaison relatives aux travaux sur l'ASN.1 et les identificateurs d'objet soient traitées en temps voulu et de façon appropriée.

h) Elaborer les tutoriels ou pages web supplémentaires susceptibles d'aider les utilisateurs de l'ASN.1 et les utilisateurs d'identificateurs d'objet.

i) Obtenir l'accord de l'ISO/CEI JTC 1/SC 6 et de la CE 17 concernant les attributions supplémentaires d'identificateurs d'objet qui sont jugées nécessaires.

j) Sous la responsabilité du chef du projet OID:

– fournir des indications générales aux utilisateurs d'identificateurs d'objet;

– promouvoir l'utilisation de l'ASN.1 et des identificateurs d'objet internationaux dans les autres Commissions d'études et dans les organismes de normalisation externes;

– aider les pays à établir et à maintenir une autorité d'enregistrement nationale pour les identificateurs d'objet (y compris les identificateurs d'objet internationaux).

## 3.3 Tâches concernant la tenue à jour des Recommandations OSI

a) Apporter les modifications ou améliorations nécessaires aux Recommandations OSI sur la base des contributions reçues ou pour corriger les erreurs signalées.

b) Mettre à jour le guide de mise en œuvre OSI.

## 3.4 Tâches concernant la tenue à jour des Recommandations ODP

Apporter les modifications ou améliorations nécessaires aux Recommandations ODP sur la base des contributions reçues ou pour corriger les erreurs signalées.

# 4 Relations

Recommandations:

• Série H.200, H.323, série H.350, T.120, série X.600-X.609, série X.700, série X.800‑X.849, série Z.

Questions:

• Toutes les Questions de l'UIT-T relatives aux Recommandations ci‑dessus.

Commissions d'études:

• CE 2, 4, 11, 13, 16, 20 et toutes les commissions d'études de l'UIT-T qui utilisent l'ASN.1 ou des identificateurs d'objet, ou qui en ont besoin

Organismes de normalisation:

• Internet Engineering Steering Group (IESG); Internet Engineering Task Force (IETF); CEI/TC 57; ISO/CEI JTC 1/SC 6, 7, 27 et 31, ISO TC 68, 204; Organization for the Advancement of Structured Information Standards (OASIS); Object Management Group (OMG); World Wide Web Consortium (W3C).

Autres organismes:

• Union postale universelle (UPU).

projet de QUESTION L/17

**Langages formels pour les logiciels de télécommunication et les tests**

(Suite de la Question 12/17)

**1 Motifs**

La présente Question vise à encourager la poursuite du développement de divers langages formels qui sont largement utilisés dans la conception des systèmes de télécommunication et dans les tests.

La présente Question porte sur la définition et l'utilisation des langages UIT formels de conception de système pour définir les besoins, l'architecture et le comportement des systèmes de télécommunication: langages pour les besoins, langages pour la description de données, la spécification de comportement, les tests et la mise en œuvre. Ces langages formels sont largement utilisés dans les entreprises et à l'UIT‑T et des outils commerciaux les prennent en charge. Les langages peuvent être appliqués collectivement ou individuellement pour la spécification de normes et la réalisation de produits. Les langages UIT de conception de système concernés sont les suivants:

• La notation des besoins de l'utilisateur, qui est appliquée pour l'analyse des objectifs et la définition des cas d'utilisation, en particulier dans les étapes initiales de conception.

• La notation de syntaxe abstraite numéro un (ASN.1), qui s'est révélée être la notation de prédilection pour de nombreux groupes de normalisation pour la spécification des informations transmises entre les entités, et garantit, avec les règles de codage associées, que les informations peuvent être transmises sans ambiguïté, en toute sécurité et avec efficacité.

• Le langage de spécification et de description, qui permet de spécifier un stimulus et le comportement résultant d'entités, et peut être combiné avec la spécification d'unités de données en ASN.1.

• Un profil UML pour le langage de spécification et de description, qui limite les modèles UML à un comportement bien défini qui évite les variantes sémantiques intrinsèques à la norme OMG et les parties de l'UML qui ne sont pas nécessaires pour le comportement couvert par le langage de spécification et de description.

• La notation des diagrammes de séquences de messages, qui permet de décrire la séquence de messages entre les entités, et qui peut aussi être utilisée pour suivre le comportement d'un système.

• La notation de test et de commande de test version 3 (TTCN-3), qui permet de spécifier des tests de fonctionnalité et d'interopérabilité de systèmes et de concevoir des suites de tests génériques. La notation TTCN-3 est utilisée dans les Recommandations UIT-T relatives aux tests élaborées par les Commissions d'études compétentes de l'UIT-T, en particulier la CE 11, en sa qualité de commission d'études directrice pour les spécifications de test ainsi que pour les tests de conformité et d'interopérabilité. L'UIT-T produit un grand nombre de Recommandations. Pour assurer l'interopérabilité, il est essentiel que les mises en œuvre de ces Recommandations soient conformes aux Recommandations.

• CHILL, le langage de programmation de l'UIT‑T, qui a été largement utilisé par le passé, mais ces dernières années d'autres approches ont été utilisées, par exemple la production de code à partir du langage de spécification et de description.

Tous ces langages UIT de conception de système sont définis dans des Recommandations relevant de la présente Question, sauf la notation ASN.1 (et ses règles de codage associées).

En plus de définir les langages, les documents relevant de la présente Question fournissent des orientations aux autres commissions d'études, aux organisations de normalisation extérieures et aux pays pour définir, utiliser et appliquer les langages (et dans une certaine mesure la notation ASN.1). Les Recommandations UIT-T Z.110, Z.450 et Z.500 et le Supplément Z.Sup1 donnent des orientations pour l'utilisation et l'application des langages. Les Recommandations UIT-T Z.111 et Z.119 énoncent des lignes directrices sur la manière de rédiger toute nouvelle Recommandation sur un langage et sont utilisées comme références dans d'autres Recommandations (en particulier dans les séries Z.100 et Z.150).

Recommandations, Suppléments et Guides de mise en œuvre relevant de la présente Question au 23 mars 2016: X.292, Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170, Z.200, Z.450, Z.500, Z.Sup1 et Z.Imp100.

Textes en cours d'élaboration: aucun.

**2 Question**

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

a) Quelle actualisation faut-il apporter à la définition des langages UIT de conception de système existants (exception faite de la notation ASN.1) de manière à ce que ces langages soient adaptés aux nouveaux besoins des utilisateurs actuels ainsi qu'aux nouvelles architectures et aux nouveaux cadres?

b) Quels nouveaux langages sont nécessaires en ce qui concerne les nouveaux besoins des utilisateurs actuels ainsi que les nouvelles architectures et les nouveaux cadres (par exemple l'Internet des objets) compte tenu de la Recommandation UIT‑T Z.110?

**3 Tâches**

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

a) Actualiser les Recommandations relevant de la présente Question.

b)Fournir des conseils généraux aux utilisateurs des langages, méthodologies et cadres en ce qui concerne les langages étudiés au titre de la présente Question.

c) Encourager l'utilisation des méthodologies, des cadres et des langages étudiés au titre de la présente Question dans les autres commissions d'études et dans les organisations de normalisation extérieures;

**4 Relations**

**Recommandations:**

• Série X.680/X.690.

**Questions:**

• Question K/17, toutes les Questions de l'UIT-T utilisant des langages de conception de système.

**Commissions d'études:**

• CE 11, en tant que Commission d'études directrice pour les spécifications de test ainsi que pour les tests de conformité et d'interopérabilité, toutes les commissions d'études qui utilisent les langages UIT de conception de système (CE 2, 11, 13, 16 et 20 en particulier) ou qui spécifient des tests (CE 2, 9, 11, 13, 15, 16 et 20 en particulier), GCNT.

**Autres groupes de l'UIT-T:**

• JCA-CIT de l'UIT‑T.

**Organismes de normalisation:**

• Institut européen des normes de télécommunication (ETSI) (TC MTS); Internet Engineering Task Force (IETF); ISO/CEI JTC 1 et ses sous-comités qui utilisent les langages UIT de conception de système.

**Autres organismes:**

• Object Management Group (OMG); SDL Forum Society.

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