|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | | | **Union internationale des télécommunications**  **Bureau de la Normalisation des Télécommunications** | | |  |
|  | | |  | Genève, le 28 septembre 2022 | | |
| **Réf.:** | **Circulaire TSB 42**  CE 17/XY | | | - Aux Administrations des États Membres de l'Union | | |
| **Tél.:** | +41 22 730 6206 | | |
| **Fax:** | +41 22 730 5853 | | |
| **E-mail:** | [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | | | **Copie**:  - Aux Membres du Secteur UIT-T;  - Aux Associés de l'UIT-T participant aux travaux de la Commission d'études 17;  - Aux établissements universitaires participant aux travaux de l'UIT;  - Aux Président et Vice-Présidents de la Commission d'études 17 de l'UIT‑T;  - À la Directrice du Bureau de développement des télécommunications;  - Au Directeur du Bureau des radiocommunications | | |
| **Objet:** | **Consultation des États Membres au sujet des textes déterminés des projets de nouvelles Recommandations UIT-T X.1353 (X.ztd-iot), X.1380 (X.edr-sec), X.1381 (X.eivn-sec), X.1382 (X.fstsicv), X.1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS-sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec-ecs) et X.1816 (X.5Gsec-ssl), qu'il est proposé d'approuver à la séance plénière électronique de la Commission d'études 17 de l'UIT-T (Genève, 21 février – 3 mars 2023)** | | | | |

Madame, Monsieur,

1 La Commission d'études 17 de l'UIT-T (Sécurité) a l'intention d'appliquer la procédure d'approbation traditionnelle énoncée à la section 9 de la Résolution 1 (Rév. Genève, 2022) de l'AMNT pour l'approbation des projets de Recommandations mentionnés ci-dessus à sa prochaine réunion virtuelle, qui se tiendra du 21 février au 3 mars 2023. L'ordre du jour ainsi que tous les renseignements pertinents concernant la réunion de la Commission d'études 17 de l'UIT-T seront disponibles dans la Lettre collective [3/17](https://www.itu.int/md/T22-SG17-COL-0003/en).

2 Vous trouverez dans l'**Annexe 1** le titre, le résumé et la localisation des projets de Recommandations UIT‑T qu'il est proposé d'approuver.

NOTE 1 DU TSB – Exception faite des projets de Recommandations UIT-T X.1382 (X.fstsicv), X.1815 (X.5Gsec-ecs) et X.1816 (X.5Gsec-ssl), aucun document de justification UIT-T A.5 n'a été élaboré pour ces projets de textes déterminés.

NOTE 2 DU TSB – À la date de la présente Circulaire, le TSB n'avait reçu aucune déclaration concernant les droits de propriété intellectuelle relative à ces projets de textes. Pour obtenir des renseignements actualisés, les membres sont invités à consulter la base de données relative aux droits de propriété intellectuelle à l'adresse [www.itu.int/ipr/](https://www.itu.int/fr/ITU-T/ipr/Pages/default.aspx).

3 La présente Circulaire a pour objet d'engager le processus de consultation formelle des États Membres de l'UIT, qui devront indiquer si ces textes peuvent être examinés en vue de leur approbation à la prochaine réunion, conformément au paragraphe 9.4 de la Résolution 1. Les États Membres sont priés de remplir le formulaire de l'**Annexe 2** et de le renvoyer d'ici au **9 février 2023** à 23 h 59 (UTC).

4 Si au moins 70% des réponses des États Membres sont en faveur de l'examen, aux fins d'approbation, de ces textes, une séance plénière sera consacrée à l'application de la procédure d'approbation. Les États Membres qui n'autorisent pas la commission d'études à procéder ainsi doivent informer le Directeur du TSB des motifs de cette décision et lui faire part des éventuelles modifications qui permettraient la poursuite des travaux.

Veuillez agréer, Madame, Monsieur, l'assurance de ma considération distinguée.

A picture containing text

Description automatically generatedChaesub Lee  
Directeur du Bureau de la normalisation   
des télécommunications

**Annexes**: 2

Annexe 1  
  
Résumé et localisation des textes déterminés des projets de nouvelles Recommandations UIT-T X.1353 (X.ztd-iot), X.1380 (X.erd-sec), X.1381 (X.eivn-sec), X.1382 (X.fstsicv), X.1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS-sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec‑ecs) et X.1816 (X.5Gsec-ssl)

# 1 Projet de nouvelle Recommandation UIT-T X.1353 (X.ztd-iot) [[R18](https://www.itu.int/md/T22-SG17-R-0018/fr)]

Méthode de sécurité applicable au déploiement sans intervention dans l'IoT massif fondé sur la chaîne de blocs

Résumé

L'Internet des objets massif (mIoT en anglais) est une application importante des futurs réseaux de communication. Compte tenu de la diversité des cas d'utilisations envisagés dans l'Internet des objets massif, les fabricants peinent à préinstaller leurs dispositifs IoT manufacturés avec des informations propres à un opérateur mobile et/ou à un service spécifique (identités et clés, par exemple), puisqu'il arrive qu'ils ne sachent pas où ceux-ci seront déployés et activés à terme. L'approche actuelle repose sur la configuration manuelle des dispositifs par les consommateurs. Si elle est acceptable pour les applications IoT à petite échelle, une telle approche ne peut convenir pour les dispositifs de l'IoT massif, étant donné son caractère chronophage, peu rentable et laborieux. La fourniture automatique de justificatifs d'identité "sans intervention", c'est-à-dire ne nécessitant aucune action de la part de l'utilisateur, s'impose donc pour l'Internet des objets massif.

Cette Recommandation définit une méthode de sécurité applicable à la conception d'un système de gestion des identités décentralisé destiné à permettre le déploiement sans intervention du futur Internet des objets massif. Le déploiement sans intervention permettra aux dispositifs IoT de trouver automatiquement leur opérateur de réseau mobile et leur fournisseur de services, d'obtenir automatiquement auprès de ces derniers leurs justificatifs d'identité et de se connecter automatiquement au réseau et au service. Cette approche facilitera grandement le futur déploiement des dispositifs de l'IoT massif pour les processus verticaux. Cette Recommandation aborde l'architecture de sécurité, les considérations liées à la sécurité et les procédures de sécurité connexes (telles que les attestations relatives aux dispositifs, l'authentification et la fourniture de justificatifs d'identité) qui sont nécessaires pour mettre en place une telle plate-forme de déploiement sans intervention de l'IoT massif.

# 2 Projet de nouvelle Recommandation X.1380 (X.edr-sec) [[R22](https://www.itu.int/md/T22-SG17-R-0022/fr)]

Lignes directrices relatives à la sécurité des enregistreurs de données fondés sur le nuage dans les environnements automobiles

Résumé

Les enregistreurs de données d'incident (EDR) sont parmi les composants les plus importants installés dans les véhicules automobiles en vue d'enregistrer l'état d'un véhicule, ses mouvements et les actions du conducteur au moment où un accident se produit. L'analyse des données d'incident permet de comprendre les causes d'un accident et d'utiliser les informations correspondantes pour améliorer la sécurité dans les environnements automobiles. Le système de stockage des données pour la conduite autonome est lui aussi un composant important permettant d'enregistrer des données qui donneront une image claire des interactions entre le conducteur et le système de conduite autonome. Or, les enregistreurs de données d'incident classiques enregistrent et gèrent toutes les données de manière locale, ce qui pourrait entraîner un risque de perte et de destruction des données.

On considère que l'informatique permet d'offrir un accès par le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service. Des secteurs tels que celui de l'aviation essaient déjà d'appliquer des services en nuage aux systèmes d'enregistrement des données d'incident afin de renforcer la sécurité dans l'environnement aéronautique. Vu l'évolution actuelle de la connectivité entre véhicules, les enregistreurs EDR et les systèmes de stockage des données pour la conduite autonome seront mis en œuvre pour améliorer la sécurité en général. Toutefois, ces enregistreurs et systèmes présentent diverses vulnérabilités s'agissant de la collecte, du transfert, du stockage, de la gestion et de l'utilisation des données enregistrées en raison des spécificités de l'environnement automobile. Par conséquent, il est nécessaire d'étudier ces vulnérabilités, les exigences de sécurité et les cas d'utilisation pour les enregistreurs de données fondés sur le nuage dans les environnements automobiles.

Cette Recommandation donne des lignes directrices relatives à la sécurité des enregistreurs de données fondés sur le nuage dans les environnements automobiles. Elle décrit les menaces, les vulnérabilités, les exigences de sécurité et les cas d'utilisation pour les enregistreurs de données fondés sur le nuage dans les environnements automobiles.

3 Projet de nouvelle Recommandation X.1381 (X.eivn-sec) [[R23](https://www.itu.int/md/T22-SG17-R-0023/fr)]

Lignes directrices relatives à la sécurité des réseaux embarqués basés sur Ethernet

Résumé

Cette Recommandation définit des lignes directrices relatives à la sécurité des réseaux embarqués (IVN) basés sur Ethernet. La tendance actuelle observée dans l'architecture électrique et électronique (E/E) consiste à intégrer l'Ethernet dans des réseaux IVN d'ancienne génération, comme le gestionnaire de réseau de communication (CAN), le réseau local d'interconnexion (LIN), le transport dans des systèmes orientés média (MOST) et FlexRay. Autrefois, l'Ethernet n'était considéré que comme un moyen de connexion entre des véhicules et des environnements extérieurs. Des protocoles types permettant des connexions selon le protocole Internet sur l'Ethernet (communication de diagnostic au travers du protocole internet ou protocole universel de mesure et de calibration, par exemple) sont utilisés pour permettre des communications entre l'environnement extérieur et les véhicules. En général, il n'est pas nécessaire que ces cas d'utilisation respectent des contraintes de temps réel rigoureuses. Cependant, les applications embarquées utilisant la communication Ethernet doivent présenter certaines caractéristiques, notamment une sensibilité temporelle et une fiabilité élevées.

Les évolutions actuelles concernant les technologies de communication embarquées nécessitent une plus grande bande passante dans le réseau. En comparaison avec l'Ethernet, les réseaux IVN d'ancienne génération sont insuffisants pour offrir la bande passante nécessaire aux applications embarquées actuelles. Par conséquent, aujourd'hui et demain, les réseaux IVN basés sur Ethernet constituent et constitueront un élément majeur de l'architecture E/E.

Cependant, les contre-mesures connues des réseaux informatiques ordinaires ne peuvent pas convenir à une application automobile, car elles n'ont pas été élaborées compte tenu des besoins et des capacités des automobiles.

Pour répondre à ce besoin, cette Recommandation définit des lignes directrices relatives à la sécurité de la technologie Ethernet automobile. Elle contient un modèle de référence de l'Ethernet automobile ainsi qu'une analyse des menaces et des vulnérabilités concernant les réseaux IVN basés sur Ethernet. En outre, cette Recommandation présente des exigences de sécurité et des cas d'utilisation des réseaux IVN basés sur Ethernet.

# 4 Projet de nouvelle Recommandation UIT-T X.1382 (X.fstsicv) [[R24](https://www.itu.int/md/T22-SG17-R-0024/fr)]

Lignes directrices relatives au partage des informations sur les menaces de sécurité pour les véhicules connectés

Résumé

Le développement rapide des véhicules connectés s'accompagne de problèmes de sécurité des réseaux de plus en plus importants. Les informations sur les menaces de sécurité des véhicules connectés, qui jouent un rôle essentiel dans la sécurisation de ces derniers, sont toutes les informations qui peuvent aider un organisme à identifier un véhicule connecté, à l'évaluer, à le surveiller et à lui répondre. Les organismes qui partagent des informations sur les menaces pour les véhicules connectés peuvent améliorer leurs propres dispositifs de sécurité et ceux d'autres organismes.

Cette Recommandation fournit des orientations concernant les principes, les règles, la méthodologie et les procédures relatifs au partage d'informations concernant la sécurité des véhicules connectés. Elle contient également une brève description des différents domaines de compétence, des rôles et de l'efficacité des divers organismes lorsqu'ils participent au cycle de vie du partage d'informations sur les menaces de sécurité.

Cette Recommandation est destinée à aider les organismes à rester en contact avec les spécialistes du partage d'informations en lien avec les véhicules connectés et à fournir des informations sur les menaces propres à appuyer les pratiques liées à la protection de la sécurité des véhicules connectés. De manière générale, elle vise à améliorer le partage d'informations sur les menaces de sécurité et à atténuer les incidences potentielles des attaques de cybersécurité sur les véhicules connectés.

Le projet de texte déterminé de cette Recommandation contient des références normatives qui nécessitent un document de justification UIT-T A.5, qui est reproduit dans le Document [SG17‑TD510](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0510/fr).

# 5 Projet de nouvelle Recommandation UIT-T X.1383 (X.srcd) [[R25](https://www.itu.int/md/T22-SG17-R-0025/fr)]

Exigences de sécurité pour les données classées dans les communications de véhicule à tout (V2X)

Résumé

La sécurité des données est l'une des considérations les plus importantes pour les communications de véhicule à tout (V2X). Or, dans un environnement à ressources limitées tel que celui des communications embarquées, la protection des données consomme beaucoup de ressources étant donné que des fonctions de chiffrement sont requises.

Cette Recommandation classe les données utilisées dans les communications V2X en plusieurs types (par exemple les données relatives à l'attribut de l'objet, à l'état du véhicule, à la perception de l'environnement, à la commande du véhicule ou aux services d'application ou encore les données personnelles de l'utilisateur) et attribue trois niveaux de sécurité pour les types de données classées. Sur la base de ces types de données classées et des niveaux de sécurité des données attribués, cette Recommandation fournit des exigences de sécurité pour les données classées dans les communications V2X.

# 6 Projet de nouvelle Recommandation X.1410 (X.sa-dsm) [[R26](https://www.itu.int/md/T22-SG17-R-0026/fr)]

Architecture de sécurité pour la gestion du partage de données reposant sur la technologie des registres distribués

Résumé

Les technologies de registres distribués (DLT) offrent des solutions novatrices, qui sont en train de transformer les différents secteurs et de modifier le mode de fonctionnement des pouvoirs publics, des institutions et des entreprises. Les caractéristiques de décentralisation et d'inviolabilité des technologies DLT leur permettent d'offrir une solution pour répliquer, partager et synchroniser les données de manière sécurisée dans un réseau informatique distribué. Les approches actuelles en matière de partage de données opérationnelles et de données contenant des informations d'identification personnelle (PII) avec des entreprises et des plates-formes numériques entraînent des vulnérabilités en matière de respect de la vie privée, découlant du piratage ou d'une mauvaise gestion des données. L'adoption de la technologie DLT ou de la chaîne de blocs pour la gestion du partage de données permet aux particuliers, ou aux entreprises, d'exercer un contrôle plus direct sur leurs propres informations confidentielles. Dans le cas d'une solution basée sur la technologie DLT, seules les données ne contenant pas d'informations PII, par exemple les valeurs de données hachées, sont stockées dans la chaîne, tandis que les données PII relatives au propriétaire des données sont stockées en dehors de la chaîne. Une solution basée sur la technologie DLT permet d'améliorer la traçabilité des données, la possibilité de vérifier les données ainsi que la possibilité de modifier leur statut.

Cette Recommandation définit une architecture de sécurité pour la gestion du partage de données reposant sur les technologies de registres distribués (DLT). Sur la base de cette architecture, cette Recommandation définit les interfaces entre les entités fonctionnelles, ainsi que les procédures applicables à la gestion du partage de données reposant sur la technologie DLT.

# 7 Projet de nouvelle Recommandation X.1411 (X.BaasS-sec) [[R20](https://www.itu.int/md/T22-SG17-R-0020/fr)]

Lignes directrices relatives à la sécurité de la chaîne de blocs en tant que service

Résumé

La chaîne de blocs en tant que service est désormais couramment utilisée dans le développement de la chaîne de blocs, en raison des capacités prometteuses qu'offre cette technologie et de l'appui massif dont elle fait l'objet dans le secteur, en particulier de la part des grands fournisseurs de services en nuage. La chaîne de blocs en tant que service offre le service et les ressources fondamentales pour les applications de la chaîne de blocs; toutefois, elle est associée à des problèmes sur le plan de la sécurité, liés aux technologies de base de la chaîne de blocs et aux plates-formes en nuage. Dans ce contexte, il est essentiel et nécessaire d'avoir des orientations concernant la sécurité de la chaîne de blocs en tant que service.

Cette Recommandation contient des lignes directrices génériques sur la sécurité de la chaîne de blocs en tant que service. En premier lieu, les menaces et les failles sur le plan de la sécurité de la chaîne de blocs en tant que service sont analysées, puis les mesures de sécurité de la chaîne de

blocs en tant que service sont indiquées. Cette Recommandation porte également sur les exigences en matière de sécurité et fournit des lignes directrices pour toutes les activités liées à la création, au fonctionnement et à l'utilisation de la chaîne de blocs en tant que service.

# 8 Projet de nouvelle Recommandation X.1454 (X.strvms) [[R19](https://www.itu.int/md/T22-SG17-R-0019/fr)]

Mesures de sécurité pour les services de bureau intelligent fondés sur la localisation

Résumé

Les services de bureau intelligent, qui combinent plusieurs applications intelligentes, visent à améliorer la qualité des activités officielles et à améliorer la gestion de l'efficacité. Les technologies de l'information et de la communication (TIC) servant de base aux technologies utilisées dans les services de bureau intelligent, l'opérateur de télécommunication joue un rôle important parmi les parties prenantes de ces services.

Les services de bureau intelligent types comprennent le stationnement intelligent, la conduite intelligente, le magasin de vente au détail intelligent, le bureau intelligent, la gestion des salles de réunion intelligentes, la gestion de l'eau intelligente, la gestion de la consommation d'énergie intelligente, etc. Parmi ces services de bureau intelligent types, les données de localisation fournies par l'opérateur constituent l'un des éléments clés de la plupart des mises en œuvre des services de bureau intelligent.

Afin de garantir la sécurité des services de bureau intelligent fondés sur la localisation, il est nécessaire d'analyser les menaces pour la sécurité et les exigences de sécurité pertinentes propres aux services fondés sur la localisation et d'établir des mesures globales en matière de sécurité.

Cette Recommandation analyse les scénarios d'application types des services de bureau intelligent fondés sur la localisation, spécifie les menaces et les exigences en matière de sécurité et établit des mesures de sécurité pour l'opérateur et les principales parties prenantes d'un bureau intelligent afin de protéger les services fondés sur la localisation.

# 9 Projet de nouvelle Recommandation X.1644 (X.sgdc) [[R21](https://www.itu.int/md/T22-SG17-R-0021/fr)]

Lignes directrices relatives à la sécurité du nuage réparti

Résumé

Cette Recommandation contient une analyse des menaces et des problèmes de sécurité concernant le nuage réparti, et vise à proposer des lignes directrices relatives à la sécurité afin de lutter contre les menaces visant le nuage réparti, y compris des lignes directrices relatives à la sécurité du nuage central, du nuage régional et du nuage en périphérie.

# 10 Projet de nouvelle Recommandation X.1815 (X.5Gsec-ecs) [[R16](https://www.itu.int/md/T22-SG17-R-0016/fr)]

Lignes directrices et exigences en matière de sécurité pour les services informatiques en périphérie fondés sur les IMT-2020

Résumé

Le réseau IMT-2020 permettra de fournir une large gamme de services, parmi lesquels les services large bande mobiles évolués (eMBB), les services fondés sur des communications massives de type machine (mMTC) et les services fondés sur des communications ultra-fiables et à faible temps de

latence (uRLLC), sur une infrastructure de réseau et de ressources informatiques. Conformément aux principales caractéristiques et aux exigences identifiées pour le réseau IMT-2020, il est exigé que ce réseau soit plus efficace, personnalisé, intelligent, fiable et souple.

Pour assurer les services types dans le réseau IMT-2020, en particulier les services eMBB et uRLLC, l'informatique en périphérie est reconnue comme étant l'une des principales technologies permettant de satisfaire les indicateurs fondamentaux de performance (IFP) particulièrement exigeants du réseau IMT-2020, surtout pour ce qui est du faible temps de latence et de l'efficacité d'utilisation de la largeur de bande.

L'informatique en périphérie permet à l'opérateur et au fournisseur de services tiers de déployer les services à proximité du point d'accès de l'utilisateur, ce qui permet de fournir des services avec une grande efficacité, grâce à la réduction du temps de latence et de la charge sur le réseau de transport.

Afin de garantir la sécurité du déploiement et de l'application des services informatiques en périphérie, il est nécessaire d'analyser les menaces pour la sécurité et les exigences de sécurité propres à ces services et d'établir un cadre général pour la sécurité.

Ce projet de Recommandation vise à analyser le modèle de déploiement et les scénarios d'application types des services informatiques en périphérie, à décrire les menaces pour la sécurité et les exigences de sécurité propres aux services informatiques en périphérie dans les réseaux IMT‑2020 et à établir en conséquence les capacités de sécurité à l'intention de l'opérateur, pour qu'il puisse protéger ses applications.

Le projet de texte déterminé de cette Recommandation contient des références normatives qui nécessitent un document de justification UIT-T A.5, qui est reproduit dans le Document [SG17‑TD605](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0605/fr)

# 11 Projet de nouvelle Recommandation UIT-T X.1816 (X.5Gsec-ssl) [[R17](https://www.itu.int/md/T22-SG17-R-0017/fr)]

Lignes directrices et exigences relatives à la classification des capacités de sécurité des tranches de réseau IMT-2020

Résumé

La définition des fonctions et processus de base liés aux technologies de découpage de réseau a établi des bases solides en vue de la première étape du déploiement des IMT-2020 et de l'utilisation commerciale des services de découpage de réseau. En tant que réseau logique de bout en bout qui est personnalisé à la demande, le découpage peut fournir des capacités de sécurité différenciées.

Premièrement, le découpage des réseaux IMT-2020 permet de prendre les mesures de sécurité nécessaires à la mise en œuvre de réseaux différenciés. Deuxièmement, les réseaux IMT-2020 permettent de prendre certaines mesures de sécurité facultatives au niveau des tranches. Certaines mesures de sécurité peuvent aussi offrir plusieurs options de sécurité et les opérateurs peuvent disposer de différentes ressources de sécurité pouvant assurer différents niveaux de garantie de la sécurité ou de qualité de fonctionnement en ce qui concerne des aspects autres que la sécurité.

Les clients de tranches ont également des exigences de sécurité particulières et peuvent demander des tranches de réseau personnalisées avec des niveaux de protection de la sécurité différents aux opérateurs de tranches. Les clients de tranches et les opérateurs de tranches doivent faire face à un certain nombre de difficultés lorsqu'ils choisissent les capacités de sécurité de leurs tranches, notamment en ce qui concerne les coûts de gestion et le manque d'homogénéité des définitions.

Cette Recommandation décrit des capacités de sécurité des tranches de réseau IMT-2020 différenciées et donne des orientations relatives à la classification de ces capacités de sécurité pour aider l'écosystème des IMT-2020 à choisir les capacités de sécurité des tranches de réseau.

Le projet de texte déterminé de cette Recommandation contient des références normatives qui nécessitent un document de justification UIT-T A.5, qui est reproduit dans le Document [SG17‑TD552](https://www.itu.int/md/T22-SG17-220823-TD-PLEN-0552/fr).

Annexe 2  
  
Objet: Réponse des États Membres à la Circulaire TSB 42:  
Consultation au sujet des textes déterminés des projets de nouvelles Recommandations UIT-T X.1353 (X.ztd-iot), X.1380 (X.erd-sec), X.1381 (X.eivn‑sec), X.1382 (X.fstsicv), X.1383 (X.srcd), X.1410 (X.sa-dsm), X.1411 (X.BaaS‑sec), X.1454 (X.sles), X.1644 (X.sgdc), X.1815 (X.5Gsec-ecs) et X.1816 (X.5Gsec-ssl)

|  |  |  |  |
| --- | --- | --- | --- |
| **Au**: | Directeur du Bureau de la normalisation des télécommunications  Union internationale des  télécommunications  Place des Nations  CH-1211 Genève 20, Suisse | **De**: | [Nom]  [Rôle/titre officiel]  [Adresse] |
| **Télécopie**: **Courriel**: | +41 22 730 5853 [tsbdir@itu.int](mailto:tsbdir@itu.int) | **Télécopie**: **Courriel**: |  |
|  |  | **Date:** | [Lieu,] [Date] |

Madame, Monsieur,

Dans le cadre de la consultation des États Membres au sujet des projets de textes déterminés dont il est question dans la Circulaire TSB 42, je souhaite vous faire connaître par la présente l'opinion de mon Administration, qui figure dans le tableau ci-après.

|  | Cochez l'une des deux cases pour chaque texte |
| --- | --- |
| Projet de nouvelle Recommandation UIT-T X.1353 (X.ztd‑iot) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |

|  |  |
| --- | --- |
| Projet de nouvelle Recommandation UIT-T X.1380 (X.edr‑sec) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1381 (X.eivn‑sec) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1382 (X.fstsicv) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1383 (X.srcd) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |

|  |  |
| --- | --- |
| Projet de nouvelle Recommandation UIT-T X.1410 (X.sa‑dsm) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1411  (X.BaaS-sec) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1454 (X.sles) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1644 (X.sgdc) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |

|  |  |
| --- | --- |
| Projet de nouvelle Recommandation UIT-T X.1815 (X.5Gsec-ecs) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |
| Projet de nouvelle Recommandation UIT-T X.1816 (X.5Gsec-ssl) | **autorise** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (dans ce cas, sélectionnez l'une des deux options ⃝):  ⃝ Pas de commentaire ou de proposition de modification  ⃝ Des commentaires ou propositions de modification sont joints à la présente |
| **n'autorise pas** la Commission d'études 17 à procéder à l'examen de ce document en vue de son approbation (les motifs de cette décision et une description des éventuelles modifications qui permettraient la poursuite des travaux sont joints à la présente) |

Veuillez agréer, Madame, Monsieur, l'assurance de ma considération distinguée.

[Nom]  
[Rôle/titre officiel]  
Administration de [État Membre]

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