|  |  |
| --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **Union internationale des télécommunications****Bureau de la Normalisation des Télécommunications** |
|  |  | Genève, le 23 avril 2024 |
| **Réf.:** | **Circulaire TSB 195**CE 17/XY | **Aux:**– Administrations des États Membres de l'Union**Copie:**– Aux Membres du Secteur de l'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;– Au Président et aux Vice-Présidents de la Commission d'études 17 de l'UIT-T;– Au Directeur du Bureau de développement des télécommunications;– Au Directeur du Bureau des radiocommunications |
| **Tél.:** | +41 22 730 6206 |
| **Télécopie:****Courriel:** | +41 22 730 5853tsbsg17@itu.int |
| **Objet:** | **Consultation des États Membres au sujet du texte déterminé des projets de nouvelles Recommandations** **UIT‑T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd‑iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec) et X.1820 (X.5Gsec-srocvs), qu'il est proposé d'approuver à la réunion de la Commission d'études 17 de l'UIT-T (Genève, 2-6 septembre 2024)** |

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 physique, qui se tiendra à Genève du 2 au 6 septembre 2024. L'ordre du jour et tous les renseignements utiles concernant la réunion de la Commission d'études 17 de l'UIT-T pourront être consultés dans la Lettre collective [8/17](https://www.itu.int/md/T22-SG17-COL-0008/fr).

2 On trouvera dans l'**Annexe 1** le titre, le résumé et la localisation des projets de Recommandation UIT-T qu'il est proposé d'approuver.

NOTE 1 DU TSB – À l'exception du projet de nouvelle Recommandation UIT-T X.1820 (X.5Gsec‑srocvs), aucune justification UIT-T A.5 n'a été soumise pour les autres 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 textes déterminés. 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 **21 août 2024** 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.

Seizo Onoe
Directeur du Bureau de la normalisation
des télécommunications

**Annexes**: 2

Annexe 1

Résumé et localisation du texte déterminé des projets de nouvelles Recommandations UIT-T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7),
X.1819 (X.5Gsec-netec) et X.1820 (X.5Gsec-srocvs)

# 1 Projet de nouvelle Recommandation UIT-T X.1237 (X.tsfpp) [[R62](https://www.itu.int/md/T22-SG17-R-0062/fr)]

Exigences de sécurité applicables à la protection des informations d'identification personnelle dans le cadre de la lutte contre le spam par messagerie mobile.

Résumé

Aujourd'hui, les contenus de spam s'infiltrent dans tous les médias pour nous parvenir à des fins commerciales (publicité). Les opérateurs, les développeurs de logiciels et les autres organisations explorent différents types de technologies, de plates-formes, de services et d'applications pour lutter contre le spam. Cependant, si la protection des informations d'identification personnelle n'est pas prise en compte dans la conception et l'exécution de ces solutions, le fonctionnement et l'efficacité de celles-ci risquent d'être compromis.

Cette Recommandation vise à prendre en compte la protection des informations d'identification personnelle (PII) dans la conception et l'exécution des solutions de lutte contre le spam par messagerie mobile. Elle donne un aperçu des processus de lutte contre le spam par messagerie mobile et propose des exigences de sécurité applicables à la lutte contre ce type de spam. Les fonctions d'entité ainsi que les procédures de traitement y sont également présentées.

# 2 Projet de nouvelle Recommandation UIT-T X.1283 (X.gpwd) [[R66](https://www.itu.int/md/T22-SG17-R-0066/fr)]

Analyse des menaces et lignes directrices pour la sécurisation des solutions d'authentification avec et sans mot de passe.

Résumé

Les professionnels de la sécurité s'efforcent de remplacer l'authentification par mot de passe par d'autres solutions dites d'authentification sans mot de passe. Malheureusement, un grand nombre de solutions sans mot de passe proposées présentent les mêmes limites que les solutions avec mot de passe utilisées actuellement. Elles sont vulnérables aux attaques par intercepteur et à l'hameçonnage, entre autres.

La Recommandation UIT-T X.1283 (X.gpwd) contient une analyse de la sécurité des solutions d'authentification reposant sur l'utilisation de secrets partagés, ainsi que des menaces qui pèsent sur ces solutions. Elle vise à examiner de manière approfondie les risques de sécurité associés aux systèmes à mots de passe et aux solutions sans mot de passe émergentes.

Cette Recommandation contient une analyse des menaces et définit des lignes directrices ainsi que des bonnes pratiques pour assurer la protection des utilisateurs et des comptes à l'aide de ces méthodes. Son contenu peut être utilisé par ceux qui adopteront cette Recommandation, afin d'appuyer les solutions existantes au moment de passer à des méthodes d'authentification plus efficaces basées sur l'infrastructure de clés publiques (PKI) (par ex. celles décrites dans les Recommandations UIT-T X.1277 et X.1278).

# 3 Projet de nouvelle Recommandation UIT-T X.1353 (X.ztd-iot) [[R63](https://www.itu.int/md/T22-SG17-R-0063/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'utilisation 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 justificatifs d'identifié décentralisé destiné à permettre le déploiement sans intervention du futur Internet des objets massif sur la base de la technologie de la chaîne de blocs. Il s'agit d'une méthode réalisable et prometteuse pour parvenir au déploiement sans intervention du futur Internet des objets massif. Le déploiement sans intervention permettra aux dispositifs IoT d'obtenir automatiquement leurs justificatifs d'identité auprès de leur opérateur de réseau mobile et de leur fournisseur de services, et ainsi 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 essentielles pour mettre en place une telle plate-forme de déploiement sans intervention de l'IoT massif.

# 4 Projet de nouvelle Recommandation UIT-T X.1354 (X.sc-iot) [[R64](https://www.itu.int/md/T22-SG17-R-0064/fr)]

Contrôles de sécurité pour les systèmes IoT.

Résumé

La Recommandation UIT-T X.1354 (X.sc-iot) contient des lignes directrices pratiques en matière de sécurité destinées à trois types d'acteurs, à savoir les fournisseurs, les concepteurs et les utilisateurs des services au sujet des systèmes de l'Internet des objets (IoT) dont le concept, les risques et les contrôles de sécurité connexes sont également décrits.

Les systèmes IoT posent des problèmes particuliers en matière de sécurité de l'information, car ils sont largement répartis et font intervenir un grand nombre d'entités diverses. De ce fait, la surface d'exposition aux attaques est très large et il est extrêmement difficile pour un système de gestion de la sécurité d'appliquer et de maintenir des contrôles de sécurité appropriés dans l'ensemble du système.

# 5 Projet de nouvelle Recommandation UIT-T X.1384 (X.itssec-5) [[R67](https://www.itu.int/md/T22-SG17-R-0067/fr)]

Exigences et lignes directrices de sécurité en matière d'informatique en périphérie pour les véhicules.

Résumé

La Recommandation UIT-T X.1384 (anciennement X.tssec-5) définit des exigences et des lignes directrices de sécurité en matière d'informatique en périphérie pour les véhicules (VEC). L'informatique en périphérie VEC est un modèle informatique déployant une capacité de traitement en périphérie du réseau afin de répartir des ressources informatiques dans un nuage central dans les environnements des systèmes de transport intelligents (ITS). De plus, cette technologie fournit des services de stockage et d'application plus localisés aux usagers des routes, ce qui permet de réduire les temps de latence, d'améliorer les temps de réponse, de détecter l'emplacement et d'offrir un niveau de disponibilité ainsi qu'une qualité de service élevés pour les applications de transmission en continu en temps réel, dans la mesure où les données sont traitées à proximité plus directe du véhicule.

L'informatique en périphérie VEC pose de nombreux défis et problèmes de sécurité, étant donné qu'elle exige un temps de réponse réduit de la part des services pour les utilisateurs finals. Cette Recommandation a pour but d'analyser les vulnérabilités identifiées de cette technologie ainsi que les menaces connexes et de définir les exigences de sécurité correspondantes. De plus, elle contient une description des cas d'utilisation pour les services reposant sur cette technologie.

# 6 Projet de nouvelle Recommandation UIT-T X.1471 (X.websec-7) [[R65](https://www.itu.int/md/T22-SG17-R-0065/fr)]

Contrôle de référence pour les services d'analyse en ligne.

Résumé

Le service d'analyse des mégadonnées est basé sur les données non structurées non définies, notamment le comportement des utilisateurs, les achats, les paiements, la localisation et la consommation de divers contenus Internet. Il peut fournir de nouvelles informations qui n'avaient pas été découvertes auparavant et prédire les états futurs. Cependant, certaines données non autorisées peuvent être utilisées de manière malveillante dans le cadre du processus d'analyse.

Cette Recommandation contient une description concernant un contrôle de référence permettant aux services d'analyse et d'exploitation des mégadonnées de détecter une utilisation non autorisée des données. Elle vise à analyser les menaces et les défis en matière de sécurité dans le domaine de l'analyse des mégadonnées, et donne une description des exigences de sécurité qui pourraient atténuer ces menaces, tout en répondant aux défis de sécurité grâce à des mécanismes de contrôle d'accès. Une méthodologie de contrôle de référence basée sur le contrôle d'accès est fournie pour déterminer quelles capacités de sécurité sont nécessaires pour atténuer les menaces de sécurité, et relever les défis de sécurité dans le cadre de l'analyse des mégadonnées.

# 7 Projet de nouvelle Recommandation UIT-T X.1819 (X.5Gsec-netec) [[R60](https://www.itu.int/md/T22-SG17-R-0060/fr)]

Capacités de sécurité de la couche réseau pour l'informatique en périphérie fondée sur les IMT‑2020/la 5G.

Résumé

L'informatique en périphérie fondée sur les réseaux IMT-2020/5G (5G EC) jouera un rôle essentiel dans les services à faible temps de latence et dans les services de délestage du trafic pour les réseaux IMT de prochaine génération. Plusieurs facteurs déterminants pourraient accroître la complexité de la couche réseau prenant en charge l'informatique en périphérie 5G EC et l'exposer à un éventail de risques plus larges, voire engendrer de nouveaux problèmes de sécurité pour le fonctionnement du réseau. Parmi ces facteurs, on peut citer les architectures de réseau souples des IMT-2020/de la 5G, les emplacements de déploiement variables de l'informatique en périphérie, les scénarios d'application divers, les différents types de réseaux privés et de réseaux d'accès utilisés par les clients, etc. Les frontières entre les réseaux de télécommunication et les réseaux privés seraient plus ambiguës et la surface d'exposition plus large. Par conséquent, il convient de préciser les exigences et les mesures de sécurité associées à la couche réseau, y compris pour les réseaux de télécommunication et les réseaux privés.

# 8 Projet de nouvelle Recommandation UIT-T X.1820 (X.5Gsec-srocvs) [[R61](https://www.itu.int/md/T22-SG17-R-0061/fr)]

Exigences de sécurité applicables à l'exploitation du réseau central IMT-2020/5G pour la prise en charge des services verticaux.

Résumé

Avec le développement du système IMT-2020/5G, les services verticaux sont devenus des scénarios essentiels pour les IMT-2020/5G. Dans les services verticaux destinés aux usines intelligentes et aux villes intelligentes qui utilisent un réseau IMT-2020/5G, de nombreux dispositifs d'utilisateur recourent à des services verticaux avec des communications massives de type machine et des communications ultra fiables à faible temps de latence (URLLC)

Pour prendre en charge les cas d'utilisation verticaux qui nécessitent des communications URLLC, certaines fonctions du réseau central IMT-2020/5G pourraient être déployées sur des sites locaux à proximité plus directe des utilisateurs des services verticaux, tandis que d'autres fonctions de réseau central IMT-2020/5G continuent d'être déployées sur un site central. Par rapport au réseau central IMT-2020/5G déployé dans son ensemble, le réseau central IMT-2020/5G fonctionnant dans ce type de scénario de déploiement peut être exposé à des menaces de sécurité particulières.

Afin de garantir la sécurité du fonctionnement du réseau central IMT-2020/5G pour prendre en charge les services verticaux, il est nécessaire d'analyser les menaces de sécurité particulières et de définir des exigences de sécurité pertinentes.

Cette Recommandation vise à analyser les menaces pour la sécurité des données et des réseaux, ainsi que les menaces pour la sécurité physique propres à l'exploitation du réseau central IMT‑2020/5G déployé à la fois sur un site central et sur des sites locaux pour prendre en charge des services verticaux, et à définir les exigences de sécurité pertinentes.

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‑[TD1739](https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1739/fr).

Annexe 2

Objet: Réponse des États Membres à la Circulaire TSB 195:
Consultation sur le texte déterminé des projets de nouvelles Recommandations UIT-T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot),
X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec)
et X.1820 (X.5Gsec-srocvs)

|  |  |  |  |
| --- | --- | --- | --- |
| **Au:** | Directeur du Bureau de la normalisation des télécommunicationsUnion internationale des télécommunicationsPlace des NationsCH-1211 Genève 20, Suisse | **De**: | [Nom][Rôle/titre officiel][Adresse] |
| **Télécopie**:**Courriel**: | +41 22 730 5853tsbdir@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 195, je souhaite vous faire connaître par la présente le point de vue 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.1237 (X.tsfpp)** | [ ]  **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 modification⃝ 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.1283 (X.gpwd)** | [ ]  **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 modification⃝ 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.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 modification⃝ 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.1354(X.sc-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 modification⃝ 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.1384 (X.itssec-5)** | [ ]  **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 modification⃝ 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.1471 (X.websec-7)** | [ ]  **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 modification⃝ 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.1819 (X.5Gsec-netec)** | [ ]  **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 modification⃝ 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.1820 (X.5Gsec-srocvs)** | [ ]  **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 modification⃝ 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]

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