|  |  |  |
| --- | --- | --- |
| itu_logo | **Union internationale des télécommunications****Bureau de la Normalisation des Télécommunications** | ITUT60_blue |
|  |  |

 Genève, le 28 novembre 2016

|  |  |  |
| --- | --- | --- |
| **Réf.:****Tél.:Fax:** | **Circulaire TSB 246**CE 17/MEU+41 22 730 5866+41 22 730 5853 | - Aux administrations des Etats Membres de l'Union |
| **E-mail:** | tsbsg17@itu.int | **Copie**:- Aux Membres du Secteur UIT-T;- Aux Associés de l'UIT-T;- Aux établissements universitaires participant aux travaux de l'UIT;- Aux Président et Vice-Présidents de la Commission d'études 17 de l'UIT‑T;- Au Directeur du Bureau de développement des télécommunications;- Au Directeur du Bureau desradiocommunications |
| **Objet:** | **Réunion de la Commission d'études 17 de l'UIT‑T, qui se tiendra à Genève du 22 au 30 mars 2017, en vue d'approuver les projets de Recommandation UIT-T X.1058 (X.gpim), X.1080.0 (X.pbact), X.1126 (X.msec-11), X.1212 (X.cogent), X.1362 (X.iotsec-1), X.1373 (X.itssec-1) et X.1550 (X.nessa), conformément aux dispositions de la Section 9 de la Résolution 1 de l'AMNT (Rév.Dubaï, 2012)** |

Madame, Monsieur,

1 A la demande du Président de la Commission d'études 17 de l'UIT‑T, *Sécurité*, j'ai l'honneur de vous informer que ladite Commission d'études, qui se réunira du 22 au 30 mars 2017, a l'intention d'appliquer la procédure décrite dans la Section 9 de la Résolution 1 de l'AMNT (Dubaï, 2012) pour l'approbation des projets de Recommandation mentionnés ci-dessus.

2 Vous trouverez dans l'**Annexe 1** le titre, le résumé et la localisation des projets de Recommandation UIT-T proposés pour approbation.

3 Tout Etat Membre, Membre de Secteur, Associé de l'UIT ou établissement universitaire participant aux travaux de l'UIT, constatant qu'un brevet, dont lui ou une autre organisation est titulaire, couvre peut-être, en totalité ou en partie, des éléments des projets de Recommandation qu'il est proposé d'approuver est invité à communiquer ces renseignements au TSB, conformément à la politique commune de l'UIT-T, l'UIT-R, l'ISO et la CEI en matière de brevets.

Les renseignements existants sur les brevets sont accessibles en ligne sur le site web de l'UIT‑T ([www.itu.int/ITU-T/ipr/](http://www.itu.int/ITU-T/ipr/)).

4 Compte tenu des dispositions de laSection 9 de la Résolution 1, je vous serais reconnaissant de bien vouloir me faire savoir au plus tard **le 13 mars 2017** à 24 heures UTC si votre Administration autorise la Commission d'études 17 de l'UIT‑T à examiner, lors de sa réunion, lesdits projets de Recommandation aux fins d'approbation.

Si des Etats Membres estiment que la procédure d'approbation ne doit pas se poursuivre, ils sont invités à faire connaître leurs raisons et à proposer les modifications susceptibles de permettre la reprise des procédures d'examen et d'approbation des projets de Recommandation.

5 Si au moins 70% des réponses des Etats Membres sont en faveur de l'examen, aux fins d'approbation, de ces projets de Recommandation lors de la réunion de la Commission d'études, une séance plénière se tiendra **le 30 mars 2017** pour appliquer la procédure d'approbation.

En conséquence, j'invite votre Administration à se faire représenter à cette réunion. **Les administrations des Etats Membres de l'Union sont invitées à communiquer le nom du Chef de leur délégation. Si votre Administration souhaite se faire représenter à cette réunion par une exploitation reconnue**, un organisme scientifique ou industriel, ou une autre entité s'occupant de questions de télécommunications, le Directeur doit en être informé, conformément à l'article 19, numéro 239, de la Convention de l'UIT.

6 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 1/17.

7 Après la réunion, le Directeur du TSB fera connaître, par voie de circulaire, la décision prise au sujet de ces Recommandations. Cette information sera également publiée dans le Bulletin d'exploitation de l'UIT.

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

Chaesub Lee
Directeur du Bureau de la normalisation
des télécommunications

**Annexe**:1

Annexe 1

**(de la Circulaire TSB 246)**

Résumé et localisation des textes

# 1 Projet de Recommandation UIT-T X.1058 (ex X.gpim) ([R 69(Rév.1](http://www.itu.int/md/T13-SG17-R-0069))

Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle

**Résumé**

Le nombre d'organisations chargées de traiter des informations d'identification personnelle (IIP) ne cesse de croître, tout comme le volume de données que ces organisations doivent gérer. Parallèlement, la société exige toujours plus de protection de ces informations et de sécurité des données personnelles. Face au nombre croissant d'atteintes sophistiquées à des données personnelles, un certain nombre de pays ont entrepris de renforcer leur législation. Cette Recommandation | Norme internationale définit un certain nombre de buts et de mesures de contrôle, et contient des directives permettant de mettre ces mesures en œuvre. Elle vise à répondre aux besoins recensés dans le cadre des évaluations de risque et d'impact effectuées dans le domaine de la protection des IIP. Certaines de ces directives, qui sont fondées sur la norme ISO/CEI 27002, tiennent notamment compte des besoins de traitement des IIP et peuvent être pertinentes au regard des risques de sécurité pesant sur les informations d'une organisation particulière.

# 2 Projet de Recommandation UIT-T X.1080.0 (ex X.pbact) ([R 75](http://www.itu.int/md/T13-SG17-R-0075))

Contrôle d'accès pour la protection des données télébiométriques

**Résumé**

La Recommandation UIT-T X.1080.0, Contrôle d'accès pour la protection des données télébiométriques, spécifie comment protéger les informations télébiométriques contre l'accès non autorisé. Pour ce faire, elle adopte un point de vue orienté services, selon lequel seules les informations nécessaires pour un but particulier sont fournies, c'est-à-dire que l'accès est accordé non seulement en fonction du droit de savoir, mais aussi en fonction du besoin de savoir. Cette Recommandation définit essentiellement une spécification d'attribut incluse dans un certificat d'attribut ou de clé publique qui spécifie en détails les privilèges dont une entité particulière dispose pour un ou plusieurs types de service. La sécurité est assurée grâce à l'utilisation d'un profil de la syntaxe de message cryptographique (CMS). Le profil CMS permet d'assurer l'authentification, l'intégrité et, si nécessaire, la confidentialité (chiffrement). Il est destiné à fournir un appui en matière de sécurité pour les spécifications télébiométriques en général. Ce profil repose sur l'hypothèse et la condition du déploiement correct d'une infrastructure de clé publique (PKI). La Recommandation UIT-T X.1080.0 dépend aussi du déploiement d'une infrastructure de gestion des privilèges (PMI).

# 3 Projet de Recommandation UIT-T X.1126 (ex X.msec-11) ([R 76](http://www.itu.int/md/T13-SG17-R-0076))

Lignes directrices relatives à l'atténuation des effets négatifs des terminaux infectés dans les réseaux mobiles

Résumé

La Recommandation UIT-T X.1126 fournit aux opérateurs mobiles des lignes directrices visant à restreindre le nombre de terminaux infectés en utilisant, dans le réseau mobile, des technologies destinées à protéger à la fois les abonnés et les opérateurs mobiles. Cette Recommandation décrit les caractéristiques et les effets des logiciels malveillants dont l'existence est rendue possible par des écosystèmes malsains dans l'environnement mobile. Fondée sur des technologies côté réseau, cette Recommandation traite essentiellement de l'atténuation des effets pervers causés par les terminaux infectés. Elle définit et organise les mesures d'atténuation ainsi que les techniques correspondantes.

# 4 Projet de Recommandation UIT-T X.1212 (ex X.cogent) ([R 71](http://www.itu.int/md/T13-SG17-R-0071))

Considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité

**Résumé**

Différents types d'attaque ont lieu au moyen de contenus reproduits à partir de ceux de fournisseurs de services de confiance, ce qui conduit des utilisateurs finals à croire à tort à la fiabilité de ces contenus. La Recommandation UIT-T X.1212 expose des considérations relatives à la conception pour l'amélioration de la perception par l'utilisateur final des indicateurs de fiabilité. Ses appendices décrivent des techniques de représentation servant à mesurer la perception par l'utilisateur final de ces indicateurs.

# 5 Projet de Recommandation UIT-T X.1362 (ex X.iotsec-1) ([R 77](http://www.itu.int/md/T13-SG17-R-0077))

Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT)

**Résumé**

L'Internet des objets (IoT) est considéré comme l'un des domaines les plus importants pour les futurs travaux de normalisation. A l'UIT-T, l'IoT est défini comme étant une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels). Dans certains environnements de l'IoT, en particulier pour les dispositifs de l'IoT, l'exigence de traitement en temps réel veut que les tâches soient traitées dans un laps de temps déterminé. Afin d'assurer la confidentialité des données et la protection de l'intégrité, l'une des mesures fondamentales est l'application d'algorithmes de chiffrement des données/d'authentification. L'application habituelle d'algorithmes de chiffrement des données/d'authentification est problématique en ce sens qu'elle ne satisfait pas l'exigence de traitement en temps réel. La Recommandation UIT-T X.1362 définit la procédure de chiffrement avec données de gabarit associées (EAMD) pour les dispositifs de l'IoT. Elle décrit la procédure EAMD et la façon dont elle assure un ensemble de services de sécurité pour le trafic qui utilise un tel chiffrement.

# 6 Projet de Recommandation UIT-T X.1373 (ex X.itssec-1) ([R 78(Rév.2](http://www.itu.int/md/T13-SG17-R-0078))

Capacité de mise à jour sécurisée des logiciels pour les dispositifs de communication des systèmes de transport intelligents

Résumé

Au fur et à mesure de l'amélioration des technologies des systèmes de transport intelligents (ITS), les communications entre un véhicule et une autre entité, par exemple les communications de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I), se généralisent et les dispositifs électriques à l'intérieur d'un véhicule, notamment les unités de commande électroniques (ECU), le système de télépéage (ETC) et le système de navigation routière, sont de plus en plus sophistiqués. Il en résulte qu'une mise à jour appropriée des modules logiciels présents dans ces dispositifs électriques est indispensable afin de corriger les bogues et d'améliorer la performance et la sécurité de manière à éviter des accidents graves. Pour répondre à ce besoin, la Recommandation UIT-T X.1373 définit des procédures de mise à jour sécurisée des logiciels entre un serveur de mise à jour de logiciels et des véhicules moyennant des contrôles de sécurité appropriés. Concrètement, les constructeurs automobiles et les entreprises s'occupant de systèmes ITS peuvent utiliser cette Recommandation comme un ensemble normalisé de bonnes pratiques.

# 7 Projet de Recommandation UIT-T X.1550 (ex X.nessa) ([R 72](http://www.itu.int/md/T13-SG17-R-0072))

Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents

Résumé

La Recommandation UIT-T X.1550 présente les approches existantes pour mettre en oeuvre les politiques de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents. Elle présente divers modèles de contrôle d'accès qui ont fait leur preuve, des modèles de partage d'informations ainsi que des critères pour évaluer les performances des réseaux d'échange d'informations sur les incidents. On considère que les solutions fondées sur les normes facilitent la mise en oeuvre de différents modèles de contrôle d'accès dans le cadre de divers modèles de partage d'informations sur la cybersécurité et dans différents environnements de confiance.

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