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

Genève, le 29 janvier 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Réf.: | **Addendum 1 à la  Lettre collective TSB 5/17** | – Aux administrations des Etats Membres de l'Union;  – 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-T | |
| Tél.: Fax: E-mail: | +41 22 730 5866 +41 22 730 5853 [tsbsg17@itu.int](mailto:tsbsg17@itu.int) |
| Objet: | **Réunion de la Commission d'études 17; Genève,** **8-17 avril 2015** | |

Madame, Monsieur,

Les deux textes à l'étude ci-après relevant de la procédure AAP ont fait l'objet d'observations pendant la période du dernier appel et seront soumis pour examen à la réunion de la Commission d'études 17 qui aura lieu à Genève du 8 au 17 avril 2015:

**1) Projet de nouvelle Recommandation UIT-T X.1341 (X.cmail)**,*Protocoles de transport de courrier certifié et de bureau de poste certifié*

**Emplacement des observations formulées pendant la période du dernier appel et du projet de texte:** [COM 17 – TD 1634 Rév.1](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1634).

**Résumé**

L'objectif de cette Recommandation est de définir le protocole de transfert de courrier certifié (CMTP) et le protocole de bureau de poste certifié (CPOP) afin d'encourager les échanges de courriers électroniques certifiés dans le monde de manière sécurisée en assurant la confidentialité, l'identification des correspondants, l'intégrité et la non-répudiation.

**2) Projet de nouvelle Recommandation UIT-T X.1157 (X.sap-7)**,*Capacités techniques de détection de fraude et de réponse pour les services exigeant un niveau de garantie élevé*

**Emplacement des observations formulées pendant la période du dernier appel et du projet de texte**: [COM 17 – TD 1638](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1638).

**Résumé**

La Recommandation UIT-T X.1157 définit les capacités nécessaires pour prendre en charge un service de détection de fraude et de réponse pour les applications des technologies de l'information et de la communication (TIC) sensibles sur le plan de la sécurité. Le service de détection de fraude et de réponse assure la détection, l'analyse et la gestion des fraudes parmi les utilisateurs, les comptes, les produits, les processus et les voies.

Il surveille et analyse les activités et les comportements des utilisateurs au niveau des applications (et non au niveau des systèmes, des bases de données ou des réseaux) et observe ce qui se passe à l'intérieur des comptes et parmi les comptes, via toute voie dont dispose les utilisateurs. Il analyse aussi les comportements entre des utilisateurs, des comptes ou d'autres entités en lien les uns avec les autres, à la recherche d'activités anormales, de corruptions ou d'utilisations abusives. Il est très couramment utilisé dans des secteurs d'activité gérant l'argent de clients, comme la finance en ligne, l'accès à distance aux entreprises, etc., mais est également couramment utilisé pour détecter des fraudes internes et d'autres types d'activités non autorisées.

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

Chaesub Lee  
Directeur du Bureau de la normalisation   
des télécommunications