|  |  |  |
| --- | --- | --- |
| itu_logo | **International telecommunication union****Telecommunication Standardization Bureau** |  |
|  | Geneva, 29 January 2015 |
| Ref: | **Addendum 1 toTSB Collective letter 5/17** | - To Administrations of Member States of the Union; - To ITU‑T Sector Members;- To ITU‑T Associates participating in the work of Study Group 17 and - To ITU‑T Academia |
| Tel: | +41 22 730 5866 |
| Fax: | +41 22 730 5853 |
| E-mail: | tsbsg17@itu.int  |  |
| Subject: | **Meeting of Study Group 17; Geneva, 8 – 17 April 2015** |

Dear Sir/Madam,

The following two work items under AAP received comments during Last Call and will be submitted for consideration at the meeting of Study Group 17 in Geneva, 8 – 17 April 2015:

1. **Draft new Recommendation ITU-T X.1341 (X.cmail),** *Certified mail transport and certified post office protocols*

**Location of the Last Call comments and draft text:** [COM 17 – TD 1634 Rev.1](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1634).

**Summary**

The objective of this Recommendation is to define the certified mail transfer protocol (CMTP) and certified post office protocol (CPOP) in order to foster the exchanges of electronic certified mails in the world in a secure way by providing confidentiality, identification of the correspondents, integrity and non-repudiation.

1. **Draft new Recommendation ITU-T X.1157 (X.sap-7),** *Technical capabilities of fraud detection and response for services with high assurance level requirements*

**Location of the Last Call comments and draft text:** [COM 17 – TD 1638](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1638).

**Summary**

Recommendation ITU-T X.1157 provides capabilities required to support fraud detection and response service in security sensitive information and communication technology (ICT) application services. Fraud detection and response services support the detection, analytics and management of fraud across users, accounts, products, processes and channels. It monitors and analyses user activity and behaviour at the application level (rather than at the system, database or network level) and watches what transpires inside and across accounts, using any channel available to a user. It also analyses behaviour among related users,

accounts or other entities, looking for abnormal activity, corruption or misuse. It is most commonly used in verticals managing customer money, such as e-finance, enterprise remote access, etc., but is equally commonly used to detect internal fraud and other types of unauthorized activities.

Yours faithfully,

ChaeSub Lee
Director of the Telecommunication
Standardization Bureau