|  |  |  |
| --- | --- | --- |
| itu-logo | **国 际 电 信 联 盟****电信标准化局** | ITUT60_blue |
|  |  |

 2016年11月28日，日内瓦

|  |  |  |
| --- | --- | --- |
| **文号：****电话：****传真：** | **电信标准化局第246号通函**SG 17/MEU+41 22 730 5866+41 22 730 5853 | – 致国际电联各成员国主管部门 |
| **电子邮件：** | tsbsg17@itu.int | **抄送：**– ITU-T部门成员；– ITU-T部门准成员；– 国际电联学术成员；– ITU-T第17研究组正副主席；– 电信发展局主任；– 无线电通信局主任 |

|  |  |
| --- | --- |
| **事由：** | **ITU-T第17研究组会议按照世界电信标准化全会（2012年，迪拜，修订版）第1号决议第9节的规定批准ITU-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)和X.1550 (X.nessa)建议书草案，2017年3月22-30日，日内瓦** |

尊敬的先生/女士：

1 应ITU-T第17研究组（安全）主席的请求，我荣幸地告知您，该研究组将于2017年3月22日至30日召开会议，并将采用世界电信标准化全会（2012年，迪拜）第1号决议第9节规定的程序来批准上述建议书草案。

2 建议批准的ITU-T建议书草案的标题、摘要及其出处见**附件1**。

3 所有了解自己或他人持有的专利可能整体或部分地涉及建议批准的建议书草案内容的国际电联成员国、部门成员、部门准成员或学术机构，均需按照ITU-T/ITU-R/国际标准化组织（ISO）/国际电工委员会（IEC）的共同专利政策，向电信标准化局披露此类信息。

可通过ITU-T网站（[www.itu.int/ipr/](http://www.itu.int/ipr/)）在网上获取已公布的专利信息。

4 考虑到第1号决议第9节的规定，请您在**2017年3月13日**协调世界时24时之前告知我，贵主管部门是否同意授权ITU-T第17研究组在该研究组会议上审议并批准上述建议书草案。

如有成员国认为不应进入审议批准程序，应阐明其反对原因并提出可能的修改意见，以推动对建议书草案的进一步审议，以便批准。

5 如果70%以上的成员国在回复中支持在该研究组会议上审议批准上述建议书草案，则将于**2017年3月30日**召开一次全体会议，实施该批准程序。

为此，我邀请贵主管部门派出一名代表参加会议。**请国际电联成员国的主管部门提供其代表团团长的姓名**。如果贵主管部门希望由一家经认可的运营机构、一个科学或工业组织或处理电信问题的另一实体作为代表参加会议，则应按照国际电联《公约》第19条第239款的规定，将有关情况适时向主任通报。

6 有关ITU-T第17研究组会议的议程和所有相关信息将在第1/17号集体函中提供。

7 会后，电信标准化局主任将以通函的形式通报就这份建议书做出的决定。此信息还将在《国际电联操作公报》中公布。

顺致敬意!

电信标准化局主任
李在摄

**附件：1件**

**附件1
（附于电信标准化局第246号通函）**

案文摘要和出处

# 1 ITU-T X.1058 (ex X.gpim)建议书草案 ([R 69 Rev.1](http://www.itu.int/md/T13-SG17-R-0069))

**信息技术 – 安全技术 – 个人识别信息保护的行为准则**

## 摘要

处理个人可识别信息（PII）组织的数量在不断增加，经这些组织处理的PII数量也有增无减。同时，对于个人可识别信息保护和个人数据安全的社会期望也在不断提高。许多国家正致力于完善其法律，加大对愈发猖獗的资料外泄事件的打击力度。本建议书|国际标准制定了控制目标、控制手段，并为实施控制制定相应指南，以期满足在对个人可识别信息（PII）保护进行风险和影响评估时出现的各项要求。特别是，本建议书|国际标准基于ISO/IEC 27002，对有关指南进行规定，考虑到了处理PII的要求，可用于应对组织信息安全面临的各项风险环境。

# 2 ITU-T X.1080.0 (ex X.pbact)建议书草案 ([R 75](http://www.itu.int/md/T13-SG17-R-0075))

**电子生物特征数据保护的访问控制**

## 摘要

ITU-T X.1080.0建议书，电子生物特征数据保护的访问控制，是一个关于如何保护电子生物特征信息免受未经授权访问的规范。它通过面向服务的观点来实现，仅提供某个特定目的所需的必要信息，例如，访问不仅建立在有权知道的基础上，而且建立在按需知道的基础上。本建议书的核心是一个属性规范，它包含在一个属性证书或公开密钥证书中，用于详细规定针对一种或多种服务类型某个特定的实体有哪些权限。安全性通过使用一个加密消息语法（CMS）概要文件来提供。CMS概要文件规定了认证、完整性，以及需要的话还有机密性（加密）。该概要文件旨在为电子生物特征通用规范提供安全支持。该概要文件假定并取决于公开密钥基础设施（PKI）的正确部署。ITU-T X.1080.0建议书也取决于权限管理基础设施（PMI）的部署。

# 3 ITU-T X.1126 (ex X.msec-11)建议书草案 ([R 76](http://www.itu.int/md/T13-SG17-R-0076))

**减缓移动网络中受感染终端负面影响的导则**

## 摘要

ITU-T X.1126建议书为移动运营商提供了采用技术手段遏制受感染终端，以保护用户和移动运营商的导则。该建议书描述了移动环境中不健康生态系统所导致的恶意软件的特性和影响。基于网络侧的技术，本建议书侧重于减缓受感染终端所引发的恶劣影响。本建议书定义并组织了缓解措施及对应的技术。

# 4 ITU-T X.1212 (ex X.cogent)建议书草案 ([R 71](http://www.itu.int/md/T13-SG17-R-0071))

**改善最终用户对可信赖指标看法的设计考虑**

## 摘要

各类攻击采用来自可信服务提供商的复制内容，从而使最终用户误信其虚假的可信性。ITU-T X.1212建议书说明了增强最终用户对可信指示符的感知的设计考虑。附录介绍了测量最终用户对这些指示符的感知的代表性技术。

# 5 ITU-T X.1362 (ex X.iotsec-1)建议书草案 ([R 77](http://www.itu.int/md/T13-SG17-R-0077))

**物联网（IoT）环境的简单加密程序**

## 摘要

人们认为，物联网（IoT）是未来最重要的标准化领域之一。从ITU-T的角度而言，IoT被定义为信息社会的全球性基础设施，通过（物理和虚拟）物体的互连促成先进业务。在某些IoT环境中，特别是IoT设备方面，存在在一定时间段内对任务进行实时处理的需求。为确保数据保密性和完整性，最基本的对策之一即是采用数据加密/认证算法。数据加密/认证算法的标准应用存在的问题是无法满足上述要求。ITU-T X.1362建议书规定物联网（IoT）设备的、带有相关掩膜数据的加密（EAMD）。本建议书具体阐明EAMD以及该加密方法如何为使用它的流量提供一系列安全业务。

# 6 ITU-T X.1373 (ex X.itssec-1)建议书草案 ([R 78 Rev.2](http://www.itu.int/md/T13-SG17-R-0078))

**智能交通系统通信设备的安全软件更新功能**

## 摘要

随着智能交通系统（ITS）技术的改善，车辆对其他实体（如其他交通工具）、车辆对车辆(V2V)以及车辆对基础设施（V2I）的通信已经很普遍。由于诸如电子控制单元（ECU），电动收费系统（ETC），系统和汽车导航系统等车辆内的电气设备变得越来越复杂，为了错误修复、性能和安全改善以避免重大事故，这些电气设备内的软件模块需要适当更新。为了实现上述要求，ITU-T X.1373建议书在软件更新服务器和有适当安全控制的车辆之间提供了安全软件更新程序。本建议书可以被车辆制造商和ITS相关的产业实际应用，作为一套最佳实践的标准化功能。

# 7 ITU-T X.1550 (ex X.nessa)建议书草案 ([R 72](http://www.itu.int/md/T13-SG17-R-0072))

**事件交换网络的接入控制模式**

## 摘要

ITU-T X.1550建议书介绍了实施事件交换网访问控制策略的现有方法。本建议书阐述了各种十分成熟的访问控制模型，分享了事件交换网性能评估的模型和标准。本文考虑到将基于标准的方案，用于在不同网络安全信息内部和在不同的信息环境下推进落实不同的访问控制模型。

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