|  |  |  |
| --- | --- | --- |
| itu_logo | **世界电信标准化全会** **（WTSA-16）2016年10月25日-11月3日，哈马马特-亚斯敏** | Title: CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| **全体会议** | **文件 20-C** |
|  | **2016年6月** |
|  | **原文：英文** |
|  |  |
| ITU-T第17研究组 |
| **安全性** |
| ITU-T第17研究组提交世界电信标准化全会（WTSA-16）的报告：第二部分 – 下个研究期（2017-2020年）的拟议课题 |

|  |  |
| --- | --- |
| **摘要：** | 此文稿包含向WTSA-16提交的ITU-T第17研究组在下个研究期（2017-2020年）的拟议课题。 |

电信标准化局的说明：

第17研究组提交2016年世界电信标准化全会（WTSA-16）的报告见以下文件：

第一部分：**19号文件** – 概述；其中包括附件2所载的对WTSA第2号决议的拟议修改

第二部分：**20号文件** – 2017-2020年研究期的拟议课题

# 1 第17研究组的拟议课题列表

|  |  |  |
| --- | --- | --- |
| 课题号 | 课题名称 | 状况 |
| A/17 | 电信/ICT安全协调 | 第1/17号课题的继续 |
| B/17 | 安全架构和框架 | 第2/17号课题的继续 |
| C/17 | 电信信息安全管理 | 第3/17号课题的继续 |
| D/17 | 网络安全 | 第4/17号课题的继续 |
| E/17 | 利用技术手段打击垃圾信息 | 第5/17号课题的继续 |
| F/17 | 电信业务和网络的安全问题 | 第6/17号课题的继续 |
| G/17 | 安全应用业务 | 第7/17号课题的继续 |
| H/17 | 云计算安全 | 第8/17号课题的继续 |
| I/17 | 远程生物识别 | 第9/17号课题的继续 |
| J/17 | 身份管理架构和机制 | 第10/17号课题的继续 |
| K/17 | 支持安全应用的通用技术（目录、公钥基础设施（PKI）、特权管理基础设施（PMI）、抽象语法记法1（ASN.1）、对象标识符（OID）） | 第11/17号课题的继续 |
| L/17 | 电信软件和测试的形式语言 | 第12/17号部分课题的继续 |

# 2 课题的措辞

第A/17号课题草案

电信/ICT安全协调

（第1/17号课题的继续）

### 1 目的

电信和信息通信技术（ICT）基础设施面临的安全威胁每日俱增且日益复杂。多年以来保护基础设施的做法一直是头痛医头、脚痛医脚，而且总是亡羊补牢，因此至今为止未能实现预期的保护目标。由于为数众多的组织研究安全问题的不同层面内容，反而使这个问题变得更加复杂，也使得协调与合作难以开展且困难重重。

由于世界上很多商业交易是通过电信链路完成的，保障使用网络基础设施的安全是确保企业的正常运行、公民的福祉及政府的有效运作必不可少的。蠕虫、病毒和其他有害代码攻击已影响到全世界数百万台计算机和电信网络。这些攻击的经济影响巨大。为防范这些威胁需要做出坚持不懈、有的放矢的努力。

安全议题涉及面广。安全可以涉及到电信信息技术的方方面面。处理安全问题的方法多种多样：

• 自下而上的方法是由专家提出安全措施，使用专门的生物识别和加密等反击措施和技术加强并保护某一领域的网络。尽管这种方式很普遍，但它是一种局部方法，往往造成安全措施不均衡地实施。

• 自上而下的方法是一种采用高屋建瓴式战略手段处理安全问题的方法。这种方法需要掌握全局。这种方法通常更加难以实施，因为比起熟悉一两个领域的专家，全面了解网络各个部分情况及其安全要求的专家更加难以寻觅。

• 自下而上与自上而下相结合的方法将各方努力协调一致。但在涉及到不同利益和议程时，这种方法往往极具挑战性。

在前一个研究期，本课题推出了很多ITU-T认为在推广其工作方面极具价值的工作成果。这些成果包括安全标准路线图、安全手册和安全工作大纲。本课题将继续着重于ITU-T所有电信安全活动的协调和组织，同时继续制定和完善相关文件以支持协调和联络活动。在与其他研究组和标准制定组织（SDO）合作时将采用自上而下的安全方法。这种做法力图在第17研究组内外将主要精力集中在项目和战略层面上。

第17研究组关于安全性的工作包括对以下决议的审议：世界电信标准化全会（WTSA）第7、11、40、50、52、58、64、65、67、70、73、75、76和78号决议；全权代表大会（PP）第101、123、130、136、174、177、178、179、181; 188、189、197、199、200和201号决议；世界电信发展大会（WTDC）第23、30、34、45、47、54、63、67、69和80号决议。

第17研究组还支持信息社会世界峰会（WSIS）的行动方面C5“树立使用ICT的信心和提高安全性”以及2014年世界电信发展大会通过的《迪拜行动计划》中关于加强安全性和树立使用ICT应用的信心的部门目标3。

自2016年3月23日开始由该课题负责拟定的技术报告：关于“电信和信息技术安全”的技术报告。

制定中的文本：关于成功使用安全标准的技术报告（X.TRsuss）。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 电信系统安全项目有哪些成果？

b) 该项目实现上述成果需要哪些程序、工作内容、工作方法和时间安排？

c) 国际电联须制定和完善哪些普及性文件（路线图、安全工作大全、技术报告、传单、网页等）？

d) 需要举办哪些安全研讨会，如何组织？

e) 为推进有关安全工作，如何与其他SDO建立有效关系？

f) 关键的里程碑和成功标准如何？

g) 如何激发部门成员和主管部门对安全工作的兴趣，如何保持后劲？

h) 如何使安全功能对市场产生更大的吸引力？

i) 如何向政府和私营部门宣传电信安全的重要性以及保护依赖于稳健而安全的电信的全球经济利益的迫切需求？

j) 国际电联其他研究组和其他SDO开展了什么安全活动？

### 3 任务

任务包括，但不局限于：

a) 作为第17研究组的主要联络人，协调电信/ICT安全事宜。

b) 完善并更新ICT安全标准路线图。

c) 完善并更新ITU-T安全工作大全。

d) 帮助电信标准化局完善安全手册并提出建议，此手册作为技术报告发布，题为“电信和信息技术的安全”。

e) 继续起草关于成功使用安全标准的技术报告。

f) 帮助确定在电信/ICT安全标准化工作中的差距并努力解决这些问题。

g) 提供电信/ICT安全标准的实施指南。

h) 推动电信/ICT安全标准制定工作组之间的合作和协调。

i) 审议建议书并与其他研究组和SDO酌情开展联络以评估安全协调的影响。

j) 在必要时提供帮助以确保有效的安全协调。

k) 帮助外部各组与ITU-T相关研究组建立直接联络。

l) 在国际电联中酌情牵头组织和规划安全研讨会和讨论会。

m) 确保有效而高效地参加与其他组织的安全协调工作。

n) 协助提高第17研究组的工作效率（例如，通过创建模板、工具或程序）。

o) 鼓励各区域发展中国家的主管部门和运营商携手合作，根据第17研究组的职责范围更好地为ITU-T第17研究组的各项活动献计献策以及实施第17研究组的安全性建议书。例如，第17研究组专门设立了非洲组来开展相关工作。

p) 协助第17研究组缩小标准化工作差距，以支持WTSA第44号决议、PP第123号决议和WTDC第47号决议。

q) 切实有效地参与SG 17内部的安全协调工作，确保SG 17的工作计划反映SG 17现有的安全活动，并解决ITU-T成员关切的问题。

### 4 关系

建议书：

• X系列和其他与电信/ICT安全相关的系列。

课题：

• ITU-T第B/17、C/17、D/17、E/17、F/17、G/17、H/17、I/17、J/17、K/17和L/17号课题。

研究组：

• ITU-D、ITU-R、ITU-T第2、5、9、11、13、15、16和20研究组；包括相关JCA和FG的TSAG。

标准化机构：

• 电信行业解决方案联盟（ATIS）；云安全联盟（CSA）；欧洲电信标准协会（ETSI）；电气和电子工程师协会（IEEE）；互联网工程任务组（IETF）；国际标准化组织/国际电工委员会第一联合技术委员会第6和27分委员会、国际标准化组织第292技术委员会、国际标准化组织技术管理局；结构化信息标准促进组织（OASIS）；第三代合作伙伴计划（3GPP）；第三合作代伙伴项目2（3GPP2）。

其他机构：

• 欧洲网络信息安全机构（ENISA）、国家标准与技术研究院（NIST）、亚洲区域性信息安全交流（RAISE）论坛。

第B/17号课题草案

安全架构和框架

（第2/17号课题的继续）

### 1 目的

X.800、X.802和X.803建议书阐述了开放系统内的安全问题。有关提供端到端通信的系统安全架构见ITU-T X.805建议书。涉及认证、接入控制、非拒绝、保密性、完整性和安全审计及告警等安全各方面的全面且详实的安全框架已经得到确立（X.810、X.811、X.812、X.813、X.814、X.815和X.816）。为提供通用高层安全（GULS），ITU-T X.830、X.831、X.832、X.833、X.834和X.835建议书已完成制定。通过与ISO/IEC JTC 1/SC 27的合作，
ITU-T X.841、X.842和X.843建议书有关安全信息对象和可信赖第三方业务的建议书也已制定完成。

为满足新兴技术（如，下一代网络（NGN）、软件定义网络（SDN）/网络功能虚拟化（NFV）的安全问题、长期演进/系统架构演进（LTE/SAE）、端到端通信系统的技术实施指南和基于互联网协议的网络）及业务的需求需要做出进一步努力以便充实并改进这些安全建议书。这些努力体现在详细阐述密码认证钥匙交流协议和政策分配与增强的X.1035和X.1036建议书中。

由于融合和移动的发展，电信运营商网络及其相关信息系统面临新的安全威胁。进攻者已进入到网络深层，不需要多少技能就可对网络产生更大的破坏。病毒、黑客和服务拒绝攻击已无处不在，对网元及其支撑系统造成不良影响。

电信和信息技术行业正在努力寻求成本高效且全面的、与技术无关的安全解决方案，从而为大量业务和应用提供保护。为能在多厂商环境中实现这些解决方案，网络安全必须在标准安全架构和标准安全技术的基础上加以设计。考虑到电信环境面临的安全威胁以及目前针对这些威胁所采取的安全措施的进步，应研究新的安全要求和解决方案。为全面落实新兴网络和服务的安全性，有必要制定新的建议书，将技术标准与安全框架结合起来。

自2016年4月29日起本课题负责的建议书和增补包括：X.800、X.802、X.803、X.805、X.810、X.811、X.812、X.813、X.814、X.815、X.816、X.830、X.831、X.832、X.833、X.834、X.835、X.841、X.842、X.843、X.1031、X.1032、X.1033、X.1034、X.1035、X.1036、X.1037、X系列增补2、增补3、增补15、增补16和增补23。

制定中的文本：X.salcm、X.sdnsec-2、X.sgmvno、X.tigsc和X.voLTEsec-1。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 如何定义全面且一致的电信安全解决方案？

b) 全面一致的电信安全解决方案的架构如何？

c) 为产生新的安全解决方案，实施安全架构的框架如何？

d) 为评估（并进而改进）现有安全解决方案，实施安全架构的框架如何？

e) 安全的架构基础是什么？

i) 端到端安全的架构是什么？

ii) 开放系统安全架构是什么？

iii) 移动环境的安全架构是什么？

iv) 演变网络的安全架构是什么？

v) 与第7/17号课题合作的应用服务的安全架构是什么？

f) 在不断变化的环境中提供安全解决方案需要哪些新的安全架构和新的框架建议书？

g) 对现有有关安全的建议书应如何组织架构标准?

h) 对现有先进的安全技术应如何组织架构标准?

i) 为适应新兴技术应如何修改安全框架建议书，需要哪些新的框架建议书？

j) 为提供安全解决方案如何实施安全业务？

k) 如何对电信/ICT基础设施进行监测用以提供安全解决方案？

### 3 任务

任务包括，但不局限于：

a) 通过与其他标准制定组织和ITU-T研究组合作，为提供电信标准安全解决方案制定全面架构和框架建议书。

b) 研究并制定有关整合了先进安全技术的可信电信网络架构的建议书。

c) 完善并改进X.800系列和X.103x系列建议书及增补。

### 4 关系

建议书：

• X系列和其他与安全相关的系列。

课题：

• ITU-T第A/17、C/17、D/17、E/17、F/17、G/17、H/17、I/17、J/17和K/17号课题。

研究组：

• ITU-D第2研究组、ITU-R WP6B、ITU-T第2、9、11、13、16和20研究组。

标准化机构：

• 电信行业解决方案联盟（ATIS）；欧洲电信标准协会（ETSI）；国际不规则网络接入论坛（FIINA）；国际标准化组织/国际电工委员会第一联合技术委员会第27和37分委员会；国际标准化组织第25技术委员会；国际标准化组织第12技术委员会；互联网工程任务组（IETF）；第三代合作伙伴计划（3GPP）、第三代合作伙伴计划2（3GPP2）。

第C/17号课题草案

电信信息安全管理

（第3/17号课题的继续）

### 1 目的

对于电信机构而言，信息和支撑程序、电信设施、网络和传输媒体是重要的电信企业资产。为使电信机构适当管理这些企业资产并开展正常企业运作，信息安全管理不可或缺。为此，为电信机构制定的ITU-T X.1051建议书阐述了有关信息安全管理的实用指南。

根据信息安全管理指南，有关治理、管理框架、风险、事件和资产的详尽管理领域亦得到开发。应研究与ITU-T X.1051建议书相关的新的领域。此外，必须完善和更新该系列建议书，反映最新的信息安全管理事宜。主要宗旨是在ITU-T X.1051建议书的基础上制定一套有关电信安全管理的建议书。

在根据ITU-T X.1051建议书制定有关详尽管理领域的建议书的同时，应关注电信/ICT的新领域，包括云计算、IPv4过渡到IPv6和个人可识别信息保护，这些迫切要求全球采取应对措施。因此，应考虑重点研究上述新领域的管理方面事宜。

在研究过程中，ITU-T应继续与ISO/IEC JTC 1开展全面合作，最大程度地确保安全解决方案的协调统一。同时，还应考虑众多国家所落实的作为国家标准的成功解决方案。

本课题不同于第2研究组的课题，因为第2研究组处理网元和管理系统之间以及TMN环境中管理系统之间的网络管理信息交换。本课题主要涉及企业资产的保护，包括信息安全管理中的信息和程序。

自2016年3月23日起本课题负责的建议书包括：E.409（与第2研究组合作）、X.1051、X.1052、X.1054、X.1055、X.1056、X.1057和X系列增补13。

制定中的文本：X.gpim、X.sgsm、X.sup-gisb和sup-gpim。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 应如何确定电信组织的具体安全管理问题？

b) 应如何为小型和中型电信组织（SMTO）实施具体的安全管理问题？

c) 应如何使用现有标准（ITU‑T和ISO/IEC等）来合理实施电信组织的信息安全管理？

d) 应如何明确并管理对电信系统中信息安全管理的衡量？

e) 应如何对云计算环境实施恰当的信息安全管理？

f) 应如何对个人可识别信息实施恰当管理？

g) 应如何在IP（包括从IPv4到IPv6的过渡）环境下实施信息安全管理？

h) 正在审议的现有建议书或正在制定的新的建议书应做出哪些改进以减少电信/ICT或其他行业对气候变化的直接或间接影响（如，节约能源、减少温室气体排放、实施监测系统等）？

### 3 任务

任务包括，但不局限于：

a) 研究并制定ITU-T X.1051建议书所述信息安全管理功能框架。

b) 根据现有标准（ITU-T和ISO/IEC等）为电信机构研究并制定实施信息安全管理的方法。

c) 为实施面向小型和中型电信组织（SMTO）的信息安全管理而研究并制定指南。

d) 研究并制定云计算环境下构建信息安全管理的指南。

e) 研究并制定IPv6环境下构建信息安全管理的指南或框架。

f) 研究并制定有关个人可识别信息保护指南的建议书。

g) 提出新的建议书大纲。

h) 从电信设施和服务的可用性角度评估上述活动的成果。

i) 生成建议书草案。

j) 完善并改进X.105x系列建议书。

### 4 关系

建议书：

• X.800系列、X.1000系列、X.1100系列、X.1200系列和X.1300系列。

课题：

• ITU-T第A/17、B/17、D/17、E/17、F/17、G/17、H/17、I/17、J/17、K/17和14/15号课题。

研究组：

• ITU-D；ITU-R；ITU-T第2、9、11、13、15和16研究组。

标准化机构：

• 云安全联盟（CSA）；欧洲电信标准协会（ETSI）； 国际标准化组织/国际电工委员会第一联合技术委员会第27分委员会；国际标准化组织第68技术委员会、国际标准化组织第215技术委员会；国家标准与技术研究院（NIST）；电信技术委员会（TTC）；第三代合作伙伴计划（3GPP）。

第D/17号课题草案

网络安全

（第4/17号课题的继续）

### 1 目的

网络安全的格局在不断变化，而相应的电信/ICT的安全要求亦由此而变。在此网络环境中，非常需要确保协议、基础设施和各种应用能作为我们日常通信的组成部分。

网络安全不仅涉及对服务、个人信息和个人可识别信息的安全和保护，还为互动实体提供信息保障（IA）。

网络攻击已成为普遍问题，为用户、服务提供商、运营商和网络带来了一系列复杂问题。利用技术手段打击网络攻击需要制定检测、保护、缓解和从网络攻击中得到恢复的框架和要求，并交换网络安全信息。

自2016年3月23日起本课题负责的建议书及其增补包括：X.1205、X.1206、X.1207、X.1208、X.1209、X.1210、X.1211、X.1303、X.1303之二、X.1500、X.1500.1、X.1520、X.1521、X.1524、X.1525、X.1526、X.1528、X.1528.1、X.1528.2、X.1528.3、X.1528.4、X.1541、X.1544、X.1546、X.1570、X.1580、X.1581、X.1582和增补X系列增补8、X系列增补9、X系列增补10、X系列增补18、X系列增补20。

制定中的文本：X.1542 (X.simef)、X.cogent、X.metric、X.nessa、X.samtn和X.sbb。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 电信/ICT提供商应如何保障基础设施的安全、维护安全运作并在电信/ICT网络中使用安全保障机制？

b) 软件、电信协议、通信系统设计人员和制造商在设计、开发和共享网络环境最佳做法中需要考虑哪些安全要求？

c) 如何有效分享薄弱环节信息以帮助完成处理薄弱环节的生命周期程序？

d) 电信/ICT为保障可组合系统的灵活性、安全性和完整性需要哪些要求和解决方案？

e) 电信/ICT数字取证、事件响应、威胁监测和风险通信需要哪些要求和解决方案？

f) 为共享网络系统（包括云计算、嵌入式和可合系统）的安全和保障信息需要何种机制？

g) 在国家紧急状态下如何安全使用网络以提供关键服务，例如使用公共告警协议？

h) 为确定、缓和及减少网络威胁（包括恶意软件、分布式拒绝服务和社会工程）的影响应采用哪些必要的安全准则和最佳做法？

i) 正在审议的现有建议书或正在制定的新建议书应做出哪些改进以减少电信/ICT或其他行业对气候变化的直接或间接影响（如，节约能源、减少温室气体排放、实施监测系统等）？

### 3 任务

任务包括，但不局限于：

a) 与ITU-T各研究组、ETSI、FIRST、IETF、IEEE、ISO/IEC JTC 1、OASIS、OMA、TCG、3GPP、3GPP2和其他有关网络安全的标准化机构开展合作。

b) 研究框架和建议书以处理电信/ICT提供商如何保障其基础设施安全并维护安全运作和交换网络安全信息的问题。

c) 为向电信/ICT数字取证、保障和事件响应提供安全解决方案制定一套建议书。

d) 为服务提供商协调和交流有关薄弱环节、平台、网络攻击等信息，研究并规范安全技术和能力。

e) 规范如何在电信/ICT网络中应用数字取证、保障和事件响应机制。

f) 制定和开发利用CYBEX技术来保护个人信息以及个人可识别信息（PII）的指南和技术。

g) 帮助ITU-T其他研究组在具体安全解决方案中应用相关网络安全建议书。

h) 为分享薄弱环节信息和补救措施制定最佳做法和指南，以帮助完成消除薄弱环节的生命周期程序。

### 4 关系

建议书：

• X系列和其他与安全相关的建议书。

课题：

• ITU-T第A/17、B/17、C/17、E/17、F/17、G/17、H/17、I/17、J/17、K/17和7/11号课题。

研究组：

• ITU-D SG2 (Q3/2)、ITU-T第2、9、11、13（7/13号课题）和16研究组。

标准化机构：

• 欧洲电信标准协会（ETSI）；电气和电子工程师协会（IEEE）；互联网工程任务组（IETF）； 国际电工委员会第57技术委员会，国际电工委员会第65技术委员会/第10工作组； 国际标准化组织/国际电工委员会第一联合技术委员会第27分委员会；国家标准与技术研究院（NIST）；结构化信息标准促进组织（OASIS）；开放移动联盟（OMA）；公开组；对象管理组织（OMG）；第三代合作伙伴计划（3GPP）；第三代合作伙伴计划2（3GPP2）；可信计算组（TCG）。

其他机构：

• 反钓鱼工作组（APWG）；计算机安全应急响应团队协调中心（CERT/CC）；国家计算机事件响应团队（CIRT）；欧洲网络与信息安全局（ENISA）； GSM协会（GSMA）；事件响应与安全团队论坛（FIRST）；国际打击网络威胁多边伙伴关系（IMPACT）；经济合作与发展组织（OECD）。

第E/17号课题草案

以技术手段打击垃圾信息

（第5/17号课题的继续）

### 1 目的

垃圾邮件已成为一个普遍的问题，造成全球互联网服务提供商、电信运营商、移动业务运营商和业务用户潜在的收入损失。此外，垃圾邮件作为网络钓鱼和传播病毒、蠕虫病毒、间谍软件和其他形式的恶意软件等的工具，产生出信息和通信网络安全问题。因此，WTSA-08第52号决议责成相关研究组继续支持，特别是支持第17研究组正在进行的关于打击垃圾邮件并加速其关于垃圾信息的工作，以便酌情在ITU-T的职责和专长范围内处理现有和未来的威胁。此外，还责成研究组继续与相关组织合作，作为紧急事项，制定技术建议书，以便通过联合讲习班、培训活动等方式交换最佳做法并传播信息，并进一步责成第17研究组定期向电信标准化顾问组汇报本决议相关工作的进展情况。

反垃圾邮件已被公认为一个全球性的问题，需要多个层面的综合措施。第17研究组作为研究通信安全和支持WTSA第52号决议活动的牵头研究组，将尽其所能地研究潜在的反垃圾邮件技术手段范围，因为这关系到电信网络的稳定性和稳健性问题。除此之外，对现有和潜在的有关通过技术手段打击垃圾邮件的建议书，已确定其技术结构便于建议书的制定。此外，还应出版新的建议书以应对新形式的垃圾邮件。

自2016年3月23日起本课题负责的建议书及其增补包括：X.1231、X.1240、X.1241、X.1242、X.1243、X.1244、X.1245、X.1246、X.1247和增补X系列增补6、X系列增补11、X系列增补12、X系列增补14和X系列增补25。

制定中的文本：X.cspim、X.gcspi、X.tfcma和X.ticsc。

### 2 课题

研究课题包括，但不局限于：

a) 如何了解和识别垃圾邮件？

b) 现有网络和未来网络垃圾邮件的新形式是什么？

c) 垃圾邮件带来的严重后果是什么？

d) 哪些技术因素在造成确定垃圾信息来源的困难方面起到了推波助澜作用？

e) 新技术、服务和应用（例如，即时消息、社交网络、移动应用、LTE话音（VoLTE）/富通信套件（RCS）等）如何给创建和传播垃圾邮件滋生机会？

f) 在IETF、3GPP、GSMA、M3AAWG以及其他论坛和私营部门实体中，目前正在开展哪些旨在解决垃圾信息问题的技术工作？

g) 需要开展哪些电信网络标准化工作，以便有效打击垃圾信息，因为这关系到电信网络的稳定性和稳健性问题？

h) 打击垃圾信息的有效且高效的解决方案是什么？

i) 如何为分享打击垃圾信息方面的资料而制定一般和具体要求？

j) 打击垃圾信息的最佳做法是什么？

### 3 任务

任务包括，但不局限于：

a) 按照第2研究组对垃圾信息的描述，牵头开展ITU-T有关以技术手段打击垃圾信息的工作。

b) 确定并审查不断变化的垃圾信息性质所带来的电信网络安全风险（网络边缘和网络核心出现的问题）。

c) 制定最新的综合性资源一览表，列出电信网络中目前正在使用或正在开发过程中的有关打击垃圾信息的现有技术措施。

d) 为打击现有和新形式垃圾信息而制定新的建议书。

e) 制定有关共享打击垃圾信息方面的资料的一般和具体要求。

f) 新的建议书或现有建议书的完善包括打击广告邮件、恶意软件和其他恶意内容以及打击已感染的网络设备（例如僵尸网络）的方法，确定这些建议书是否有助于有效打击垃圾信息，因为该项工作关系到电信网络的安全性和稳健性问题。

g) 定期向电信标准化顾问组和电信标准化局主任提供最新信息，以便将该信息纳入向理事会提交的年度报告之中。

### 4 关系

建议书：

• X系列。

课题：

• ITU-T A/17、B/17、C/17、D/17、F/17、G/17、H/17、I/17和J/17号课题。

研究组：

• ITU-D第1和2研究组；ITU-T第2、11、13和16研究组。

标准化机构：

• 国际标准化组织/国际电工委员会第一联合技术委员会；互联网工程任务组（IETF）；欧洲电信标准协会（ETSI）；第三代合作伙伴计划（3GPP）；第三代合作伙伴计划2（3GPP2）；开放移动联盟（OMA）及其他相关国家和国际标准组织。

其他机构：

• GSM协会（GSMA）；消息、恶意软件和手机反滥用工作组（M3AAWG）；事件响应与安全团队论坛（FIRST）；国家标准与技术研究院（NIST）；经济合作与发展组织（OECD）。

第F/17号课题草案

电信业务和网络的安全问题

（第6/17号课题的继续）

### 1 目的

ITU-T X.1101建议书为多播通信提供安全要求和框架。ITU-T X.1111、X.1112、X.1113和X.1114建议书描述了归属网的安全框架，包括设备凭证介绍、认证机制和授权框架。
ITU-T X.1121、X.1122、X.1123、X.1124和X.1125建议书为移动网络安全提供了全面的安全规范。ITU‑T X.1171、X.1311和X.1312建议书则相应为移动NID业务规定了隐私框架、为无处不在的感应网络（USN）规定了安全框架、为无线感应网络选路规定了USN中间件安全指南和安全要求。ITU‑T X.1191、X.1192、X.1193、X.1194、X.1195、X.1196、X.1197和X.1198建议书草案描述了用于IPTV业务安全的一组综合性要求、机制和框架。ITU‑T X系列增补19和24阐述了移动电话的安全问题。要求该课题继续努力以完善和改进这些安全方面的建议书和增补，以满足新兴的技术和业务之所需。

电信业务和网络指能使每个人以用户友好的方式随时随处使用任何设备获取任何需要的信息的业务。电信行业在基于移动技术的电信业务方面已呈指数增长。具体而言，使用无处不在的感应网络（包括物联网(IoT)、机器对机器(M2M)、智能运输系统和第5代网络）、家庭网络、使用软件定义网络（SDN）/网络功能虚拟化（NFV）的安全方面、智能电网、移动网络（包括近场通信（NFC）、嵌入式订户身份模块（SIM）和智能电话）、组播网络、IPTV网络等应用层面技术的异质设备之间的电信业务和网络各领域的安全对于行业、网络运营商和服务提供商的未来发展至关重要。

最佳全面安全解决方案的标准化对于在多厂商国际电信环境中运行的网络运营商和服务提供商而言非常重要。由于移动电信的一些具体特性（如，空中传输、小型移动设备的有限计算能量和内存），保障安全是一项特别具有挑战性的工作，需要特别关注和研究。

自2016年3月23日起本课题负责的建议书和增补包括：X.1101、X.1111、X.1112、X.1113、X.1114、X.1121、X.1122、X.1123、X.1124、X.1125、X.1171、X.1191、X.1192、X.1193、X.1194、X.1195、X.1196、X.1197、X.1198、X.1311、X.1312、X.1313、X.1314； X系列增补19、24和26。

制定中的文本：X.iotsec-1、X.iotsec-2、X.itsec-1、X.itssec-2、X.msec-9、X.msec-11、X.sdnsec-1、X.sgsec-2和X.sotavsu。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 应如何确定并定义移动电信中的电信业务和网络的安全问题？

b) 应如何确定并处理电信业务和网络面临的威胁？

c) 支持电信业务和网络需要哪些安全技术？

d) 如何保持并改进电信业务和网络之间的安全互连？

e) 新兴的电信业务和网络，特别是新兴的数字内容保护服务需要什么安全技术、机制和协议？

f) 对电信业务和网络（包括基于电信/ICT网络的智能电网和智能交通系统等业务）需采用什么全球安全解决方案？

g) 安全的电信业务和网络有哪些最佳做法或指南？

h) 正在审议的现有建议书或正在制定的新的建议书应做出哪些改进以减少电信/ICT或其他行业对气候变化的直接或间接影响（如，节约能源、减少温室气体排放、实施监测系统等）？

i) 为确保电信业务和网络的安全需要何种PII（个人身份信息）保护和管理机制？

### 3 任务

任务包括，但不局限于：

a) 与其他ITU-T研究组和标准制定组织，特别是IETF、ISO/IEC JTC 1/SC 6、25、27和31合作，制定一套旨在为安全的电信业务和网络提供全面安全解决方案的建议书。

b) 审议有关归属网、智能电网、移动网络（包括智能电话安全）、移动IoT业务和感应网络的现有ITU-T和ISO/IEC建议书/标准，以确定安全的电信业务和网络。

c) 进一步开展研究，以为国际多厂商环境中的电信业务和网络确定安全问题，同时确定新兴的业务（如：基于电信/ICT网络的智能交通系统和智能电网业务）。

d) 研究并制定有关安全的电信业务和网络中的安全问题和威胁的建议书。

e) 为安全的电信业务和网络研究和制定安全机制。

f) 为单一或多厂商电信环境内安全的电信业务和网络研究并制定互连机制。

g) 研究并确定安全的电信业务和网络中的PII保护问题和威胁。

h) 研究并开发安全的电信业务和网络中的PII保护和管理机制。

### 4 关系

建议书：

• X系列和其他有关安全的建议书。

课题：

• ITU-T第A/17、B/17、C/17、D/17、E/17、G/17、H/17、I/17、J/17、K/17、7/13、13/16和21/16号课题。

研究组：

• ITU-R；ITU-T第9、11、13、15、16和20研究组、JCA-IoT、JCA-IPTV；关于ITS的通信标准合作（CITS）。

标准化机构：

• GSM协会（GSMA）；互联网工程任务组（IETF）；国际电工委员会智慧城市系统评估组第6组（微电网）、国际电工委员会标准化管理局第3工作组、国际电工委员会第57和65技术委员会；国际标准化组织/第一联合技术委员会第6、25、27和31分委员会；国际标准化组织第204技术委员会、开放移动联盟（OMA）；第三代合作伙伴计划（3GPP）、第三代合作伙伴计划2（3GPP2）

其他机构：

• 电信行业解决方案联盟（ATIS）；中国通信标准化协会（CCSA）；欧洲电信标准协会（ETSI）（网络技术委员会、ITS技术委员会）、M2M联盟；NFC论坛；国家标准与技术研究院（NIST）；oneM2M；电信技术委员会（TTC）；电信技术协会（TTA）；通用即插即用（UPnP）。

第G/17号课题草案

安全应用业务

（第7/17号课题的继续）

### 1 目的

ITU-T X.1141、X.1142、X.1143建议书、X.1144建议书提供了一套可在网络服务消息中用于认证/授权和安全架构的建议书。ITU-T X.1151、X.1152、X.1153建议书、X.1153建议书、X.1154建议书、X.1155建议书、X.1156建议书、X.1157建议书、X.1158建议书和X.1159建议书分别为有关具有密钥交换和各种可信赖第三方（TTP）服务的、基于密码的安全认证制定了指导原则。ITU-T X.1161、X.1162、X.1163和X.1164建议书为对等（P2P）服务的安全提供了全面的框架和机制。为满足新兴技术和业务的需求，还需继续做出努力，充实并改进上述安全建议书。

电信行业在可信赖第三方（TTP）服务方面已呈指数增长。包括社交网络服务、P2P和TTP服务在内的基于电信的安全应用服务对于行业的未来发展至关重要。安全应用协议在提供安全应用服务上起着至关重要的作用。最佳全面安全解决方案的标准化对于行业、网络运行商和运行在多厂商国际环境中的服务提供商而言也是非常重要的。因此，有必要研究并开展其他类型安全应用服务，例如时戳服务、安全公证服务、安全数字金融（电子支付、电子银行、电子商务）服务、数据分析服务和恶意软件检测/响应服务，包括分析受控环境下恶意软件的行为，使用安全确定替代基于PKI协议和PKI应用服务等的证书使用。诸如安全确认和接入控制确认的安全技术在电信网络中异常重要。

自2016年3月23日起本课题负责的建议书包括：X.1141、X.1142、X.1143、X.1144、X.1151、X.1152、X.1153、X.1154、X.1155、X.1156、X.1157、X.1158、X.1159、X.X.1161、X.1162、X.1163、X.1164和X系列增补17、21和22。

制定中的文本：X.websec-6、X.websec-7和X.websec-8。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 应如何确定并处理这些安全应用服务背后的威胁？

b) 采用哪些安全技术来提供安全应用服务？

c) 应如何保留和维护应用服务之间的安全互连？

d) 对安全应用服务需要哪些安全技术或协议？

e) 对新兴安全应用服务需要哪些安全技术或协议？

f) 对安全应用服务及其应用有哪些全球安全解决方案？

### 3 任务

任务包括，但不局限于：

a) 与其他ITU-T研究组和标准制定组织，特别是与ISO/IEC JTC 1/SC 27开展合作，制定一套全面的有关为应用通信服务提供全面安全解决方案的建议书。

b) 审议ITU‑T和ISO/IEC在安全应用服务领域制定的现有建议书/标准。

c) 进一步研究以规定安全应用服务和新兴新服务的安全方面。

d) 研究和探求安全应用服务的安全和威胁事宜。

e) 研究和探求安全应用服务的安全机制。

### 4 关系

建议书：

• X.800系列和其他有关安全的建议书。

课题：

• ITU-T第A/17、B/17、C/17、D/17、E/17、F/17、H/17、I/17、J/17、K/17、7/13和13/16号课题。

研究组：

• ITU-T第2、9、11、13、16和20研究组。

标准化机构：

• 互联网工程任务组（IETF）；欧洲电信标准协会（ETSI）；GSM协会（GSMA）；国际标准化组织/国际电工委员会第一联合技术委员会第27分委员会、国际标准化组织第68技术委员会；坎塔拉倡议；结构化信息标准促进组织（OASIS）；开放移动联盟（OMA）；万维网联盟（W3C）

其他机构：

• 欧洲理事会（COE）；欧洲网络与信息安全局（ENISA）；快速身份在线（FIDO）联盟；国际打击网络威胁多边伙伴关系（IMPACT）。

第H/17号课题草案

云计算安全

（第8/17号课题的继续）

### 1 目的

云计算作为一种服务模式，可以使服务用户通过网络随时随地、便捷地按需访问可配置计算资源（包括网络、服务器、存储、应用和服务）共享池。共享池能以最少的管理或服务提供商互动迅速提供计算资源和与其断开。云计算模式具备五个基本特征（按需服务、借助宽带网络接入提供服务、资源整合、快速灵活、可计量的自主服务），分为五种云计算服务模式（分别是软件即服务（SaaS）、通信即服务（CaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）以及网络即服务（NaaS）），并拥有不同的部署模型（公共云、私有云、混合云...）。随着云计算开始成为发现、外包和组合计算资源，工作流程中服务复用以及开展各类应用和基于通信的应用的首选工具，安全需求成为新的关注重点。

云计算的预期效益包括实现灵活动态的资源配置和简化的IT基础设施自动化管理。虚拟化使共用近乎于无限的资源成为可能，同时又可以提高基础设施管理的可测量性，大幅降低基础设施的管理成本。然而，云计算的开放系统和资源共用引发了许多安全方面的顾虑，这些顾虑有可能成为最重要的云计算使用壁垒。迈向云计算意味着从安全、传统的内部IT系统过渡到危险、“云化”的开放基础设施。因此，这需要重新深入考虑安全问题。

多年来，云计算一直被视为以信息技术服务为中心，由互联网行业主体掌控。然而，电信行业在新兴的云计算市场及生态系统中也具有十分重要的作用。由于云服务借助电信网络提供，因此电信行业主体必须确保高度的服务保障等级。强劲灵活的安全保护将在整个云市场和云生态系统中发挥关键推动作用。

除此之外，灵活使用云计算环境中丰富的资源可以催生当前本地防御系统无法提供的新型安全服务（例如云服务中的反恶意软件服务）。因此，有必要对云计算在不久的将来可以提供的安全措施做出研究。

ITU-T X.1601、X.1602和X.1631建议书围绕云安全综述、架构和框架、跨层云安全和具体的网络服务安全提供了一系列有关安全服务的建议。目前，基于云计算的关键语音服务、多媒体服务、基于身份的服务、信息保障服务、身份和数据服务和应急服务方面的安全需求极为强烈。该课题计划根据云计算焦点组技术报告第5部分制定有关以下内容的新建议书：

– 关于如何保障云计算环境安全的最佳做法和指导原则；

– 云计算生态环境中主要参与者和相关角色的责任澄清、安全要求及其面临的威胁；

– 以第18/13号课题提供的参考框架为基础的安全框架；

– 安全管理和信任管理的审计技术。

第H/17号课题将与第B/17、C/17、D/17、G/17、J/17和K/17号课题等相关课题协作，共同制定有关云计算安全的建议书。

自2016年3月23日起本课题负责的建议书包括：X.1601、X.1602、X.1631和X.1642。

制定中的文本：X.1641（X.CSCDataSec）、X.dsms和X.SRIaaS。

### 2 课题

需要审议的研究项目包括，但不局限于：

a) 为了提高云计算安全，应该为服务提供商、服务用户和服务合作伙伴等主要参与者及其他关键行业利益攸关方制定哪些新的建议书或其他类型的文件？

b) 为使安全架构和安全功能结构与参考架构保持一致，应该制定哪些新的建议书？

c) 为了在不同的云计算参与者之间建立信任关系，应该围绕保障机制、审计技术和相关风险评估制定哪些新的建议书？

d) 为了最大限度的减少与其他课题、研究组和标准制定组织（SDO）的重复工作，应该开展哪些必要合作？

e) 为了保护电信/ICT系统，应该如何开发“安全即服务”的服务模式？

### 3 任务

任务包括，但不局限于：

a) 制定相应建议书或其他类型的文件以提高云计算安全。

b) 根据ITU-T第13研究组确定的云计算一般要求制定相应建议书，明确云计算服务的安全要求以及面临的威胁。

c) 根据ITU-T第13研究组确定的参考架构制定相应建议书，确定云计算的安全架构和安全功能。

d) 制定相应建议书，确定一个强大、灵活且具有较强适应性的安全架构并在云计算系统中予以实施。

e) 为了在云计算生态系统中建立信任关系，制定有关保障机制、审计技术和风险评估的建议书。

f) 负责第17研究组有关云计算安全的所有活动。

g) 在云计算联合协调活动中代表第17研究组开展与云计算安全相关的工作。

### 4 关系

建议书：

• 与云计算相关的Y系列建议书。

课题：

• ITU-T第A/17、B/17、C/17、D/17、G/17、J/17和K/17号课题。

研究组：

• ITU-T第2、13、16和20研究组。

标准化机构：

• 互联网工程任务组（IETF）；国际标准化组织/国际电工委员会第一联合技术委员会第27和38分委员会（ISO/IEC JTC 1/SC 27、SC38）；结构化信息标准促进组织（OASIS）和其他相关机构。

其他机构：

• 云安全联盟（CSA）；分布式管理任务组（DMTF）。

第I/17号课题草案

远程生物识别

（第9/17号课题的继续）

### 1 目的

在前一研究期内，第9/17号课题为在电信应用中使用生物识别奠定了基础并完成了必要的建议书。由于在电子商务和远程医疗等应用中生物识别已广泛用于身份识别，生物识别应用系统在生物安全类应用的隐私保护、可靠性和生物识别数据安全方面带来了多重挑战。当生物识别认证用于开放网络环境中时，这些挑战变得更为复杂和苛刻。

目前，使用移动终端和互联网服务的电信应用要求认证方法不仅能够提供高安全性能，同时还应方便用户。移动电话上使用网上银行，使用网络摄像头或闭路电视进行录像监控是这种新兴应用的实例，而预计生物识别认证能满足这些要求。因此，有必要规定使用这些与安全和隐私保护相关的建议书的要求。此外，要求该课题解决建议书的一致性和可互操作性测试问题，同时推广用于安全的生物识别数据库。

自2016年3月23日起本课题负责的建议书包括：X.1080.1、X.1081、X.1082、X.1083、X.1084、X.1086、X.1088、X.1089、X.1090、X.1091和X.1092。

制定中的文本：X.bhsm、X.pbact、X.tam、X.th2、X.th3、X.th4、X.th5、X.th6和X.th13。

### 2 课题

需要审议的研究项目包括，但不局限于：

a) 如何进一步改进或修订目前的建议书，以便广泛部署和使用？

b) 在NGN这样功能性强的网络中生物识别认证有何要求？

c) 应如何评定某些生物识别特定应用的安全措施？

d) 应如何开发生物识别系统和操作，以符合任何远程生物识别应用（包括云计算服务）的安全要求？

e) 如何使用远程生物识别方法的互操作模型改进用户识别和认证的安全方面？

f) 需要支持哪些机制以确保现有和将来的远程生物识别应用（如，电子卫生、远程医疗、电子商务、网上银行或视频监控）中生物识别数据的安全处理？

### 3 任务

任务包括，但不局限于：

a) 改进和修订现有有关远程生物识别认证的建议书，并推广远程生物识别数据库。

b) 审议ITU-T中现有有关远程生物识别建议书和ISO/IEC标准之间的相同之处和不同之处。

c) 使用包含第B/17号课题制定的架构和框架来研究并制定用于远程生物识别应用的安全要求和指南。

d) 研究和制定使用隐私保护技术评估用于远程生物识别应用的安全、一致性和可互操作性的要求。

e) 研究并制定用于高功能性网络中的远程生物识别的应用要求。

f) 研究并制定用于云计算和数据存储环境的远程生物识别架构的综合框架和要求。

g) 研究并制定用于信任识别框架的远程生物识别的认证要求。

h) 研究并制定提供安全性、隐私保护及同意在任何远程生物识别应用（如，电子卫生、远程医疗、电子商务、网上银行或视频监控）中“使用生物识别数据”的适当通用协议要求。

i) 研究并制定用于生物指标传输的生物到机器（B2M）协议，该协议可与机器到机器（M2M）协议互操作。

j) 研究并制定使用生物信号的远程生物识别应用，包括但不限于：认证、鉴定和卫生信息的监测。

k) 研究并制定全球（holospheric）通信协议。

### 4 关系

建议书：

• X.200、X.273、X.274、X.509、X.680、X.805和X.1051。

课题：

• ITU-T第A/17、B/17、C/17、D/17、E/17、F/17、G/17、H/17、J/17、K/17、7/13和14/15号课题。

研究组：

• ITU-D第2/2研究组；ITU-R第7研究组；ITU-T第2、5、9、11、13、15和16研究组。

标准化机构：

• 国际电工委员会第25技术委员会、国际电工委员会第25技术委员会第1联合工作组；电气和电子工程师协会（IEEE）；互联网工程任务组（IETF）；国际标准化组织/国际电工委员会第一联合技术委员会第17、27和37分委员会、国际标准化组织第12、68和215技术委员会、国际标准化组织第12技术委员会第20联合工作组。

其他机构：

• 国际计量局（BIPM）；国际辐射单位与度量委员会（ICRU）；快速身份在线（FIDO）联盟；国际劳工组织（ILO）；世界卫生组织（WHO）。

第J/17号课题草案

身份管理架构和机制

（第10/17号课题的继续）

### 1 目的

身份管理（IdM）是对证书、标识符、属性、认证、证明和实体（如，服务提供商、最终用户、社交网络、组织、网络设备、应用和服务）获得一定程度信任的形式的终生管理和使用（创建、维护、使用、提供和撤销）。根据情况的不同，一个实体在不同安全要求下及在不同地点可能采用多个身份。在云和公众网中，IdM在经授权实体之间就可信赖的信息交流进行讨论，这种信息交流则以分布系统间的身份验证和确认为基础。IdM能保护个人信息，确保只分发授权信息。IdM是电信/ICT网络（如，云计算和移动计算、服务和产品）进行正常操作的关键组成部分，因为它支持建立和维护可信赖的通信。它不仅支持对一实体身份的认证，还可以授权特权，并在实体角色变化时轻而易举地改变特权并提供下放、移动和其他重要的基于身份的服务。

IdM在管理网络安全，实现移动、按需网络接入和最终用户所期待的电子服务中发挥重要作用。除其他防御性机制外，IdM有助于防止欺诈，识别盗窃，由此增强使用者对安全而可靠的电子交易的信心（例如，不由用户机构直接控制的物联网、云计算和移动计算系统）。

国家/区域性专用IdM规范和解决方案将继续保留和发展。不同国家/区域性IdM方法、规范和解决方案的协调对于全球通信来说至关重要。为达成这一目标，IdM标准利用对制定者友好的环境，提倡使用各种各样的网络技术（即HTTP、JSON、OAUTH和OpenID连接等）大范围开发应用和工具。

本课题致力于确定ITU-T内整体IdM活动的目标设置及协调和组织。在与其他研究组和其他标准制定组织（SDO）和机构合作的过程中将使用自上而下的方法处理IdM。认识到其他课题将涉及有关IdM的具体方面（即协议、要求和网络设备标识）的研究。

自2016年3月23日起本课题负责的建议书和增补包括：X.1250、X.1251、X.1252、X.1253、X.1254、X.1255、X.1256、X.1257、X.1275和X系列增补7。

制定中的文本： X.1258 (X.eaaa)和X.te。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 通用身份管理（IdM）基础设施的功能概念如何？

b) 支持以用户为中心的参与、表示IdM信息并支持相关各方之间（例如，用户、依赖方和身份提供商）安全交流IdM信息的、独立于网络技术的适当IdM模型是什么？

c) 把社交、移动和企业IdM放到一起推动更安全数字交易所需组成部分是什么？

d) IdM模型的功能性问题是什么？

e) 服务提供商和服务消费者的具体IdM要求是什么？

f) 身份提供商在信赖框架内可共享的实体属性是什么？

g) 实现不同IdM系统（如，身份保证、互操作）之间互操作性的要求、能力和可能的战略是什么？

h) IdM互操作性有哪些被选机制以便将减少互操作问题的标识和定义概要文件包含进去？

i) 为保护和防止披露个人识别信息（PII）涉及哪些要求和机制？

j) 保护IdM系统免受网络攻击有哪些要求？

k) 哪些IdM能力可用来应对网络攻击？

l) 如何将IdM与先进的安全技术加以整合？

m) 与云计算相关的IdM有何独特要求？

n) 与移动计算相关的IdM有何独特要求？

o) 哪些独特的IdM要求与各种分布式环境（如物联网和云计算）相关？

p) 如何把身份证明整合到IdM系统？

q) 如何把安全凭证管理整合到IdM系统？

r) 如何把认证技术结合到IdM系统？

### 3 任务

任务包括，但不局限于：

a) 规定在不断变化的环境中支持IdM所需要的发现、政策和信任模型、认证和授权、确认和证书生命周期管理的IdM框架。

b) 定义IdM功能架构概念，在考虑到先进的安全技术的情况下，将网络间和IdM系统间的IdM桥接包含进去。

c) 规定身份保证的要求并提出身份保证机制建议。规定不同网络可能接受的不同身份保证方法之间的映射/互联标准。在此情况下，身份保证包括身份模式和声誉。

d) 针对IdM系统的互操作性建议相关导则。

e) 规定保护IdM系统的要求（并提出机制建议），包括如何将IdM能力作为服务提供商协调和交流有关网络攻击信息的手段。

f) 充实并协调IdM术语和定义动态清单并继续开展现有工作。

g) 研究并规定IdM安全风险和威胁。

### 4 关系

建议书：

• X和Y系列。

课题：

• ITU-T 第A/17、C/17、D/17、F/17、G/17和H/17课题。

研究组：

• ITU-D 第1、2研究组；ITU-T第2、3、11、13、16和20研究组；电信标准化顾问组

标准化组织：

• 互联网工程任务组（IETF）；欧洲电信标准协会（ETSI）；国际标准化组织/国际电工委员会第一联合技术委员会第6、27和37分委员会

其他机构：

• 国家标准与技术研究院（NIST）；结构化信息标准促进组织（OASIS）；第三代合作伙伴计划（3GPP）；第三代合作伙伴计划2（3GPP2）。

第K/17号课题草案

支持安全应用的通用技术（如目录、公钥基础设施（PKI）、
抽象语法记法1（ASN.1）、对象标识符（OID））

（第11/17号课题的继续）

### 1 目的

本课题支持继续开发广泛应用于支持安全应用的各种通用技术。这些包括：

• 目录服务（X.500系列）；

• 公共密钥基础设施（PKI – X.509）；

• 特权管理基础设施（PMI – X.509）；

• ASN.1（X.680和X.690系列）、对象标识符及其注册机构（X.660和X.670系列）；

• 快速网络服务和快速Infoset（X.890系列）；

• OSI和ODP维护。

#### 1.1 目录、PKI和PMI工作的目的

ITU-T X.500系列建议书对电信行业有重要的影响。这些建议书是当前广泛应用技术的主要部分，这些技术包括公共密钥基础设施（PKI）和轻量级目录访问协议（LDAP），用于包括金融、医疗和法律在内的诸多领域。当需要高级安全目录服务时，例如军事领域，X.500是唯一的答案。

ITU-T X.500建议书提供详尽的接入控制和数据隐私保护。它是一个开放式的规范，适应多种不同的应用。它还可扩展使未来的需求得到满足。广泛使用的LDAP是建立在ITU-T X.500目录模型上。ITU-T X.500建议书包含与LDAP的互操作能力。ITU-T X.500和LDAP目录解决方案是一个身份管理（IdM）的重要组成部分。目录供应商在进行市场营销，把目录作为身份管理系统的解决方案。通过使用目录服务能满足几个IdM和NGN的要求（例如，基于标签的应用）。

X.509是一份重要的ITU-T建议书，公钥证书被广泛使用。在每一个使用传输层安全（TLS）的安全浏览器会话中，使用证书来验证网络服务器，并同意将用于保护会话上交换信息的加密密钥。公钥证书也用于身份验证和保护电子邮件。IETF PKIX工作组、CA浏览器论坛、ETSI电子签名和基础设施（ESI）等的工作在ITU-T X.509中能找到依据。

属性证书提供了一种安全的方法，用于传输特权信息，特别是在联合身份管理系统的特权。OASIS SAML规范是基于ITU-T X.509属性证书的。当由其他主管部门而不是公钥证书签发部门来指配特权时，或当要求长期和可撤销的特权，例如组成员时，属性证书特别有用。

ITU-T X.500系列建议书需要与时俱进，以应对未来的IdM、NGN和近场通信的要求。

需要与其他研究组合作发展并完善ITU-T X.509建议书，以反映并受益于公钥基础设施（PKI）领域和特权管理基础设施（PMI）领域内取得的经验。ITU-T X.509建议书需要得到加强，以应对新的要求，如机器对机器的通信、智能电网的安全性和物联网的安全性。

自2016年3月23日起本课题负责的建议书包括：E.104（与第2研究组联合）、E.115（与第2研究组联合）、F.500、F.510、F.511、F.515、X.500、X.501、X.509、X.511、X.518、X.519、X.520、X.521、X.525和X.1341。

制定中的文本：X.pki-em（公共密钥基础设施：建立和维护）及X.pki-prof（公共密钥基础设施：配置文件）。

#### 1.2 ASN.1工作的目的、对象标识符及其登记机构

为反映技术的进步、并满足ASN.1表示法及其编码规则用户国际对象标记登记机构用户和提供商提出的更多要求，必要时将制定更多建议书。

事实证明，ASN.1是众多ITU-T标准化组的首选表示法。很多组不断请求解决上述建议书最近的增补和修正案中所遗留的含糊不清的问题。

对象标识符（OID）是一个倍受青睐的命名空间，主要基于采用整数值标记的分层注册机构的树型结构。最近扩展成为国际OID后可以采用统一码（Unicode）标签标记弧。这些扩展也是各种应用所需要的，由此可能引发进一步开发、扩展和划分的要求。

其他研究组、外部标准制定机构（SDO）和不同国家在ASN.1表示法方面，特别是OID命名空间的管理上不断需要得到建议和帮助。随着国际OID的引入且发展中国家越来越多地使用国家登记机构，预计对帮助和建议的需求将随之增加。因此，有必要继续建立ITU-T“OID项目”并指定项目负责人，以便提供此类建议和帮助。

自2016年3月23日起本课题负责的建议书包括：X.660、X.662、X.665、X.666、X.667、X.668、X.669、X.670、X.671、X.672、X.674、X.675、X.680、X.681、X.682、X.683、X.690、X.691、X.692、X.693、X.694、X.695、X.696、X.891、X.892和X.893。

制定中的文本：X.894（X.cms）、X.jsoner、X.oid-IOT（物联网对象标识符使用指南）、X.oiddev（信息技术-使用对象标识符来识别物联网设备）和X.cms（加密消息语法）。

#### 1.3 OSI维护工作的目的

基于这些OSI建议书的系统可能要在相对较长的时间内得到实施。在按照这些建议书实施系统的工作中可能会发现这些建议书的技术错误或希望改进的地方。因此，X系列OSI建议书需要得到持续不断的完善。

有关开放系统互连（OSI）的基础建议书已经完成。

自2016年3月23日起本课题负责的建议书包括：

a) OSI架构 – X.200、X.210、X.220、X.630、X.650

b) OSI消息处理 – F.400、F.401、F.410、F.415、F.420、F.421、F.423、F.435、F.440、F.471、F.472、X.200、X.207、X.210、X.211、X.212、X.213、X.214、X.215、X.216、X.217、X.217bis、X.218、X.219、X.220、X.222、X.223、X.224、X.225、X.226、X.227、X.227bis、X.228、X.229、X.233、X.234、X.235、X.236、X.237、X.237bis、X.245、X.246、X.247、X.248、X.249、X.255、X.256、X.257、X.260、X.263、X.264、X.273、X.274、X.281、X.282、X.283、X.284、X.287、X.400、X.402、X.404、X.408、X.411、X.412、X.413、X.419、X.420、X.421、X.435、X.440、X.445、X.446、X.460、X.462、X.467、X.481、X.482、X.483、X.484、X.485、X.486、X.487、X.488、X.610、X.612、X.613、X.614、X.622、X.623、X.625、X.630、X.633、X.634、X.637、X.638、X.639、X.641、X.642、X.650、X.851、X.852、X.853、X.860、X.861、X.862、X.863、X.880、X.881和X.882。

制定中的文本：无。

#### 1.4 ODP维护工作的目的

电信系统开发的关键部分是可获得支持开放分布式处理(ODP)的软件。提供ODP需要参考模型、体系结构、功能、接口和语言（ITU-T X.900系列）的标准化。

自2016年3月23日起本课题负责的建议书和增补包括：X.901、X.902、X.903、X.904、X.906、X.910、X.911、X.920、X.930、X.931、X.950、X.952和X.960。

### 2 课题

应考虑研究的内容包括，但不局限于：

#### 2.1 与目录、PKI和PMI相关工作的研究事项

与目录服务相关的事项：

a) F系列建议书需要哪些新的服务定义或修改以确定如何使用现有能力，对ITU-T X.500有哪些新的要求？

b) E系列建议书需要做出哪些改进以应对新的服务要求？

c) 目录需要哪些改进以满足新的PKI要求？

d) 目录信息中有哪些新的安全和隐私要求？

e) 为进一步改善ITU-T X.500的有效性可能要求ITU-T X.500的其他编码规则是什么，例如XML？

f) 公钥和属性证书需要哪些进一步改进以便用于各种环境，如资源有限的环境、机器对机器和大型网络？

g) 公钥和属性证书需要做出哪些进一步改进以增强其在生物识别、认证、接入控制和电子商务领域的有用性？

h) ITU-T X.509建议书需要进行哪些修改，以便明确改进的地方并修正错误？

此项工作将与ISO/IEC JTC 1/SC 6有关扩展ISO/IEC 9594的工作联合进行。维护与IETF的合作，特别是在LDAP和PKI领域的合作。

#### 2.2 与ASN.1、对象标识符和登记机构相关工作的研究事项

a) 需要对抽象语句表示法第一版（ASN.1）及其相关编码规则进行哪些改进以满足未来应用？

b) 为支持在各种环境中使用OID需要哪些辅导活动？

c) 为支持此项工作和其他课题还需要哪些其他登记机构及程序？

d) 超越现有的协议之上，需要与其他机构进行什么样的合作产生法律上或事实上的标准，以确保国际电联在有关ASN.1和OID的工作中仍然是提供协议定义并明确命名的表示法方面的领导者？

#### 2.3 与OSI维护相关工作的研究事项

a) 继续完善有关OSI架构和各层的建议书，以提供任何必要的改进并解决所报告的错误；

b) 继续完善有关OSI消息处理服务和系统、可靠传送、远程操作、CCR和交易处理的建议书，以做出任何必要的改进并解决所报告的错误。

我们迫切希望和其他研究组和其他实施OSI的国际组织开展紧密合作和联络，以确保最终建议书得到最广泛的应用。

该项工作将与国际标准化组织/国际电工委员会第一联合技术委员会及其分委员会协同开展。

#### 2.4 与ODP维护相关工作的研究事项

继续完善相关ODP建议书。

我们迫切希望和其他研究组和其他实施ODP的国际组织开展紧密合作和联络，以确保最终建议书得到最广泛的应用。

该项工作将与ISO/IEC JTC 1/SC 7/WG 19协同开展。

### 3 任务

任务包括，但不局限于：

#### 3.1 与目录、PKI和PMI相关工作的任务

a) 通过继续做出错误报告和技术勘误对目录加以完善。

b) 为支持新的和现有技术确定新的目录要求。

c) 制定第九版ITU-T X.500系列建议书。

d) 进一步充实ITU-T X.509、X.pki-prof和X.pki-em，以支持新要求。

#### 3.2 与ASN.1、对象标识符和登记机构相关工作的任务

a) 在上一研究期末，监督和公布所有手头工作的进展情况。

b) 就共同关心的领域与ISO/IEC JTC 1 SC6合作。

c) 为满足用户需求，在本研究期内对ITU-T X.660、X.670、X.680、X.690和X.890系列建议书予以更新，并酌情拟订新的版本。

d) 需要改进数据传送时，特别在低带宽的情况下，向所有涉及与ITU-T建议书（现有的或正在制定的）定义的XML模型相当的ASN.1模块提供的各研究组的其他课题提供帮助。

e) 监督和帮助已批准建议书|国际标准和技术勘误的出版进程。

f) 在研究期开始时解决所有出现的错误报告（以及在研究期内出现的任何新的错误报告），并在必要时发展技术勘误表。

g) 确保所有与ASN.1和OID工作相关的联络得到及时妥当地处理。

h) 开发任何有可能协助ASN.1或OID用户的附加教程或网页。

i) 获得ISO/IEC JTC 1/SC6与SG17达成的协议，认可任何附加的OID划分为必要的。

j) OID项目负责人的职责包括：

• 向OID用户提供一般性建议；

• 促进ASN.1和国际OID在其他研究组和外部标准制定组织（SDO）的使用；

• 帮助各国建立并维护国家OID（包括国际OID）登记机构。

#### 3.3 与OSI维护相关工作的任务

a) 按照收到文稿对OSI建议书进行必要的修正或改进以解决任何报告的错误；

b) 完善《OSI实施者指南》。

#### 3.4 与ODP维护相关工作的任务

按照收到的文稿对ODP建议书进行必要的修正或改进，以解决任何报告的错误。

### 4 关系

建议书：

• H.200系列、H.323、H.350系列、T.120、X.600-X.609系列、X.700系列、X.800-X.849系列、Z系列。

课题：

• 所有与以上建议书相关的ITU‑T课题。

研究组：

• ITU-T第2、4、11、13、16、20研究组以及使用或需要ASN.1或OID的各研究组。

标准化机构：

• 互联网工程指导小组（IESG）；互联网工程任务组（IETF）；国际电工委员会第57技术委员会；国际标准化组织/国际电工委员会第一联合技术委员会第6、7、27和31分委员会、国际标准化组织第68、204技术委员会；结构化信息标准促进组织（OASIS）；对象管理组织（OMG）；万维网联盟（W3C）。

**其他机构：**

• 万国邮政联盟（UPU）。

第L/17号课题草案

电信软件和测试的形式语言

（第12/17号课题的继续）

### 1 目的

本课题支持继续开发广泛应用于电信系统设计和测试的多种形式语言。

制定中的文本：无。

本课题涵盖了规定电信系统的需求、架构和行为的国际电联系统设计形式语言的定义和使用方面的内容，具体包括：需求语言、数据描述、行为规范、测试和实施语言。这些工程领域的形式语言广泛用于业界和ITU-T，同时拥有商业支持工具。这些语言可被综合或单独应用于标准的规范和产品的实现。相关的国际电联系统设计语言包括：

• 用户要求的表示法应用于目标的分析和用例的定义，尤其是在设计初始阶段。

• 抽象语法标记1（ASN.1）是众多信息规范标准化组的首选表示法，因为有相应的编码规则，可以确保这些信息在实体之间准确、安全和高效地传递。

• 规范和描述语言允许对指定实体的刺激和反应行为，并可与ASN.1中的数据单位规范相结合。

• 规范和描述语言的UML配置文件，此文件将UML模型限定为经良好界定的行为，以规避OMG标准中固有的语义变化以及对规范和描述语言所涵盖的行为而言并不需要的部分UML。

• 消息序列图的符号，以描述实体之间的消息序列，亦可用于跟踪系统的行为方式。

• 测试和测试控制表示法第3版（TTCN-3）允许测试系统的功能性和互操作性并加以明确，测试通用测试套件并加以书写。

TTCN-3正被用于测试相关的ITU-T研究组制定的ITU-T建议书，对第11研究组而言更是如此，该组是关于测试规范、一致性和互操作性测试的牵头小组。ITU-T正在制定多种建议书。要实现互操作性，重要的是确保建议书的实施符合标准。

• CHILL（ITU-T编程语言）在过去已得到广泛使用，但最近几年已开始使用替代方法，如从规范和描述语言生成代码。

所有这些国际电联系统设计语言均由各建议书在此课题范围内进行定义，但ASN.1（及其相关的编码规则）除外。

除定义语言外，此课题范围内的文件就语言的定义、使用和应用问题（在一定程度上亦包括ASN.1）为其他研究组、外部标准制定组织和国家给出了指导意见。ITU-T Z.110、Z.450、Z.500建议书和Z系列建议书增补1就语言的使用和应用给出了指导意见。ITU-T Z.111和Z.119建议书则就在编写建议书时应如何使用任何新的语言以及此类语言应如何作为参引纳入其他建议书（尤其是Z.100系列和Z.150系列）给出了指导意见。

自2016年3月23日起本课题负责的建议书、增补和实施者指南包括：X.292、Z.100、Z.101、Z.102、Z.103、Z.104、Z.105、Z.106、Z.107、Z.109、Z.110、Z.111、Z.119、Z.120、Z.121、Z.150、Z.151、Z.161、Z.161.1、Z.161.2、Z.161.3、Z.161.4、Z.161.5、Z.162、Z.163、Z.164、Z.165、Z.165.1、Z.166、Z.167、Z.168、Z.169、Z.170、Z.200、Z.450、Z.500、Z系列增补1和Z系列实施者指南100。

制定中的文本：无。

### 2 课题

应考虑研究的内容包括，但不局限于：

a) 为适应当前用户进一步的要求和新兴架构和框架，需要对现有国际电联系统设计语言（ASN.1除外）的定义做出哪些完善？

b) 为适应当前用户进一步的要求和新兴架构和框架（如物联网），在考虑到ITU-T Z.110建议书的情况下需要哪些新的语言？

### 3 任务

任务包括，但不局限于：

i. 按照本课题的责任继续完善相关建议书；

ii. 为本课题所涵盖的各种语言的用户提供语言、方法、框架方面的通用建议；

iii. 向其他研究组和外部标准制定机构（SDO）推广使用本课题所涵盖的方法、框架和语言。

### 4 关系

建议书：

• X.680/X.690系列。

课题：

• K/17课题、使用系统设计语言的所有ITU-T课题。

研究组：

• 第11研究组（关于测试规范、一致性和互操作性测试的牵头研究组）、使用国际电联系统设计语言的各研究组（特别是第2、11、13、16和20研究组）或规范测试的研究组（特别是第2、9、11、13、15、16和20研究组）、电信标准化顾问组。

其他ITU-T小组：

• ITU-T JCA-CIT。

标准化机构：

• 欧洲电信标准协会（ETSI）（TC MTS）；互联网工程任务组（IETF）；使用国际电联系统设计语言的国际标准化组织/国际电工委员会第一联合技术委员会及其分委员会。

其他机构：

• 对象管理组（OMG） 、SDL论坛协会。

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