|  |  |
| --- | --- |
| **世界电信标准化全会（WTSA-20）****2022年3月1-9日****，日内瓦** |  |
|  |  |
|  |  |
| **全体会议** | **文件 20 (Rev.1)-C** |
|  | **2022年2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-20）的报告：第二部分 – 提议在2022-2024年研究期研究的课题 |

|  |  |
| --- | --- |
| **摘要：** | 此文稿含有ITU-T第17研究组向2020年世界电信标准化全会（WTSA-20）提交的关于其在2017-2021年研究期内活动的报告。作为WTSA第二部分报告的惯例，修订1采用课题号与字母的对应。 |
| **联系人：** | ITU-T第17研究组主席Heung Youl Youm韩国 | 电子邮件： hyyoum@sch.ac.kr |

**电信标准化局的说明：**

第17研究组提交2020年世界电信标准化全会（WTSA-20）的报告见以下文件：

第一部分：**19号文件** – 概述

第二部分：**20号文件** – 提议在2022-2024年研究期研究的课题

1 引言

本文件载有第17研究组同意提交WTSA-20的课题案文。

表1列出了各课题及其与2021年1月11日至18日电信标准化顾问组（TSAG）会议认可的有效课题集之间的关系。

**表1 – 所提议的第17研究组课题（左）与先前课题（右）之间的关系**

| **序号** | **课题标题** | **状态** | **原序号** | **先前的课题标题** |
| --- | --- | --- | --- | --- |
| A/17 | 安全标准化策略和协调 | 继续 | 1/17 | 安全标准化策略和协调 |
| B/17 | 安全架构和网络安全 | 继续 | 2/17 | 安全架构和网络安全 |
| C/17 | 电信信息安全管理和安全服务 | 继续 | 3/17 | 电信信息安全管理和安全服务 |
| D/17 | 网络安全和打击垃圾邮件 | 继续 | 4/17 | 网络安全和打击垃圾邮件 |
| E/17 | 电信服务和物联网的安全 | 继续 | 6/17 | 电信服务和物联网的安全 |
| F/17 | 安全应用服务 | 继续 | 7/17 | 安全应用服务 |
| G/17 | 云计算和大数据基础设施安全 | 继续 | 8/17 | 云计算和大数据基础设施安全 |
| H/17 | 身份管理和远程生物识别的架构和机制 | 继续 | 10/17 | 身份管理和远程生物识别的架构和机制 |
| I/17 | 支持安全应用的通用技术（如目录、PKI、正式语言、对象标识符） | 继续 | 11/17 | 支持安全应用的通用技术（如目录、PKI、正式语言、对象标识符） |
| J/17 | 智能交通系统的安全 | 继续 | 13/17 | 智能交通系统的安全 |
| K/17 | 分布式账本技术（DLT）的安全 | 继续 | 14/17 | 分布式账本技术（DLT）的安全 |
| L/17 | 新兴技术的安全性，包括基于量子的安全性 | 继续 | 15/17 | 新兴技术的安全性，包括基于量子的安全性 |

2 课题的措辞

拟议课题案文见本文件以下部分。

第A/17号课题

安全标准化策略和协调

（第1/17号课题的继续）

### A.1 目的

电信和信息通信技术（ICT）基础设施面临的安全威胁日益复杂。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，因此至今为止未能及时实现预期的保护目标。这种攻击和威胁的经济影响巨大，给政府和实体造成了财务和机构损失。为防范这些威胁需要做出坚持不懈、有的放矢的努力。

这项工作的复杂性要求为数众多的组织在各自的专业和职责领域内研究安全问题不同层面的内容。对不同利益攸关方提出的协调与合作要求难以开展且困难重重。

安全议题涉及面广。安全可以涉及到ICT和网络技术的方方面面。处理安全问题的方法多种多样，其中包括：

– 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。

本课题推出了很多ITU-T认为是其工作与成果推广基础的交付产品，同时还为国际电联和外部组织提供了宝贵的资源。这些成果包括安全标准路线图、安全手册、安全工作大纲和成功应用安全标准的指南。课题将提出一个愿景以及第17研究组（SG17）的组织架构。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。本课题支持S第17研究组的活动，以确保这些活动能够反映及时开发高质量、市场驱动电信/ICT技术标准的有效流程。此外，这一课题通过执行关于弥合标准化差距的WTSA第44号决议，致力于满足发展中国家和区域研究组的需求。

安全标准化策略是第17研究组中所有课题中最重要的课题之一。第17研究组需要考虑安全标准化架构和设计如何能够改进当前和未来安全工作项目的开发。

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2、7、11、18、32、40、44、50、52、54、58、64、65、67、73、75、76、77、78、80、84、86、89、90、92、93、94、96、97和98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、201、204、205和206号决议；世界电信发展大会（WTDC）第30、34、43、45、47、63、67、69、79、80和84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2017年世界电信发展大会通过的《布宜诺斯艾利斯行动计划》中关于“现代化且安全的电信/ICT基础设施：推动基础设施和业务的发展，包括树立使用电信/ICT的信心并提高安全性”的部门目标2。

自2022年1月7日起由该课题负责拟定的技术报告：TR.sec-manual、TR.SUSS。

自2022年1月7日起制定中的文本：X.arch-design。

### A.2 课题

有待考虑的研究项目包括、但不限于：

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、成功标准以及辅助性绩效标准如何？

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相关性？

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？

k) 如何满足发展中国家和区域研究组在执行WTSA第44号决议方面的需求？

l) 有哪些支持全面一致电信安全解决方案的标准化战略？

m) 标准化战略应该如何涵盖现有的安全建议书？

### A.3 任务

任务包括、但不限于：

a) 作为第17研究组的主要联络人，协调电信/ICT安全事宜。

b) 制定并充实完善组织架构路线图 – 提供愿景和详细计划，以确定需要研究的安全领域的水平和范围。路线图须确定所有相关组成部分（结构、流程）及其相互关系、参与组织和各自的角色。需对新兴系统/网络和现有系统/网络加以区分。

c) 完善并更新ICT安全标准路线图。

d) 完善并更新ITU-T安全工作大全。

e) 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”。

f) 完善并更新关于成功使用安全标准的技术报告。

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、绩效指标）。

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。

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) 切实有效地参与第17研究组内部的安全协调工作，确保第17研究组的工作计划反映第17研究组现有的安全活动，并解决ITU-T成员关切的问题。

r) 与其他标准制定组织和ITU-T研究组合作，编写一套包括架构文件在内的全面的安全标准化策略文件，为安全解决方案的标准化提供支持。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### A.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施），
17（实现目标的伙伴关系）。

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2/17、3/17、4/17、6/17、7/17、8/17、10/17、11/17、13/17、14/17和15/17号课题。

研究组：

ITU-D、ITU-R、ITU-T第2、3、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）；亚太电信组织的标准化计划（ASTAP）。

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）；oneM2M；亚洲区域性信息安全交流（RAISE）论坛。

第B/17号课题

安全架构和网络安全

（第2/17号课题的继续）

### B.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、网络切片（NS）、服务功能链（SFC）、多址边缘计算（MEC）、长期演进/系统架构演进（LTE/SAE）、IMT-2020/5G网络及以后、服务/应用的共同安全框架和架构、人工智能/机器学习在支持树立使用ICT的信心和安全方面的基础，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。此外，X.1037建议书介绍了IPv6安全导则、X.1038、X.1042、X.1043和X.1044建议书提供了软件定义网络（SDN）和网络功能虚拟化（NFV）的安全要求等，X.1045建议书阐述了基于服务功能链（SFC）的定制安全服务。

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，从而为大量网络、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和优化。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、服务和应用的安全性，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2022年1月7日起由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.1011、X.1031、X.1032、X.1033、X.1034、X.1035、X.1036、X.1037、X.1038、X.1039、X.1040、X.1041、X.1042、X.1043、X.1044、X.1045、X.1046、X.1047、X.1811、X系列增补2、增补3、增补15、增补16、增补23和增补30。

自2022年1月7日起制定中的文本：X.5GSec-ecs、X.5GSec-guide、X.5Gsec-message、X.5Gsec-netec、X.5Gsec-ssl、X.5Gsec-t（X.1812）、X.5Gsec-vs、TR.zt-acp和XSTP-5Gsec-RM。

### B.2 课题

有待考虑的研究项目包括、但不限于：

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？

l) 人工智能/机器学习（AI/ML）在支持树立使用ICT的信心和提高安全性方面有哪些基础？

m) 新兴网络技术（如SDN、NFV、网络切片、SFC、MEC、LTE/SAE、IMT‑2020/5G网络等）带来了哪些新的安全威胁和挑战？

n) IMT-2020/5G网络及以后的安全需求是什么，第17研究组如何解决？

o) 新兴网络技术的常见安全机制是什么？

### B.3 任务

任务包括、但不限于：

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) 研究和编写关于人工智能/机器学习（AI/ML）基础的建议书，以树立使用ICT的信心和提高安全性。

d) 完善并改进X.800系列和X.103x系列建议书及增补。

e) 研究并编写公共网络安全建议书。

f) 研究IMT-2020/5G网络及以后的安全需求，协调第17研究组各种问题的相关工作，充当第17研究组IMT-2020/5G网络及以后安全问题的单一联系人，领导IMT‑2020/5G网络及以后安全标准的研发。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### B.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施），
11（智慧城市和社区）。

建议书：

X系列和其他与安全相关的系列。

课题：

ITU-T第1/17、3/17、4/17、6/17、7/17、8/17、10/17、11/17、13/17、14/17和15/17号课题。

研究组：

ITU-D第2研究组、ITU-R WP6B、ITU-T第2、9、11、13、15、16和JCA-IMT2020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）；GSM协会（GSMA）；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C/17号课题

电信信息安全管理和安全服务

（第3/17号课题的继续）

### C.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控制的实操法则。

根据实操法则，有关风险、资产、治理、管理框架和事件的详尽管理领域在将最佳做法作为补充的同时亦得到开发。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，应关注电信和ICT的新领域，例如网络防御中心服务，其中包括安全运营中心（SOC）服务、托管安全服务（MSS）和计算机事件响应团队（CIRT）服务、针对安全控制和有效风险管理的生命周期管理以及个人可识别信息保护管理，这些新领域迫切要求全球采取应对措施。因此，应考虑重点研究上述信息安全和网络安全新领域的管理事宜。

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，因为该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2022年1月7日起由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.1053、X.1054、X.1055、X.1056、X.1057、X.1058、X.1059、X.1060、X.1061、X系列增补13、增补27、增补32、增补34和增补36。

自2022年1月7日起制定中的文本：X.1051rev2。

### C.2 课题

有待考虑的研究项目包括、但不限于：

a) 应如何确定电信组织的具体安全管理问题？

b) 应该如何识别和电信安全管理方面的测量？

c) 应如何实现控制目标与控制对应并将其整合至电信机构的组织管理和运营？

d) 如何应用信息安全治理的概念和原则，使组织可以通过这些概念和原则来评估、指导、监控和交流组织内部开展的与信息安全相关的活动？

e) 应如何采用风险处理方案管理安全事故的影响？

f) 应如何应用为安全服务提供指导的最佳实践，如CDC服务（包括SOC服务、MSS服务和CIRT服务）？

g) 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？

h) 应该如何有效实施个人身份信息管理？

i) 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和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）？

### C.3 任务

任务包括、但不限于：

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) 研究并制定安全服务的框架/导则，如CDC服务（包括SOC服务、MSS服务和CIRT服务）。

d) 研究并制定安全控制生命周期管理导则。

e) 研究并制定有效管理风险的导则，例如用于风险处理的网络保险。

f) 研究并制定有关管理个人可识别信息的导则。

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。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### C.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施）。

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1/17、2/17、4/17、6/17、7/17、8/17、10/17、11/17、13/17、14/17、15/17和14/15号课题。

研究组：

ITU-D；ITU-R；ITU-T第2、9、11、13、15、16和20研究组。

标准化机构：

亚太电信组织标准化计划（ASTAP）；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/IEC JTC1 SC40、ISO/第68技术委员会、国际标准化组织第215技术委员会；ISO/TC 307、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）；论坛事件响应和安全团队（FIRST）。

第D/17号课题

网络安全和打击垃圾邮件

（第4/17课题的继续）

### D.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，对电信/ICT的威胁和攻击逐渐变得更加复杂、更有针对性，并给用户、服务提供商、运营商和网络带来一系列复杂的问题。这就非常需要制定网络安全框架和要求 – 编写一套建议书，在书中提供帮助相关组织管理网络安全风险的最佳做法。

遏制威胁和攻击的网络安全框架和要求由一系列操作构成，这些操作应包括识别、保护、检测、响应和恢复。通过技术手段对抗网络攻击需要遵循以下整体要求：降低风险，及早发现并对事件做出响应，同时从事件的影响中恢复过来；交流网络安全信息，如网络安全信息交换技术（CYBEX）和结构化威胁信息表达（STIX）；确保协议、基础设施和应用程序的安全，这些都是我们日常通信不可或缺的组成部分。

人工智能和机器学习在行业和应用中的采用比以往任何时候都更广泛。由人工智能和机器学习启用的技术手段，应该提高其针对威胁和攻击的技术活动的质量和效率。托管安全服务（MSS）是外包给服务提供商的服务。该服务涉及两个方面：技术方面和管理方面。

网络安全技术涉及对托管安全服务、端点检测和响应、入侵预防/检测和攻击者来源识别的技术支持，其目的是保护服务和包括个人身份信息（PII）在内的个人信息，并在交互实体之间提供信息保证（IA）。

使用网络安全信息交换框架（CYBEX）技术和网络威胁情报进行网络安全信息共享，对于保护电信/ICT基础设施和促进电信/ICT提供商的网络安全至关重要。

此外，网络威胁演变的迅猛步伐要求对技术方面进行检讨，从而为网络安全程序、技术政策和框架提供支持。鉴于网络安全需要所有利益攸关方之间开展合作，因此实现最低程度的协调充满挑战。

在网络安全挑战领域，垃圾邮件已成为一个普遍问题，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。

随着移动互联网的快速发展和ICT技术的融合，垃圾邮件威胁凭借新的特征变得更具挑战性。垃圾邮件的主要构成已从传统的广告和欺诈演变为混合型恶意软件，如勒索软件和有针对性的攻击。新一代垃圾邮件亦属不请自来，对ICT服务消费者进行骚扰，但其造成的损害比传统垃圾邮件更加严重。有针对性的攻击通常使用鱼叉式网络钓鱼（一种社会工程），通过电子邮件等合法手段获得网络访问权。勒索软件是一种恶意软件，威胁如果不向攻击者支付赎金就公布受害者数据或永久阻止其访问功能。一些恶意软件，尤其是大多数的勒索软件，可以通过恶意的电子邮件附件和被攻陷的网站传播。随着人工智能/机器学习（AI/ML）技术的演进，一些通信可由机器但非人类发起，如自动呼叫、机器人聊天、自动短信等。AI/ML算法还可以更准确地利用个人信息找到目标收件人，制作大规模的商业营销垃圾邮件甚至欺诈垃圾邮件。

随着IMT-2020、物联网等电信/ICT技术的广泛部署，垃圾邮件也逐渐开始影响工业系统。

打击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2022年1月7日起由本课题负责的建议书增补和技术报告包括：X.1205、X.1206、X.1207、X.1208、X.1209、X.1210、X.1211、X.1212、X.1213、X.1214、X.1215、X.1216、X.1217、X.1218、X.1231、X.1232、X.1233、X.1234、X.1235、X.1240、X.1241、X.1242、X.1243、X.1244、X.1245、X.1246、X.1247、X.1248、X.1249、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.1542、X.1544、X.1546、X.1550、X.1570、X.1580、X.1581、X.1582、增补X系列增补6、X系列增补8、X系列增补9、X系列增补10、X系列增补11、X系列增补12、X系列增补14、X系列增补18、X系列增补20、X系列增补25、X系列增补29和技术报告TR.usm。

自2022年1月7日起制定中的文本：X.1246Amd.1、X.1247Amd.1、X.arc-ev、X.ics-schema X.tsfpp和X.Sup-cs-ml.

### D.2 课题

在电信/ICT网络和系统方面有待考虑的研究项目包括、但不限于：

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、弱点和攻击手段，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韧性、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、受控安全服务、网络攻击属性、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）的网络安全和保障信息需要何种机制？

g) 如何利用人工智能和机器学习快速识别并分析新的威胁及漏洞？

h) 电信/ICT提供商应如何利用威胁情报加强其安全活动？

i) 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？

j) 相关组织可使用网络安全框架的哪些组成部分应对风险？

k) 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？

l) 可编写何种技术报告和建议为网络安全程序、技术政策和框架提供支持？

m) 如何了解和识别垃圾邮件？

n) 现有网络和未来网络垃圾邮件的新形式是什么？

o) 垃圾邮件带来的严重后果是什么？

p) 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？

q) 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？

r) 如何识别垃圾邮件的路线、来源和数量，从而能够应对并打击此类垃圾邮件？

s) 如何实现消息安全？

t) 如何防止恶意软件通过电子邮件传播？

u) 如何确定垃圾邮件的路线、来源和数量，并为应对和打击此类垃圾邮件估算设施和其他技术手段方面的投资金额？

v) 如何防止使用鱼叉式网络钓鱼的定向攻击？

w) 如何防止通过电子邮件分发的勒索软件？

x) 如何识别和防范垃圾邮件的AL/ML通信形式？

y) 如何采用AI/ML技术保护个人信息，避免垃圾信息传播？

z) 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？

aa) 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？

bb) 打击垃圾信息的有效且高效的解决方案是什么？

cc) 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？

dd) 打击垃圾信息的最佳做法是什么？

### D.3 任务

电信/ICT网络和系统方面要考虑的任务包括、但不限于：

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、事件响应和恢复（包括受控安全服务的技术问题）提供安全解决方案编写一套建议书。

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

e) 研究并确定网络安全框架，该框架由一系列组件构成，其中包括识别、保护、检测、响应和恢复。

f) 指定如何使用人工智能和机器学习快速识别和分析新的威胁和漏洞。

g) 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。

h) 制定和开发利用CYBEX、STIX和TAXII技术以及相关安全工具来保护个人信息以及个人可识别信息（PII）的指南和技术。

i) 研究并制定技术指南，以支持威胁管理，识别网络攻击者的来源。

j) 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。

k) 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。

l) 与其他标准制定组织合作（例如，OASIS将STIX和TAXII纳入ITU文件）。

m) 就如何应对网络安全挑战的建议书和技术报告开展工作。

n) 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。

o) 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）。

p) 确定垃圾邮件的路线、来源和数量，并为应对和打击此类垃圾邮件估算设施和其他技术手段方面的投资金额？

q) 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。

r) 为打击现有和新形式垃圾信息而制定新的建议书。

s) 开发一套支持消息安全的技术措施。

t) 为防止通过电子邮件传播的恶意软件制定新的建议书。

u) 为防止通过电子邮件使用鱼叉式网络钓鱼进行有针对性的攻击开发一套解决方案。

v) 防止通过电子邮件分发勒索软件起草新的建议书。

w) 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。

x) 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稳定性和强健性问题。

y) 开发一套解决方案或新的建议书，用于计算人工智能/机器学习沟通形式的垃圾邮件。

z) 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。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### D.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施）。

建议书：

X系列和其他与安全相关的建议书。

课题：

ITU-T第1/17、2/17、3/17、6/17、7/17、8/17、10/17、11/17、13/17、14/17和15/17号课题。

研究组：

ITU-D SG1和2；ITU-T第2、9、11、13、16和20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292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）；消息、恶意软件和移动反滥用工作组（M3AAWG）；事故响应和安全团队论坛（FIRST）；国家标准和技术研究所（NIST）；经济合作与发展组织（OECD）。

第E/17号课题

电信服务和物联网的安全

（第6/17号课题的继续）

### E.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。ITU-T X.1331、X.1332和ITU-T X.建议书增补26描述了智能电网的安全问题。ITU-T X.1361、X.1362、X.1363、X.1364和X.1365建议书规定了与物联网相关的安全要求、机制和框架。该课题应继续努力以完善和改进这些安全方面的建议书和增补，以满足新技术和业务之所需。

电信业务、网络和物联网是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所需信息的业务。电信行业在基于移动技术的电信业务方面出现了指数级的增长。具体而言，物联网和智能城市（包括机器对机器（M2M）、射频识别、近场通信（NFC）和传感器网络）、家庭网络、工业控制系统（例如智慧工厂）、智能电网、嵌入式用户识别模块（eSIM）、智能手机和IPTV网络等应用层面的技术，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。由于物联网环境的一些具体特性（例如小型移动设备有限的计算能力和存储器的大小、长生命周期、定制的操作系统和软件），提供安全和个人身份信息保护（PII）是一项特别具有挑战性的工作，需要特别关注和研究。

自2022年1月7日起由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.1126、X.1127、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.1331、X.1332、X.1333、X.1361、X.1362、X.1363、X.1364、X.1365、X.1366、X.1367、X.1368、X.1369、X.1453、X系列增补19、X系列增补24和X系列增补26。

自2022年1月7日起制定中的文本：X.iotsec-4、X.ra-iot、X.sc-iot、X.ztd-iot和TR.ibc-cd。

### E.2 课题

有待考虑的研究项目包括、但不限于：

a) 应如何确定并定义移动电信中的电信业务和物联网的安全问题？

b) 应如何确定并处理电信业务和物联网面临的威胁？

c) 支持电信业务和物联网需要哪些安全技术？

d) 如何保持并改进电信业务和物联网之间的安全互连？

e) 应该如何为电信业务和物联网研究并开发使用基于AI/ML技术的安全技术？

f) 新电信业务和物联网，特别是新数字内容保护服务需要什么安全技术、机制和协议？

g) 对电信业务和物联网（包括基于电信/ICT网络的智慧城市、智能电网和ICS（例如智慧工厂））需采用什么全球安全解决方案？

h) 安全的电信业务和物联网有哪些最佳做法或指南？

i) 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）？

j) 为确保电信业务和物联网的安全需要何种PII（个人身份信息）保护和管理机制？

### E.3 任务

任务包括、但不限于：

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、31和41合作，制定一套旨在为安全的电信业务和物联网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、智能电话安全、IoT和泛在感应网络的现有ITU-T和ISO/IEC建议书/标准，以确定安全的电信业务。

c) 进一步开展研究，以为国际多厂商环境中的电信业务和物联网确定安全问题，同时确定新业务（如基于电信/ICT网络的智慧城市、智能电网和ICS（例如智慧工厂））。

d) 研究并制定有关安全的电信业务和物联网中的安全问题和威胁的建议书。

e) 为安全的电信业务和物联网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物联网研究并制定互连机制。

g) 研究并确定安全的电信业务和物联网中的PII保护问题和威胁。

h) 研究并开发安全的电信业务和物联网中的PII保护和管理机制。

i) 为安全电信业务和物联网研究并开发安全技术。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### E.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施），
11（智慧城市和社区）。

建议书：

X系列和其他有关安全的建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、7/17、8/17、10/17、11/17、13/17、14/17和15/17号课题。

研究组：

ITU-R；ITU-T第9、11、13、15、16和20研究组、JCA-IoT和SC&C。

标准化机构：

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、31和41分委员会；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）；GSM协会（GSMA）；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F/17号课题

安全应用服务

（第7/17号课题的继续）

### F.1 目的

ITU-T X.1141、X.1142、X.1143、X.1144、X.1145、X.1146、X.1147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建议书、X.1152建议书、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）服务方面已出现指数增长。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。此外亦有必要研究并开发其他类型安全平台、应用服务，例如时戳服务、安全公证服务、安全金融技术（开放式银行、点对点贷款、汇款、移动钱包、保险）服务、安全的过顶（OTT）业务和数字对；在基于PKI的协议和PKI应用服务等方面，使用安全确认替代证书。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。

在电信和ICT开发应用服务的过程中，将面临两个需要研究的新领域：应用程序正在生成和处理越来越多的数据，如今需要人工智能为此提供支持。安全应用服务需要扩展，以涵盖广泛的研究和广阔的市场，且研究数据保护操作和技术的基础，要建立在数据分析服务的现有工作基础之上。

关于人工智能，服务提供商面临若干挑战，特别是要从开放源和行业中选择、吸纳和集成几十（如果不是几百）种人工智能组件，他们必须在各种基础架构上（现场部署、专用云、混合云、公共云）以各种形式封装这些组件（集成的人工智能应用、作为更加通用平台的人工智能、平台即服务人工智能等）。与大数据开始时一样，这带来了新的安全互操作性问题，除此之外还有确保人工智能输入培训数据和人工智能输出数据的机密性、完整性和可用性问题。所有这些都对人工智能形成了一个有待研发的新攻击面。同样，这可以建立在现有初步数据分析服务工作的基础上。

自2022年1月7日起由本课题负责的建议书包括：X.1141、X.1142、X.1143、X.1144、X.1145、X.1146、X.1147、X.1148、X.1149、X.1151、X.1152、X.1153、X.1154、X.1155、X.1156、X.1157、X.1158、X.1159、X.1161、X.1162、X.1163、X.1164、X.1450、X.1451、X.1452、X.1470和X系列增补17、X系列增补21和X系列增补22。

自2022年1月7日起制定中的文本：X.1144rev、X.guide-cdd、X.rdda、X.saf-dfs、X.scpa、X.sec-grp-mov、X.sg-dtn、X.sles、X.smdtsc、X.smsrc、X.vide、X.websec-7和TR.cta。

### F.2 课题

有待考虑的研究项目包括、但不限于：

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) 对服务平台、金融技术服务和OTT服务等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？

g) 如何为应用服务定义运营和技术数据保护策略？

h) 如何定义保护人工智能攻击面的策略？

### F.3 任务

任务包括、但不限于：

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金融技术服务和OTT服务等新兴新服务的安全问题。

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。

f) 研究并制定应用服务数据保护操作和技术方面的策略和建议书。

g) 为保护人工智能攻击面开展研究并制定策略和建议书。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### F.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施），
11（智慧城市和社区）。

建议书：

X.800系列和其他有关安全的建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、6/17、8/17、、10/17、11/17、14/17、15/17、7/13和13/17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/国际电工委员会第一联合技术委员会第42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307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G/17号课题

云计算和大数据基础设施安全

（第8/17号课题的继续）

### G.1 目的

云计算作为一种模式，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、专用云、混合云...）和业务交付类型的灵活拓展（核心、区域、边缘）。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。边缘计算的引入使得云能力能够分布到网络的边缘。这引入了具有低确定性延迟和高可靠性的云服务。然而，云计算的开放系统、资源共用以及云与边缘内在的互操作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。特别是在边缘计算提供更多本地云资源分布时，会导致云边缘、区域和核心实现之间的关系更加复杂。

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）。

我们认为大数据是用于处理大量数据的技术、工具集、数据和分析。此外，随着数据呈指数级增长并成为电信/ICT网络的重要资产，通过在云计算的支持下对大量数据集进行分析，将揭示原本不为人知的模式和关系。大数据的数据收集、存储、分析、管理及可视化等核心流程是在云计算的基础上实现的，如果没有云计算，就无法使用传统技术（如大数据即服务）对大数据进行快速传输和分析。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8/17号课题将与第2/17、3/17、4/17、7/17、10/17和11/17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2022年1月7日起由本课题负责的建议书和技术报告包括：X.1601、X.1602、X.1603、X.1604、X.1605、X.1606、X.1631、X.1641、X.1642、X.1643、X.1750、X.1751、X.1752和技术报告TR.XAASL。

自2022年1月7日起制定中的文本：X.BaaS-sec、X.gecds、X.nssa-cc、[X.sa-ec](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16951" \o "See more details)、X.sgcnp、X.sgdc、X.sgmc和X.sr-cphr。

### G.2 课题

有待考虑的研究项目包括、但不限于：

a) 为了提包括高云计算安全、边缘计算安全、互通安全等在内的整个云计算生态系统的安全，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) 对于大数据平台和基础架构安全的安全解决方案、最佳实践或导则，应该编写哪些新的建议书？

e) 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？

f) 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？

### G.3 任务

任务包括、但不限于：

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) 依据ITU-T第13研究组规定的参考架构，研究并制定有关大数据平台和基础设施安全建议书。

g) 负责第17研究组有关云计算安全、大数据平台和基础设施安全的所有活动。

h) 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。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### G.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），
9（工业、创新和基础设施），
11（智慧城市和社区）。

建议书：

与云计算相关的Y系列建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、7/17、10/17、11/17和15/17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H/17号课题

身份管理和远程生物识别的架构和机制

（第10/17号课题的继续）

### H.1 目的

生物识别技术在电子商务、远程医疗和电子医疗等身份验证应用中得到了越来越多的认可。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，服务器侧的生物识别认证变得更为复杂和苛刻。使用移动终端和互联网服务的电信应用（如远程生物识别）需要通过认证方法来提供高安全性和友好的使用。有必要以安全、可靠的增强型操作和数据保护方式，规定远程生物识别数据的使用要求。

身份管理（IdM）是对证书、标识符、属性（如服务提供商、最终用户、组织、网络设备、应用和服务）获得适当程度信任的形式的终生管理和使用（创建、维护、使用和撤销）。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。根据身份模型的差异，对身份的控制可以采用集中的或分散形式，或二者兼而有之。在公共网络中，IdM支持授权实体之间进行可信赖信息的交换。这种交换是基于多个服务提供商在分布式系统之间的身份声明。交换亦可基于各种服务环境，如云和5G。IdM还改进了对私人信息的保护，且基于信任模型可确保只传播经授权的信息。

IdM是电信/ICT网络、业务和产品的主要组成部分，因为它支持建立并保持可信赖的通信。IdM不仅支持对实体身份的认证，还可以依据特权授予访问权限。在实体角色改变下放和其他基于身份的服务时，IdM亦支持改变特权。

IdM是管理网络安全，实现移动、按需网络接入和最终用户所期待服务的关键组成部分。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。鉴于IdM以互信的方式工作，这种增强的信任水平同样适用于最终用户和服务提供商。

国家/区域性专用IdM规范和解决方案将继续保留和发展。除远程生物识别的研究之外，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）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等）的研究。建立一个可实施协调解决方案的基础非常重要。

自2022年1月7日起由本课题负责的建议书包括：X.1080.0、X.1080.1、X.1080.2、X.1081、X.1082、X.1083、X.1084、X.1085、X.1086、X.1087、X.1088、X.1089、X.1090、X.1091、X.1092、X.1093、X.1094、X.1250、X.1251、X.1252、X.1253、X.1254、X.1255、X.1256、X.1257、X.1258、X.1261（with SG2）、X.1275、X.1276、X.1277、X.1278、X.1279、X系列增补7和X系列增补35。

自2022年1月7日起制定中的文本：X.1250rev、X.gpwd、X.oob-sa、X.pet\_auth、X.srdidm和X.tec-idms。

### H.2 课题

有待考虑的研究项目包括、但不限于：

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) 在功能性强大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？

g) 应如何开发生物识别系统和操作，以符合使用远程生物识别对宠物进行实体认证的功能要求？

h) 通用身份管理（IdM）基础设施的功能概念如何？

i) 支持以用户为中心的参与、基于云的身份、分散身份模型并支持IdM信息在相关各方之间（例如，用户、依赖方和身份提供商）安全交流的、独立于网络技术的适当IdM模型是什么？

j) IdM通用框架和要求包括哪些内容？

k) 服务提供商有哪些具体的IdM要求？

l) 实现不同IdM系统（如，身份保证、互通）之间互操作性有何要求、能力和可能的战略？

m) 在分布式账本技术上为身份提供支持需要考虑哪些问题，例如钱包、分散的标识符和可验证的凭据？

n) 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？

o) 保护和披露个人识别信息（PII）有哪些要求和机制？

p) 当涉及基于身份的关系和交互时，实体如何控制其关系？

q) 保护IdM系统免受网络攻击有哪些要求？

r) 哪些IdM能力可用来应对网络攻击？

s) 如何将IdM与先进的安全技术加以整合？

t) 如何在没有共享秘密的情况下进行身份验证？

u) 基于PKI的认证能否以可互操作和安全的方式进行？

v) 能否将生物识别作为强认证和信任层的一部分，以实现网络上的可信交互？

w) 在不依赖密码的情况下，基于消费者的身份管理系统在身份审查和账户恢复方面有哪些独特要求？

x) 在与依赖方打交道时，如何利用信任和关系增强账户恢复、用户安全和体验？

### H.3 任务

任务包括、但不限于：

a) 改进和修订现有有关远程生物识别认证的建议书。

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2/17号课题制定的架构和框架来研究并制定所有用于远程生物识别应用的安全要求和指南。

d) 研究和制定所有用于远程生物识别应用的安全、操作和技术数据保护的技术评估要求。

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应用的综合框架和要求。

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、操作和技术数据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) 研究和开发基于远程生物识别的宠物实体认证服务。

l) 规定支持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框架。

m) 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。

n) 规定身份保证的要求（并提出机制建议），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。在此情况下，身份保证包括身份模式和声誉。

o) 定义IdM系统互操作界面。

p) 规定保护和披露个人可识别信息（PII）的要求（及机制建议）。

q) 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。

r) 充实并协调IdM术语和定义动态清单并继续开展现有工作。

s) 研究并定义IdM安全风险和威胁。

t) 研究并开发分散的身份管理系统，以支持用户控制其身份。

u) 支持可跨系统、服务、设备、物联网和应用联合的可信赖身份管理系统。

v) 支持身份管理系统，为云代理、5G网络和移动设备提供身份管理服务。

w) 规定验证与联合的身份保证要求并提出相关机制。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。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### H.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），

9（工业、创新和基础设施）。

建议书：

X和Y系列

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

课题：

ITU-T第1/17、2/17、3/17、4/17、6/17、7/17、8/17、11/17、15/17、7/13和14/15号课题。

研究组：

ITU-D第1研究组、第2/2研究组；ITU-R第7研究组；ITU-T第2、5、9、11、13、15、16和20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6、17、27和37分委员会、国际标准化组织第12、68、215和307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；ETSI；OASIS；坎塔拉倡议；3GPP；3GPP2。

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；DID联盟：国际劳工组织（ILO）；世界卫生组织（WHO）。

第I/17号课题

支持安全应用的通用技术（如目录、PKI、正式语言、对象标识符）

（第11/17号课题的继续）

### I.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）

– 安全通信（X.510）

– 特权管理基础设施（PMI – X.509）

– 抽象句法表示法一（ASN.1）

– 对象标识符及其注册机构

– 测试和测试控制表示法（TTCN-3）

– 维护正式语言

• 规范和描述语言（SDL）

• 统一建模语言（UML）概要设计

• 消息序列图（MSC）

• 用户要求表示法（URN）

• CHILL，ITU-T编程语言

– OSI和ODP维护。

#### I.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。

X.500建议书提供详尽的接入控制和数据隐私保护。此建议书是一个开放式的规范，适应多种不同的应用。通过扩展可使未来的需求得到满足。广泛使用的LDAP是建立在X.500目录模型之上。ITU-T X.500建议书包含与LDAP的互操作能力。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。

X.509是一份重要的ITU-T建议书，公钥证书被广泛使用。

除作为电子商务、电子银行、电子健康的主要组成部分之外，该建议书现在还用于具有机器对机器通信和受限实体大型网络特征的其他业务，例如物联网（IoT）和智能电网（智慧电网）。

公钥证书也适用于几个IETF规范，例如传输层安全性（TLS）。

属性证书提供了一种安全的方法，用于传输对接入控制很重要的特权信息。OASIS SAML规范是基于X.509属性证书。属性证书亦用于供电系统。当由其他主管部门而不是公钥证书签发部门指配特权时，属性证书特别有用。

需要与其他研究组合作发展并完善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。X.509需要得到加强，以应对新的要求，如机器对机器通信、智能电网安全性、物联网安全性、量子安全算法和分布式账本技术。目前正在开发一种使用区块链的分散式公钥基础设施机制。

自2022年1月7日起由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.510、X.511、X.518、X.519、X.520、X.521、X.525、X.530和X.1341。

自2022年1月7日起制定中的文本：X.510 Amd.1、X.pki-em。

#### I.1.2 ASN.1工作的目的

为反映技术的进步、并满足ASN.1表示法及其编码规则，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遗留的含糊不或缺乏透明度的问题。

自2022年1月7日起由本课题负责的建议书：X.680、X.681、X.682、X.683、X.690、X.691、X.692、X.693、X.694、X.695、X.696、X.697、X.891、X.892、X.893和X.894。

自2022年1月7日起制定中的文本：无。

### I.1.3 对象标识符及其注册机构的工作目的

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，特别在是OID命名空间的管理上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。

对象标识符的任何创新使用均应与ITU-T第2研究组共同开发。

自2022年1月7日起由本课题负责的建议书和技术论文包括：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.676、X.677和技术论文XSTP-OID-ORS。

自2022年1月7日起制定中的文本：X.672rev。

### I.1.4 TTCN-3工作的目的

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。

自2022年1月7日起由本课题负责的建议书：X.292、Z.161、Z.161.1、Z.161.2、Z.161.3、Z.161.4、Z.161.5、X.161.6、Z.161.7、Z.162、Z.163、Z.164、Z.165、Z.165.1、Z.166、Z.167、Z.168、Z.169、Z.170和Z.171。

自2022年1月7日起制定中的文本：无。

### I.1.5 正式语言维护工作的目的

预计不会进一步发展以下正式语言：

– 规范和描述语言（SDL）

– 统一建模语言（UML）概要

– 消息序列图（MSC）

– 用户要求表示法（URN）

– CHILL，ITU-T编程语言

但有必要持续充实并完善。

自2022年1月7日起由本课题负责的建议书、增补和实施人员指南：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.200、Z.450和增补Z.Suppl.1以及实施人员指南Z.Imp100。

### I.1.6 OSI维护工作的目的

有关开放系统互连（OSI）的基础建议书已经完成。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。

自2022年1月7日起由本课题负责的建议书和实施人员指南：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、X.882和实施人员指南X.ImpOSI。

### I.1.7 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2022年1月7日起由本课题负责的建议书包括：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。

### I.2 课题

有待考虑的研究项目包括、但不限于：

#### I.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和ITU-T X.510建议书需要进行哪些修改，以支持量子安全算法和分布式账本技术？

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。

### I.2.2 与ASN.1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) 超越现有的协议之上，需要通过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ITU-T在有关ASN.1的工作中仍是提供协议定义表示法方面的领导者？

此项工作将与ISO/IEC JTC 1/SC 6协作开展。

### I.2.3 与对象标识符和登记机构相关工作的研究事项

a) 为支持在各种环境中使用OID需要哪些辅导活动？

b) 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？

c) 超越现有的协议之上，需要通过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ITU-T在有关OID的工作中仍是明确命名方面的领导者？

此项工作将与ISO/IEC JTC 1/SC 6协作开展。

### I.2.4 与TTCN相关工作的研究事项

为了满足未来应用的需求，TTCN-3需要哪些增强功能？

此项工作将与ETSI TC MTS协作开展。

### I.2.5 正式语言的维护

维护充实并完善与SDL、UML概要、MSC、URN和CHILL相关的建议书。

### I.2.6 OSI的维护

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；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。

### I.2.7 ODP的维护

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。

### I.3 任务

任务包括、但不限于：

#### I.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.510和X.pki-em，以支持诸如建立和维护公钥基础设施（PKI）的自动程序之类的新要求。

#### I.3.2 与ASN.1相关工作的任务

a) 为满足用户需求，在本研究期内对ITU-T 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。

b) 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。

c) 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。

d) 解决所有出现的错误报告并在必要时继续编写技术勘误表。

e) 确保所有与ASN.1工作相关的联络得到及时妥当地处理。

f) 开发任何有可能协助ASN.1用户的附加教程或网页。

### I.3.3 与对象标识符和登记机构相关工作的任务

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

b) 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。

c) 解决所有出现的错误报告并在必要时继续编写技术勘误表。

d) 确保所有与OID工作相关的联络得到及时妥当地处理。

e) 开发任何有可能协助OID用户的附加教程或网页。

f) 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。

g) 审查ITU-T X.660 | ISO/IEC 9834-1建议书涵盖的各种名称在各注册机构的候选资格，就负责指定的机构向第17研究组提出建议，并使用所保留候选资格的联络声明向ISO/IEC/JTC 1/SC 6通报相关情况。

h) OID项目负责人的职责包括：

• 向OID用户提供一般性建议；

• 促进国际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。

### I.3.4 与TTCN工作相关的任务

a) 按照本课题的责任继续完善相关建议书。

b) 促进TTCN在其他研究组和外部标准制定组织的使用。

### I.3.5 与维护正式语言工作相关的任务

根据需要，对与SDL、UML概要、MSC、URN和CHILL相关的建议书进行修正或改进。完善《SDL实施人员指南》。

#### I.3.6 与OSI维护相关工作的任务

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。完善《OSI实施人员指南》

### I.3.7 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。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### I.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），

9（工业、创新和基础设施）。

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课题以及与分布式PKI相关的第14/17号课题。

研究组：

ITU-T第2、9、11、13、15、16、20研究组以及使用或需要目录、ASN.1、OID、一致性和互操作性测试的各研究组。

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）；欧洲电信标准协会（ETSI）TC MTS；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使用国际电联系统设计语言的分组委员会。

**其他机构：**

万国邮政联盟（UPU）；SDL论坛学会。

第J/17号课题

智能交通系统的安全

（第13/17号课题的继续）

### J.1 目的

自动驾驶系统等智能交通系统（ITS）为提高道路安全提供各种类型的应用，目的是减少交通产生的环境足迹，加强交通管理，让公共和商业用户最大限度地享受交通部门带来的利益。

智能交通系统包括各类车内通信（例如，车辆到移动设备）、车辆之间的通信（例如，车辆到车辆（V2V））以及车辆和固定位置间的通信（例如，车辆到基础设施（V2I））即车辆到万物（V2X）的通信。信息通信技术（ICT）用于实现包括公路运输、铁路、水运和空运在内的智能交通系统，其中亦涵盖导航系统。

自动和辅助驾驶系统由各种系统组件构成，其中汽车的感知、决策和操作由电子和机械设备代替人类驾驶员执行，将自动化引入道路交通。

在包含自动和辅助驾驶系统的智能交通系统环境中，鉴于这些车辆相互连接，因此某一车辆的弱点会传递给其他车辆。所以，应当管理和处理车辆V2X通信系统的漏洞，以免影响众多其他车辆。

车辆内部的电子设备，如电子控制单元（ECU）和电子收费设备（ETC），正变得越来越复杂。因此，需要适当更新这些实体内部的软件模块，以提高其性能和安全性。

2017年3月批准的ITU-T X.1373建议书为ITS通信设备提供了安全的软件更新能力。X.1373建议书目前正在修订中。

最佳综合安全解决方案的标准化对智能交通系统环境至关重要。鉴于车辆通信的一些特有特征，提供安全性成为极具有挑战性的任务，值得深入研究。

自2022年1月7日起由本课题负责的建议书：X.1371、X.1372、X.1373、X.1374、X.1375、X.1376。

自2022年1月7日起制定中的文本：X.1373rev、X.1373rev、X.edrsec、X.eivnsec、X.evtol-sec、X.fstiscv、X.idse、X.ipscv、X.itssec-5、X.rsu-sec和X.srcd.。

### J.2 课题

有待考虑的研究项目包括、但不限于：

a) 在智能交通系统与自动和辅助驾驶系统环境中，应如何识别和定义安全问题（如安全架构和子系统）？

b) 如何识别和处理智能交通系统、自动和辅助驾驶系统服务和网络中的威胁和漏洞？

c) 在智能交通系统和自动和辅助驾驶系统环境中，针对缓解威胁提出了哪些安全要求（如身份识别和认证要求）？

d) 支持智能交通系统服务和网络的安全技术有哪些？

e) 在智能交通系统和自动和辅助驾驶系统环境中，应如何保持和维护实体之间的安全互联？

f) 智能交通系统、自动和辅助驾驶系统服务及网络需要哪些安全技术、机制和协议？

g) 基于电信/ICT网络的智能交通系统与自动和辅助驾驶系统和网络有哪些全球认可的安全解决方案？

h) 智能交通系统和自动和辅助驾驶系统安全的最佳实践或导则有哪些？

i) 人工智能/机器学习技术如何为智能交通系统以及自动和辅助驾驶系统提供安全性和信心？

j) ITS服务需要何种有关个人身份信息（PII）的保护和管理机制？

### J.3 任务

任务包括、但不限于：

a) 编写建议书，为智能交通系统、自动和辅助驾驶系统提供全面的安全解决方案。

b) 进一步研究，以确定智能交通系统及基于电信/ICT网络的自动和辅助驾驶系统服务和网络的安全问题。

c) 研究并识别智能交通系统、自动和辅助驾驶系统中的安全问题和威胁。

d) 研究并确定特定智能交通系统、自动和辅助驾驶系统服务及应用的需求和使用案例。

e) 研究并开发智能交通系统、自动和辅助驾驶系统的安全机制、协议和技术。

f) 研究并开发针对特定智能交通系统、自动和辅助驾驶系统服务及应用的安全配置、分级认证方案和机制。

g) 为快速移动的网络节点和动态变化的网络拓扑研发高效的加密和解密算法应用。

h) 研究并开发智能交通系统、自动和辅助驾驶系统的事件数据记录技术。

i) 研究并开发智能交通系统的安全互联机制以及电信环境中的自动驾驶和辅助驾驶系统。

j) 研究并识别智能交通系统、自动和辅助驾驶系统中的PII保护问题和威胁。

k) 研究并发展PII智能交通系统以及自动驾驶和辅助驾驶系统的保护和管理机制。

1) 研究并开发基于人工智能/机器学习技术的安全智能交通系统以及自动和辅助驾驶系统。

m) 研究并进一步完善现有建议书草案：X.1373rev、X.itssec-5、X.srcd、X.edrsec、X.eivnsec、X.fstiscv、X.ipscv、X.rsu-sec、X.evtol-sec。

n) 与相关标准制定组织合作，共同编写建议书。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### J.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），

9（工业、创新和基础设施），

11（智慧城市和社区）。

建议书：

X系列和其他与安全有关的建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、6/17、7/17、8/17、10/17、11/17和15/17号课题。

研究组和焦点组：

ITU-T第11、13、16和20研究组；ITU-R WP5A；有关智能交通系统通信标准（CITS）的合作；ITU-T FG-VM（车载多媒体）。

标准化机构：

ISO TCs 22和204；ISO/IEC JTC 1/SCs 6和27；IETF WG ITS；IEEE 802.11工作组和1609工作组；SAE国际（例如，车辆网络安全系统工程委员会、联网车辆指导委员会和DSRC技术标准委员会）；ETSI TC ITS；W3C汽车工作组。

其他机构：

GSMA；ATIS；CCSA；TIA；TTA；TTC；联合国欧洲经济委员会（UNECE）第29工作组及其附属机构（如网络安全任务组（TFCS））；AGL（汽车级Linux）。

第K/17号课题

分布式账本技术（DLT）的安全

（第14/17号课题的继续）

### K.1 目的

分布式账本技术（DLT）是一种新型的、在分布式环境中共享、复制和同步的安全分类账，其最突出的实现方式是区块链。分布式账本中的数据由多方控制。

作为一种特定的分布式数据库技术，分布式账本技术具有内在的防数据修改属性 – 记录完成后，块中数据就无法进行追溯性地改变。在早期数字加密货币，即比特币的应用取得成功后，分布式账本技术的这一显著特征已广为人知。

分布式账本技术拥有巨大的潜力，已成为改变经济、文化和社会的颠覆性技术之一。分布式账本技术支持创新型金融/非金融分散应用，使人们不再依赖第三方中介。分布式账本技术将引入新的数据管理基础设施，这将加速以电信为基础行业（例如银行和金融、政府、医疗保健和超级物流）的服务革命。

分布式账本技术将对包括电信服务提供商在内的电信用户和行业产生深远影响。

我们需要确定电信用户、运营商和服务提供商在分布式账本技术环境安全方面的角色和责任。

最佳综合安全解决方案的标准化对分布式账本技术而言至关重要，这一点在包括电信业在内的各行各业都有许多使用案例。鉴于分布式账本技术的一些独有特点，提供安全成为一项特别具有挑战性的任务，值得深入研究。

自2022年1月7日起由本课题负责的建议书：X.1400、X.1401、X.1402、X.1403、X.1404、X.1405、X.1406、X.1407和X.1408。

自2022年1月7日起制定中的文本：X.sa-dsm、X.sc-dlt、X.srscm-dlt、X.ss-dlt和TR.qs-dlt。

### K.2 课题

有待考虑的研究项目包括、但不限于：

a) 在分布式账本技术环境中，应如何根据基础信息（术语和定义、概念和分类、用例）识别和定义安全问题（例如架构和子系统）？

b) 如何处理基于分布式账本技术的应用和服务中的威胁和漏洞？

c) 在分布式账本技术环境中，为减轻威胁提出了哪些安全要求？

d) 有哪些安全技术支持基于分布式账本技术的应用和服务？

e) 应如何保持和维护分布式账本技术环境下各实体之间的安全互联？

f) 基于分布式账本技术的应用和服务需要哪些安全技术、机制和协议？

g) 基于电信/ICT网络的分布式账本技术应用和服务有哪些全球认可的安全解决方案？

h) 基于分布式账本技术的应用和服务的最佳安全实践或准则有哪些？

i) 基于分布式账本技术的应用和服务的保护和信息安全管理需要哪些PII（个人身份信息）？

j) 如何利用分布式账本技术为安全提供支持？

k) 如何评估、评价和保证分布式账本技术的安全？

l) 第17研究组应与哪些利益攸关方合作？

### K.3 任务

任务包括、但不限于：

a) 针对分布式账本技术，对其他组织中正在实施的相关安全工作开展差距分析。

b) 进一步研究以分布式账本技术和电信/ICT网络为基础的应用和服务的安全问题。

c) 研究与分布式账本技术网络的安全和PII保护相关的基础，如术语和定义、概念和分类以及使用案例。

d) 研究并识别基于分布式账本技术的应用和服务中的安全问题和威胁。

e) 研究并开发基于分布式账本技术的应用和服务的安全机制、协议和技术。

f) 研究并制定基于分布式账本技术的应用和服务的安全互联机制。

g) 研究并确定基于分布式账本技术的应用和服务中的PII保护问题和威胁。

h) 为以分布式账本技术为基础提供应用和服务的实体，研究并开发信息管理系统。

i) 研究并制定支持安全分布式账本技术的用法指南。

j) 研究并制定分布式账本技术的安全评估、评价和保证指南。

k) 编写一套建议书，为基于分布式账本技术的应用和服务提供全面的安全解决方案。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### K.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），

9（工业、创新和基础设施），

11（智慧城市和社区）。

建议书：

X系列和其他与安全有关的建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、6/17、7/17、8/17、10/17、11/17、13/17和15/17号课题。

研究组：

ITU-T第5、11、13、16和20研究组。

标准化机构：

ISO TC 307；ISO/IEC JTC 1/SC 27。

其他机构：

GSMA；W3C；IEEE；联合国欧洲经济委员会（UNECE）；FIGI；ATIS；CCSA；
TIA；TTA；TTC。

第L/17号课题

新兴技术的安全性，包括基于量子的安全性

（第15/17号课题的继续）

### L.1

第17研究组认识到，安全研究的动态属性在很大程度上取决于攻击者/防御者的技术竞赛和双方利用创新产生的连锁反应。因此而出现的一系列新兴安全技术有些需要全球标准化。

从本质上讲，我们无法预测第17研究组何时能主动建立并运行相关孵化机制（TP.inno）以及这个机制的内容。该机制可为新兴安全领域的研究提供可控的灵活性，为新兴的基于电信/ICT的服务和应用提供保障。

这种孵化机制使第17研究组能够以有效的方式在新兴领域引入新的工作项目，并鼓励将非规范性文本（技术论文和技术报告）作为一种经验证的最佳实践，从而使第17研究组的成员有时间熟悉这些新兴领域，让新加入者能够熟悉第17研究组和ITU-T的工作程序和环境。在新工作项目的开发过程中，有时新兴安全技术的性质表明其与现有课题更加靠近，且可以通过移交该工作项目，最大限度地实现第17研究组工作的一致性、效率和质量。

此外，这种孵化机制可以识别本课题正在研究的新兴安全技术的发展趋势。一些新兴技术来自：

– 本主题具有新颖性，例如基于量子的安全性、安全多方计算、同态或机器人潜在的安全可识别性等。

– 此主题并不新鲜，但这是其首次进入全球标准化领域，例如恶意软件分析、预防数据丢失等。

– 与其他任何课题都不匹配的运营安全架构差距，例如安全产品本身的差距以及展示新兴交叉主题的解决方案、安全数据模式等大量集成和组合问题。

孵化机制发现的一个新兴领域是基于量子的安全性。大规模量子计算机的出现可能会给基于ICT的传统电信系统带来重大干扰，亦给安全造成了重大风险。

事实上，当前的密码安全依赖于计算难题：离散对数问题和整数分解问题。考虑到当今可用计算机的现有体系结构，人们认为很难在合理的时间内得出这些问题的结果。然而，使用非对称密钥的公钥加密是公共网络认证的基石。就其本质而言，量子计算机可以在相当快的时间内解决整数因式分解和离散对数问题，其通过连锁反应，能够打破目前密码学赖以建立的基础，威胁到当今网络生活和数字化的生存基石。

量子密钥分发（QKD）使双方能够生成一个只有他们自己知晓的共享随机密钥，该密钥可使用传统加密算法加密和解密消息。QKD存在两个会产生网络拓扑和集成问题的限制：a) 具有点对点（p-t-p）的性质，只能应用于两方，A和B；b) 对地面网络有距离限制。为了克服这两个限制，QKD网络概念在业内的推广包括(1) 利用在p-t-p中工作的QKD系统链接在一起的节点集合，以及(2) 在各QKD节点之间共享并嵌入其中的管理系统。该管理系统的目的是在同一QKD网络内可能并无直接链接的两个或多个节点之间分发密钥。目前，商业QKD系统足够稳定和成熟，可以开始规划大规模QKD网络。一些公司/机构提出了若干发展QKD网络的举措，但对于QKD系统的构成尚无广泛接受的标准。

此外，随机数是工程中的一项基本要素，在密码学中有着重要的应用。量子力学核心的内在随机性使量子系统成为熵的完美来源。量子随机数生成是最成熟的量子技术之一，有许多替代的生成方法。

总之，基于量子的安全性能够确保通信不易受到量子计算机的攻击。实现基于量子的安全需要几个关键元素，其中包括量子密钥分发和量子随机数生成器（QRNG）。此外，QKD和QRNG关键要素和功能的互操作性，对其在实际电信网络中的广泛使用非常重要。

反之，第17研究组非常需要研究抵抗量子攻击的量子安全问题。

自2022年1月7日起由本课题负责的建议书和技术文件/报告：X.1702、X.1710、X.1712、X.1714、X.1770和技术文件TP.inno、TP.sgstruct以及TR.sec-qkd。

自2022年1月7日起制定中的文本：X.1712 Corrigendum、X.icd-schemas、X.sec\_QKDN\_AA、X.sec\_QKDN\_CM、X.sec\_QKDN\_intrq、X.sec-QKDN-tn、TR.hybsec-qkdn、TR.sec-ai和TR.sgfdm。

### L.2 课题

有待考虑的研究项目包括、但不限于：

a) 有哪些新兴的安全技术？

b) 新出现的安全技术有哪些类别？

c) 如何安全开发新兴安全技术？

d) 实施孵化机制最有效的机制是什么？

e) 大规模量子计算机的出现给传统通信带来了哪些影响和挑战？

f) 建立基于量子的安全性的关键要素是什么？

g) 建立基于量子的安全性的过渡策略是什么？

h) 如何处理基于量子的安全威胁和漏洞？

i) 针对基于量子的安全，有哪些旨在缓解威胁的安全要求？

j) 有哪些支持基于量子安全的安全技术？

k) 针对基于量子的安全，应如何保持并维护实体间的安全互连？

l) 基于量子的安全需要制定哪些安全要求、技术、机制和协议？

m) 基于电信/ICT通信的量子安全有哪些全球认可的安全解决方案？

n) 针对基于量子的安全，有哪些最佳实践或安全指南？

### L.3 任务

任务包括、但不限于：

a) 确定新兴的安全技术。

b) 确定新兴安全技术的新类别，以巩固课题M的战略。

c) 如果NWI课题的发展使其与现有课题的匹配更加清晰，则有可能将其重新分配给其他课题

d) 纳入孵化机制，以处理ITU-T第17研究组内的新兴领域问题。

e) 起草一套技术建议书，提供全面的安全解决方案，以建立基于量子的安全性。

f) 研究并界定基于电信/ICT基础设施的量子安全问题。

g) 研究并确定基于量子安全的安全问题和威胁。

h) 研究并开发基于量子安全的安全要求、机制、协议和技术。

i) 研究并开发基于量子安全的安全互联机制。

j) 为提供量子安全的实体研究并开发信息管理系统。

此课题的最新工作状况见第17研究组的工作计划：
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>。

### L.4 关系

WSIS行动方面：

C5。

可持续发展目标：

8（体面工作和经济增长），

9（工业、创新和基础设施），

11（智慧城市和社区）。

建议书：

X系列和其他与安全有关的建议书。

课题：

ITU-T第1/17、2/17、3/17、4/17、6/17、7/17、8/17、10/17、11/17、13/17和14/17号课题。

研究组：

ITU-T第2、3、5、9、11、12、13、15、16和20研究组。

标准化机构：

ETSI TC Cyber、ISG-QKD；ISO/IEC JTC 1/SC 27；OASIS；IETF。

其他机构：

GSMA；ATIS；CCSA；TIA；TTA；TTC。

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