|  |  |
| --- | --- |
| **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 19-C** |
|  | **2021年12月** |
|  | **原文：英文** |
|  | |
| ITU-T第17研究组 | |
| 安全 | |
| ITU-T第17研究组提交世界电信标准化全会（WTSA-20）的报告： 第一部分 – 概述 | |
|  | |

|  |  |  |
| --- | --- | --- |
| **摘要：** | 此文稿含有ITU-T第17研究组提交WTSA-20的关于该组在2017-2021年研究期内所开展活动的报告。 | |
| **联系人：** | Heung Youl Youm先生 ITU-T第17研究组主席 韩国 | 电子邮件：[hyyoum@sch.ac.kr](mailto: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

|  |  |  |
| --- | --- | --- |
| |  | | --- | | **目录**  **页码**  [1 引言 4](#_Toc94117642)  [1.1 第17研究组的职责范围 4](#_Toc94117643)  [1.2 第17研究组的管理班子和召开的会议 5](#_Toc94117644)  [2 工作的组织 15](#_Toc94117645)  [2.1 研究的组织和工作的分配 15](#_Toc94117646)  [2.2 课题和报告人 18](#_Toc94117647)  [3 2017-2020年研究期实现的工作成果 25](#_Toc94117648)  [3.1 概述 25](#_Toc94117649)  [3.2 主要成果 25](#_Toc94117650)  [a) 第1/17号课题：电信/ICT的安全协调（2017-2020年）/安全标准化策略与协调（2021-） 25](#_Toc94117651)  [b) 第2/17号课题：安全架构和框架（2017-2020年）/安全架构和网络安全（2021-） 26](#_Toc94117652)  [c) 第3/17号课题：电信信息安全管理（2017-2020年）/电信信息安全管理和安全服务（2021-） 27](#_Toc94117653)  [d) 第4/17号课题：网络安全（2017-2020年）/网络安全和打击垃圾邮件（2021-） 28](#_Toc94117654)  [e) 第5/17号课题：以技术手段打击垃圾信息（2017-2020年） 30](#_Toc94117655)  [f) 第6/17号课题：电信业务、网络和物联网的安全问题（2017-2020年）/电信业务和物联网的安全（2021-） 31](#_Toc94117656)  [g) 第7/17号课题：安全应用服务 33](#_Toc94117657)  [h) 第8/17号课题：云计算和大数据基础设施的安全 34](#_Toc94117658)  [i) 第9/17号课题：电子生物特征识别（2017-2020年） 35](#_Toc94117659)  [j) 第10/17号课题：身份管理架构和机制（2017-2020年）/身份管理和远程生物识别的架构和机制（2021-） 35](#_Toc94117660)  [k) 第11/17号课题：支持安全应用的通用技术（目录、公钥基础设施（PKI）、权限管理基础设施（PMI）、抽象句法符号一（ASN.1）、对象标识符（OID））（2017-2020年）/支持安全应用的通用技术（例如目录、公钥基础设施、正式语言、对象标识符）（2021-） 36](#_Toc94117661)  [l) 第12/17号课题：电信软件和测试的形式语言 41](#_Toc94117662)  [m) 第13/17号课题：智能交通系统的安全问题（2017-2020年）/智能交通系统的安全（ITS）性（2021-） 44](#_Toc94117663)  [n) 第14/17号课题：分布式账本技术的安全问题（2018-2020年）/分布式账本技术（DLT）的安全性（2021-） 45](#_Toc94117664)  [o) 第15/17号课题：新兴技术的安全性，包括基于量子的安全性 46](#_Toc94117665)  [3.3 牵头研究组活动报告、全球标准举措（GSI）、联合协调活动（JCA）、区域组和项目的报告 46](#_Toc94117666)  [3.3.1 就有关安全开展的牵头研究组活动 47](#_Toc94117667)  [3.3.2 身份管理（IdM）牵头研究组活动 50](#_Toc94117668)  [3.3.3 关于语言和描述技术的牵头研究组活动 51](#_Toc94117669)  [3.3.4 有关身份管理的活动（JCA-IdM） 52](#_Toc94117670)  [3.3.5 第17研究组非洲区域组（SG17RG-AFR） 52](#_Toc94117671)  [3.3.6 第17研究组阿拉伯区域组（SG17RG-ARB） 52](#_Toc94117672)  [3.4 项目 52](#_Toc94117673)  [3.4.1 ASN.1项目 53](#_Toc94117674)  [3.4.2 OID项目 53](#_Toc94117675)  [3.5 缩小标准化工作差距 53](#_Toc94117676)  [4 有关未来工作的考虑 54](#_Toc94117677)  [5 WTSA第2号决议在2022-2024年研究期的更新 55](#_Toc94117678)  附件1：[本研究期制定或删除的建议书、增补及其它资料清单 56](#_Toc94117679)  附件2：[第17研究组针对WTSA第2号决议提出的拟议修订 70](#_Toc94117680) | |  | |

# 1 引言

## 1.1 第17研究组的职责范围

世界电信标准化全会（2016年，哈马马特）委托第17研究组开展有关树立使用信息通信技术（ICT）的信心并提高安全性的12个课题的研究。

WTSA-16第2号决议附件A规定了第17研究组的以下任务，安全：

ITU-T第17研究组负责树立使用信息通信技术（ICT）的信心和安全性，其中包括与网络安全、安全管理、反垃圾邮件和身份管理相关的研究。其职责还包括安全架构和框架、保护个人可识别信息以及物联网（IoT）、智能电网、智能手机、软件定义网络（SDN）、互联网协议电视（IPTV）、网络业务、社交网络、云计算、大数据分析、移动金融系统和电子生物特征识别应用及业务的安全性。ITU-T第17研究组还负责开放系统通信应用，包括目录和对象标识符，以及技术语言、其使用方法及与电信系统的软件方面相关的其他问题以及为支持提高建议书质量而开展得合规性测试规范语言。

WTSA-16第2号决议附件A规定了第17研究组的如下牵头研究组职责，安全：

– 安全牵头研究组。

– 身份管理（IdM）牵头研究组。

– 语言和描述技术牵头研究组。

WTSA-16第2号决议附件B为第17研究组提供以下指导：

ITU-T第17研究组负责开展树立使用信息通信技术（ICT）的信心和安全性方面的研究工作，涉及与安全相关的研究（网络安全、反垃圾邮件和身份管理）。其职责还涉及安全架构和框架、安全管理、保护个人可识别信息（PII）以及物联网（IoT）、智能电网、智能手机、软件定义网络（SDN）*、*互联网协议电视（IPTV）、网络业务、社交网络、云计算、移动金融系统和电子生物特征识别应用及业务的安全性。第17研究组还负责开放系统通信应用，包括号码薄和对象标识符，以及技术语言、其使用方法及与电信系统的软件方面相关的其他问题，同时为提高建议书质量，还负责开展一致性测试。

在安全方面，该组负责编制安全架构和框架等有关ICT安全问题的核心建议书；威胁、易受攻击性和风险等与网络安全相关的基本内容；事件处理/响应和数字取证以及包括PII在内的安全管理和通过技术手段打击垃圾信息。另外，第17研究组还负责ITU-T安全相关工作的总协调。

此外，第17研究组还负责制定IPTV、智能电网、IoT、软件定义网络（SDN）*、*社交网络、云计算、大数据分析*、*智能手机、移动金融系统和电子生物特征识别领域相关应用和业务安全方面的核心建议书。

第17研究组还负责制定有关独立于网络技术并支持实体之间身份信息安全交换的一般身份管理模型的核心建议书。这项工作还包括研究用于发现身份信息的权威来源的程序；用于多样化身份信息格式桥接/互操作性的通用机制；身份管理威胁及防范机制，保护个人可识别信息（PII），并制定机制以确保只有在适当情况下才能经授权访问PII。

在开放系统通信方面，第17研究组负责制定涉及以下内容的建议书：

• 号码薄业务和系统，包括公钥基础设施（PKI）（ITU-T F.500和ITU-T X.500系列）；

• 对象识别符（OID）和相关注册管理机关（ITU-T X.660/ITU-T X.670系列）；

• 开放系统互连（OSI），包括抽象句法记法一（ASN.1）（ITU-T F.400系列、ITU-T X.200系列、ITU-T X.400系列、ITU-T X.600系列、ITU-T X.800系列）；及

• 开放式分布处理（ODP）（ITU-T X.900系列）。

在语言方面，第17研究组负责研究建模、规范和描述技术。此项工作涉及诸如ASN.1、SDL、MSC、URN和TTCN-3等语言。

需要根据第2、第9、第11、第13、第15、第16和第20（在IoT和SC&C安全问题上）研究组的要求并与其合作进行研究。

第17研究组将根据每个研究组的职责范围与负责研究IoT的第20研究组和第2研究组合作开展相关身份管理方面的工作。

WTSA-16第2号决议附件C（由电信标准化顾问组（TSAG）修改）规定了第17研究组在2017-2020年研究期内所负责的建议书清单：

– ITU-T E.104、ITU-T E.115、ITU-T E.409（与第2研究组共同负责）

– ITU-T F.400系列；ITU-T F.500 − ITU-T F.549

– ITU-T X系列，第2、第11、第13、第15和第16研究组负责的建议书除外

– ITU-T Z系列，ITU-T Z.300系列和ITU-T Z.500系列除外。

## 1.2 第17研究组的管理班子和召开的会议

WTSA-16任命YOUM Heung Youl先生（韩国）为第17研究组主席，并任命了下列九名副主席：DOLMATOV Vasiliy（俄罗斯联邦）、ISHAG Muataz Elsadig（苏丹）、EVREN Gökhan（土耳其）、FUREY Inette女士（美国）、LATROUS Wala Turki女士（突尼斯）、林兆骥先生（Zhaoji LIN中国）、MIGUEL Hugo Darío先生（阿根廷）、MIYAKE Yutaka 先生（日本）和KETTIN ZANGA Patrick-Kennedy先生（中非）。KETTIN ZANGA Patrick-Kennedy先生未在本研究期参加过第17研究组的任何会议。

2018年3月，FUREY Inette女士（美国）由GONZALES Juan先生（美国）接替，担任第17研究组副主席。2020年3月，MIGUEL Hugo Darío先生（阿根廷）由MOLINARI Lia女士（阿根廷）接替，担任第17研究组副主席。2020年8月，KETTIN ZANGA Patrick-Kennedy 先生（中非）由Eric Anicet MBATHAS先生（中非）接替，担任第17研究组副主席。

第17研究组在本研究期召开了13次全体会议（见表1）。

表1

第17研究组及其工作组的会议

| 会议 | 日期 | 报告 |
| --- | --- | --- |
| SG/WP 17 | 2017年3月22 – 30日，日内瓦 | SG17-R1至R9 |
| SG/WP 17 | 2017年8月29 – 9月6日，日内瓦 | SG17-R10至R17 |
| SG/WP 17 | 2018年3月20 – 29日，日内瓦 | SG17-R18至R24 |
| SG/WP 17 | 2018年8月29 – 9月7日，日内瓦 | SG17-R25至R32 |
| SG/WP 17 | 2019年1月22 – 30日，日内瓦 | SG17-R33至R37 |
| SG/WP 17 | 2019年8月27 – 9月5日，日内瓦 | SG17-R38至R50 |
| SG/WP 17 | 2020年3月17 – 26日，虚拟 | SG17-R51至R66 |
| SG17 | 2020年5月29日，虚拟 | SG17-R67 |
| SG/WP 17 | 2020年8月24 – 9月3日，虚拟 | SG17-R68至R77 |
| SG17 | 2021年1月7日，虚拟 | SG17-R78 |
| SG/WP 17 | 2021年4月20 – 30日，虚拟 | SG17-R79至R85 |
| SG/WP 17 | 2020年8月24 – 9月3日，虚拟 | SG17-R86至R102 |
| SG17 | 2022年1月7日，虚拟 | SG17-R103 |

管理班子扩大会议与每次第17研究组会议联合召开。

此外，在本研究期内在不同地点召开了诸多次报告人会议（包括电子会议（见表1之二））。

表1之二

本研究期在第17研究组下组织的报告人会议

| 日期 | 地点/东道主 | 课题 | 活动名称 |
| --- | --- | --- | --- |
| 2016-12-12 至 2016-12-13 | 中国北京 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5710&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0057)] | Q8/17过渡期报告人组会议 |
| 2017-01-12 至 2017-01-13 | 电子会议 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5711&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0054)] | Q4/17过渡期报告人组电子会议 |
| 2017-02-06 至 2017-02-10 | 突尼斯的 突尼斯城 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5716&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0058)] | 与ISO/IEC JTC 1/SC 6/WG10的第11/17号课题联合报告人组会议 |
| 2017-02-08 至 2017-02-09 | 韩国首尔 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5712&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0053)] | Q3/17过渡期报告人组会议 |
| 2017-02-08 至 2017-02-09 | 韩国首尔 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=5713&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170322-TD-PLEN-0056)] | Q6/17过渡期报告人组会议 |
| 2017-06-22 至 2017-06-23 | 韩国首尔 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6903&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0392)] | Q3/17中期报告人组会议 |
| 2017-06-22 至 2017-06-23 | 韩国首尔 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6904&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0393)] | Q6/17中期报告人组会议 |
| 2017-06-27 至 2017-06-28 | 中国北京 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6909&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0394)] | Q8/17中期报告人组会议 |
| 2017-06-29 | 日本东京 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6916&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0395)] | Q4/17中期报告人组会议 |
| 2017-06-30 | 日本东京 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6905&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6906&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=6907&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0390)] | 与Q3/17、Q4/17和Q10/17有关DFS的联合报告人组会议 |
| 2017-07-03 | 日本东京 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=7916&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0396)] | Q10/17中期报告人组会议 |
| 2017-07-14 | 韩国首尔 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=8918&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-170829-TD-PLEN-0397)] | Q13/17中期报告人组会议 |
| 2017-10-30 至 2017-11-03 | 韩国 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9047&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Q11/17与ISO/IEC JTC1/SC6的联合会议 |
| 2017-11-30 至 2017-12-01 | 韩国盆唐 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9048&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0817)] | Q14/17报告人组会议 |
| 2017-12-13 至 2017-12-14 | 中国北京 | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9050&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0822)] | Q7/17报告人组会议 |
| 2018-01-09 | 加拿大温哥华 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9051&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0821)] [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9052&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-1006)] | Q4/17和Q10/17的联合会议 |
| 2018-01-22 至 2018-01-23 | 中国北京 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9057&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0823)] | Q14/17报告人组会议 |
| 2018-01-24 至 2018-01-25 | 韩国首尔 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9056&Group=17)[ [会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0818)] | Q13/17报告人组会议 |
| 2018-01-25 至 2018-01-26 | 韩国首尔 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9054&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0820)] | Q3/17报告人组会议 |
| 2018-01-25 至 2018-01-26 | 韩国首尔 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9055&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180320-TD-PLEN-0819)] | Q6/17报告人组会议 |
| 2018-06-04 至 2018-06-06 | 中国北京 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9265&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1252)] | Q14/17中期报告人组会议 |
| 2018-06-07 至 2018-06-08 | 韩国首尔 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9261&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1246)] [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9262&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1251)] | Q6/17和Q13/17中期报告人组会议 |
| 2018-06-20 至 2018-06-21 | 中国银川 | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9259&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1247)] | Q7/17报告人组会议 |
| 2018-06-26 至 2018-06-27 | 美国华盛顿州西雅图 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9264&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1249)] | Q10/17中期报告人组会议 |
| 2018-06-27 至 2018-06-28 | 中国北京 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9263&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1248)] | Q8/17中期报告人组会议 |
| 2018-08-27 至 2018-08-31 | 日本东京 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9260&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-180829-TD-PLEN-1250)] | Q11/17与ISO/IEC JTC 1/SC 6/WG 10的联合中期报告人组会议 |
| 2018-11-08 至 2018-11-09 | 新加坡 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9405&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1727)] | Q13/17中期报告人组会议 |
| 2018-11-12 至 2018-11-13 | 日本东京 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9406&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Q10/17中期报告人组会议 |
| 2018-11-12 至 2018-11-13 | 日本东京 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9407&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190122-TD-PLEN-1726)] | Q14/17中期报告人组会议 |
| 2019-04-22 至 2019-04-26 | 中国北京 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9560&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2057)] | Q11/17与ISO/IEC JTC 1/SC 6/WG 10的联合中期报告人组会议 |
| 2019-06-04 至 2019-06-05 | 电子会议 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9559&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2056)] | Q10/17中期报告人组电子会议 |
| 2019-06-04 至 2019-06-05 | 电子会议 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9563&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2059)] | Q14/17中期报告人组 |
| 2019-06-10 至 2019-06-12 | 中国上海 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9574&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2051)] | Q4/17中期报告人组 |
| 2019-06-11 至 2019-06-12 | 中国北京 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9561&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2058)] | Q13/17中期报告人组 |
| 2019-06-18 至 2019-06-19 | 中国重庆 | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9556&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2053)] | Q7/17中期报告人组 |
| 2019-06-24 至 2019-06-25 | 中国北京 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9557&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2054)] | Q8/17中期报告人组 |
| 2019-06-27 至 2019-06-28 | 日本东京 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9555&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2052)] | Q6/17中期报告人组 |
| 2019-06-27 | 电子会议 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9554&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-190827-TD-PLEN-2050)] | Q3/17中期报告人组电子会议 |
| 2019-10-22 至 2019-10-23 | 中国海口 | [Q7/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9763&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2564)] | Q7/17中期报告人组会议 |
| 2019-12-05 至 2019-12-06 | 瑞士弗里堡 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9767&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)]和[Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9768&Group=17) [[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2762)] | Q11/17和Q14/17的联合会议 |
| 2019-12-11 至 2019-12-13 | 中国济南 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9882&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2562)] | Q4/17中期报告人组会议 |
| 2019-12-11 | 电子会议 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9766&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2567)] | Q11/17中期报告人组会议 |
| 2019-12-11 | 中国济南 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9760&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2754)] | Q4/17和Q16/13同地举办的报告人组会议 |
| 2019-12-12 | 日本东京 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9765&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2566)] | Q10/17中期报告人组会议 |
| 2019-12-13 | 日本东京 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9759&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2561)] | Q3/17中期报告人组会议 |
| 2020-01-07 至 2020-01-08 | 中国北京 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9764&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2565)] | Q8/17中期报告人组会议 |
| 2020-01-07 至 2020-01-08 | 日本福冈 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9769&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2569)] | Q13/17中期报告人组会议 |
| 2020-01-08 | 电子会议 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9771&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2570)] | Q14/17中期报告人组会议 |
| 2020-01-13 至 2020-01-14 | 马来西亚 吉隆坡 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9783&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2563)] | Q6/17中期报告人组会议 |
| 2020-02-03 至 2020-02-07 | 英国伦敦 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=9770&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200317-TD-PLEN-2568)] | Q11/17与ISO/IEC JTC 1/SC 6/WG 10的联合中期报告人组会议 |
| 2020-04-17 | 电子会议 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10081&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2963)] | Q4/17中期报告人组会议 |
| 2020-04-22 | 电子会议 | [Q11/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10087&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2966)] | Q11/17中期报告人组会议 |
| 2020-05-11 至 2020-05-12 | 电子会议 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10083&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3093)] | Q6/17中期报告人组会议 |
| 2020-05-13 | 电子会议 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10088&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200529-TD-PLEN-2979)] | Q13/17中期报告人组会议 |
| 2020-06-02 至 2020-06-03 | 电子会议 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10080&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3090)] | Q3/17中期报告人组会议 |
| 2020-06-10 至 2020-06-11 | 电子会议 | [Q13/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10089&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3096)] | Q13/17中期报告人组会议 |
| 2020-06-19 | 电子会议 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10347&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3091)] | Q4/17中期报告人组会议 |
| 2020-06-22 至 2020-06-23 | 电子会议 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10090&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3097)] | Q14/17中期报告人组会议 |
| 2020-07-13 | 电子会议 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10086&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3095)] | Q10/17中期报告人组会议 |
| 2020-07-16 至 2020-07-17 | 电子会议 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=10084&Group=17)[[会议报告](http://www.itu.int/md/T17-SG17-200824-TD-PLEN-3094)] | Q8/17中期报告人组会议 |
| 2020-10-19 至 2020-10-30 | 电子会议 | [Q11/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11694&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3447)] | Q11/17与ISO/IEC JTC 1/SC 6/WG 10的联合中期报告人组会议 |
| 2020-11-18 | 电子会议 | [Q10/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11588&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3462)] | Q10/17中期报告人组会议 |
| 2020-11-25  至 2020-11-26 | 电子会议 | [Q13/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11589&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3467)] | Q13/17中期报告人组会议 |
| 2020-11-26 至 2020-11-27 | 电子会议 | [Q4/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11570&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3460)] | Q4/17中期报告人组会议 |
| 2020-12-07 至 2020-12-08 | 电子会议 | [Q2/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11569&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3459)] | Q2/17中期报告人组会议 |
| 2020-12-09  至  2020-12-10 | 电子会议 | [Q3/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11727&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3468)] | Q3/17中期报告人组会议 |
| 2020-12-21  至  2020-12-22 | 电子会议 | [Q6/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11571&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3463)] | Q6/17中期报告人组会议 |
| 2021-01-04 至 2021-01-05 | 电子会议 | [Q14/17](https://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11590&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210107-TD-PLEN-3469)] | Q14/17中期报告人组会议 |
| 2021-02-01 至 2021-02-02 | 电子会议 | [Q3/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11832&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210420-TD-PLEN-3547)] | Q3/17中期报告人组会议 |
| 2021-02-01 至 2021-02-02 | 电子会议 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11830&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210420-TD-PLEN-3548)] | Q4/17中期报告人组会议 |
| 2021-02-04 | 电子会议 | [Q6/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=11836&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210420-TD-PLEN-3549)] | Q6/17中期报告人组会议 |
| 2021-06-17 至 2021-06-18 | 电子会议 | [Q15/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12574&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3876)] | Q15/17中期报告人组会议 |
| 2021-06-17 至 2021-06-18 | 电子会议 | [Q8/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12539&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3875)] | Q8/17中期报告人组会议 |
| 2021-06-24 至 2021-06-25 | 电子会议 | [Q4/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12534&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3877)] | Q4/17中期报告人组会议 |
| 2021-06-24 | 电子会议 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12575&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3878)] | Q10/17中期报告人组会议 |
| 2021-06-28 至 2021-06-29 | 电子会议 | [Q14/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12592&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3879)] | Q14/17中期报告人组会议 |
| 2021-07-01 至 2021-07-02 | 电子会议 | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12533&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-210824-TD-PLEN-3880)] | Q2/17中期报告人组会议 |
| 2021-10-05 | 电子会议 | [Q3/17[[会议报告](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en)]](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4199/en) | Q3/17中期报告人组会议 |
| 2021-11-19 | 电子会议 | [Q10/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12744&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4178)] | Q10/17中期报告人组会议 |
| 2021-11-24 至 2021-11-25 | 电子会议 | [Q2/17](http://www.itu.int/net/itu-t/lists/rgmdetails.aspx?id=12733&Group=17)[[会议报告](https://www.itu.int/md/T17-SG17-220107-TD-PLEN-4159)] | Q2/17中期报告人组会议 |
| 2022-01-20 至 2022-01-21 | 电子会议 | Q15/17[会议报告] | Q15/17中期报告人组会议 |
| 2022-02-07 | 电子会议 | Q3/17[会议报告] | Q3/17中期报告人组会议 |
| 2022-02-15 | 电子会议 | Q10/17[会议报告] | Q10/17中期报告人组会议 |
| 2022-02-17 | 电子会议 | Q6/17[会议报告] | Q6/17中期报告人组会议 |
| 2022-02-23 至 2022-02-24 | 电子会议 | Q2/17[会议报告] | Q2/17中期报告人组会议 |
| 2022 -02-?? | 电子会议 | Q4/17[会议报告] | Q4/17中期报告人组会议 |

# 2 工作的组织

## 2.1 研究的组织和工作的分配

**2.1.1** 在其本研究期的第一次会议上，第17研究组决定成立4个工作组。表2注明了每个工作组的编号和名称，以及分配给工作组的课题和2017至2020年间工作组正副主席的姓名。

表2

第17研究组工作的组织（2017-2020年）

| 分配给 | 待研究课题 | 工作组名称 | 主席和副主席 |
| --- | --- | --- | --- |
| PLEN | Q1/17； |  |  |
| WP1/17 | Q2/17；Q3/17；Q6/17；Q13/17(7)； | 电信/ICT 安全 | Miyake Yutaka 先生（主席） Dolmatov Vasiliy 先生（副主席） Evren Gökhan 先生（副主席） |
| WP2/17 | Q4/17；Q5/17；Q14/17(8)； | 网络空间安全 | Nakao Koji 先生（主席） Furey Inette 女士（副主席）(1) Gonzalez Juan 先生（副主席）(2) |
| WP3/17 | Q7/17；Q8/17；Q12/17； | 应用安全 | Taddei Arnaud 先生（主席） 林兆骥先生（副主席）(3) 白晓媛女士（副主席）(4) |
| WP4/17 | Q9/17；Q10/17；Q11/17； | 身份管理和认证 | 李克鹏先生（主席）(5) Nah Jae Hoon 先生（副主席/共同主席）(5, 6) 林兆骥先生（共同主席）(6) |

注：

(1) 担任副主席至2017年9月。

(2) 担任副主席至2018年3月。

(3) 担任副主席至2018年9月。

(4) 自2019年1月担任副主席。

(5) 担任主席/副主席至2018年9月

(6) 自2019年1月担任共同副主席。

(7) 第17研究组于2017年9月建立第13/17号课题。

(8) 第17研究组于2018年3月建立第14/17号课题。

**2.1.2** 由于全球爆发新冠肺炎疫情，原定于2020年举行的世界电信标准化全会（WTSA-20）推迟至2022年，2017-2020年研究期也相应延长至WTSA-20。在2020年8月/9月的会议上，第17研究组商定了12个课题请WTSA-20批准（见第2.2节），并为筹备下一研究期成立了一个任务组。

随着WTSA-20推迟至2022年3月，2021年1月11日至18日召开的TSAG会议认可了这组新SG17课题（参考[电信标准化局第295号通函](https://www.itu.int/md/T17-TSB-CIR-0295/en)）。在2021年4月20至30日的会议上，SG17同意将这一组12个课题形成一个由五个工作组构成的新结构。

表3给出了每个工作组的人数和名称，以及分配给工作组的课题和2021年工作组主席的姓名。

表3

第17研究组工作的组织（2021-）

| 分配给 | 待研究课题 | 工作组名称 | 主席和副主席 |
| --- | --- | --- | --- |
| WP1/17 | Q1/17；Q15/17； | 安全策略和协调 | 主席：  Dolmatov Vasily先生（俄罗斯）  副主席：  Kim Jonghyun先生（韩国） |
| WP2/17 | Q2/17；Q6/17；Q13/17； | 5G、物联网和人工智能和智能交通 系统（ITS）的安全性 | 主席：  Miyake Yutaka先生（KDDI）  副主席：  Hu Zhiyuan女士（诺基亚上海贝尔）  Mills Philip先生（英国） |
| WP3/17 | Q3/17；Q4/17； | 网络安全和管理 | 主席：  Nakao Koji先生（日本国家信息通信技术研究所（NICT））  副主席：  Molinari Lia女士（阿根廷） |
| WP4/17 | Q7/17；Q8/17；Q14/17； | 服务和应用安全 | 主席：  Nah Jae Hoon先生（韩国电子通信研究院（ETRI））  副主席：  Bai Xiaoyuan女士（阿里巴巴） |
| WP5/17 | Q10/17；Q11/17 | 基本安全技术 | 主席：  Lin Zhaoji先生（中兴通信）  副主席：  空缺 |

**2.1.3** 表4列出第17研究组在本研究期设立的其它组。

**2.1.4** 按照WTSA-16第54号决议，第17研究组在2017年3月会议上成立了第17研究组阿拉伯区域组；见第3.3.5节。

**2.1.5** 在本研究期内，由第17研究组提议的两个**联合协调活动（JCA）**继续进行，并得到TSAG的赞同。

**– 关于身份管理的联合协调活动（JCA-IdM）**

关于身份管理的联合协调活动（JCA-IdM）延续上一个研究期继续进行，其目的是协调ITU‑T身份管理（IdM）工作与外部机构的协作。JCA-IdM的主要成果见第3.3.4段。

**– 关于保护上网儿童的联合协调活动（JCA-COP）**

延续上一个研究期的、关于保护上网儿童的联合协调活动（JCA-COP）自2017年3月第17研究组的第一次会议停滞下来。

**2.1.6** 在本研究期内，两个**项目**由第17研究组继续进行。

**– ASN.1项目**

ASN.1是在2001-2004年研究期内设立的，旨在继续向ITU-T内部和外部现有的ASN.1（ITU-T X.680系列、X.690系列和X.890系列建议书）用户提供帮助，并在广泛的行业部门和标准机构中推广使用ASN.1。该项目的主要成果见第3.4.1段。

**– OID项目**

OID项目是在2001-2004年研究期内设立的，旨在继续向ITU-T内部和外部现有的根据X.660系列和X.670系列系列建议书注册的对象标识符的用户提供帮助和支持。该项目的主要成果见第3.4.2段。

表4

其它组（如有的话）

| 小组名称 | 主席 | 副主席 | |
| --- | --- | --- | --- |
| JCA-IdM | 共同主席： Barbir Abbie**先生**(1)、Park Keundug**先生**(1)、Takechi Hiroshi**先生**(1) 、Youm Heung Youl先生(8) |  |
| JCA-COP | 无 |  |
| SG17RG-AFR | Katundu Michael 先生(2) Njiraini Mwende 女士(3) | Elhaj **Mohamed先生(**2)**,** Mwesigwa **Patrick先生**(2)**,** Toure **Mohamed**先生(2) |
| SG17RG-ARB | Latrous Wala Turki女士(4)**,** Al Salehi Badar Ali Said先生(5) | Abdelkader Manel女士(6)**,** Abouche Chehrazed女士(6)**,** Almansoury Laial女士(7) |
| ASN.1项目 | 项目负责人：Thorpe Paul先生 |  |
| OID项目 | 项目负责人：Dubuisson Olivier先生 |  |

注：

(1) 自2017年3月担任共同主席。

(2) 直到2018年9月担任主席/副主席。

(3) 自2019年4月担任主席。

(4) 自2017年12月至2018年10月担任共同主席。

(5) 直到2017年12月担任（共同）主席。

(6) 自2017年12月至2018年10月担任副主席。

(7) 自2017年12月担任副主席。

(8) 自2021年4月起担任代理共同主席。

## 2.2 课题和报告人

**2.2.1** WTSA-16将表5中列出的以下12个课题分配给第17研究组，且第17研究组任命了所列出的本研究期的报告人和副报告人。

表5

第17研究组 – WTSA-16分配的课题和报告人（2017-2020年）

| 课题 | 课题的标题 | 工作组 | 报告人(19) |
| --- | --- | --- | --- |
| Q1/17 | 电信/ICT安全  协调 | PLEN | Latrous Wala女士（报告人）(13) Elhaj Mohamed M. K先生（报告人）(1) Ki Juhee女士（副报告人）(2) Najarian Paul先生（副报告人）(3) Senga Wataru先生（副报告人）(3) 王一雯女士（副报告人）(3) |
| Q2/17 | 安全架构和框架 | WP1/17 | 胡志远女士（共同报告人）(3) Oh Heung Ryong先生（共同报告人）(3) Chaabane Emna女士（副报告人）(10) Lee Jinmyung先生（副报告人）(16) |
| Q3/17 | 电信信息安全管理 | WP1/17 | Naganuma Miho女士（报告人）(3) 闵京华先生（副报告人）(7) Mustafa Thaib先生（副报告人）(5) Fischer Andres先生（副报告人）(4) |
| Q4/17 | 网络安全 | WP2/17 | Kadobayashi Youki先生（报告人）(6) Kim Jong-Hyun先生（报告人）(7) Sim Dong-Hi先生（副报告人）(2) 张晨先生（副报告人）(15) Casanovas Eduardo先生（副报告人）(4) |
| Q5/17 | 用技术手段打击垃圾信息 | WP2/17 | 张炎滨先生（报告人）(3) Kim ChangOh先生（副报告人）(3) |
| Q6/17 | 电信服务、网络和物联网的安全方面(17) | WP1/17 | Baek Jonghyun先生（共同报告人）3) 左敏女士（共同报告人）(14) 阎军智先生（共同报告人）(8) Lee Gunhee先生（副报告人）(9) Takahashi Takeshi先生（副报告人）(3) 俞播先生（副报告人）(3) Pazo Robles Maria Eugenia女士（副报告人）(4) |
| Q7/17 | 安全应用服务 | WP3/17 | Nah Jae Hoon先生（报告人）(3) 高枫女士（副报告人）(7) 刘立军先生（副报告人）(3) |
| Q8/17 | 云计算和大数据基础设施 安全(18) | WP3/17 | 魏亮先生（报告人）(3) Sang-Woo Lee先生（副报告人）(9) McFadden Mark先生（副报告人）(5) |
| Q9/17 | 生物特征 | WP4/17 | Caras John George先生（报告人）(3) 李克鹏先生（副报告人）(11) 王萌希女士（副报告人）(12) |
| Q10/17 | 身份管理架构和机制 | WP4/17 | Barbir Abbie先生（报告人）(3) Park Keundug先生（副报告人）(3) Takechi Hiroshi先生（副报告人）(3) 夏俊杰先生（副报告人）(3) |
| Q11/17 | 通用技术（目录、公共密钥（PKI），优势管理基础设施（PMI），抽象句法记法一（ASN.1），对象标识（OID））支持安全应用 | WP4/17 | Lemaire Jean-Paul先生（报告人）(3) Kaddachi Olfa女士（副报告人）(18) |
| Q12/17 | 电信软件和测试的形式语言 | WP3/17 | Hogrefe Dieter先生（报告人）(3) Mussbacher Gunter先生（副报告人）(5) Duhalde Enacom Martin先生（副报告人）(4) |

注：

(1) 任命于2019年9月5日。

(2) 任命于2019年1月30日。

(3) 任命于2017年3月30日。

(4) 任命于2017年3月30日，2018年3月29日离任。

(5) 任命于2017年9月6日。

(6) 任命于2017年3月30日，2018年3月29日解聘（再分配）

(7) 任命于2018年3月29日。

(8) 任命于2019年1月30日。

(9) 任命于2018年9月7日。

(10) 任命于2017年3月30日，2018年9月7日离任。

(11) 任命于2017年3月30日，2018年9月7日辞职。

(12) 任命于2017年9月6日，2018年9月7日离任。

(13) 任命于2017年3月30日，2018年1月离任。

(14) 任命于2017年3月29日，2019年1月30日离任。

(15) 任命于2018年9月7日。

(16) 任命于2017年9月6日，2018年9月7日离任

(17) 第6/17号课题的标题从“电信业务和网络的安全问题”改为“电信业务、网络和物联网的安全问题”。

(18) 第8/17号课题的标题从“云计算的安全”改为“云计算和大数据基础设施的安全”。

(19) 任命于2021年4月20日生效

**2.2.2** 随着WTSA-20推迟至2022年3月，2021年1月11日至18日召开的TSAG会议认可了这组新SG17课题。SG17在2020年8月/9月召开的会议上批准了表5a中所列课题（参考[电信标准化局第295号通函](https://www.itu.int/md/T17-TSB-CIR-0295/en)）。

**表5a**

第17研究组 –TSAG批准的课题（自2021年1月18日起）

| **新序号** | **新课题标题** | **状态** | **原序号** | **先前的课题标题** | **工作组** | **报告人(1)** |
| --- | --- | --- | --- | --- | --- | --- |
| 1/17 | 安全标准化策略和协调 | 继续 | 1/17 | 电信/ICT安全协调 | WP1/17 | 共同报告人：  - Elhaj Mohamed M. K先生 - Ki Juhee女士  副报告人： - Najarian Paul先生 - Senga Wataru先生 -王一雯女士 |
| 2/17 | 安全架构和网络安全 | 继续 | 2/17 | 安全架构和框架 | WP2/17 | 共同报告人：  - 胡志远女士 - Oh Heung Ryong先生 |
| 3/17 | 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 | WP3/17 | 报告人：  - Naganuma Miho女士  副报告人：  -闵京华先生 - Mustafa Thaib先生 |
| 4/17 | 网络安全和打击垃圾邮件 | 4/17和5/17号课题的继续 | 4/17 | 网络安全 | WP3/17 | 共同报告人：  - Kim Jong-Hyun先生 - 张炎滨先生  副报告人：  - Kim ChangOh先生 |
| 5/17 | 利用技术手段打击垃圾信息 |
| 6/17 | 电信服务和物联网的安全 | 继续 | 6/17 | 电信业务、网络和物联网的安全问题 | WP2/17 | 共同报告人：  - Baek Jonghyun先生  - 阎军智先生  副报告人：  - Lee Gunhee先生 - Takahashi Takeshi先生 - 俞播先生 |
| 7/17 | 安全应用服务 | 继续 | 7/17 | 安全应用业务 | WP4/17 | 报告人：  - Nah Jae Hoon先生  副报告人：  - 高枫女士  - 刘立军先生 |
| 8/17 | 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的安全 | WP4/17 | 报告人：  - 魏亮先生  副报告人：  - McFadden Mark先生 |
| 10/17 | 身份管理和远程生物识别的架构和机制 | 9/17和10/17号课题的继续 | 9/17 | 远程生物识别 | WP5/17 | 共同报告人：  - Barbir Abbie先生 - Caras John George先生  副报告人：  - Kim Jason先生 - Park Keundug先生 - Takechi Hiroshi先生 - 夏俊杰先生 |
| 10/17 | 身份管理架构和机制 |
| 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） | 11/17和12/17号课题的继续 | 11/17 | 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）、抽象语法记法一（ASN.1）、对象标识符（OID）） | WP5/17 | 报告人：  - Lemaire Jean-Paul先生  副报告人：：  - Hogrefe Dieter先生 |
| 12/17 | 电信软件和测试的形式语言 |
| 13/17 | 智能交通系统的安全 | 继续 | 13/17 | 智能交通系统安全方面 | WP2/17 | 报告人：  - Lee Sang-Woo先生  副报告人：  - Park Seungwook先生  -张屹女士 |
| 14/17 | 分布式账本技术（DLT）的安全 | 继续 | 14/17 | 分布式账本技术的安全问题 | WP4/17 | 共同报告人：  - Kadobayashi Youki先生 - Oh Kyeong Hee女士  副报告人： - 白晓媛女士 - 王珂女士 |
| 15/17 | 新兴技术的安全性，包括基于量子的安全性 | 新课题 | – | – | WP1/17 | 报告人：  - Sim Donghee先生  副报告人：  - Kenyoshi Kaoru先生 - Yoon ChunSeok先生 - 张晨先生 |

(1) SG17在2021年4月20-30日的会议上重新任命

**2.2.3** 表5b所列课题在本研究期期间已获得通过。

**表5b**

第17研究组 – 通过的新课题以及报告人

| 课题 | 课题的标题 | 工作组 | 报告人 |
| --- | --- | --- | --- |
| Q13/17 | 智能交通系统的安全方面**(10)** /智能交通系统（ITS）的安全性**(11)** | WP1/17**(10) /** WP2/17**(11)** | Lee Sang-Woo先生（报告人）(1) Park Seungwook先生（副报告人）(1) 张屹女士（副报告人）(2) |
| Q14/17 | 分布式账本技术的安全方面**(10)** /分布式账本技术（DLT）**(11)** | WP2/17**(10) /** WP3/17**(11)** | Kadobayashi Youki先生（共同报告人）(3) Oh Kyeong Hee女士（共同报告人）(3) 白晓媛女士（副报告人）(4) 王珂女士（副报告人）(4)  左敏女士（副报告人）(5) |
| Q15/17 | 新兴技术的安全性，包括基于量子的安全性 | WP1/17**(11)** | Sim Dong-hi先生（报告人） **(6)**  Kenyoshi Kaoru先生（副报告人）**(7)**  Yoon Chun Seok先生（副报告人） **(8)**  张晨先生（副报告人）**(9)** |

注：

(1) 任命于2017年3月30日。

(2) 任命于2018年9月7日。

(3) 任命于2017年9月6日。

(4) 任命于2018年3月29日。

(5) 任命于2017年9月6日，2018年3月29日解聘（再分配）。

(6) 任命于2021年4月20日。

(7) 任命于2021年4月20日。

(8) 任命于2021年4月20日，负责孵化任务。

(9) 任命于2021年4月20日。

(10) 2017-2020年

(11) 2021-2022年

**2.2.4** 表6中列出的课题在此研究期内已并入SG17的其它课题。

表6

第17研究组 – 删除的课题

| 课题 | 课题的标题 | 报告人 | 注 |
| --- | --- | --- | --- |
| Q5/17（已取消） | 通过技术手段打击垃圾邮件 | 张炎滨先生（报告人） Kim ChangOh先生（副报告人） | TSAG 2021年1月18日，经TSAG认可，Q5/17与Q4/17合并 |
| Q9/17（已取消） | 远程生物识别 | Caras John George（报告人） | 2021年1月18日，经TSAG认可，Q9/17与Q10/17合并 |
| Q12/17（已取消） | 电信软件和测试的形式语言 | Hogrefe Dieter先生（报告人） Mussbacher Gunter先生（副报告人） | 2021年1月18日，经TSAG批准，Q12/17与Q11/17合并 |

3 2017-2020年研究期实现的工作成果

## 3.1 概述

在直到2022年1月会议的研究期内，第17研究组审查了大量文稿和迟到文稿（TD）及联络声明。

基于这些文件，第17研究组于2022年1月7日：

– 起草了53份（AAP）+47份（TAP）新建议书；（3份采用TAP方式批准的建议书已确定）

– 修订了93份（AAP）+3份（TAP）现有建议书；

– 修正了4份建议书；

– 起草了8份新建议书增补，一份经修订的增补和一份对现有增补的勘误；

– 制定了17份技术勘误；

– 起草了2份技术文稿以及6份技术报告（未编写任何手册）。

在直到2022年1月电子会议的研究期内，第17研究组：

– 吸引了2163（2063+100）位与会者（以往的会议：100、223、231、91、262、69、225、206、178、168、130、134、146）

– 建立了162个新的工作项目（以往的会议：7、15、0、15、7、26、13、25、21、26、7）

– 收到179份文稿（以往的会议：1、98、104、2、110、121、151、118、144、113、106、78）

– 产生了4220份临时文件（以往的会议：106、336、305、44、434、35、439、508、380、420、395、426、368）

– 收到585份输入联络声明并拟定了328发出的联络声明（以往的会议：55+1、51+23、36+17、21+0、58+32、1+2、77+24、64+42、47+30、40+37、46+37、49+40、40+38）

## 3.2 主要成果

现将分配给第17研究组的各项课题方面所取得的主要成果简介如下：

对课题的正式答复见本报告附件1中的提要表。

a) 第1/17号课题：电信/ICT的安全协调（2017-2020年）/安全标准化策略与协调（2021-）

第1/17号课题充当第17研究组内和与其他研究组以及组织外部有关电信/ICT安全事项协调的联系方。第1/17号课题制定和充实完善了ITU‑T认为对促进其安全工作和实际成果有价值的宣传、推广和参考文件示例包括：

– 题为《电信和信息技术安全 – 关于电信安全的若干问题综述及ITU-T现有建议书应用简介》的安全手册重点介绍了ITU-T研究组的主要安全工作。在本研究期内第1/17号课题拟定了手册第七版。

– 《关于成功使用安全标准的技术报告》侧重于如何成功部署经批准的与安全相关的ITU-T建议书。单个建议书（如ITU-T X.805）和系列建议书（如CYBEX）都经过审议并描述了使用它们可能获得的潜在好处。在本研究期第1/17号课题拟定了第二版。

– ICT安全标准路线图包含一个在线可搜索数据库，其中包含来自ITU-T研究组和外部标准制定组织的2600多项经批准的ICT安全标准包括3D@home、3GPP、3GPP2、ATIS、ETSI、IEEE、IETF、ISO/IEC JTC 1、OASIS、oneM2M、SmartBan和TETRA。在本研究期第1/17号课题批准了许多更新。

– 安全建议书大全在第一部分中提供了经批准的ITU-T电信安全建议书目录；第二部分为经批准的ITU-T安全定义摘要。在本研究期该《大全》在每次召开的第1/17号课题的会议上都经过更新。

针对第17研究组的所有课题、其他与安全问题相关的研究组和从事ICT安全标准工作的外部标准制定组织之间的协调已经建立。

第1/17号课题协助举办了6场国际电联讲习班。第1/17号课题还促进举办安全讲习班支持第17研究组两个区域组（非洲和阿拉伯）并通过创建模板、工具和流程提高了第17研究组的工作效率。在本研究期第1/17号课题于2021年底协助国际电联举办了13次国际电联讲习班。

b) 第2/17号课题：安全架构和框架（2017-2020年）/安全架构和网络安全（2021-）

第2/17号课题开发一套全面的安全架构和框架建议书为电信提供标准的安全解决方案。其内容包括5G的安全性以及软件定义网络、长期演进语音和网络虚拟化的安全框架。

本研究期内第2/17号课题制定了八份新建议书和一份新增补：

– X.1011 – 持续保护服务访问过程的导则 – 分析了服务访问过程面临的安全威胁，指明了检测异常访问活动的安全保护措施，并引入了增强的服务访问授权机制。

– X.1040 – 电子商务业务数据生命周期管理安全参考架构 *–* 分析电子商务服务生态系统面临的主要特征和典型威胁，为电子商务业务数据生命周期管理提供安全参考架构。

– X.1041 – 长期演进语音网络（VoLTE）运营的安全框架 *–* 分析VoLTE网络面临的安全威胁并为电信运营商提供确保安全运营的对策建议。它还为VoLTE网络提供了一个安全参考框架。

– X.1043 – 基于软件定义网络的服务功能链接的安全框架和要求 – 分析了基于软件定义网络的服务功能链接的安全威胁，并规定了其安全要求。并给出了相应的安全对策。ITU-T X.1043建议书亦旨在帮助理解在使用基于安全数据网的服务功能链和实施基于安全数据网服务功能链时遇到的安全风险。

– X.1044 – 网络虚拟化的安全要求 *–* 分析了网络虚拟化（NV）的安全挑战和威胁并规定了网络虚拟化中物理资源层、虚拟资源层和逻辑隔离网络分区层（LINP）的安全要求。

– X.1045 – 网络和应用的安全服务链架构 *–* 支持为网络和应用提供定制的动态和自适应安全服务。本建议定义了安全服务链和安全服务链的架构设计。本建议将安全服务链应用于网络和应用。此建议书还支持在高性能的服务功能链（SFC）覆盖网络中跟踪网络攻击及其资源，并自动减轻/防止这些攻击。

– X.1046 – 软件定义网络/网络功能虚拟化网络中的软件定义安全框架 *–* 规定了软件定义安全框架 – 软件定义网络（SDN）和网络功能虚拟化（NFV）网络。该建议书分析了运营商基于SDN/NFV的网络中的主要安全挑战，包括技术和操作方面。该建议书定义了安全要求以解决SDN/NFV网络中的这些挑战。该建议书引入了“软件定义的安全性”的概念，并设计了“软件定义的安全性”的框架。该建议书对软件定义安全性的实施做出规定。

– X.1047 – 网络切片管理和编排的安全要求和体系架构 – 制定了网络切片管理和编排的安全要求和体系结构，同时对自动创建具有定制安全功能的端到端（E2E）网络切片做出了规定以便消费者、企业和政府部门能够部署全面的E2E网络切片。

– ITU-T X.805 X.Suppl.30 – 移动虚拟网络安全导则 *–* 为移动虚拟网络运营商（MVNO）提供了安全导则。安全性对MVNO非常重要，大多数MVNO都有很多安全性相似之处。该增补分析了MVNO的主要特征及其面临的典型安全威胁。该增补基于MVNO的结构为MVNO提供了一个安全框架，包括安全目标和安全要求。

c) 第3/17号课题：电信信息安全管理（2017-2020年）/电信信息安全管理和安全服务（2021-）

第3/17号课题制定有关电信信息安全管理的建议书，如用于电信组织、中小电信企业的PII行为守则。

在本研究期内，第3/17号课题制定了五份新建议书、一份勘误、两份经修订的和三份新的增补：

– X.1051（修订版）勘误1 – 信息技术 – 安全技术 – 电信组织在ISO/IEC 27002基础上进行信息安全控制的行为守则。

– X.1052（修订版） – 电信机构的信息安全管理流程 – 为电信机构的信息安全管理提供了最佳实践信息，可为ITU-T X.1051建议书提供支持。此建议书是基于阐述一组安全管理领域的流程方法，为电信组织实现ITU-T X.1051建议书定义的控制目标提供了指南。上述管理领域包括资产管理、事件管理、风险管理策略管理，并与ITU-T X.1051建议书定义的控制建立了对应关系，从而能够提供相关方法。

– X.1053 – 基于ITU-T X.1051的中小型电信组织信息安全控制行为守则 – 根据ITU-T X.1051建议书建立了在中小型电信组织中启动、实施、维护和改进信息安全控制的导则和一般原则。该建议书还为中小型电信组织提供了信息安全控制的实施基准 以确保电信设施和服务以及由设施和服务处理、处理或存储的信息的机密性、完整性和可用性。

– X.1058 – 信息技术 – 安全技术 – 个人可识别信息保护行为准则 – 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。特别是该规范基于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。

– X.1059 – 电信组织全球可接入知识产权网络资产风险管理实施指南 *–* 为电信组织全球可接入知识产权网络资产的风险管理提供指导，这些资产直接暴露给黑客和攻击者。这些资产也可能连接到传统电信网络的传统（甚至旧）资产，这些传统电信网络可能具有一些难以修复的设计级漏洞。因此，将电信组织的基于IP的网络（AGIT）中的所有全球可接入资产视为一个整体，并引入一些特定的安全控制措施以不断降低总体风险并加强电信服务和网络的总体安全性将是切实可行的。

– X.1060 – 创建和运营网络防御中心的框架 *–* 将网络防御中心（CDC）定义为在组织中发挥核心作用以应对网络安全风险的一个实体。CDC应实际实施的三个过程（建造、管理和评估）被描述为一个框架。此外，还提供了某组织为实施更具体的网络安全措施而应提供的服务。

– X.1061–信息通信技术服务（ICT）提供商网络保险收购导则。本网络保险收购导则为将网络保险作为风险处理方案，藉此对网络安全事件影响进行管理的组织提供对网络保险覆盖范围的理解，并提出了对网络安全风险评估、保险人的选择、保险人评估和对保险人进行评估的要求。

– ITU-T X.1051 X.Suppl.13（修订版）– 信息安全用户导则。

– ITU-T X.1058 X.Suppl.32 *–* 电信组织个人可识别信息保护的行为守则 *–*  旨在通过为个人可识别信息（PII）保护提供额外的实施指南补充ITU-T X.1058中提供的信息，ITU-T X.1058中未对此进行描述，但应进一步适用于电信组织，以解决PII保护问题。

– ITU-T X.1051 X.Suppl.34 *–* 电信机构信息安全控制行为守则 – 强调并分享马来西亚信息和通信业根据ITU-T X.1051 建议书实施信息和网络安全管理行为守则的情况。

– X.Suppl.36、ITU-T X.1051–电信机构信息和网络安全管理的关键安全控制方法–在ITU-T X.1051建议书的范围内，利用关键安全控制方法提供网络安全管理的最佳实践。关键安全控制（CSC）框架和相关关键安全控制方法的使用是对ITU-T X.1051建议书的支持和补充。

Q3/17在信息安全管理方面与ISO/IEC JTC 1/SC 27/ WG 1密切配合。

d) 第4/17号课题：网络安全（2017-2020年）/网络安全和打击垃圾邮件（2021-）

第4/17号课题就网络安全框架和电信/ICT提供商如何保护其基础设施和维持安全运行以及交流网络安全信息的要求制定了建议书。在本研究期，第4/17号课题还在2020年整合了孵化功能，以解决新出现的问题，如量子环境中的安全性并于2021年1月将此职能转至第15/17号课题。同样在2021年1月，第4/17号课题承担了之前正由第15/17号课题开展研究的打击垃圾邮件的工作。

在本研究期内，第4/17号课题制定了14份新建议书、一份份修订建议书、两份新修正案、两份新的技术文稿和两份新的技术报告：

– X.1212 – 增强最终用户对可信指示符的感知的设计考虑 – 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。

– X.1213 – 对于反击基于智能手机的僵尸网络的安全能力要求 – 分析基于智能手机的网络僵尸的背景和潜在的安全威胁 并提供安全能力需求。

– X.1214 – 电信/信息通信技术网络的安全评定技术手段 *–* 向电信领域的开发者、制造商、运营商和个人安全专家描述了针对基于软件的电信/信息通信技术（ICT）网络元素的安全评定方法和最佳做法，以解决其基于软件的元素的安全问题。传统的电路交换网络和基于分组的网络皆面临来自外部和内部的、以电信/ICT网络各个部分为目标的不同威胁与攻击。在电信/ICT网络中，该建议书涉及薄弱环节的发现以及安全性评定方法两个方面。

– X.1215 – 结构化威胁信息表达式的用例 *–* 提供了结构化威胁信息表达式（STIX）语言如何用于支持网络威胁情报（CTI）和信息共享的各种用例。

– X.1216 – 收集和保存网络安全事件证据的要求 – 阐述了网络安全事件响应和调查的一般程序。此建议书分析了网络安全事件证据的来源，并规定了调查过程中用于收集和保存此类证据的工具的能力要求。本建议书还规定了这些工具的可靠性保证要求，作为工具设计开发人员指南。

– X.1217 – 电信网络运营中的威胁情报使用导则 – 从电信运营商的角度来看，威胁情报是经过组织、分析和提炼的关于可能威胁某个组织的潜在和当前攻击的信息集合。这些信息还可以包括攻击者的动机、意图、特征和方法，以及他们的操作方式或技术、战术和程序。在网络和信息安全领域，大规模突发网络安全事件的发生引发了对威胁情报的迫切需求。威胁情报可以帮助一个组织降低风险、提高整体安全性。已经定义了威胁情报的统一分类、语法和表示，以便不同组织之间可以共享威胁情报。此建议书规定了在进行概述分析后，电信网络运营使用威胁情报的导则。

– X.1218 – 沙箱环境中动态恶意软件分析的要求和指南 – 未知恶意软件通常用于高级攻击 特别是高级持续威胁（APT），以避免被发现。例如，使用以未知恶意软件为武器的网络钓鱼电子邮件进行有针对性的攻击，可以轻松实现成功的初次破坏。因此，为了发现高级攻击，应采取特别的注意和防御措施来发现未知恶意软件。ITUT-T X.1218建议书分析与未知恶意软件相关的威胁，并基于动态行为分析规定了未知恶意软件发现方面的要求。

– X.1233 – 打击通过即时消息传播的垃圾邮件的导则规定了即时消息（IM）服务提供商和用户打击即时消息垃圾邮件（SPIM）、以减少SPIM在网络空间的传播并改善即时消息用户体验的指导原则。为即时消息服务提供商指定了应对SPIM的技术措施和机制，并为IM用户提供了应对SPIM的建议。

– X.1234 – 关于打击多媒体消息服务（MMS）垃圾信息的导则规定了关于打击MMS垃圾信息的导则。建议书对MMS垃圾信息的典型场景、特性和识别方法做出分析，提供MMS垃圾信息识别技术框架、工作程序和一些关键性技术，以帮助MMS提供商和MMS用户对抗垃圾信息。

– X.1235 – 电信组织打击网站欺骗的技术为电信机构及时识别网站欺骗并保护其网站不受欺骗推荐相关技术。

– X.1500建议书修正11和12 –网络安全信息交流概况 – 提供了一系列结构化网络安全信息技术手段。这些技术随着技术演变和扩展不断得到更新、扩大、重新确定和取代。上述一系列技术在建议书正文的概述后提供。这些修正案反映了建议技术分别截至2017年3月和2018年3月的情况，包括参考资料。

– X.1541（修订版） – 事件对象描述交换格式（版本2）*–* 阐述了事件对象描述交换格式（IODEF）（版本2），提供了用XML规定的相关数据模型。事件对象描述交换格式（IODEF）规定了一种数据模型表示法，可用于共享通常交换的有关计算机安全或其它类型事件的信息。这是通过列出IETFREC 7970的相关段落和说明它们属于规范性还是资料性实现的。

– X.1550 – 事件交换网络的访问控制模型 *–* 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。

– X.1702 – 量子噪声随机数生成器架构规范 *–* 定义了量子熵源的通用功能架构、评估和验证所评估噪声源熵的通用方法，以及当随机提取程序为实现系统的组成部分时，指定随机提取程序的通用方法。

– X.1710 – 量子密钥分发网络安全框架 – 规定的框架中包括为应对量子密钥分发网络（QKDN）安全威胁提出的要求和措施。此框架规定了一个简化的QKDN结构，用于分析相关的安全威胁。接下来在此基础之上规定了安全要求和相应的安全措施。

– X.1714 –量子密钥分发网络的密钥组合和机密密钥供应 – 描述了量子密钥分发网络（QKDN）的密钥组合方法，并规定了密钥组合的安全要求以及从QKDN到加密应用密钥供应的安全要求。

– TP.inno – 孵化机制描述及改进方法 – 描述了由第17研究组建立的整个孵化机制。以更及时的方式处理创新。然后，该建议书列举了国际电联和其他标准制定组织接受创新的其他方式和机制。

– TP.sgstruct – 安全研究转型的战略方法 – 涵盖了安全研究转型的短期、中期和长期方面。

– TR.sec-qkd – 量子密钥分发网络的安全考虑 – 从电信网络的角度开发了一个QKD框架以满足需求。

– TR.usm – 统一安全模型 – 一种中立的网络安全集成系统方法，呈现了一种通用的“一切与安全有关”的架构，具有中立性和不可知性。此方法具有推动实现安全控制大规模互操作和安全响应自动化的潜力。

在本研究期，第4/17号课题于2019年1月24日在日内瓦举办了一次关于安全量子通信的小型讲习班。

e) 第5/17号课题：以技术手段打击垃圾信息（2017-2020年）

第5/17号课题制定通过技术手段抵制垃圾信息的建议书，如抵制广告垃圾、抵制即时消息垃圾信息、抵制移动应用程序内广告垃圾信息、抵制短信服务网络钓鱼和恶意攻击以及抵制电话服务欺诈。

在本研究期内，第5/17号课题制定了三份新建议书和两份新增补：

– X.1232 – 打击用户生成信息中的广告垃圾信息的技术框架 – 分析广告垃圾的场景和特征，并指定参考框架和处理流程帮助互联网服务提供商打击广告垃圾信息。

– X.1248 – 打击垃圾即时消息的技术要求 – 定义了垃圾即时消息的特征，并详述了打击垃圾即时消息（SPIM）的技术要求。随着即时通讯（IM）的普及，垃圾即时消息扩散的问题日益严重。即时通讯的特点（例如基于网际协议（IP）、应用广泛、免费使用）很大程度上导致了垃圾即时消息广泛地、肆无忌惮地传播。如果垃圾即时消息问题未得以认真解决，可能会对即时消息服务本身的使用产生负面影响。

– X.1249 – 打击手机应用内植入的广告垃圾信息的技术框架 – 提供了一个打击手机应用内植入广告垃圾信息的技术框架。手机应用内植入广告垃圾信息是指手机应用内显示的强行推介的广告。这类强行推介的广告会以屏幕上方或下方的横幅、移动插页广告和重叠式广告等形式出现在移动装置显示屏上。

– ITU-T X.1242X.Suppl.29 – 打击钓鱼短信和钓鱼短信攻击的导则的增补 *–* 提供关于短信服务（SMS）网络钓鱼的通用指南。网络钓鱼是一种通过手机进行的欺诈技术，通过智能手机引发网络钓鱼欺诈，获取智能手机上的个人信息，或者在账户持有人在对核准不知情的情况下批准并支付少量款项。

– ITU-T X.1231 X.Suppl.33 – 打击电话诈骗的技术框架的增补 *–* 为打击电话服务诈骗提供技术框架和相关最佳做法。在该框架中，规定了实体功能和处理程序。最佳做法涵盖那些在阻止已知电话服务诈骗方法方面最有效的做法。

f) 第6/17号课题：电信业务、网络和物联网的安全问题（2017-2020年）/电信业务和物联网的安全（2021-）

第6/17号课题针对电信业务、移动网络、智能电网网络、IPTV和物联网的安全要求和框架制定建议书。

在本研究期内，第6/17号课题制定了17份新建议书、一份修正案和一份对现有增补的勘误。

– X.1042 – 使用软件定义网络的安全业务 – 支持对使用基于软件定义网络（SDN）安全业务的网络资源形成保护。首先，本建议书对基于SDN的安全业务网络资源进行分类：SDN应用、SDN控制器、SDN交换机和安全管理器（SM）。之后，ITU-T X.1042建议书对基于SDN的安全业务作出规定。

– X.1126 – 减缓移动网络中受感染终端负面影响的导则 – 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。

– X.1127 – 手机防盗措施的功能安全性要求和架构 – 以全球移动通信系统协会（GSMA）描述的一般要求为基础，主要讨论智能手机防盗机制功能安全性要求和功能架构。

– X.1197修正案1 – 选择用于IP电视服务和内容保护的加密算法的标准导则 – 更新附录一和附录二，以反映截至2019年8月的最新情况，包括参考书目。

– X.1331 – 智能电网系统中家域网（HAN）设备的安全导则 – 对智能电网中的家域网所面临的威胁进行分析，说明安全性要求和安全功能。由于每个家域网设备的作用和功能皆不相同，所以按设备分别介绍了它们的安全性要求和安全功能。

– X.1332 *–* 智能电网系统中智能电表业务的安全导则 *–* 为智能计量服务提供安全指南，以便服务提供商能够正确实施安全措施，从而确保服务的安全性。从服务水平的角度分析了智能计量服务的一般模型。基于通用模型，该建议书讨论了针对智能计量服务的安全威胁和攻击方法，并确定了安全要求和降低这些风险的能力。此外，该建议书引入了有用的安全标准，当服务提供商实现安全功能时可以考虑这些标准。

– X.1333 – 在联网控制系统中使用远程访问工具的安全导则，描述安全使用远程访问工具（RAT）进行监测、控制和维护的整体情况。

– X.1361 – 基于网关模型的物联网安全框架 – 描述了使用安全网关的物联网（IoT）的安全框架。物联网是信息社会的一种全球基础设施，基于现有的和正在出现的、可互操作的信息和通信技术，通过（物理和虚拟）之物的相互连接，提供先进的服务。本建议书分析物联网环境中面临的安全威胁和挑战，并阐明可解决和减缓这些威胁和挑战的能力。本建议书提供的框架方法用于确定在减缓和解决物联网的这些安全威胁和挑战中所需的安全能力。

– X.1362 *–* 物联网（IoT）环境的简单加密程序 – 规定物联网（IoT）设备的、带有相关掩膜数据的加密（EAMD）。该建议书具体阐明EADM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。

– X.1363 – 物联网（IoT）环境下处理个人可识别信息（PII）的技术框架 – 规定了在物联网环境下通过一个或多个服务提供商处理个人可识别信息的技术框架。

– X.1364 – 窄带物联网的安全要求和框架 *–* 阐述了针对NB-IoT部署的安全威胁和要求，从而为运营商建立了安全框架，以保护这些新技术应用。

– X.1365 – 在电信网络上使用基于身份的密码来支持物联网（IoT）服务的安全方法 – 为支持包括身份管理、密钥管理架构、密钥管理操作和鉴权机制在内的电信网上的物联网服务的IBC公钥技术的使用提供了一种安全方式。

– X.1366 – 物联网环境的汇集消息认证方案 – 规定了两种消息认证方案。一种是将物联网作为基本机制的物联网汇集消息认证（AMA）方案。另一种是以轻量和安全的方式、采用交互协议的交互式汇集消息认证（IAMA）方案。两种汇集消息认证方案均可用于确保“实体（身份）认证”以及确保“消息认证”。

– X.1367 *–* 物联网安全事件操作的错误日志标准格式 – 规定了一种标准化的、可置于协议有效载荷中的错误日志格式（例如syslog）（见IETF RFC 5424），用于将边缘设备发出的错误日志信息转换为标准的错误日志格式。此建议书还对标准化的错误代码表做出规定以解决第二个问题。因此，可以对计算机网络和物联网边缘设备网络之间的安全事件进行整合管理。

– X.1368 – 物联网设备的安全固件或软件更新 – 规定：1) 安全更新物联网（IoT）设备固件或软件（FW/SW）的基本模型和程序；2) 更新物联网固件的要求和能力。

– X.1369 – 物联网服务平台的安全要求 – 规定了物联网服务平台的安全要求。它评估了物联网业务服务平台面临的安全威胁和挑战 并描述了可以缓解安全威胁和挑战的安全措施。

– X.1453 – 视频管理系统的安全威胁和要求 – 分析了运行在IP网络上的、基于服务器平台的视频管理系统（VMS）面临的安全威胁，并对抵制已确定安全威胁的安全要求做出具体规定。

– X.1811 – 在IMT-2020系统中应用量子安全算法的安全导则 – 通过评估当前使用的加密算法的安全强度，确定量子计算对国际移动通信-2020（IMT-2020）系统带来的威胁。本建议书简要回顾了量子安全算法（包括对称和非对称类型），并提供了在IMT-2020系统中应用量子安全算法的导则

– ITU-T X.1111 X.Suppl.26 勘误1 – 关于使用电信网络的智能电网服务安全功能架构的增补。

g) 第7/17号课题：安全应用服务

第7/17号课题制定关于诸如增值服务和金融技术（Fintech）服务等安全应用服务的安全要求的建议书。

在本研究期内，第7/17号课题制定了九份新建议书：

– X.1145 *–* 电信服务开放能力的安全框架和要求 – 侧重对电信业务开放能力的安全性要求进行分析，并提供了一个安全框架。

– X.1146 *–* 电信运营商提供的增值服务的安全保护导则 – 为电信运营商提供的增值服务提供了安全保护导则。除分析了典型的服务情形、安全威胁和攻击方法外，ITU-T X.1146建议书还提供了应对威胁和攻击的技术措施。这将有助于运营商确保增值服务的安全，还将包含用户的利益。

– X.1147 *–* 移动互联网服务大数据分析的安全要求和框架 *–* 将分析移动互联网服务大数据分析的安全要求并提供安全框架。

– X.1148 – 电信服务提供商的去身份识别进程框架 *–* 阐述了去身份识别的进程框架，基于数据生命周期模型、利益攸关方的作用，为电信业务提供商给出了去身份识别进程的操作步骤并规定了数据释放模型和数据阶段。

– X.1149 – 金融技术（FinTech）服务的开放平台架构 – 阐述了金融技术（FinTech）服务的开放平台架构，开放平台的威胁和漏洞，金融技术服务开放应用程序接口（API）的使用程序，以及金融公司和金融技术公司对金融技术服务开放平台的详细安全要求。该建议书的附录包括一些拟议开放平台的用例。

– X.1450 – 客户端 – 服务器模型中混合认证和密钥管理机制的指南 – 提供了客户端 – 服务器模型中混合认证和密钥交换机制的指南。底层机制建议使用共享秘密和公钥技术进行认证和密钥交换。该建议书涵盖服务情形、安全威胁以及减轻此类攻击的方法。

– X.1451 – 风险识别优化用户认证 – 规定了作为调用认证功能前的预处理器对ICT服务系统中风险识别功能的启用。有了这种特定风险识别功能，ICT服务系统可以根据用户的需求以自适应的方式选择认证机制并实现多种好处，例如：1) 改善用户体验；2) 增加容量并降低用户认证的单位交易成本；以及3) 降低用户身份伪造的风险。

– X.1452 – 运营商提供的安全业务导则 –对运营商所提供安全服务的潜在使用案例进行分类，并分析对安全服务的具体要求，为运营商维护和改善其安全服务提供指导原则。

– X.1470 – 网络在线客服安全导则 – 从网络安全、系统安全、服务安全三个方面分析了网络在线客服面临的安全威胁。此建议书规定了基于网络的在线客户服务的安全导则和相应的安全措施。书中还提出了测试程序，用以验证相应安全措施是否满足规定的安全要求。

h) 第8/17号课题：云计算和大数据基础设施的安全

第8/17号课题制定有关云计算和大数据基础设施安全威胁和要求的建议书。

在此研究期，第8/17号课题制定了八份新的建议书：

– X.1603 – 云计算监测业务的数据安全性要求 *–* 分析了云计算监测业务的数据安全性要求，包括监测数据范围要求、监测数据生命周期、监测数据采集的安全性要求和监测数据存储的安全性要求。

– X.1604 – 云计算中网络即服务（NaaS）的安全要求 – 分析了云计算中网络即服务（NaaS）面临的安全威胁和挑战，并根据相应的云能力类型，从NaaS应用、NaaS平台和NaaS连接等方面对NaaS的安全要求进行了详细说明。

– X.1605 – 云计算中公共基础设施即服务（IaaS）的安全要求 – 旨在记录公共IaaS的安全要求，以帮助IaaS提供商在整个规划、建设和运行阶段提高IaaS平台的安全性。

– X.1606 – 通信即服务应用环境的安全要求 – 识别安全威胁，并针对通信即服务（CaaS）的应用环境提出了有关安全要求的建议。本建议书阐述了包含多种通信能力的CaaS场景和特征。接下来，建议书确定了由独特CaaS特性引发的特定威胁，并就CaaS安全要求提出了适当的建议。

– X.1643 – 云计算环境中虚拟化容器的安全导则 – 分析了云计算环境中虚拟化容器面临的安全威胁和挑战，并为云中虚拟化容器规定了一个包括安全导则的参考框架。

– X.1750 – 面向大数据服务提供商的大数据即服务安全导则 – 分析大数据即服务（BDaaS）面临的安全挑战、确定提供BDaaS的安全方面作用和责任以及大数据基础设施的安全框架。该建议书还规定了与BDaaS相关的服务和构成成分应满足的安全保护措施。

– X.1751 – 电信运营商大数据生命周期管理安全导则 –分析了安全漏洞并为电信运营商的大数据生命周期管理制定安全导则。该建议书介绍电信大数据业务的具体特性和数据类别，分析大数据生命周期管理的安全漏洞，并为电信运营商具体提出安全导则。

– X.1752 – 大数据基础设施和平台的安全导则 – 分析了大数据基础设施和平台的安全威胁和挑战，并规定了一个参考框架，以针对大数据基础设施和平台的威胁制定安全导则。

– TR.XAASL – 虚拟服务的安全标准化框架 – 是一份关于开发虚拟服务标准、要求和框架的讨论文件。

i) 第9/17号课题：电子生物特征识别（2017-2020年）

第9/17号课题制定有关利用电子生物特征识别认证用户的电子生物特征识别建议书并保护电子生物特征识别信息免受未经授权的访问。

在本研究期内，第9/17号课题制定了三份新建议书，一份经修订的建议书和一份勘误：

– X.1080.0和 X.1080.0勘误1 – 电子生物特征数据保护的访问控制 – 提供了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句法（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。本建议书也取决于权限管理基础设施（PMI）的部署。

– X.1080.1（修订版） – 电子卫生和全球远程医疗 – 通用通信协议 – 通过提供电子生物特征识别通信方面的总体模式定义ITU-T 1080.x系列建议书其它部分的框架。它提供了对象标识符的基本分配，用于在数据传输过程中以独一无二的方式识别信息片段，并且它定义了通用电信协议。它提供了一种用于对象的正式规范的技术，并且它指定了一种通用协议，支持患者本地的医疗站和提供更强专业知识的远程医疗中心之间的交互。ITU-T X.1080.x系列建议书的其他部分将使用和扩展该协议。

– X.1093 – 用智能ID进行生物特征访问控制 – 描述使用卡上生物特征技术进行逻辑和/或物理访问控制的一般方案。本建议书可应用于最近出现的要求安全物理和逻辑访问控制管理的领域。

– X.1094 – 使用生物信号的电子生物特征识别认证 – 规定了使用生物信号的新的安全和强大的电子生物特征识别认证方法。

j) 第10/17号课题：****身份管理架构和机制（2017****-****2020年）/身份管理和远程生物识别的架构和机制（2021-）****

第10/17号课题制定有关包括认证框架的身份管理主题的建议书。2021年1月，Q10/17承担了之前Q9/17研究的远程生物识别工作。

在本研究期内，第10/17号课题制定了五份新建议书，两份经修订的建议书和一份新的增补。

– X.1080.2 – 生物到机器（B2M）协议 – 定义了一个通用协议，用于患者所用设施与医疗专家设施进行生物信息交换，以使医疗中心可以远程监控患者并从该患者处检索信息。

– X.1252（修订版） – 身份管理基准术语和定义 – 提供了用于身份管理（IdM）的关键术语的定义。这些术语来源广泛，但均被认为通用于IdM领域。本建议书并不是要成为与IdM相关术语的一个大纲要。相反，本建议书中规定的术语仅限于那些被认为是最重要和最常用的、与IdM相关的基准术语。本建议书包含的附件A解释了某些关键术语的理论基础。

– X.1254（修订版）– 实体认证保证框架 – 规定了三个实体认证保证等级，以及有关这三个等级的标准和威胁。

此外，该框架：

• 建立了管理AAL的框架；

• 基于风险评估，为用于缓解认证威胁的控制技术提供了指南；

• 为将三个AAL映射到其他认证保证方案提供了指南；以及

• 为交换基于三个AAL的认证结果提供了指南。

– X.1276 – 认证升级协议和元数据1.0版 – 提出了简单的信任提升架构模式，展示了信任提升在现代访问控制架构中的使用，描述了用于信任提升信息交换的通用元数据集机制和协议元素，并促进了信任提升元素的使用，以促进当前用于减轻凭证和认证风险的许多技术和方法的标准化。

– X.1277 – 通用认证框架 – 描述了FIDO通用认证框架（UAF），该框架使在线服务和网站（无论是在开放的互联网上还是在企业内）能够透明地利用最终用户计算设备的本机安全功能进行强大的用户认证，并减少与创建和记住许多在线凭据相关的问题。

– X.1278 –客户端到认证器协议/通用2因素框架 – 描述了一个应用层协议，用于外部认证器和另一个客户端/平台之间的通信，以及将该应用协议绑定到使用不同物理介质的各种传输协议。

– X.1279 – 使用具有反欺骗检测机制的电子生物特征识别的增强认证框架 *–* 提供使用具有反欺骗检测机制的电子生物特征识别的增强认证架构框架。本建议书对传统远程生物特征识别认证解决方案面临的威胁做了分析，并针对使用具有反欺骗检测机制的远程生物特征识别的增强认证，规定了架构框架、认证流程和安全考虑。

– ITU-T X.1254 X.Suppl.35 – 有关实体认证保证（EAA）框架用例的增补 – 包含在安全实施中应用实体认证保证框架的三个用例，包括风险评估中的详细安全考虑、适当保证级别的选择和认证技术的选择。

第17研究组在2020年5月29日的第17研究组电子全体会议上同意为ITU-T D.1140 –包括数字身份基础设施原则的政策框架 – 分配编号X.1261，成为有关身份管理的、具有ITU-T D系列和ITU-T X系列双重编号的建议书。

k) 第11/17号课题：支持安全应用的通用技术（目录、公钥基础设施（PKI）、权限管理基础设施（PMI）、抽象句法符号一（ASN.1）、对象标识符（OID））（2017-2020年）/支持安全应用的通用技术（例如目录、公钥基础设施、正式语言、对象标识符）（2021-）

第11/17号课题研究有关号码簿服务和系统的建议书，包括X.500系列中的公钥/属性凭证。第11/17号课题维护ASN.1建议书，并进一步详细制定关于OID的建议书。按被称为“对象标识符树”的分层注册机构制定了全球识别方案。2021年1月，Q11/17承担了之前在Q12/17进行的语言研究工作。

在本研究期内，第11/17号课题制定了五份新的建议书、二十份建议书修订案、和X.500-、X.680-及X.690-系列建议书的十四份技术勘误（X.680 Cor.1、X.680 Cor.2、X.680 Amd.1、X.680 Cor.3、X.681 Cor.1、X.682 Cor.1、X. 682 Cor.2、X.683 Cor.1、X.693 Cor.1、X.694 Cor.1、X.696 Cor.1、X.696 Cor.2、X.696 Cor.3、X.893 Cor.1、X.894 Cor.1）、一份增补以及一份技术报告：

– X.500（修订版） – 信息技术 – 开放系统互连 – 号码簿：概念、模型和服务概述 – 引入号码簿和DIB（号码簿信息库）的概念，并概括它们提供的服务和功能。

– X.501（修订版）– 信息技术 – 开放系统互连 – 号码簿：模型 – 提供了各种不同模式的号码簿作为X.500系列中其他ITU-T建议书的框架。这些模式为综合模式（功能）、行政机关模式、提供关于号码簿信息的号码簿用户和管理用户观点的通用号码簿信息模式、通用号码簿系统代理（DSA）、DSA信息模式、业务框架和安全模式。

– X.501修正1，信息技术 – 开放系统互连 –目录：模型，更新了第9.2款和附件A

– X.509（修订版）– 信息技术 – 开放系统互连 – 号码簿：公钥和属性证书框架 – 为公钥基础设施（PKI）和特权管理基础设施（PMI）定义了一个框架。该建议书介绍非对称加密技术的基本概念。并规定了两种数据类别：公钥证书、属性、证书、证书吊销清单（CRL）和管理吊销清单（ACRL）。该建议书确定了若干证书和CRL扩展以及方便PKI和PMI相关数据在号码薄中存储的号码薄模式信息。此外，该建议书定义了实体类别，如证书管理机构（CA）、属性管理机构（AA）、依赖方、特权证实方、诚信经纪人和诚信主持人。该建议书具体规定了证书证实原则、证实途径、证书政策等。该建议书包含授权证实清单，有助于快速证实和限制通信。该建议书还包含完善授权证实清单所需的协议以及访问诚信经纪人所需的协议。

– X.501勘误1，信息技术 – 开放系统互连 –目录：模型，更正了第6.2.2款和附件B。

– X.510 *–* 信息技术 – 开放系统互连 – 目录：安全操作的协议规范 *–* 定义了一个通用协议，称为包装协议，通过提供身份验证、完整性和可选的机密性（加密），为包装协议保护设计的协议提供网络安全。包装协议允许独立于受保护的协议提供网络安全，这意味着可以在不影响受保护的协议规范的情况下增强安全性。

– X.511（修订版）– 信息技术 – 开放系统互连 – 号码簿：抽象服务定义 – 以抽象的方式定义外部可见的号码簿提供的服务，包括绑定和取消绑定操作、读操作、搜索操作、修改操作以及支持密码政策和支持与LDAP互通的操作。该修订版还定义了误码。

– X.518（修订版）– 信息技术 – 开放系统互连 – 号码簿：分布式操作程序 – 规定分布式号码薄所需的程序，前者由号码薄系统代理（DSA）和轻量号码薄接入协议（LDAP）服务器一同向其用户提供一致的服务，无论接入点如何。该修订版还描述号码簿接入协议/号码簿系统协议（DAP/DSP）与LDAP协议之间的转换程序。

– X.519（修订版）– 信息技术 – 开放系统互连 – 号码簿：协议规范 – 规定号码簿访问协议、号码簿系统协议、号码簿信息遮蔽协议和号码簿业务绑定管理协议，这些都履行ITU‑T X.501建议书 | ISO/IEC 9594-2、ITU‑T X.511建议书 | ISO/IEC 9594-3、ITU‑T X.518建议书 | ISO/IEC 9594-4和ITU‑T  X.525建议书 | ISO/IEC 9594-9中规定的抽象业务。该修订版还包含支持下层协议、以减少对外部规范依赖性的规范。可采用各项标准ASN.1编码规则对所述协议进行编码。

– X.520（修订版） – 信息技术 – 开放系统互连 – 号码簿：选择属性类型 – 定义了一些属性类型和匹配规则，可能涉及号码簿的各种应用范围。许多定义的属性的特定用途之一是名称的形成，特别是ITU‑T X.521建议书 | ISO/IEC 9594-7中定义的对象类别。被称为通知属性的其他属性类别提供诊断信息。该建议书|国际标准确定提供与属性值相关的特性的语境类别。此外，该建议书还包含与属性类别和匹配规则相关的LDAP句法定义。

– X.521（修订版） – 信息技术 – 开放系统互连 – 号码簿：选择对象分类 – 定义一些选定对象类别和名称形式，可能涉及号码簿的各种应用范围。一个对象类别定义规定的属性类型与该类别的对象相关。名称形式定义规定要形成给定类别的对象的名称所使用的属性。

– X.525（修订版） – 信息技术 – 开放系统互连 – 号码簿：复制 – 描述号码簿系统代理（DSA）可能用来复制号码薄信息的遮蔽业务。该业务有助于DSA之间复制信息，以改善向用户提供的号码薄服务，并提供该信息的自动更新。

– X.676 – 物联网（IoT）分组服务的基于对象标识符的解析框架 – 规定了用于识别物联网环境中各种服务的基于对象标识符（OID）的解析框架。OID是一个标识符，用来命名一个具有分层命名空间的对象。在物联网（IoT）中，数以千计的基于异构资源的物联网服务将作为各种服务的组合提供。为了提高效率，需要各种技术，如服务绑定、动态服务或频繁切换服务，以及分组服务的解析和识别。该建议书描述了物联网分组服务的概念、考虑因素、架构以及基于OID的物联网分组服务解决方案框架的程序。

– X.677 – 使用对象标识符的无人机识别机制 *–* 从安全考虑出发，分析了无人机（UAV）全寿命周期管理和操作身份识别的要求。此建议书还规定了使用对象标识符的无人机识别机制，包括无人机所用对象标识符（OID）的分配规则和登记程序的详细说明。

– X.680（修订版及修订前的修正1和勘误1-3） – 信息技术 *–* 抽象语句表示法第一版：基本符号规范 *–* 介绍了被称为抽象语句表示法第一版（ASN.1）的表示法，用来定义信息数据的句法。该建议书定义了若干简单数据类型并为参考这些类型的标识法以及这些类型的数值制定了规范。

– X.681（修订版及修订前的勘误1） – 信息技术 *–* 抽象语句表示法第一版（ASN.1）：信息对象规范 *–* 介绍了可定义信息对象类别以及单个信息对象并获得参考名称的ASN.1表示法。信息对象类别定义了概念表形式（信息对象集），每一栏定义信息对象类别的一个字段，每个完整的一行定义一个信息对象。

– X.682（修订版及修订前的勘误2） – 信息技术 *–* 抽象语句表示法第一版（ASN.1）：限制规范 *–*为强制和除外规范的一般情况提供ASN.1记法，由此可以限制结构化数据类型的数据值。该表示法还适用于违反约束的信令。

– X.683（修订版及修订前的勘误1） – 信息技术 *–* 抽象语句表示法第一版（ASN.1）：ASN.1规范的参数化 *–* 定义了参数化的参考名称和数据类参数分配，这有助于制定规范的设计人员解决在规范制定的某个阶段未予确定而欲在稍后阶段补充以产生完整的抽象句法定义的问题。

– X.690（修订版） – 信息技术 *–*ASN.1编码规则：基本编码规则（BER）的规范、规范编码规则（CER）和区分编码规则（DER） *–* 定义一套基本编码规则（BER），可用于利用ASN.1记法定义的各类数值。应用这些编码规则可生成上述数值的传送语法。这些编码规则的规范暗示，它们也可用于解码。本建议书|国际标准还定义了一套区分编码规则（DER）和一套规范编码规则（CER），以便对基本编码规则（BER）加以约束。它们之间的主要区别是，DER使用确定长度的编码形式，而CER使用不确定长度的编码形式。DER是更适合于小的编码数值，而CER更适合大的数值。这些编码规则的规范暗示，它们也可用于解码。

– X.691（修订版） – 信息技术 *–*ASN.1编码规则：分组编码规则（PER）的规范 *–* 描述了一组适用于所有ASN.1类型数值的编码规则，以实现一个比采用基本编码规则及其衍生物（述于ITU-T X.690建议书| ISO/IEC 8825-1国际标准）远为紧凑的表述形式。

– X.692（修订版） – 信息技术 *–*ASN.1编码规则：编码控制记法（ECN）的规范 *–* 定义了编码控制记法（ECN），该记法所明确的编码类别（ASN.1类）与基本编码规则（BER）和压缩编码规则（PER）等标准编码规则规定的编码不同。

– X.693（修订版及修订前的勘误1） – 信息技术 *–*ASN.1编码规则：XML编码规则（XER）的规范 *–* 详述了利用可扩展标记语言（XML）对ASN.1类数值进行编码的规则。

– X.694（修订版及修订前的勘误1） – 信息技术 *–*ASN.1编码规则：将W3C XML方案定义映射至ASN.1 *–* 定义了XSD方案（符合W3C XML方案规范的方案）向抽象语法标记1（ASN.1）方案映射的规则，以便使用基本编码规则（BER）、区分编码规则（DER）、压缩编码规则（PER）或相同可扩展标记语言（XML）编码规则等ASN.1编码规则，传送用XSD方案定义的信息。

– X.695（修订版） – 信息技术 *–*ASN.1编码规则：注册并应用PER编码指令 *–* 规定了利用类型前缀或编码控制部分执行PER编码指令的规则。编码指令是为某些具体的编码规则（此处的PER）修改ASN.1类型编码的手段。可利用方括号（与基本编码规则（BER）的标签极为相似）将它们插入受其影响的类型（类型前缀）之前，或者将它们在ASN.1模块（编码控制部分）的结尾处汇总。建议书还规定了不时制定、登记和公布新PER编码指令的程序

– X.696（修订版及修订前的勘误1-3） – 信息技术 *–* ASN.1编码规则：八位字节编码规则（OER）的规范*–* 描述了两套可适用于所有ASN.1类型数值二进制编码规则，该规则使用的处理资源要少于基本编码规则及其衍生物（述于ITU-T X.690建议书| ISO/IEC 8825-1国际标准）和成套编码规则（见ITU-T X.691建议书| ISO/IEC 8825-2国际标准。

– X.697 信息技术 *–* ASN.1编码规则：JavaScript对象表示法的编码规则（JER）的规范 *–* 定义了一套JavaScript对象表示法的编码规则（JER），可用于衍生ITU-T X.680建议书 | ISO/IEC 8824-1、ITU-T X.681建议书 | ISO/IEC 8824-2、ITU-T X.682建议书 | ISO/IEC 8824-3 和ITU-T X.683 建议书| ISO/IEC 8824-4国际标准定义的数值类型的传送语法。这些编码规则的规范暗示，它们也可用于解码。

– X.893勘误1 – 信息技术 *–* ASN.1的一般应用：快速infoset安全性 *–* 是对信息附件和参考资料的更正，删除了对过时的三重DES算法的引证。

– X.894（及勘误1和勘误2） – 信息技术 – ASN.1的普遍应用：加密消息语句 – 提供抽象句法表示法 – （ASN.1）模块，用于在ITU-T建议书中使用加密句法。加密消息句法（CMS）提供可靠的信息交换和强身份验证所需的数据完整性、机密性、来源真实性和不可否认性服务。它还汇集了一套加密密钥管理技术，以支持灵活的密钥建立机制，如建设性的密钥管理、密钥协议、密钥交换和基于密码的加密。这些技术可以用来防止欺诈，并保护个人可识别和其他敏感信息。该建议书|国际标准支持基于ITU-T X.500系列国际标准化组织/国际电工委员会 | 9594多部分标准中定义的公钥技术的数字签名、加密和签密技术。支持ASN.1的所有标准化编码规则。

– Z.161（修订版） – 测试和测试控制表示法版本3：TTCN-3核心语言 – 定义了测试和测试控制表示法版本3（TTCN-3），旨在对独立于平台、测试方法、协议层和协议的测试套件进行规范。模块TTCN-3可用来对许多通信端口上的所有类型的反应系统测试进行规范。

– Z.162（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：配置及部署支持 – 定义了TTCN-3的配置和部署支持包。TTCN-3可用来对许多通信端口上的所有类型的反应系统测试进行规范。

– Z.163（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：高级参数化 – 定义了TTCN-3的高级参数化包。TTCN-3可用来对不同通信端口上的所有类型的反应系统测试进行规范。

– Z.164（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：行为类型 – 定义了TTCN-3的行为类型包。TTCN-3可用来对大量不同通信端口的所有类型的反应系统测试进行规范。

– Z.167（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：面向对象的功能 – 定义了对TTCN-3面向对象的功能的支。TTCN-3可用来对大量不同通信端口上的所有类型的反应系统测试进行规范。

– Z.167（修订版） – 测试及测试控制表示法版本3：通过TTCN-3使用ASN.1 – 定义了按ITU-T X.680 ITU-T X.681 ITU-T X.682和ITU-T X.683建议书所述使用TTCN-3的方式使用抽象句法表示法一（ASN.1）的规范方法。

– Z.168（修订版） – 测试及测试控制表示法版本3：IDL到TTCN-3的映射 – 定义了公共对象请求代理体系架构（CORBA）接口定义语言（IDL）到TTCN-3（如ITU-T Z.161建议书的定义）的映射规则，从而可以对CORBA系统进行测试。CORBA IDL到TTCN-3的映射原则可用来对其他基于对象/部件的技术的界面规范语言进行映射。

– Z.169（修订版） – 测试及测试控制表示法版本3：利用TTCN-3使用XMLS模式 – 定义了万维网联盟（W3C）模式到测试和测试控制标表示法3（TTCN-3）的映射规则，从而可以对基于XML系统、界面和协议进行测试。

– Z.171（修订版） – 测试及测试控制表示法版本3：利用TTCN-3使用JSON – 规定了定义TTCN-3中JSON数据结构模式的规则，从而可以对基于JSON的系统、接口和协议进行测试，此外还定义TTCN-3和JSON之间的转换规则，以便在不同系统之间交换JSON格式的TTCN-3数据。

– ITU-T X.660X.增补31 *–* 物联网对象标识符使用指南 – 提供关于如何使用对象标识符（OID）识别物联网（IoT）中的对象的指南。它包括关于如何构建OID、如何实施解决方案系统以及如何根据现有的ITU-T建议书和国际标准建立管理程序的指南。

– XSTP.OID-ORS – OID解决方案系统：问题、要求和潜在解决方案 – 确定OID解决方案的问题、要求和潜在解决方案。这些问题包括本地性能和丢失OID子树的全局解决方案。还讨论了可能的解决方案的技术要求。最后，提供了潜在的技术解决方案、管理和操作指导。

– Z.Imp100（修订版） – 规范和描述语言实施者指南 – 4.0.1版 – 汇编了规范和描述语言方面的ITU-T Z.100、Z.101、Z.102、Z.103、Z.104、Z.105、Z.106、Z.109、Z.111和Z.119建议书所上报的缺陷以及维护中出现的问题和解决方案。

l) 第12/17号课题：电信软件和测试的形式语言

第12/17号课题制定有关形式语言的建议书（如SDL、MSC、URN）以定义电信系统的要求、体系结构和行为：要求语言、规范和执行语言。第12/17号课题还制定有关测试语言（如TTCN-3）的建议书，作为支持互操作性和一致性的手段。

在本研究期内，第12/17号课题制定了三份新建议书，64份经修订的建议书和两份修订实施者指南：

– Z.100（修订版） – 规范和描述语言（SDL）– SDL‑2010概述 – 介绍规范和描述语言，旨在明确规范和描述电信系统。

– Z.100附件F1（修订版） – SDL‑2010的正式定义：一般性概述 – 提供了目的，概述了正式语义的结构，并介绍了用于定义SDL‑2010语义的抽象状态机（ASM）的形式体系。

– Z.100附件F2（修订版） – SDL‑2010的正式定义：静态语义 – 阐述了静态语义限制，并介绍了通过ITU-T Z.100建议书引证归并的ITU-T Z.101、Z.102、Z.103、Z.104、Z.105和Z.107建议书“范例”章节中确定的变换。

– Z.100附件F3（修订版） – SDL‑2010的正式定义：动态语义 – 定义了SDL-2010的动态语义。

– Z.101（修订版） – 规范和描述语言 – 基本SDL‑2010 – 定义了规范和描述语言的基本特征。此文件定义的语言包括语言的基本特征，在Z.100系列其他建议书中对其进一步予以进一步定义。

– Z.102（修订版） – 规范和描述语言 – 综合SDL‑2010 – 定义了规范和描述语言的综合特征。本文件中定义的语言涵盖ITU‑T Z.101建议书不包括的基本SDL 2010语言功能，这些功能综合涵盖语言的抽象句法，Z.104（以及关于面对对象数据的TU-T Z.107）包括的一些数据的功能除外。

– Z.103（修订版） – 规范和描述语言 – SDL‑2010中的简化表示法和注释 – 定义了规范与描述语言的简化表示法和注释特性。本文件定义的语言包含了ITU-T Z.101建议书中基本SDL2010或ITU-T Z.102建议书中综合SDL2010未包括的语言的特性。本建议书定义的特性或者没有自己的抽象句法且已转换为由ITU-T Z.101、ITU-T Z.102和ITU-T Z.104（以及关于面对对象数据的TU-T Z.107）建议书定义的具体句法，或者只是没有正式含义的注释。

– Z.104（修订版） – 规范和描述语言 – SDL‑2010中的数据和行动语言 – 定义了规范和描述语言的数据特性，从而充分确定了数据定义和表达。本文件定义的语言部分覆盖了ITU-T Z.101建议书中基本SDL‑2010的语言特性，并用于ITU-T Z.102的综合SDL‑2010和ITU-T Z.103建议书的特性。

– Z.105（修订版） – 规范和描述语言 – SDL‑2010与ASN.1模块的结合 – 定义了与规范和描述语言2010（SDL‑2010）可一起使用的抽象句法表示法（ASN.1）模块。本建议书文本取代ITU-T Z.105建议书（2003年），在SDL-2010方面与ITU-T Z.100、ITU T Z.101、ITU-T Z.102、ITU-T Z.103、ITU-T Z.104和ITU-T Z.106建议书进行统一。ITU-T Z.105建议书（2003年）代替了ITU-T Z.105建议书（1999年）定义的ASN.1至SDL‑2010的语义映射。

– Z.106（修订版） – 规范和描述语言 – SDL‑2010的通用交换格式 – 定义规范和描述语言的通用交换格式（SDL CIF）。SDL CIF意在交换未使用同样存储格式的各种工具上制作的图形SDL‑2010规范（SDL GR）。本建议书介绍了SDL CIF的另外两层，还定义了一致性的另外两个级别，一个是更开放的SDL PR级别，第二个包含了图形信息。

– Z.107（修订版） – 规范和描述语言 – SDL‑2010内面向对象的数据 – 在ITU-T Z.104建议书定义的数据定义和表示形式的基础上定义了规范和描述语言面向对象的数据特性。本建议书定义的语言与 ITU-T Z.101建议书中基本SDL2010包括的、ITU-T Z.102建议书中综合SDL2010使用的语言特性以及ITU-T Z.103和ITU-T Z.104建议书的特性有部分重叠。

– Z.151（修订版） – 用户要求表示法（URN）– 语言要求 – 定义用户要求表示法（URN）用于要求的获取、分析、规范和验证。URN结合建模概念和目标表示法（主要用于非功能性要求和质量属性）和方案（主要为业务要求、功能要求、性能和建筑推理）。目标子表示法被称为面向目标的要求语言（GRL），场景子表示法被称为使用案例图（UCM）。

– Z.161（修订版） – 测试和测试控制表示法版本3：TTCN-3核心语言 – 定义了测试和测试控制表示法3（TTCN-3），其目的是对独立于平台、测试方法、协议层和协议的测试套件进行规范。TTCN-3可用来对不同通信端口的所有类型的反应系统测试进行规范。应用的典型领域包括协议测试（移动和互联网协议）、业务测试（附加业务）、模块测试，对基于共同对象要求经纪人（CORBA）的平台进行测试以及应用编程接口（API）。

– Z.161.1（修订版） – 测试和测试控制表示法版本3：TTCN-3语言扩展：支持连续信号接口 – 定义了TTCN 3“连续信号支持”软件包。TTCN 3可用来对许多通信端口上的所有类型的反应系统测试进行规范。典型的应用范围有协议测试（包括移动和互联网协议）、业务测试（包括补充业务）、模块测试、CORBA平台测试、API等。TTCN 3不限于一致性测试，还可用于许多其他各种测试，包括互操作性、坚固性、拟合系统和集成测试。物理层协议测试套件的规范不再本文件范围内。

– Z.161.2（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：配置及部署支持 – 定义了TTCN 3的配置和部署支持软件包。

– Z.161.3（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：先进参数化 – 定义了TTCN 3的高级参数化软件包。

– Z.161.4（修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：行为类型 – 定义了TTCN 3的行为模式软件包。

– Z.161.6（新版本和修订版） – 测试及测试控制表示法版本3：TTCN-3语言扩展：高级匹配 – 定义了测试和测试控制表示法-3（TTCN-3）的先进匹配。

– Z.161.7（新版本和修订版） – 测试及测试控制表示法版本3 – 定义了测试和测试控制表示法版本3（TTCN-3）中“对面向对象的特征的支持”。

– Z.164（修订版） – 测试和测试控制表示法版本3：TTCN-3的操作语义学 – 定义了TTCN-3（测试与测试控制表示法3）的操作语义学。操作语义学对明确解释TTCN-3的相关规范是必要的。本建议书依据的是ITU-T Z.161建议书定义的TTCN-3核心语言。此为该建议书的修订版，其中包含了修正、澄清、勘误和编辑性校正。

– Z.165（修订版） – 测试和测试控制表示法版本3：TTCN-3运行时间接口（TRI）– 分别为特定处理平台和被测系统的测试系统的定时和通信提供推荐的适配。该建议书将接口定义为一组独立于目标语言的操作。

该接口被确定符合ITU-T Z.161建议书。该建议书使用通用对象请求代理架构（CORBA）接口定义语言（IDL）完全确定TRI。ETSI ES 201 873-5 V4.8.1的第6、7和8段规定了抽象规范到目标语言Java和ANSI-C的语言映射。基于IDL的接口规范的概要见ETSI ES 201 873-5 V4.8.1的附录A。

本建议书的该修订案包含修改、澄清、勘误和编辑性校正。

– Z.166（修订版） – 测试和测试控制表示法版本3：TTCN-3控制接口（TCI）– 规定了测试和测试控制表示法3（TTCN-3）的控制接口。TTCN-3控制接口（TCI）为测试系统的管理、测试器件处理和编解码提供了针对具体测试平台的适应方式。该建议书定义了独立于目标语言的一套操作接口。

接口被确定符合TTCN-3标准（参见ETSI ES 201 873-6 V4.11.1第2段）。接口定义使用通用对象请求代理架构接口定义语言完全确定TCI。ETSI ES 201 873-6 V4.11.1的第8、9和9.7段给出了该抽象规范到目标语言Java和ANSI C的语言映射。

本建议修订版包含修正、澄清、更正和编辑更正。

– Z.167（修订版） – 测试和测试控制表示法版本3：来自ASN.1的TTCN-3映射 – 定义了使用ASN.1的规范方法，定义方式有如TTCN-3相关的ITU-T X.680、ITU-T X.681、ITU-T X.682和ITU-T X.683建议书。其他语言与TTCN-3的协调不再属于本建议书的范围。

该建议书的首次修订包含了修正（一致性和兼容性、objid类型有关的要求和描述从其他ITU-T Z.16x系列建议书已被移至该建议书，支持ASN.1模块中的XML值、OID-IRI和RELATIVE-OID-IRI类型的转换，特殊实际值和包含特殊值和专属边界的子类别、更新的预定义语言串等），澄清（如导入ASN.1定义的可见性转换规则）勘误和编缉校正。

该建议书的修订包含修正、澄清、更正和编辑更正。

– Z.168（修订版） – 测试和测试控制表示法版本3：来自公共对象请求代理体系结构（CORBA）的接口定义语言（IDL）的TTCN-3映射 – 定义了CORBA IDL到TTCN-3（如ITU-T Z.161建议书的定义）的映射规则，可以对CORBA系统进行测试。CORBA IDL到TTCN-3的映射还可用于其他对象/基于元素的技术的接口规范怨言的映射。其他映射的规范不在该建议书范围内。Z.168的修订包含了修正、澄清、勘误和编缉校正。

– Z.169（修订版） – 测试和测试控制表示法版本3：使用带有TTCN-3的XML模式（Schema） – 规定了W3C模式（Schema）到TTCN-3的映射规则，从而可以对基于XML的系统、界面和协议进行测试。建议书该修订版包含了一些修正内容、澄清、勘误和编辑性校正。

– Z.170（修订版） – 测试和测试控制表示法版本3：TTCN-3文件注解规范 – 规定了使用特殊文件注释对TTCN-3源码进行记录的方法。Z.170的本修订含有修正、澄清、勘误和编辑性校正。

– Z.171（新版本和修订版） – 测试和测试控制表示法版本3：使用带有TTCN-3的JSON模式 – 规定了定义TTCN-3中JSON数据结构模式的规则，从而可以对基于JSON的系统、接口和协议进行测试，此外还定义TTCN-3和JSON之间的转换规则，以便在不同系统之间交换JSON格式的TTCN-3数据。

– Z.100Imp（修订版） – 规范和描述语言实施者指南 – 3.0.2版 – 汇总了有关规范和描述语言的ITU-T Z.100、Z.101、Z.102、Z.103、Z.104、Z.105、Z.106、Z.109、Z.111和Z.119建议书所上报的缺陷以及维护中出现的问题和解决方案。

– Z.100Imp（修订版） – 规范和描述语言实施者指南 – 4.0.0版 – 汇总了有关规范和描述语言的ITU-T Z.100、Z.101、Z.102、Z.103、Z.104、Z.105、Z.106、Z.109、Z.111和Z.119建议书所上报的缺陷以及维护中出现的问题和解决方案。

m) 第13/17号课题：智能交通系统的安全问题（2017-2020年）/智能交通系统的安全（ITS）性（2021-）

第13/17号课题设立于2017年9月，负责制定智能交通系统（ITS）安全方面的建议书，其中包括车辆中、车辆之间以及车辆和固定位置之间的各种类型的通信。

在此研究期，第13/17号课题制定了六份新建议书：

– X.1371 – 联网车辆面临的安全威胁 – 描述联网车辆和车辆生态系统面临的安全威胁。

– X.1372 – 车联网（V2X）通信的安全导则 – 为车联网（V2X）通信系统提供安全导则。该建议书确定V2X通信环境中的威胁并根据威胁规定V2X通信的安全要求。该建议书还提供有关V2X通信安全服务的用例。

– X.1373 – 智能交通系统通信设备的安全软件更新功能 – 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。该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。

– X.1374 – 具有接入车辆能力的外部接口和设备的安全要求 – 分两部分分析了对连接车辆造成的安全威胁：对车辆与外部设备通信接口的威胁，以及对与车辆进行通信的外部设备的威胁。ITU-T X.1374建议书规定了此类外部接口和具有车辆接入能力的外部设备在电信网络环境下的安全要求，从而根据接入接口的类型解决已识别的威胁。具有车辆访问能力的接口和外部设备包括配有智能钥匙的遥控无钥匙进入（RKE）系统、使用车载诊断II（OBD‑II）端口的诊断工具和无线加密狗、带有无线通信设备的远程信息处理控制单元等。

– X.1375 – 车载网络入侵检测系统导则 – 确立了车载网络（IVN）入侵检测系统（IDS）的指导原则。此建议书主要关注如何检测智能虚拟网络的入侵和恶意活动，例如那些使用控制器局域网（CAN）的IVN，而这些网络是目前部署在互联网上的一般IDS不支持的。ITU-T X.1375建议书包括针对IVN攻击的分类和分析。该建议书提出了在基于CAN的车载网络中检测入侵和恶意活动，且一般入侵检测系统所不能支持的方法和实施指南。

– X.1376 – 利用大数据针对与联网车辆安全相关的不当行为开展检测的机制 – 描述一种针对联网车辆的安全相关不当行为检测机制，以帮助利益攸关方利用汽车数据来提高车辆安全性。随着车辆连通性的增加，由于复杂技术的发展，漏洞的数量也在增加。这些漏洞给联网车辆带来了更多威胁。对大量汽车数据进行分析对于评估联网车辆的安全性非常有用。

在此研究期，第13/17号课题于2019年8月26日在日内瓦举办了有关自动驾驶中的网络安全挑战的小型讲习班。

n) 第14/17号课题：分布式账本技术的安全问题（2018-2020年）/分布式账本技术（DLT）的安全性（2021-）

第14/17号课题设立于2018年3月 为分布式账本技术（DLT），亦称为区块链，制定安全方面的建议书。这包括为基于DLT的应用和服务提供全面的安全解决方案。

在此研究期内，第14/17号课题制定了九份新建议书：

– X.1400 – 分布式账本技术的术语和定义 – 包含分布式分类账技术（DLT）的一套基线术语和定义。这些定义提供了该术语的基本特征且在适当的情况下，还包括一个可提升明确度的注释。

– X.1401 – 分布式账本技术的安全威胁 – 确定对分布式账本系统各种功能组件的可能威胁，例如协议、网络和数据。该建议书可在DLT系统的设计或实施中作为参考基准加以考虑。

– X.1402 – 分布式账本技术的安全框架 – 描述了可以减轻相关安全威胁的安全能力，并规定了一种安全框架方法，以确定如何使用这些安全能力减轻DLT系统的安全威胁。

– X.1403 – 将DLT用于去中心化身份管理的安全指南 – 分布式账本技术及其特定的实施方案（如区块链）为利用信任基础设施和平台提供了独特的机遇，这对于启用可信联盟/联邦以交换身份属性和身份信息可能很有用。本建议书提供了有关在身份管理中使用DLT数据的、电信特定的隐私和安全注意事项。

– X.1404 – 分布式账本技术的安全保证 – 为促进安全保证机制的设计和开发，本建议书为分布式分类账技术（DLT）定义了三个级别的安全保证。此外，这一建议书进一步定义了包含安全保证的十个安全保证组件，并为实现安全保证组件三个级别的各个级别指定了标准和导则。最后，建议书还提供了特定威胁和安全保证组件之间的映射，以及特定安全功能和安全保证组件之间的映射。

– X.1405 – 基于分布式账本技术的数字支付服务的安全威胁和要求 – 在分析支付服务用例的基础上，ITU-T X.1405建议书描述了业务模型，还对安全威胁和挑战进行了分析并根据已确定的威胁和挑战规定了安全要求。

– X.1406 – 使用分布式账本技术对在线投票系统产生的安全威胁 – 使用基于电信或信息通信技术（ICT）基础设施的分布式分类账技术（DLT）识别在线投票系统面临的安全威胁，并分析了模型所描述在线投票过程中的安全威胁。

– X.1407 – 基于分布式账本技术的数字完整性证明服务的安全要求 – 规定了基于分布式账本技术（DLT）的数字完整性证明服务的安全威胁和需求。

– X.1408 – 基于分布式账本技术的数据访问和共享的安全威胁和要求 – 指定了一个参考模型，用以描述基于分布式账本技术（DLT）的数据访问和共享。本建议书确定了基于DLT数据访问和共享的实体及其角色以及相关的安全威胁。此外，还为应对这些已识别的安全威胁指定了安全要求。

**o) 第15/17号课题：新兴技术的安全性，包括基于量子的安全性**

第15/17号课题成立于2021年1月，负责为包括量子安全在内的新兴技术编写有关安全的建议书。第15/17号课题还负责SG17的孵化机制（TP.inno），该机制可在研究新兴安全领域时提供可控的灵活性，以确保基于新兴电信/ICT的服务和应用的安全。

在本研究期期间，Q15/17编写了两份新建议书和一份技术报告勘误：

– X.1712 – 量子密钥分发网络的安全要求和设计 – 阐述了量子密钥分发网络（QKDN）中密钥管理的安全威胁和安全要求，同时规定了满足安全要求的密钥管理的安全措施。

– X.1770 – 安全多方计算技术导则 – 规定了MPC的技术指导原则，为ICT利益攸关方在数据协作和大数据分析场景中使用MPC保护数据，提供了技术标准的基础。此外，建议书还描述了可用于MPC的应用，以及如何作为ICT利益攸关方开发MPC应用的参考。

– TR.sec-qkd勘误1 – 量子密钥分发网络的安全考虑 – 更改了关于“IT-secure”的相关表述，将“量子比特（qubits）”更改为“量子状态（quantum states）”，将“同纤（co-fiber）”更改为“同传播（co-propagation）”，并修改相关内容。

## 3.3 牵头研究组活动报告、全球标准举措（GSI）、联合协调活动（JCA）、区域组和项目的报告

第17研究组是负责电信安全、身份管理及语言和描述技术方面的牵头研究组。牵头研究组活动分享如下：

– 电信安全，由第1/17号课题管理。

– 身份管理，由第10/17号课题管理。

– 语言和描述技术，2020年底前由第11/17和第12/17号课题共同管理，2021年后由第11/17号课题管理。

### 3.3.1 就有关安全开展的牵头研究组活动

根据世界电信标准化全会（WTSA-16）第2号决议，第17研究组被指定担任安全方面研究的牵头研究组（LSG）。

作为电信安全的牵头研究组，第17研究组负责研究适用的核心安全问题。此外，与其他相关研究组协商，必要时与其他标准机构合作，第17研究组负责定义和维护整体框架和协调、分配（认可研究小组任务）和排列研究组将进行的研究的顺序，确保建议书编制的一致性、完整性和时限性。

在第17研究组中，第1/17号课题是LSG的安全活动的协调方。第17研究组与其他研究组密切合作，以确定和开发安全解决方案。然而，将这些解决方案与所开发的独特技术相结合的具体专业知识只能来自正在开发的课题。

作为研究安全问题的牵头研究组，第17研究组一直保持与所有从事安全相关工作的  
ITU-T研究组之间的联系。第17研究组还与大量ICT和电信安全方面的标准化组织和论坛合作，重点特别放在避免研究组正在开展的工作与外部机构发生潜在的冲突上。

此外，在第17研究组的每次会议上都召开安全协调会议，为所有从事与安全相关工作的研究组确立安全联系表。

在第17研究组牵头负责的研究工作方面，收到并处理了来自下列方面的有关安全问题的内部联络声明：国际电联CITS、ITU-D（第1研究组、第2研究组TDAG）、ITU-R（第1研究组、第5研究组、第6研究组、工作组（4C、5A、5D、6C））、ITU-T FIGI、ITU-T FG-（AI4EE、AI4H、AN、DFC、DLT、DPM、ML5G、NET2030、QIT4N、VM）、ITU-T JCA-（IMT2020、IoT和SC&C、MMeS、SDN）、ITU-T SCV、ITU-T研究组（2、3、5、9、11、12、13、16、16、20）和ITU-T TSAG。

在第17研究组负责牵头研究的工作方面，收到并处理了来自下列方面的外部联络声明：3GPP（SA3）、BIPM、CEN-CENELEC，JTC 19、ETSI ISG（CIM、ETI、F5G、IPE、NIN、QSC、SAI）、ETSI SAGE、 ETSI TC（CYBER、MTS）、FIDO联盟、IEEE 802.1、 IETF、WG TLS ISO TC 307、ISO/IEC JTC 1/SC（6、27/WG 1-5、29/WG1）、NIST、OASIS、OMA、oneM2M、SAE和W3C。

第17研究组向下列方面发出了内部联络声明：国际电联CITS、IPRAHG，ITU-D（第1研究组、第2研究组、TDAG）、ITU‑R研究组（4、5（5A、5D工作组））、ITU-T FIGI、ITU-T焦点组（AI4EE、DFC、DLT、NET2030、DPM、QIT4N、VM），ITU-T JCA（IMT2020、IoT和SC&C、MMeS、SDN），ITU-T SCV、ITU-T研究组（2、3、5、9、11、12、13、15、16、20）和ITU-T TSAG。

第17研究组向下列方面发出了外部联络声明：3GPP（SA3）、PT ASTAP、BSI、CEN-CENELEC JTC 19、CIS、ETSI（ISG CIM、MEC、QKD ZSM、SAGE）、ETSI TC（CYBER、ITS、MTS））、FIDO联盟、GSMA（FASG）、SIM、ICAO、IEEE区块链举措、IETF、IRTF、ISO TC（12、20、22、37、204、307）、ISO/IEC JTC 1/WG9、ISO/IEC JTC 1/SC（6（WG 10）、7、27（WG 1、WG 2、WG 3、WG 4、WG 5）、29、38、42）、Kantara举措、MEF、MITRE、NGMN、NIST、OASIS TC（CTI、OpenC2、信任提升）、OIX、oneM2M、ONF、OPIX基金会、RAISE论坛、SAE、UNECE、UPU、W3C、世界知识产权组织（WIPO）、世界卫生组织（WHO）。

为响应WTSA-16第7号决议 – 与国际标准化组织（ISO）和国际电工委员会（IEC）的协作 – 第17研究组维护在线表格，列出了与ISO和IEC的技术委员会（TC）和ISO/IEC JTC 1的小组委员会的关系，也包括将此关系的性质确定为联合工作（例如，通用文本或双文本），通过联络机制或信息联络的技术性合作。

第17研究组组织了以下讲习班：

– [国际电联/世界卫生组织关于数字新冠肺炎证书的第二次联合讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/1126/Pages/default.aspx)  
2021年11月26日，欧洲中部时间（CEST），13:00-18:00，虚拟形式

– [国际电联/世界卫生组织数字疫苗接种证书联合讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2021/0811/Pages/default.aspx)  
2021年8月11日，欧洲中部时间，13:00-18:00，虚拟形式

– [电信发展局2021年新兴技术周](https://www.itu.int/en/ITU-D/Conferences/ET/2021/Pages/Programme.aspx)，“去中心化的标识符和区块链”  
2021年7月8日，13:00-18:00，虚拟形式

– [第17研究组有关自动驾驶中的网络安全挑战的小型讲习班](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/mini-workshop_ITS.aspx)  
2019年8月26日，14:30-17:30，日内瓦

– [国际电联金融技术安全讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190826/Pages/default.aspx)  
2019年8月26日，瑞士日内瓦

– [国际电联网络量子信息技术（QIT）讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/default.aspx)  
2019年6月5-7日，中国上海

– [第17研究组有关安全量子通信的小型讲习班](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/Secure%20quantum%20communication.aspx)  
2019年1月24日，14:30-17:30，日内瓦

– [国际电联有关人工智能/机器学习和安全的讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20190121/Pages/default.aspx)  
2019年1月21日，瑞士日内瓦

– [ITU国际电联有关先进的网络安全攻击和勒索病毒的讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180828/Pages/default.aspx)  
2018年8月28日，瑞士日内瓦

– [国际电联有关5G安全的讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180319/Pages/default.aspx)  
2018年3月19日，瑞士日内瓦

– [国际电联有关智能交通系统安全问题的讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Pages/default.aspx)  
2017年8月28日，瑞士日内瓦

– [国际电联有关区块链安全问题的讲习班](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201703/Pages/default.aspx)  
2017年3月21日，瑞士日内瓦

特别是，第17研究组有关安全的工作计划考虑到：

– 实施WTSA-16第7、11、18、32、40、44、50、52、54、58、64、65、67、70、73、75、76、77、78、84、86、89、90、92、93、94、96、97和98号决议；

– 实施PP-18第101、123、130、136、174、177、178、179、181、188、189、197、199、200和201号决议；

– 实施WTDC-17第23、30、34、45、47、54、63、67、69和80号决议。

第17研究组已经制定出支持PP-14/18、WTSA-16、WTDC-17决议的活动计划并在每次会议上更新。在第17研究组2020年3月的会议上，为这些工作指定了一位编辑人员以便为工作提供便利。

此外，安全牵头研究组的网页在第17研究组网站上维护，直接链接关键的安全产品和服务。

第17研究组积极更新得到批准的ICT安全标准路线图所含标准的标准数据库，为避免重复工作，这对于标准制定者是一项重要工具。

第17研究组还更新了安全大全，该大全提供ITU-T在安全标准化活动方面的信息，包括涉及安全的ITU-T建议书目录和ITU-T批准的安全定义和缩略语目录。

有关成功使用安全标准的技术报告第二版已经发布。该报告旨在帮助用户，特别是发展中国家的用户，更好地了解在各种不同环境中（如工业、商业、政府和企业）使用ITU-T安全相关建议书的价值。

第7版安全手册作为技术报告获得批准。该《安全手册》是ITU-T的一项重要宣传工具，以简单易懂的方式突出强调了ITU-T各研究组开展的重要安全工作。

ITU-T各研究组（第17研究组以外的研究组）在其安全建议书工作方面已取得了下列成果：

批准的建议书：

| **研究组** | **建议书** | **标题** |
| --- | --- | --- |
| SG9 | J.1204 | 智能电视操作系统的安全框架 |
| SG13 | Y.2241 | 支持基于网络对象的泛在自主学习的服务框架 |
| SG13 | Y.2774 | 未来网络深度包检测的功能需求 |
| SG13 | Y.3051 | 信通技术基础设施中可信环境的基本原则 |
| SG13 | Y.3052 | ICT基础设施和服务的信任提供概述 |
| SG13 | Y.3053 | 具有以信任为中心的网络域的可信网络框架 |
| SG13 | Y.3054 | 基于信任的媒体服务框架 |
| SG13 | Y.3055 | 基于信任的个人数据管理框架 |
| SG13 | Y.3056 | 分布式生态系统中开放访问可信服务的设备和应用的自举框架 |
| SG13 | Y.3057 | ICT基础设施和服务的信任指数模型 |
| SG13 | Y.3302 | 软件定义网络的功能架构 |
| SG13 | Y.3514 | 云计算 – 可信的跨云计算框架和要求 |
| SG13 | Y.3516 | 跨云计算的功能架构 |
| SG13 | Y.3517 | 云计算 – 云间信任管理综述 |
| SG13 | Y.3650 | 基于深度包检测的大数据驱动网络框架 |
| SG13 | Y.3802 | 量子密钥分布网络 –功能架构 |
| SG13 | Y.3803 | 量子密钥分发网络 – 密钥管理 |
| SG13 | Y.3804 | 量子密钥分发网络 – 控制和管理 |
| SG13 | Y.3805 | 量子密钥分配网络 – 软件定义网络控制 |
| SG13 | Y.3806 | 量子密钥分布网络–服务质量保障的要求 |
| SG15 | G.873.1 | 光传输网络（OTN）：线性保护 |
| SG15 | G.873.3 | 光传输网络（OTN）– 共享网状保护 |
| SG15 | G.8132/ Y.1383  （修订版） | MPLS-TP环保护 |
| SG15 | G.9978 | 基于统一高速有线线路的家庭网络收发器 – 安全接纳 |
| SG16 | H.248.77 | 网关控制协议：安全实时传输协议（SRTP）包和程序 |
| SG20 | Y.4457 | 提供交通安全服务的架构框架 |
| SG20 | Y.4808 | 打击IoT中假冒行为的数字实体架构框架 |
| SG20 | Y.4810 | 异构物联网设备的数据安全要求 |

同意的增补和附录

| **研究组** | **编号** | **标题** |
| --- | --- | --- |
| SG13 | Y.3100-系列 增补44 | 与IMT-2020网络软件化相关的标准化和开源活动 |

已同意的建议书草案

|  |  |  |
| --- | --- | --- |
| **研究组** | **编号** | **标题** |
| SG13 | Y.2086  (Y.DNI-fr) | 分散可信网络基础设施的框架和要求  （于2021年7月16日同意） |
| SG13 | Y3807 (Y.QKDN-QoS-pa) | 量子密钥分发网络 –服务质量参数  （于2021年12月10日同意） |
| SG13 | Y.3808 (Y.QKDN-frint) | 量子密钥分发网络和安全存储网络的集成框架  （于2021年12月10日同意） |
| SG13 | Y.3809 (Y.QKDN-BM) | 量子密钥分发网络 – 基于业务角色的模型  （于2021年12月10日同意） |

### 3.3.2 身份管理（IdM）牵头研究组活动

根据世界电信标准化全会（WTSA-16）第2号决议，第17研究组被指定为负责身份管理（IdM）研究工作的牵头研究组。

作为身份管理的牵头研究组，第17研究组负责研究有关IdM适当的核心课题。此外，第17研究组与其他相关研究组协商和合作（必要时与其他标准机构协商和合作），负责定义和维护整体框架，并协调、分配（认识到研究组的职责）和确定各研究组将进行的研究的轻重缓急，确保建议书编制的一致性、完整性和及时性。

特别是，第17研究组负责研究开发一种通用的身份管理模式，该模式独立于网络技术，并支持实体之间的身份信息的安全交换。这项工作还包括研究发现身份信息的权威来源的过程；不同身份信息格式的桥接/互操作的通用机制；身份管理威胁以及防范机制；保护个人身份信息（PII），并开发确保仅有通过授权并适当时才能访问PII的机制。

以下是国际电联各研究组关于IdM问题的工作现状：

ITU-T各研究组（第17研究组以外的研究组）在其IdM建议书工作方面已取得了下列成果：

批准的建议书

| **研究组** | **建议书** | **标题** |
| --- | --- | --- |
| SG3  SG17 | D.1140 X.1261\*\*\* | 包括原则在内的数字身份基础设施政策框架 |
| SG2 | E.217修订版 | 水上通信：船舶电台标识 |
| SG11 | Q.4063 | 物联网识别系统测试框架 |
| SG11 | Q.5052 | 研究解决移动设备具有重复唯一标识符的问题 |
| SG15 | L.207 | 具有自动身份标签检测的无源节点元件 |
| SG16 | H.273 | 用于视频信号类型识别的独立于编码的代码点 |
| SG17 | X.1252修订版 | 基线身份管理的术语和定义 |
| SG17 | X.1403 | 将分布式账本用于去中心化身份管理的安全指南 |
| SG20 | Y.4805 | 智慧城市应用互操作性的标识符服务要求 |
| SG20 | Y.4476 | 分配给物联网（IoT）资源的分布式账本交易的、基于OID的解析框架 |
| SG20 | Y.4809 | 智能交通系统的物联网标识符 |
| SG20 | Y.4811 | 分散环境下物联网设备识别和认证融合业务的参考框架 |

\*\*\* D.1140（SG3）的双重编号 - X.1261（第17研究组）

此外，关于身份管理的牵头研究组网页在第17研究组网站上维护，与关键资源直接链接。

### 3.3.3 关于语言和描述技术的牵头研究组活动

根据世界电信标准化全会（WTSA-16）第2号决议，第17研究组被指定为关于语言和描述技术的牵头研究组。

作为语言和描述技术的牵头研究组，第17研究组负责关于电信的语言和描述技术：

– 向ITU-T成员和其他研究组提供关于语言和描述技方面的指南；

– 维护电信领域使用的关于语言和描述技术的ITU-T系列建议书和其他指南；

– 如果ITU-T的建议书未定义适用的语言，则通过使用其他渠道推荐合适的语言；

– 与其他使用或定义补充语言和描述技术的经认可机构（如IETF和OMG）互动。

第11/17和12/17号课题已经在ASN.1、SDL、MSC、URN和TTCN的语言和描述技术方面取得富有成效的成果。与其他研究组和组织的广泛合作帮助推进了相关工作。

第11/17号课题与ISO/IEC JTC 1/SC 6/WG 10就抽象句法表示法（ASN.1）的研究进行合作，该标准作为通用文本在X.680/X.690/X.890-系列中出版。[ASN.1模块数据库](http://www.itu.int/ITU-T/recommendations/fl.aspx?lang=1)继续有新的增加，使实施者能够获得句法经检查的、机器可读的、已发布的ASN.1规范。该数据库包含200多份ITU-T 建议书的大约900个模块以及它们所引用的其他标准制定组织的模块。

规范和描述语言（SDL-2010）用于定义系统，既作为建议书中的参考模型，也作为实施。SDL-2010句法在Z.101至Z.107中有定义，在Z.100的附件F中有正式定义。第12/17号课题更新了正式定义。这项研究的好处是检测和解决Z.101到Z.107文本中的歧义、错误和不一致。2019年9月5日，一个完全符合SDL-2010标准的正式定义获得AAP批准。与此同时，更新的Z.100至Z.107文本获得AAP批准，以消除歧义、错误和不一致。2019年9月5日经修订的Z.Imp100获得同意，对Z.100至Z.107文本进行了空列表修改，同意采用AAP批准，并列出以前生效的文本。最终的结果是一个定义更好的SDL-2010年和前后一致的正式定义。目前没有进一步的工作计划。

第12/17号课题与ETSI TC MTS保持密切联系并合作维护关于TTCN-3的Z.160和Z.170系列建议书。批准了三个新的和25个修订文本。

另外，关于语言和描述技术的牵头研究组主页由第17研究组网站维护，提供每种语言的概述。

### 3.3.4 有关身份管理的活动（JCA-IdM）

关于身份管理（JCA-IdM）的联合协调活动从上个研究期一直持续到本研究期（向TSAG推荐并获得认可）。CA-IdM在第17研究组会议期间举行了六次会议：2017年8月/9月、2018年3月、2018年8月/9月、2019年8月/9月、2021年4月和2021年8月/9月，与ITU-T内部小组和相关外部组织（如分散身份基金会、FIDO联盟、ISO/IEC JTC 1/SC 27/WG 5、ISO TC 307、Kantara举措、移动驾驶许可、NH-ISAC身份工作组、OASIS、OpenIdD基金会、Sovrin基金会、SSI开放标准和万国邮联）协调ITU-T身份管理（IdM）工作。

### 3.3.5 第17研究组非洲区域组（SG17RG-AFR）

第17研究组在上一个研究期于2015年4月成立的非洲区域组（SG17RG-AFR）在本研究期继续开展工作。2019年4月2日至3日在本研究期内与SG17RG-ARB举行了一次联席会议。

### 3.3.6 第17研究组阿拉伯区域组（SG17RG-ARB）

在第17研究组2017年3月会议上，第17研究组成立了阿拉伯区域组。第一次会议于2017年12月在阿曼马斯喀特举行。第二次会议于2018年10月在科威特举行，第三次会议于2019年4月2日至3日在突尼斯举行。第三次会议是与SG17RG-AFR联合召开的。

在所有第17研究组区域组会议中，第17研究组顾问都进行了缩小标准化差距辅导。来自各区域国家的与会者就网络安全议题举行了集思广益讨论，并确定了他们特别感兴趣的议题，供进一步研究。

## 3.4 项目

SG 17ASN.1 & OID项目继续协助：

– ITU-T内部和外部现有的ASN.1和对象标识符（OID）用户（例如，ITU‑T SG 16、ISO/IEC JTC 1/SC 27、ISO TC 215、3GPP等）。

– 国家，尤其是发展中国家为OID建立注册机构。

该项目提供扬声器和辅导材料，并协调支持用户和相关网站内容的提供工具。

### 3.4.1 ASN.1项目

由Thorpe先生领导的ASN.1项目旨在在ITU-T内外（如ITU-T SG16、ISO/IEC JTC 1/SC27、ISO/TC 215、ETSI LI、3GPP等）为ASN.1（ITU-T X.680、X.690和X.890系列）用户提供帮助。它还有助于电信标准化局不断更新无误差的ASN.1模块数据库。ASN.1模块数据库不断有新的增加，使实施者可以获得经检查的句法、机器可读、公布的ASN.1规范。该数据库包含200多份ITU-T建议书的模块以及这些建议书参考的其它SDO的模块。

与电信标准化局合作建立的数据库，包括一份机器可处理的拷贝，内存有所有纳入ITU-T建议书的在用版本的ASN.1模块。与其它标准制定机构相比，提供的在线ASN.1模块数据库是可供ITU-T使用的极具增值性的工具。它能够提高行业效率，节约时间和资金。相关ITU-T建议书的实施工作要求使用电子格式（使用ASCII编码），以便在现有工具中直接处理形式定义。从打印或后记（post script）文件中获得ASCII编码需要重新打字，这既妨碍了迅速实施，又可能导致错误。将所有ASN.1模块集中起来，可以极大方便相关协议的实施。ASN.1数据库还包括选自多个其它标准机构的模块。

### 3.4.2 OID项目

OID是一种对标准中使用或定义的对象进行普遍和明确引证的方式。正在积极通过与ISO/IEC JTC 1/SC 6协作，继续开展第11/17号课题的工作 – ITU-T的对象识别符（OID）分层注册（ITU-T X.660和X.670系列）。

在网站<http://www.oid-info.com>上，OID存储库截至2021年11月16日记录的国际OID树的注册超过1 643 596个（<http://www.oid-info.com/cgi-bin/display?a=count_nodes>），通过由ITU-T和ISO/IEC联合控制的分层分配方案提供对象识别（任何类别的）。OID有助于使用世界上任何语言（以结构和分层方式）识别对象。

特别是，ITU-T X.677建议书 – 使用对象标识符的无人机识别机制 – 获得批准。该建议书从安全考虑出发，分析了无人机（UAV）全寿命周期管理和操作身份识别的要求。此建议书还规定了使用对象标识符的无人机识别机制（OID）。

由Olivier Dubuisson先生领导的OID项目有助于国家主管部门和ISO/IEC的各国机构为其国家的OID确定注册机构，如巴林、贝宁、厄瓜多尔、牙买加和越南。

## 3.5 缩小标准化工作差距

在本次研究期的所有第17研究组的实体会议中，电信标准化局为第17研究组的新人举行欢迎招待会并参观国际电联办公场所。第17研究组主席组织了“第17新人迎新会和新人与第17研究组管理层的讨论”。2019年1月，第17研究组顾问组织了“第17研究组顾问诊所”，回答第17研究组代表关于第17研究组工作方法的问题。2019年9月，电信标准化局为第17研究组报告人和编辑组织了“ITU-T领导团队培训”。

2018年3月17日至2018年9月，第17研究组在其研究组会议期间定期为发展中国家组织实践培训课程。通过这些会议广泛介绍了国际电联的缩小标准化工作差距（BSG）计划、活动和项目，并为发展中国家提供了极佳的向第17研究组提出建议的平台。这些相关会议大大促进了发展中国家表达自身利益和要求。

在此研究期，第17研究组在其电子化会议期间定期为来自非洲和阿拉伯国家的代表分别组织网上非正式会议，以促进关于SG17RG-AFR和SG17RG-ARB未来规划的讨论。

# 4 有关未来工作的考虑

第17研究组的安全研究工作在整个研究期内有了持续和显著的进展，建成了一个具有安全核心能力的高级培训中心。第17研究组是标准化部门负责安全工作的牵头研究组。为安全建议书/标准的制定奠定了坚实基础，与其它机构的良好合作和协调已安排就绪，并且通过第17研究组报告的第二部分为下一研究期提出了强有力的安全课题持续研究计划。鉴于树立使用信息通信技术（ICT）的信心并提高安全性是国际电联的重点工作之一，ITU-T的这一安全能力得到培育、扩大和加强、而非分裂瓦解是至关重要的。

应通过制定建议书和技术报告，考虑到基于电信/ICT网络的新服务和新兴应用，解决影响安全的现有和未来威胁和脆弱性，以树立使用ICT的信心并提高安全性。安全技术是保护ICT系统免受其硬件、软件或信息的攻击或损害，以及免受其提供的服务的中断或误导的基本要素。

需要新的安全方法和措施以充分应对安全威胁和风险。第17研究组在制定安全领域的国际标准方面发挥着关键作用。

电信和ICtus的安全仍然是需要安全标准的一个领域。管理电信和ICT领域新出现的威胁，包括网络基础设施、系统、应用和服务，极其重要。众所周知，必须制定满足所有国家需要的可执行的安全标准和导则。

管理电信和ICT基础设施中层出不穷的新的威胁至关重要。第17研究组已开展的有关安全（包括异质网络/系统/服务的通用安全架构、框架、要求、机制、协议和管理导则）的研究工作应该延续，而且需要一个安全问题牵头研究组负责国际电联内部以及与其它标准制定组织（SDO）的协调。第17研究组了解制定满足各国需求的有关安全的可实施标准和导则的重要性。

加强个人可识别信息（PII）的安全框架和保护，是发展高度互联的信息社会和在信息通信技术（ICT）用户之间建立信任、信赖和安全的先决条件。应用程序和服务中使用的数据受到适当的安全技术以及组织和物理措施的保护。电信和ICT的安全和由二者提供的安全保障仍然是需要安全标准的领域。云计算（包括边缘云计算、多云计算）、智能电网、智能工厂、智能交通系统、第五代的蜂窝网络、软件定义的网络、网络功能虚拟化、网络切片、大数据分析、物联网、分布式账本技术、智能交通系统和基于量子的安全等新兴技术需要技术和组织措施应对各种威胁和风险，保护公民的PII，以及保护在线儿童的技术和组织措施。可能需要新的基于安全风险评估的方法和措施以充分应对安全威胁和风险。第17研究组在制定这些领域的国际标准方面发挥着关键作用。为不断演进的技术开发急需的安全方法最好由具备现有安全方法专业知识的研究组进行。

第17研究组通过其在安全方面开展的牵头研究活动以及相关联络和协调工作，作为协调方法发挥牵头作用，不断认识到其他研究组开展的安全活动和其他标准化机构及联盟进行的工作。预期在未来，第17研究组将继续开展十分重要的联络和协调活动。第17研究组以其过去良好的行动表明，它能与其他SDO进行良好协作，共同制定建议书/标准。总体而言，第17研究组作为牵头研究组，为了能够更好地支持其安全标准化活动，充分利用了联络手段（信函通信、正式的A.4/A.5/A.6联络合作）以及相互参引和共同开发（A.23/A.25）。

第17研究组亦是身份管理（IdM）牵头研究组，是全球范围内数字身份管理、建立信任、保护个人信息、实现包括网络或服务接入控制的网络运行、实施在线电子交易、Fintech、OTT和数字金融服务等的关键性促成方。鉴于身份管理在增强使用ICT的信心和安全性方面的重要作用，因此是作为ITU-T安全牵头研究组的第17研究组活动不可分割的部分。第17研究组继续在国际电联内部以及与其它SDO之间开展协调IdM（包括基于DLT的去中心化标识）的工作，其有关PKI、ASN.1和OID的工作对诸多ICT部门均十分有益。

新的电信/ICT环境，如物联网、ITS、智能工厂、智慧城市/社区以及智能电网，需要利用PKI的新的安全要求。最初的PKI只是为了保护网上银行。PKI的设计不是为了应对具有低容量实体、数百万或数十亿无人干预的实体的环境。如果不加强PKI以适应这些新环境，物联网、智能工厂和智能电网安全的主要方面将失败，对社会和人们的日常生活产生巨大影响，因为它将影响重要基础设施的主要部分的稳定性。在下一研究期，加强PKI基础建设以应付新环境的工作应获优先处理。

为有效实现安全，需要制定新的标准。国际电联电联一直都认识到，诸如抽象句法表示法一（ASN.1）等结构表达工具十分重要。在ASN.1方面，已取得了极大进步，确保ITU-T建议书中的ASN.1符合ASN.1定义并提供机器可读文档。将这一方法（和支持国际电联资源）扩大至其它规范语言（如规范和描述语言（SDL））可进一步增强优质建议书固有的安全性。产品使用这些建议书将受益匪浅。除编拟建议书的形式语言外，国际电联也为编写一致性（及其它）测试提供了测试和测试控制标记（TTCN）。

# 5 WTSA第2号决议在2022-2024年研究期的更新

附件2包含第17研究组就下一研究期的题目、总体研究领域、牵头作用、指导和建议书要点提出的、对WTSA第2号决议的更新。

附件1

本研究期制定或删除的建议书、增补及其它资料清单

本研究期内批准的新的和经修订的建议书见表7。

表7列出了本研究期内截至本表制成之日（2022年1月7日）批准的**建议书、修正和勘误**的清单。案文按建议书（字母数字）和批准日期（最早的版本在前）排序。两次编号的建议书将出现一次。其他研究组也在研究的建议书，将只出现在批准它的研究组的清单中。

表8列出第17研究组上一次会议确定/同意的建议书。

案文按建议书（字母数字顺序）排序。具有双编号的建议书将出现一次。由其他研究组跟进的建议书将仅出现在同意或确定该建议书的研究组下。

注 – 本报告中的最后一次会议指2022年1月7日的会议。

表9列出第17研究组在本研究期删除的建议书。案文按建议书（字母数字顺序）排序。具有双编号的建议书将出现一次。

表10列出第17研究组提交WTSA-20批准的建议书。

从表11之后列出第17研究组在本研究期批准和/或取消的其它出版物。

表11列出了截至2022年1月7日（生成表格期间）本研究期同意的增补。

**表7**

**第17研究组 – 本研究期批准的建议书**

| 建议书 | 批准 | 状况 | TAP/AAP | 标题 |
| --- | --- | --- | --- | --- |
| [X.500](http://handle.itu.int/11.1002/1000/14031) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：概念、模型和服务概述 |
| [X.501](http://handle.itu.int/11.1002/1000/14032) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：模型 |
| [X.501 (2019) Amd. 1](http://handle.itu.int/11.1002/1000/14790) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿 – 模型 – 修正1：各类改进 |
| [X.509](http://handle.itu.int/11.1002/1000/14033) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：公共密钥属性证书框架 |
| [X.509 (2019) Cor. 1](http://handle.itu.int/11.1002/1000/14791) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿 – 公共密钥属性证书框架：勘误 |
| [X.510](http://handle.itu.int/11.1002/1000/14320) | 2020-08-22 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：安全运行的协议规范 |
| [X.511](http://handle.itu.int/11.1002/1000/14034) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：抽象服务定义 |
| [X.518](http://handle.itu.int/11.1002/1000/14035) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：分布运行程序 |
| [X.519](http://handle.itu.int/11.1002/1000/14036) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：协议规范 |
| [X.520](http://handle.itu.int/11.1002/1000/14037) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：选择的属性类别 |
| [X.521](http://handle.itu.int/11.1002/1000/14038) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：选择的对象类别 |
| [X.525](http://handle.itu.int/11.1002/1000/14047) | 2019-10-14 | 现行 | AAP | 信息技术 – 开放系统互连 – 号码簿：复制 |
| [X.676](http://handle.itu.int/11.1002/1000/13712) | 2018-11-29 | 现行 | AAP | 物联网分组服务基于对象识别符的解析框架 |
| [X.677](http://handle.itu.int/11.1002/1000/14039) | 2020-03-08 | 现行 | AAP | 使用目标标识符的无人机识别机制 |
| [X.680 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13257) | 2017-05-14 | 取代 | AAP |  |
| [X.680 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13361) | 2017-10-14 | 取代 | AAP |  |
| [X.680 (2015) Cor.3](http://handle.itu.int/11.1002/1000/13598) | 2018-05-14 | 取代 | AAP |  |
| [X.680 (2015) Amd.1](http://handle.itu.int/11.1002/1000/13597) | 2018-05-14 | 取代 | AAP | 放松IMPORTS条款以便从给定模块的新版本导入定义 |
| [X.680](http://handle.itu.int/11.1002/1000/14468) | 2021-02-13 | 现行 | AAP | 信息技术 – 抽象语法标记1（ASN.1）：基本标记的规范 |
| [X.681 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13599) | 2018-05-14 | 取代 | AAP |  |
| [X.681](http://handle.itu.int/11.1002/1000/14469) | 2021-02-13 | 现行 | AAP | 信息技术 – 抽象语法标记1（ASN.1）：信息对象的规范 |
| [X.682 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13362) | 2017-10-14 | 取代 | AAP |  |
| [X.682 (2015) Cor.2](http://handle.itu.int/11.1002/1000/13600) | 2018-05-14 | 取代 | AAP |  |
| [X.682](http://handle.itu.int/11.1002/1000/14470) | 2021-02-13 | 现行 | AAP | 信息技术 – 抽象语法标记1（ASN.1）：限制的规范 |
| [X.683 (2015) Cor.1](http://handle.itu.int/11.1002/1000/13601) | 2018-05-14 | 取代 | AAP |  |
| [X.683](http://handle.itu.int/11.1002/1000/14471) | 2021-02-13 | 现行 | AAP | 信息技术 – 抽象语法标记1（ASN.1）：ASN.1参数化的规范 |
| [X.690](http://handle.itu.int/11.1002/1000/14472) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：基本编码规则（BER）的规范、规范编码规则（CER）和区分编码规则（DER） |
| [X.691](http://handle.itu.int/11.1002/1000/14473) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：分组编码规则（PER）的规范 |
| [X.692](http://handle.itu.int/11.1002/1000/14474) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：编码控制记法（ECN）的规范 |
| [X.693 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13363) | 2017-10-14 | 取代 | AAP |  |
| [X.693](http://handle.itu.int/11.1002/1000/14475) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：XML编码规则（XER）的规范 |
| [X.694 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/14040) | 2019-10-14 | 取代 | AAP |  |
| [X.694](http://handle.itu.int/11.1002/1000/14476) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：将W3C XML方案定义映射至ASN.1 |
| [X.695](http://handle.itu.int/11.1002/1000/14477) | 2021-02-13 | 现行 | AAP | 信息技术 –ASN.1编码规则：注册并应用PER编码指 |
| [X.696 (2015) Cor. 1](http://handle.itu.int/11.1002/1000/13258) | 2017-05-14 | 取代 | AAP |  |
| [X.696 (2015) Cor. 2](http://handle.itu.int/11.1002/1000/13364) | 2017-10-14 | 取代 | AAP |  |
| [X.696 (2015) Cor. 3](http://handle.itu.int/11.1002/1000/13602) | 2018-05-14 | 取代 | AAP |  |
| [X.696](http://handle.itu.int/11.1002/1000/14478) | 2021-02-13 | 现行 | AAP | 信息技术 – ASN.1编码规则：八位字节编码规则（OER）的规范 |
| [X.697](http://handle.itu.int/11.1002/1000/13365) | 2017-10-14 | 取代 | AAP | 信息技术 – ASN.1编码规则：规定JavaScript对象表示法的编码规则（JER） |
| [X.697](http://handle.itu.int/11.1002/1000/14479) | 2021-02-13 | 现行 | AAP | 信息技术 – ASN.1编码规则：规定JavaScript对象表示法的编码规则（JER） |
| [X.893 (2007) Cor.1](http://handle.itu.int/11.1002/1000/14041) | 2019-10-14 | 现行 | AAP |  |
| [X.894](http://handle.itu.int/11.1002/1000/12848) | 2018-10-14 | 现行 | AAP | 信息技术 – ASN.1的普遍应用 – 加密信息句法 |
| [X.894 (2018) Cor.1](http://handle.itu.int/11.1002/1000/13871) | 2019-03-16 | 现行 | AAP |  |
| [X.894 (2018) Cor. 2](http://handle.itu.int/11.1002/1000/14467) | 2021-02-13 | 现行 | AAP | ASN.1的普遍应用：加密消息语句的技术勘误2 |
| [X.1011](http://handle.itu.int/11.1002/1000/14793) | 2021-10-29 | 现行 | AAP | 持续保护服务访问过程的导则 |
| [X.1040](http://handle.itu.int/11.1002/1000/13366) | 2017-10-14 | 现行 | AAP | 用于电子商务业务数据生命周期管理的安全参考架构。 |
| [X.1041](http://handle.itu.int/11.1002/1000/13603) | 2018-05-14 | 现行 | AAP | 长期演进网络语音（VoLTE）网络操作的安全框架 |
| [X.1042](http://handle.itu.int/11.1002/1000/13803) | 2019-01-30 | 现行 | TAP | 使用软件定义网络的安全业务 |
| [X.1043](http://handle.itu.int/11.1002/1000/13872) | 2019-03-16 | 现行 | AAP | 基于软件定义网络的服务功能链的安全框架和要求 |
| [X.1044](http://handle.itu.int/11.1002/1000/14042) | 2019-10-29 | 现行 | AAP | 网络虚拟化的安全要求 |
| [X.1045](http://handle.itu.int/11.1002/1000/14043) | 2019-10-29 | 现行 | AAP | 用于网络和应用软件的安全服务链架构 |
| [X.1046](http://handle.itu.int/11.1002/1000/14442) | 2020-12-14 | 现行 | AAP | 软件定义网络/网络功能虚拟化网络中的软件定义安全框架 |
| [X.1047](http://handle.itu.int/11.1002/1000/14794) | 2021-10-29 | 现行 | AAP | 网络切片管理和编排的安全要求和体系架构 |
| [X.1051 (2016) Cor.1](http://handle.itu.int/11.1002/1000/13407) | 2017-09-06 | 现行 | 同意 |  |
| [X.1052](http://handle.itu.int/11.1002/1000/14044) | 2020-10-29 | 现行 | AAP | 电信机构的信息安全管理流程 |
| [X.1053](http://handle.itu.int/11.1002/1000/13367) | 2017-11-13 | 现行 | AAP | 基于ITU-T X.1051的中小电信组织信息安全控制行为守则 |
| [X.1058](http://handle.itu.int/11.1002/1000/13182) | 2017-03-30 | 现行 | TAP | 信息技术 – 安全技术 – 个人可识别信息保护的实施规程 |
| [X.1059](http://handle.itu.int/11.1002/1000/14045) | 2019-10-29 | 现行 | AAP | 对拥有可接入基于IP的网络的全球资产的电信组织进行风险管理的指导 |
| [X.1060](http://handle.itu.int/11.1002/1000/14721) | 2021-06-29 | 现行 | AAP | 创建和运营网络防御中心的框架 |
| [X.1061](http://handle.itu.int/11.1002/1000/14733) | 2021-08-22 | 现行 | AAP | 网络保险收购导则 |
| [X.1080.0](http://handle.itu.int/11.1002/1000/13193) | 2017-03-30 | 现行 | TAP | 电子生物特征识别数据保护的访问控制 |
| [X.1080.0 (2017) Cor.1](http://handle.itu.int/11.1002/1000/13591) | 2018-03-29 | 现行 | 同意 |  |
| [X.1080.1](http://handle.itu.int/11.1002/1000/13604) | 2018-05-14 | 现行 | AAP | 电子卫生和全球远程医疗 – 通用电信协议 |
| [X.1080.2](http://handle.itu.int/11.1002/1000/14795) | 2021-10-29 | 现行 | AAP | 生物到机器（B2M）协议 |
| [X.1093](http://handle.itu.int/11.1002/1000/13725) | 2018-11-13 | 现行 | AAP | 智能ID卡的电子生物访问控制 |
| [X.1094](http://handle.itu.int/11.1002/1000/13873) | 2019-03-16 | 现行 | AAP | 使用生物信号的电子生物特征识别认证 |
| [X.1126](http://handle.itu.int/11.1002/1000/13194) | 2017-03-30 | 现行 | TAP | 减缓移动网络中受感染终端负面影响的导则 |
| [X.1127](http://handle.itu.int/11.1002/1000/13259) | 2017-09-06 | 现行 | TAP | 手机防盗措施的功能安全性要求和架构 |
| [X.1145](http://handle.itu.int/11.1002/1000/13260) | 2017-05-14 | 现行 | AAP | 电信设备开放能力的安全框架和要求 |
| [X.1146](http://handle.itu.int/11.1002/1000/13368) | 2017-10-14 | 现行 | AAP | 电信运营商提供的增值服务的安全保护导则 |
| [X.1147](http://handle.itu.int/11.1002/1000/13726) | 2018-11-13 | 现行 | AAP | 移动互联网服务中大数据分析的安全要求和框架 |
| [X.1148](http://handle.itu.int/11.1002/1000/14249) | 2020-09-03 | 现行 | TAP | 电信服务提供商的去身份识别进程框架 |
| [X.1149](http://handle.itu.int/11.1002/1000/14250) | 2020-05-29 | 现行 | AAP | 金融技术服务开放平台的安全框架 |
| [X.1197 (2012) Amd. 1](http://handle.itu.int/11.1002/1000/14046) | 2019-09-05 | 现行 | 同意 |  |
| [X.1212](http://handle.itu.int/11.1002/1000/13195) | 2017-03-30 | 现行 | TAP | 增强最终用户对可信指示符的感知的设计考虑 |
| [X.1213](http://handle.itu.int/11.1002/1000/13261) | 2017-09-06 | 现行 | TAP | 打击基于智能电话的僵尸网路的安全能力要求 |
| [X.1214](http://handle.itu.int/11.1002/1000/13404) | 2018-03-29 | 现行 | TAP | 电信/信息通信技术网络的安全评定技术手段 |
| [X.1215](http://handle.itu.int/11.1002/1000/13849) | 2019-01-30 | 现行 | TAP | 结构化威胁信息表达式的用例 |
| [X.1216](http://handle.itu.int/11.1002/1000/14259) | 2020-09-03 | 现行 | TAP | 收集和保存网络安全事件证据的要求 |
| [X.1217](http://handle.itu.int/11.1002/1000/14443) | 2021-01-07 | 现行 | TAP | 电信网络运营中的威胁情报使用导则 |
| [X.1218](http://handle.itu.int/11.1002/1000/14444) | 2020-10-29 | 现行 | AAP | 沙箱环境中动态恶意软件分析的要求和指南 |
| [X.1232](http://handle.itu.int/11.1002/1000/14085) | 2019-10-29 | 现行 | AAP | 打击在用户生成的信息中植入推广垃圾信息的技术框架 |
| [X.1233](http://handle.itu.int/11.1002/1000/14773) | 2021-09-03 | 现行 | TAP | 打击通过即时消息传播的垃圾邮件的导则 |
| X.1234 | 2022-01-07 | 现行 | TAP | 关于打击多媒体消息服务（MMS）垃圾信息的导则 |
| X.1235 | 2022-01-07 | 现行 | TAP | 电信组织打击网站欺骗的技术 |
| [X.1248](http://handle.itu.int/11.1002/1000/13262) | 2017-09-06 | 现行 | TAP | 打击即时消息垃圾信息的技术要求 |
| [X.1249](http://handle.itu.int/11.1002/1000/13605) | 2019-01-30 | 现行 | TAP | 打击手机应用内植入的广告垃圾信息的技术框架 |
| [X.1252](http://handle.itu.int/11.1002/1000/14642) | 2021-04-30 | 现行 | TAP | 身份管理基准术语和定义 |
| [X.1254](http://handle.itu.int/11.1002/1000/14260) | 2020-09-03 | 现行 | TAP | 实体认证保证框架 |
| [X.1276](http://handle.itu.int/11.1002/1000/13606) | 2018-05-14 | 现行 | AAP | 认证升级协议和元数据1.0版 |
| [X.1277](http://handle.itu.int/11.1002/1000/13727) | 2018-11-29 | 现行 | AAP | 通用认证框架 |
| [X.1278](http://handle.itu.int/11.1002/1000/13728) | 2018-11-29 | 现行 | AAP | 客户端到认证器协议/通用双重框架 |
| [X.1279](http://handle.itu.int/11.1002/1000/14261) | 2020-09-03 | 现行 | TAP | 使用具有反欺骗检测机制的电子生物特征识别的增强认证框架 |
| [X.1331](http://handle.itu.int/11.1002/1000/13405) | 2018-03-29 | 现行 | TAP | 智能电网系统中家域网（HAN）设备的安全导则 |
| [X.1332](http://handle.itu.int/11.1002/1000/14086) | 2020-03-26 | 现行 | TAP | 智能电网系统中智能电表业务的安全导则 |
| X.1333 | 2022-01-07 | 现行 | TAP | 在联网控制系统中使用远程访问工具的安全导则 |
| [X.1361](http://handle.itu.int/11.1002/1000/13607) | 2018-09-07 | 现行 | TAP | 基于网关模型的物联网安全框架 |
| [X.1362](http://handle.itu.int/11.1002/1000/13196) | 2017-03-30 | 现行 | TAP | 物联网（IoT）环境的简单加密 程序 |
| [X.1363](http://handle.itu.int/11.1002/1000/14087) | 2020-05-29 | 现行 | TAP | 物联网环境中处理个人身份信息的技术框架 |
| [X.1364](http://handle.itu.int/11.1002/1000/14088) | 2020-03-26 | 现行 | TAP | 窄带物联网的安全要求和框架 |
| [X.1365](http://handle.itu.int/11.1002/1000/14089) | 2020-03-26 | 现行 | TAP | 在电信网络上使用基于身份的密码来支持物联网（IoT）服务的安全方法 |
| [X.1366](http://handle.itu.int/11.1002/1000/14262) | 2020-09-03 | 现行 | TAP | 物联网环境的汇集消息认证方案 |
| [X.1367](http://handle.itu.int/11.1002/1000/14263) | 2020-09-03 | 现行 | TAP | 物联网安全事件操作的错误日志标准格式 |
| [X.1368](http://handle.itu.int/11.1002/1000/14445) | 2021-01-07 | 现行 | TAP | 物联网设备的安全固件或软件更新 |
| X.1369 | 2022-01-07 | 现行 | TAP | 物联网服务平台的安全要求 |
| [X.1371](http://handle.itu.int/11.1002/1000/14090) | 2020-05-29 | 现行 | TAP | 联网车辆面临的安全威胁 |
| [X.1372](http://handle.itu.int/11.1002/1000/14091) | 2020-03-26 | 现行 | TAP | 车联网（V2X）通信的安全导则 |
| [X.1373](http://handle.itu.int/11.1002/1000/13197) | 2017-03-30 | 现行 | TAP | 智能交通系统通信设备的安全软件更新功能 |
| [X.1374](http://handle.itu.int/11.1002/1000/14446) | 2020-10-29 | 现行 | AAP | 具有接入车辆能力的外部接口和设备的安全要求 |
| [X.1375](http://handle.itu.int/11.1002/1000/14447) | 2020-10-29 | 现行 | AAP | 车载网络入侵检测系统导则 |
| [X.1376](http://handle.itu.int/11.1002/1000/14448) | 2021-01-07 | 现行 | TAP | 利用大数据针对与联网车辆安全相关的不当行为开展检测的机制 |
| [X.1400](http://handle.itu.int/11.1002/1000/14449) | 2020-10-29 | 现行 | AAP | 分布式账本技术的术语和定义 |
| [X.1401](http://handle.itu.int/11.1002/1000/14092) | 2019-11-29 | 现行 | AAP | 分布式账本技术的安全威胁 |
| [X.1402](http://handle.itu.int/11.1002/1000/14251) | 2020-07-22 | 现行 | AAP | 分布式账本技术的安全框架 |
| [X.1403](http://handle.itu.int/11.1002/1000/14264) | 2020-09-03 | 现行 | TAP | 将分布式账本技术用于去中心化身份管理的安全指南 |
| [X.1404](http://handle.itu.int/11.1002/1000/14450) | 2020-10-29 | 现行 | AAP | 分布式账本技术的安全保证 |
| [X.1405](http://handle.itu.int/11.1002/1000/14722) | 2021-06-29 | 现行 | AAP | 基于分布式账本技术的数字支付服务的安全威胁和要求 |
| [X.1406](http://handle.itu.int/11.1002/1000/14734) | 2021-07-14 | 现行 | AAP | 使用分布式账本技术对在线投票系统产生的安全威胁 |
| X.1407 | 2022-01-07 | 现行 | TAP | 基于分布式账本技术的数字完整性证明服务的安全要求 |
| [X.1408](http://handle.itu.int/11.1002/1000/14801) | 2021-10-29 | 现行 | AAP | 基于分布式账本技术的数据访问和共享的安全威胁和要求 |
| [X.1450](http://handle.itu.int/11.1002/1000/13729) | 2018-10-14 | 现行 | AAP | 客户端服务器模式中的混合认证和关键管理机制导则 |
| [X.1451](http://handle.itu.int/11.1002/1000/14252) | 2020-05-29 | 现行 | AAP | 优化身份验证的风险识别 |
| [X.1452](http://handle.itu.int/11.1002/1000/14451) | 2020-10-29 | 现行 | AAP | 运营商提供的安全业务导则 |
| X.1453 | 2022-01-07 | 现行 | TAP | 视频管理系统的安全威胁和要求 |
| [X.1470](http://handle.itu.int/11.1002/1000/14803) | 2021-11-13 | 现行 | AAP | 网络在线客服安全导则 |
| [X.1500 (2011) Amd. 11](http://handle.itu.int/11.1002/1000/13263) | 2017-03-30 | 现行 | 同意 | 经修订的结构网络安全信息交换 |
| [X.1500 (2011) Amd. 12](http://handle.itu.int/11.1002/1000/13590) | 2018-03-29 | 现行 | 同意 | 经修订的结构网络安全信息交换 |
| [X.1541](http://handle.itu.int/11.1002/1000/13264) | 2017-09-06 | 现行 | TAP | 事件对象描述交换格式版本2 |
| [X.1550](http://handle.itu.int/11.1002/1000/13198) | 2017-03-30 | 现行 | TAP | 事件交换网络的访问控制模型 |
| [X.1603](http://handle.itu.int/11.1002/1000/13406) | 2018-03-29 | 现行 | TAP | 云计算监测业务的数据安全性要求 |
| [X.1604](http://handle.itu.int/11.1002/1000/14093) | 2020-03-26 | 现行 | TAP | 云计算中网络即服务（NaaS）的安全要求 |
| [X.1605](http://handle.itu.int/11.1002/1000/14094) | 2020-03-26 | 现行 | TAP | 云计算中公共基础设施即服务（IaaS）的安全要求 |
| [X.1606](http://handle.itu.int/11.1002/1000/14265) | 2020-09-03 | 现行 | TAP | 收集和保存网络安全事件证据的要求 |
| X.1643 | 2022-01-07 | 现行 | TAP | 云计算环境中虚拟化容器的安全导则 |
| [X.1702](http://handle.itu.int/11.1002/1000/14095) | 2019-11-13 | 现行 | AAP | 量子噪声随机数生成器架构 |
| [X.1710](http://handle.itu.int/11.1002/1000/14452) | 2020-10-29 | 现行 | AAP | 量子密钥分发网络安全框架 |
| [X.1712](http://handle.itu.int/11.1002/1000/14805) | 2021-10-29 | 现行 | AAP | 量子密钥分发网络的安全要求和设计 |
| [X.1714](http://handle.itu.int/11.1002/1000/14453) | 2020-10-29 | 现行 | AAP | 量子密钥分发网络的密钥组合和机密密钥供应 |
| [X.1750](http://handle.itu.int/11.1002/1000/14266) | 2020-09-03 | 现行 | TAP | 使用具有反欺骗检测机制的远程生物特征识别的增强认证框架 |
| [X.1751](http://handle.itu.int/11.1002/1000/14267) | 2020-09-03 | 现行 | TAP | 电信运营商大数据生命周期管理安全导则 |
| X.1752 | 2022-01-07 | 现行 | TAP | 云计算环境中容器的安全导则 |
| [X.1770](http://handle.itu.int/11.1002/1000/14807) | 2021-10-29 | 现行 | AAP | 安全多方计算技术导则 |
| [X.1811](http://handle.itu.int/11.1002/1000/14454) | 2021-04-30 | 现行 | TAP | 在IMT-2020系统中应用量子安全算法的安全导则 |
| [Z.100附件F1](http://handle.itu.int/11.1002/1000/13732) | 2018-11-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010概述 |
| [Z.100附件 F2](http://handle.itu.int/11.1002/1000/13733) | 2018-11-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010概述 |
| [Z.100附件F3](http://handle.itu.int/11.1002/1000/13734) | 2018-11-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010概述 |
| [Z.100](http://handle.itu.int/11.1002/1000/14048) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – SDL‑2010概述 |
| [Z.100附件F2](http://handle.itu.int/11.1002/1000/14050) | 2019-10-14 | 取代 | AAP | 规范和描述语言- SDL-2010概述-SDL 2010的正式定义：静态语义 |
| [Z.100附件F3](http://handle.itu.int/11.1002/1000/14051) | 2019-10-14 | 取代 | AAP | 规范和描述语言- SDL-2010概述-SDL 2010的正式定义：动态语义 |
| [Z.100](http://handle.itu.int/11.1002/1000/14670) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010概述 |
| [Z.100附件F1](http://handle.itu.int/11.1002/1000/14049) | 2019-10-14 | 现行 | AAP | 规范和描述语言 – SDL‑2010概述 – SDL正式定义概述：一般性概述 |
| [Z.100附件F2](http://handle.itu.int/11.1002/1000/14702) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL概述 – SDL正式定义概述：静态语义 |
| [Z.100附件F3](http://handle.itu.int/11.1002/1000/14703) | 2021-16-13 | 现行 | AAP | 规范和描述语言 – SDL概述 – SDL正式定义概述：动态语义 |
| [Z.101](http://handle.itu.int/11.1002/1000/14052) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – 基础SDL‑2010 |
| [Z.101](http://handle.itu.int/11.1002/1000/14671) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – 基础SDL‑2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14053) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – 全面SDL‑2010 |
| [Z.102](http://handle.itu.int/11.1002/1000/14672) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – 全面SDL‑2010 |
| [Z.103](http://handle.itu.int/11.1002/1000/14054) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – SDL‑2010中的简化表示法和注释 |
| [Z.103](http://handle.itu.int/11.1002/1000/14673) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010中的简化表示法和注释 |
| [Z.104](http://handle.itu.int/11.1002/1000/14055) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – SDL‑2010的数据和行动语言 |
| [Z.104](http://handle.itu.int/11.1002/1000/14674) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010的数据和行动语言 |
| [Z.105](http://handle.itu.int/11.1002/1000/14056) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – 与ASN.1模块合并的SDL‑2010 |
| [Z.105](http://handle.itu.int/11.1002/1000/14675) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – 与ASN.1模块合并的SDL‑2010 |
| [Z.106](http://handle.itu.int/11.1002/1000/14057) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – SDL‑2010的通用交换格式 |
| [Z.106](http://handle.itu.int/11.1002/1000/14676) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010的通用交换格式 |
| [Z.107](http://handle.itu.int/11.1002/1000/14058) | 2019-10-14 | 取代 | AAP | 规范和描述语言 – SDL‑2010中面向对象的数据 |
| [Z.107](http://handle.itu.int/11.1002/1000/14677) | 2021-06-13 | 现行 | AAP | 规范和描述语言 – SDL‑2010中面向对象的数据 |
| [Z.151](http://handle.itu.int/11.1002/1000/13711) | 2018-10-14 | 现行 | AAP | 用户要求表示法（URN）– 语言定义 |
| [Z.161](http://handle.itu.int/11.1002/1000/13369) | 2017-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言 |
| [Z.161](http://handle.itu.int/11.1002/1000/13703) | 2018-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言 |
| [Z.161](http://handle.itu.int/11.1002/1000/14059) | 2019-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言 |
| [Z.161](http://handle.itu.int/11.1002/1000/14480) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言 |
| [Z.161](http://handle.itu.int/11.1002/1000/14781) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言 |
| [Z.161.1](http://handle.itu.int/11.1002/1000/13370) | 2017-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3核心语言：支持连续信号接口 |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13371) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：配置和部署支持 |
| [Z.161.2](http://handle.itu.int/11.1002/1000/13704) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：配置和部署支持 |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14060) | 2019-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：配置和部署支持 |
| [Z.161.2](http://handle.itu.int/11.1002/1000/14782) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：配置和部署支持 |
| [Z.161.3](http://handle.itu.int/11.1002/1000/13372) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级的参数化 |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14481) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级的参数化 |
| [Z.161.3](http://handle.itu.int/11.1002/1000/14783) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级的参数化 |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13373) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：行为类别 |
| [Z.161.4](http://handle.itu.int/11.1002/1000/13705) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展： 行为类别 |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14482) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展： 行为类别 |
| [Z.161.4](http://handle.itu.int/11.1002/1000/14784) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展： 行为类别 |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13374) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级匹配 |
| [Z.161.6](http://handle.itu.int/11.1002/1000/13706) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级匹配 |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14061) | 2019-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级匹配 |
| [Z.161.6](http://handle.itu.int/11.1002/1000/14483) | 2020-10-29 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：高级匹配 |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14062) | 2019-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：面向对象的功能 |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14484) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：面向对象的功能 |
| [Z.161.7](http://handle.itu.int/11.1002/1000/14785) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3语言扩展：面向对象的功能 |
| [Z.164](http://handle.itu.int/11.1002/1000/13375) | 2017-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3操作语义 |
| [Z.165](http://handle.itu.int/11.1002/1000/13376) | 2017-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3运行事件接口（TRI） |
| [Z.165.1](http://handle.itu.int/11.1002/1000/14485) | 2020-10-29 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3扩展包：扩展TRI |
| [Z.166](http://handle.itu.int/11.1002/1000/13377) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3运行事件接口（TRI） |
| [Z.166](http://handle.itu.int/11.1002/1000/13707) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3运行事件接口（TRI） |
| [Z.166](http://handle.itu.int/11.1002/1000/14063) | 2019-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：TTCN-3运行事件接口（TRI） |
| [Z.166](http://handle.itu.int/11.1002/1000/14486) | 2020-10-29 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3 控制接口（TCI） |
| [Z.167](http://handle.itu.int/11.1002/1000/13378) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用ASN.1 |
| [Z.167](http://handle.itu.int/11.1002/1000/13708) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用ASN.1 |
| [Z.167](http://handle.itu.int/11.1002/1000/14487) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用ASN.1 |
| [Z.167](http://handle.itu.int/11.1002/1000/14786) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用ASN.1 |
| [Z.168](http://handle.itu.int/11.1002/1000/13379) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：IDL到TTCN-3的映射 |
| [Z.168](http://handle.itu.int/11.1002/1000/14787) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：IDL到TTCN-3的映射 |
| [Z.169](http://handle.itu.int/11.1002/1000/13380) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用XML模式 |
| [Z.169](http://handle.itu.int/11.1002/1000/13709) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用XML模式 |
| [Z.169](http://handle.itu.int/11.1002/1000/14064) | 2019-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用XML模式 |
| [Z.169](http://handle.itu.int/11.1002/1000/14488) | 2020-10-29 | 取代 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用XML模式 |
| [Z.169](http://handle.itu.int/11.1002/1000/14788) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：通过TTCN-3使用XML模式 |
| [Z.170](http://handle.itu.int/11.1002/1000/13381) | 2017-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：TTCN-3文件评论规范 |
| [Z.171](http://handle.itu.int/11.1002/1000/13382) | 2017-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：对TTCN-3使用JSON |
| [Z.171](http://handle.itu.int/11.1002/1000/13710) | 2018-10-14 | 取代 | AAP | 测试和测试控制表示法版本3：对TTCN-3使用JSON |
| [Z.171](http://handle.itu.int/11.1002/1000/14789) | 2021-10-14 | 现行 | AAP | 测试和测试控制表示法版本3：对TTCN-3使用JSON |

表8

**第17研究组 – 同意/确定（但尚未批准）的建议书**

| 建议书 | 同意/确定 | TAP/AAP程序 | 标题 |
| --- | --- | --- | --- |
| X.672 | 2021-09-03 | AAP | 对象标识解析系统 |
| X.1246修正1 | 2021-09-03 | TAP | 电信组织应对语音垃圾邮件涉及的技术 |
| X.1247修正1 | 2021-09-03 | TAP | 应对移动短信垃圾邮件的技术框架 |
| X.1712的勘误 | 2022-01-07 | AAP | QKD网络的安全要求和措施-密钥管理 |
| [1812 (X.5Gsec-t)](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15001) | 2021-09-03 | TAP | 基于信任关系的IMT-2020生态系统安全框架 |

表9

第17研究组 – 本研究期删除的建议书

| 建议书 | 上一版 | 撤销日期 | 标题 |
| --- | --- | --- | --- |
| 无 |  |  |  |

表10

第17研究组 – 提交WTSA-20批准的建议书

| 建议书 | 提案 | 标题 | 参考 |
| --- | --- | --- | --- |
| 无 |  |  |  |

表11

第17研究组 –增补

| **建议书** | **批准** | **状况** | **标题** |
| --- | --- | --- | --- |
| [X Suppl. 13](http://handle.itu.int/11.1002/1000/13730) | 2018-09-07 | 现行 | ITU-T X.1051 – 关于ITU-T X.1051建议书信息安全用户指南的增补 |
| [X Suppl. 26 (2016)勘误1](http://handle.itu.int/11.1002/1000/13592) | 2018-03-29 | 现行 |  |
| [X Suppl. 29](http://handle.itu.int/11.1002/1000/13409) | 2017-09-06 | 现行 | ITU-T X.1242 – 打击钓鱼短信和钓鱼短信攻击的导则增补 |
| [X Suppl. 30](http://handle.itu.int/11.1002/1000/13410) | 2017-09-06 | 现行 | ITU-T X.805 – 移动虚拟网络运营商（MVNO）安全导则增补 |
| [X Suppl. 31](http://handle.itu.int/11.1002/1000/13411) | 2017-09-06 | 现行 | ITU-T X.660 – 物联网对象标识符使用指南增补 |
| [X Suppl. 32](http://handle.itu.int/11.1002/1000/13593) | 2018-03-29 | 现行 | ITU-T X.1058 – 电信组织个人可识别信息（PII）保护的行为守则增补 |
| [X Suppl. 33](http://handle.itu.int/11.1002/1000/13731) | 2018-09-07 | 现行 | ITU-T X.1231 – 打击电话服务诈骗的技术框架增补 |
| [X Suppl. 34](http://handle.itu.int/11.1002/1000/13869) | 2019-01-30 | 现行 | ITU-T X.1051 – 电信组织信息安全控制行为守则增补 |
| [X Suppl. 35](http://handle.itu.int/11.1002/1000/14066) | 2019-09-05 | 现行 | ITU-T X.1254 – 实体认证保证（EAA）框架用例增补 |
| [X Suppl. 36](http://handle.itu.int/11.1002/1000/14809) | 2021-09-03 | 现行 | ITU-T X.1051 – 有关电信组织信息和网络安全管理关键安全控制的增补 |

表12

第17研究组 – 已同意的非规范性出版物（手册、使用手册）

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **日期** | **标题** | **出版物类型** |
| [TP.inno](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15153) | 2020-09-03 | 孵化机制和改进方法的描述 | 技术文稿 |
| [TP.sgstruct](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15154) | 2020-09-03 | 安全研究转型的战略方法 | 技术文稿 |
| [TR.ors](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15256) | 2020-03-26 | OID解决系统：问题、要求和潜在解决方案 | 技术文稿 |
| [TR.sec-manual](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14367) | 2020-09-03 | 电信和信息技术安全（第7版） | 技术文稿 |
| [TR.sec-qkd](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14825) | 2020-03-26 | 量子密钥分发网络的安全考虑 | 技术文稿 |
| [TR.Suss](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14370) | 2020-09-03 | 安全标准的成功使用（第2版） | 技术文稿 |
| [TR.usm](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15241) | 2020-09-03 | 统一安全模型（USM）– 一种中立的网络安全集成系统方法 | 技术文稿 |
| [TR.XAASL](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16769) | 2021-09-03 | 技术报告：虚拟化服务的安全标准化框架 | 技术报告 |
| [XSTR-SEC-QKD Cor.1](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16969) | 2021-04-30 | 量子密钥分发网络的安全考虑.勘误1 | 技术报告 |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16983) | 2021-04-30 | Z.100规范和描述语言实施者指南-版本4.0.1 | 实施者指南 |
| [Z.Imp100](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14424) | 2018-09-07 | Z.100 规范和描述语言实施者指南 – 第3.0.2版 | 实施者指南 |
| [Z.Imp100rev](http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14816) | 2019-09-05 | Z.100规范和描述语言实施者指南 – 4.0.0版 | 实施者指南 |

表13

第17研究组 – 确定/同意和拒绝的建议书

| **建议书** | **同意/确定** | **TAP / AAP** | **标题** |
| --- | --- | --- | --- |
| 无 |  |  |  |

附件2

第17研究组针对WTSA第2号决议提出的拟议修订

附件A

第1部分 – 总体研究领域

第17研究组

**安全**

ITU-T第17研究组负责开展树立使用信息通信技术（ICT）的信心和安全性方面的研究工作。

通过ICT提供安全保障和确保ICT的安全均是第17研究组的主要研究领域。涉及与安全相关的研究、受控安全业务、端点检测和响应、网络安全、反垃圾邮件和身份管理。其职责还涉及安全架构和框架、，基于量子的安全性、分布式账本技术（DLT）的安全、智能交通系统的安全、与人工智能相关的安全问题，以及物联网（IoT）和智慧城市、各类网络（包括IMT2020/5G及以后）、智能电网、工业控制系统（ICS）、供应链、智能手机、软件定义网络（SDN）、网络功能虚拟化（NFV）、互联网协议电视（IPTV）、网络业务、过顶业务（OTT）、社交网络、云计算、大数据分析、数字金融系统和电子生物特征识别应用及业务的安全性。

建立对使用ICT的信心和安全性还涉及保护个人身份信息（PII），例如确保PII的保密性、完整性和可用性方面的数据保护技术和操作问题。

第17研究组还负责开放系统通信应用，包括目录和对象标识符，以及技术语言、其使用方法及与电信系统的软件方面并用于支持与一致测试的测试规范语言相关的其他问题，以提高建议书质量一致性测试。

第2部分 – 具体研究领域的牵头组

SG17 安全问题牵头研究组  
身份管理牵头研究组  
语言和描述技术牵头研究组

（第2号决议）  
附件B  
  
ITU-T研究组制定2020年之后工作计划的指导要点

ITU-T第17研究组

ITU-T第17研究组负责制定支持树立使用信息通信技术（ICT）的信心和提高安全性方面的主要建议书。

为此，这包括与安全相关的研究（网络安全、反垃圾邮件和身份管理）。其职责还涉及安全架构和框架、网络、应用和服务（如物联网（IoT）、智能交通系统安全应用服务、社交网络、云计算、分布式账本技术和电子生物特征识别）的安全性。第17研究组还负责开放系统通信应用，包括目录和对象标识符，以及技术语言、其使用方法及与电信系统的软件方面相关的其他问题，同时为提高建议书质量，还负责开展一致性测试。

ITU-T第17研究组的作用是为解决ICT安全问题和确保ICT安全提供技术解决方案。特别是，重点研究新兴领域的安全，如IMT2020/5G及未来的安全、物联网（IoT）、智慧城市、分布式账本技术（DLT）、大数据分析、智能交通系统、与人工智能相关的安全方面以及量子相关技术。其研究领域还包括个人可识别信息（PII）的管理，如数据保护的技术和操作方面，以确保PII的保密性、完整性和可用性。

在安全方面，第17研究组组负责编制有关ICT安全问题的核心建议书，如安全架构和框架；关于威胁、漏洞和风险等的与网络安全相关的基本资料；事件处理/响应和数字取证，以及包括个人可识别信息（PII）在内的安全管理，如数据保护的技术和操作方面；以及通过技术手段打击垃圾信息。

第17研究组作为有关安全、身份管理以及语言和描述手段的牵头研究组提供ITU-T安全相关工作的总协调。

此外，第17研究组还负责制定有关分布式账本技术的安全、智能交通协调的安全IPTV、包括IMT2020/5G及未来等不同网络、智能电网、工业控制系统（ICS）、供应链、IoT和智慧城市、SDN、NFV、社交网络、云计算、大数据分析、智能手机、数字金融系统和电子生物特征识别领域相关应用和业务安全方面的核心建议书。

第17研究组还负责制定有关独立于网络技术并支持实体之间身份信息安全交换的一般身份管理模型的核心建议书。这项工作还包括研究用于发现身份信息的权威来源的程序；用于多样化身份信息格式桥接/互操作性的通用机制；身份管理威胁及防范这些威胁的机制，保护个人可识别信息（PII），并确立机制，以确保只有在适当情况下才能经授权访问PII。

在开放系统通信方面，第17研究组负责制定涉及以下内容的建议书：

• 目录业务和系统，包括公钥基础设施（PKI）（ITU-T F.500和ITU-T X.500系列）；

• 对象识别符（OID）和相关注册机关（ITU-T X.660/ITU-T X.670系列）；

• 开放系统互连（OSI），包括抽象句法表示法一（ASN.1）（ITU-T F.400系列、ITU-T X.200系列、ITU-T X.400系列、ITU-T X.600系列、ITU-T X.800系列）；及

• 开放式分布处理（ODP）（ITU-T X.900系列）。

在语言方面，第17研究组负责研究建模、规范和描述技术，涉及诸如ASN.1、SDL、MSC、URN和TTCN-3等语言。

第17研究组协调ITU-T所有研究组的安全工作。这项工作根据第2、第9、第11、第13、第15和第16以及第20研究组的要求并与其合作进行。

第17研究组将与第20研究组以及第2研究组按照各自研究组的职责开展协作，进行身份管理相关方面问题的研究工作。

（第2号决议）  
附件C  
  
2021-2024年研究期内ITU-T各研究组和  
TSAG负责的建议书清单

ITU-T第17研究组

ITU-T E.104、ITU-T E.115、ITU-T E.409（与第2研究组共同负责）

ITU-T F.400系列、ITU-T F.500-ITU-T F.549

ITU-T X系列，第2、第3、第11、第13、第15和第16研究组负责的建议书除外

ITU-T Z系列，ITU-T Z.300系列和ITU-T Z.500系列除外

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