|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **国 际 电 信 联 盟****电信标准化局** |  |
|  | 2022年9月28日，日内瓦 |
| **文号：** | **电信标准化局第42号通函**SG17/XY | **致：**– 国际电联各成员国主管部门**抄送：**– ITU-T部门成员；– 第17研究组的ITU-T部门准成员；– 国际电联学术成员– ITU-T第17研究组正副主席；– 电信发展局主任；– 无线电通信局主任 |
| **电话：** | +41 22 730 6206 |
| **传真：** | +41 22 730 5853 |
| **电子邮件：** | tsbsg17@itu.int |
| **事由：** | **就在ITU-T第17研究组全体会议（2023年2月21日-3月3日）上批准已确定的ITU-T X.1353 (X.ztd-iot)、X.1380 (X.edr-sec)、X.1381 (X.eivn-sec)、X.1382 (X.fstsicv)、X.1383 (X.srcd)、X.1410 (X.sa-dsm)、X.1411 (X.BaaS-sec)、X.1454 (X.sles)、X.1644 (X.sgdc)、X.1815 (X.5Gsec-ecs)和X.1816 (X.5Gsec-ssl)新建议书草案与成员国进行磋商** |

尊敬的先生/女士：

1 ITU-T第17研究组（安全）准备采用世界电信标准化全会（WTSA）第1号决议（2022年，日内瓦，修订版）第9节所述的传统批准程序，在计划于2023年2月21日–3月3日召开的第17研究组下次会议上批准上述建议书草案。有关ITU-T第17研究组会议的议程和所有相关信息将在第[3/17](https://www.itu.int/md/T22-SG17-COL-0003/en)号集体函中提供。

2 建议批准的ITU-T建议书草案的标题、概要及出处见**附件1**。

电信标准化局说明1 – 除X.1382 (X.fstsicv)、X.1815 (X.5Gsec-ecs)和X.1816 (X.5Gsec-ssl)草案外，尚未就其它已确定的案文草案编写符合ITU-T A.5建议书理由的文件。

电信标准化局说明2 – 截至本通函发布之日，电信标准化局未收到有关这些案文草案的任何知识产权声明。欲了解最新情况，请各成员通过以下链接到知识产权数据库查阅：[www.itu.int/ipr/](http://www.itu.int/ipr/)。

3 本通函根据第1号决议第9.4节针对是否在即将召开的会议上考虑批准这些案文启动与国际电联成员国的正式磋商。请各成员国在**2023年2月9日**23时59分（协调世界时（UTC））之前填妥并返回**附件2**中的表格。

4 如果70%或70%以上的成员国在回复中支持考虑批准，将专门利用一节全体会议的时间应用批准程序。不授权如此办理的成员国应向电信标准化局主任通报其意见的理由并说明可能进行的修改，从而推动此项工作取得进展。

顺致敬意！

电信标准化局主任

李在摄

**附件**：2件

 **附件1**

已确定的ITU-T X.1353 (X.ztd-iot)、X.1380 (X.edr-sec)、X.1381 (X.eivn-sec)、X.1382 (X.fstsicv)、X.1383 (X.srcd)、X.1410 (X.sa-dsm)、X.1411 (X.BaaS-sec)、X.1454 (X.sles)、X.1644 (X.sgdc)、X.1815 (X.5Gsec-ecs)和X.1816 (X.5Gsec-ssl)新建议书草案的概要和出处

# 1 ITU-T X.1353 (X.ztd-iot)新建议书草案[[R18](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0018)]

有关基于区块链的大规模物联网（IoT）中零接触部署的安全方法

概要

大规模物联网（mIoT）是未来通信网络的一个重要应用。由于mIoT中预期的各种用例，制造商很难在其制造的IoT设备中预安装移动运营商特定的和/或服务特定的信息（如身份和密钥），因为制造商可能不知道其设备最终将在哪里部署和激活。目前的方法依靠的是客户的手动配置，这对于小规模IoT应用来说是可以接受的。然而，对于mIoT设备来说，上述方法是不可接受的，因为手动配置耗时、效费比低且繁琐。因此，mIoT需要无需用户参与的自动证书提供，即所谓的“零接触”。

本建议书提供了一种用于设计去中心化身份管理系统的安全方法，以支持未来mIoT的零接触部署。零接触部署将使IoT设备能够自动找到其移动网络运营商和服务提供商，自动从其处获得证书，并自动连接到网络和服务。这将极大地促进未来面向垂直行业的mIoT设备的部署。本建议书的内容涵盖构建这样一个零接触mIoT部署平台所需的安全架构、安全注意事项和相关安全程序（如设备证明、认证和证书提供）。

# 2 X.1380 (X.edr-sec)新建议书草案[[R22](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0022)]

有关汽车环境中基于云的数据记录器的安全指南

概要

事件数据记录器（EDR）是安装在汽车道路车辆中的最重要组成部分之一，用于在碰撞期间记录车辆状态、车辆运动和用户输入。通过分析事件数据，可以了解碰撞的原因，并最终用于提高汽车环境的安全性。用于自动驾驶的数据存储系统也是记录数据的一个重要组成部分，这些数据将给出驾驶者与自动驾驶系统之间交互的清晰画面。然而，传统的事件数据记录器在本地记录和管理全部数据，这样，数据可能受到丢失和破坏的威胁。

云计算被认为是自我服务供应和按需管理情况下促成网络获取一系列可伸缩且富有弹性、可共享物理或虚拟资源的重要手段。航空业等行业已经在尝试将云服务应用于事件数据记录系统，以提高航空环境的安全性。根据车辆之间连接的当前趋势，将实施用于自动驾驶的EDR和数据存储系统，以提高其整体安全性。然而，根据汽车环境的独特特性，它们在采集、传输、存储、管理和使用所记录数据的过程中具有各种漏洞。因此，有必要研究汽车环境中基于云的数据记录器的这些漏洞、安全要求和用例。

本建议书为汽车环境中基于云的数据记录器提供了安全指南。它描述了汽车环境中基于云的数据记录器的威胁、漏洞、安全要求和用例。

# 3 X.1381 (X.eivn-sec)新建议书草案[[R23](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0023)]

有关基于以太网的车载网络的安全指南

概要

本建议为基于以太网的车载网络（IVN）提供了安全指南。当前的电气和电子（E/E）架构趋势是将以太网与控制器局域网（CAN）、本地互联网络（LIN）、面向媒体的系统传输（MOST）和FlexRay等传统车载网络集成。过去，以太网仅被视为车辆与外部环境之间的连接。在以太网上实现基于互联网协议的连接的标准协议（例如，基于互联网协议或通用测量和校准协议的诊断通信），被用于外部环境和车辆之间的通信。这些用例通常不需要满足严苛的实时要求。然而，使用以太网通信的车载应用，需要高时间敏感性和可靠性等特性。

目前车载通信技术的发展需要增加网络带宽。与以太网相比，传统IVN不足以满足当前车载应用的带宽要求。因此，无论现在和将来，基于以太网的IVN都是E/E架构的骨干。

然而，从普通计算机网络得出的对策不适用于汽车应用，因为它们不是针对汽车需求和能力而设计的。

为了满足这一需求，本建议书提供的汽车以太网技术安全指南，包括一个汽车以太网参考模型和基于以太网的IVN的威胁和脆弱性分析，以及该IVN的安全要求和使用案例。

# 4 X.1382 (X.fstsicv)新建议书草案[[R24]](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0024)

有关联网汽车安全威胁信息共享的指南

概要

随着车联网的快速发展，车联网面临的网络安全问题日益突出。联网汽车的安全威胁信息在保护联网汽车方面发挥着不可或缺的作用，是可以帮助相关组织识别、评估、监控和响应联网汽车的任何信息。共享联网汽车威胁信息的组织可以改善自身和其他组织的安全状况。

本建议书为联网汽车共享安全信息的原则、规则、方法和程序提供了指导。此外，本建议书还简要描述了参与安全威胁信息共享生命周期的各个组织的不同职责范围、角色和有效性。

本建议书旨在帮助相关组织与联网汽车共享社区保持联系，并为支持联网汽车安全保护做法提供威胁信息。总体而言，本建议书旨在加强安全威胁信息共享，减轻网络安全攻击对联网汽车的潜在影响。

已确定的本草案案文包括需要进行ITU-T A.5论证的规范性参考文献，可在第17研究组[TD510](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0510)号文件中找到。

# 5 X.1383 (X.srcd)新建议书草案[[R25](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0025)]

# 车联网（V2X）通信中分类数据的安全要求

**概要**

数据安全是车联网（V2X）通信最重要的考量因素之一。但是，在资源受限的环境中（例如车载通信），由于需要加密功能，数据保护会消耗大量资源。

本建议书将V2X通信中使用的数据分为几类，如对象属性数据、车辆状态数据、环境感知数据、车辆控制数据、应用服务数据和用户个人数据，并为所分的数据类型分配了三个安全级别。根据这些分类数据类型和分配的数据安全级别，本建议为V2X通信中的分类数据提供了安全要求。

# 6 X.1410 (X.sa-dsm)新建议书草案[[R26](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0026)]

有关基于分布式账本技术的数据共享管理的安全架构

概要

分布式账本技术（DLT）提供的创新解决方案正在转变各行业并改变政府、机构和企业的运营方式。去中心化且防篡改的功能使DLT能够为在分布式计算机网络中安全地复制、共享和同步数据提供解决方案。目前与公司和数字化平台共享业务数据和个人身份信息（PII）数据的方法已致使黑客攻击隐私漏洞或数据管理不佳。在数据共享管理中采用DLT或区块链让个人或公司对自身的保密信息保持更直接的控制。在基于DLT的解决方案中，仅有非PII数据（如哈希数据值）存储在链上，而数据所有者的相关PII数据则存储在链下。基于DLT的解决方案提供了一种改善数据状态的可追溯性、可验证性和可更改性的方法。

本建议书规定了基于分布式账本技术（DLT）的数据共享管理的安全架构。基于此架构，本建议规定了功能实体与基于DLT的数据共享管理程序之间的接口。

# 7 X.1411 (X.BaaS-sec)新建议书草案[[R20](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0020)]

有关区块链即服务（BaaS）的安全指南

概要

区块链即服务（BaaS）已经成为区块链发展的主流，原因是它具有很好的功能，并且得到了业界（特别是顶级云提供商）的广泛支持。BaaS为区块链应用提供基础服务和资源，但是它面临着来自区块链核心技术和云平台的安全挑战。因此，就Baas安全性提供指导是非常重要和必要的。

本建议书为区块链即服务（BaaS）提供了通用的安全指南。首先分析了BaaS的安全威胁和脆弱性，然后提出了BaaS的安全措施。建议书还提出了安全要求，并为建设、运营和使用BaaS的所有活动提供了指南。

# 8 X.1454 (X.sles)新建议书草案[[R19](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0019)]

有关支持位置的智能办公服务的安全措施

概要

结合多种智能应用的智能办公服务旨在提高办公质量和加强效率管理。由于信息通信技术（ICT）是智能办公服务的技术基础，电信运营商在智能办公服务的利益攸关方中扮演着重要的角色。

典型的智能办公服务包括智慧停车、智能驾驶、智能零售店、智能办公室、智能会议室管理、智慧水务、智能能耗管理等。在这些典型的智能办公服务中，运营商提供的位置数据是大多数智能办公服务实施的关键要素之一。

为了确保支持位置的智能办公服务的安全性，需要分析特定于支持位置的服务的安全威胁和相关安全性要求，并制定整体的安全措施。

本建议书分析了支持位置的智能办公服务的典型应用场景，明确了其安全威胁和要求，并为智能办公场所的运营商和关键利益攸关方制定了安全措施，以保护支持位置的服务。

# 9 X.1644 (X.sgdc)新建议书草案[[R21](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0021)]

有关分布式云的安全导则

概要

该建议书分析了分布式云的安全威胁和挑战，并提出了针对分布式云的威胁的安全导则，包括核心云、区域云和边缘云。

# 10 X.1815 (X. 5Gsec-ecs)新建议书草案[[R16](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0016)]

有关IMT-2020边缘计算服务的安全导则和要求

概要

IMT-2020网络将在网络和计算资源的基础设施上实现各种服务，其中包括增强型移动宽带（eMBB）服务、基于海量机器类型通信（mMTC）的服务和基于超可靠低延迟通信（URLLC）的服务。根据为IMT-2020网络确定的关键特征和要求，它需要更加高效、个性化、智能化、可靠和灵活。

为了支持IMT-2020网络中的典型服务，尤其是eMBB服务和基于URLLC的服务，边缘计算被认为是满足IMT-2020网络的苛刻关键性能指标（KPI）的关键技术之一，尤其是就低延迟和带宽效率而言。

边缘计算使运营商和第三方服务提供商能够在靠近用户接入点的地方部署服务，从而通过减少传输网络上的端到端延迟和负载来实现高效的服务交付。

为了保证边缘计算服务部署和应用的安全性，需要分析边缘计算服务的安全威胁和相关安全需求，建立整体安全框架。

本建议书草案分析了边缘计算服务的部署方案和典型应用场景，规定了IMT-2020中针对边缘计算服务的安全威胁和要求，从而为运营商保护其应用建立了安全能力。

这项已确定的案文草案包含需要进行ITU-T A.5论证的规范性参考文献，可在第17研究组[TD605](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0605)号文件中找到。

# 11 X.1816 (X.5Gsec-ssl)新建议书草案[[R17](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0017)]

有关IMT-2020网络切片中安全能力分类的导则和要求

概要

基本网络切片技术功能和流程的定义为网络切片业务的第一波IMT-2020部署和商用奠定了坚实的基础。作为按需定制的端到端逻辑网络，切片可以提供差异化安全能力。

首先，IMT-2020网络切片为差异化网络实施方案提供了支持性安全措施。其次，IMT-2020网络在切片层面支持一些可选的安全措施。一些安全措施还可以提供多种安全选项，运营商可能拥有不同的安全资源，这可能带来不同程度的安全保证或非安全性能。

切片客户也有具体的安全需求，可能会向切片运营商请求具有不同安全保护级别的定制网络切片。切片客户和切片运营商在选择其切片的安全能力时都存在一些挑战，例如管理成本和定义不一致等。

本建议书描述了差异化IMT-2020网络切片安全能力，并为分类这些安全能力提供了指南，以协助IMT-2020生态系统选择网络切片安全能力。

这项已确定的案文草案包含需要进行ITU-T A.5论证的规范性参考文献，可在第17研究组[TD552](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-220823-TD-PLEN-0552)号文件中找到。

附件2

事由：成员国对电信标准化局第42号通函的回复：
针对已确定的ITU-T X.1353 (X.ztd-iot)、X.1380 (X.erd-sec)和X.1381 (X.eivn-sec)、X.1382 (X.fstsicv)、X.1383 (X.srcd)、X.1410 (X.sa-dsm)、X.1411 (X.BaaS-sec)、X.1454 (X.sles)、X.1644 (X.sgdc)、X.1815 (X.5Gsec-ecs)、X.1816 (X.5Gsec-ssl)
新建议书草案进行的磋商

|  |  |  |  |
| --- | --- | --- | --- |
| **致：** | 国际电信联盟电信标准化局主任Place des NationsCH 1211 Geneva 20, Switzerland | **发自：** | [姓名][正式职务][地址] |
| **传真：****电子邮件：** | +41-22-730-5853tsbdir@itu.int  | **传真：****电子邮件：** |  |
|  |  | **日期：** | [日期] [地点] |

尊敬的先生/女士：

关于针对电信标准化局第42号通函中所列的已确定案文草案与成员国进行磋商一事，我谨向您通报本主管部门的意见，如下表所述。

|  | **请选择两个方框中的一个** |
| --- | --- |
| **ITU-T X.1353 (X.ztd-iot)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1380 (X.edr-sec)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1381 (X.eivn-sec)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1382 (X.** **fstsicv)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1383 (X.** **srcd)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1410 (X.** **sa-dsm)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1411 (X.BaaS-sec)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1454 (X.sles)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1644 (X.sgdc)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1815 (X.5Gsec-ecs)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |
| **ITU-T X.1816 (X.5Gsec-ssl)新建议书草案** | [ ]  **授权**第17研究组考虑批准该草案（在这种情况下，请选择两种方案⃝中的一种）：⃝ 无意见或无建议修改⃝ 附意见和建议的修改 |
| [ ]  **不授权**第17研究组考虑批准该草案（附反对意见的理由并说明可能推动该项工作进展的可能修改概述） |

顺致敬意！

[姓名]

[正式职务]

[成员国]主管部门

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