国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Q.5050

（03/2019）

Q系列：交换和信令以及相关措施和测试

打击假冒和盗用信息通信技术（ICT）设备

打击假冒信息通信技术（ICT）设备的解决方案框架

ITU-T Q.5050 建议书

国际电信联盟

ITU-T Q 系列建议书

交换和信令以及相关措施和测试

国际人工业务中的信令	Q.1–Q.3
国际自动和半自动业务工作	Q.4–Q.59
ISDN业务的功能和信息流	Q.60–Q.99
适用于ITU-T标准系统的条款	Q.100–Q.119
四号、五号、六号、R1和R2信令系统规范	Q.120–Q.499
数字交换	Q.500–Q.599
信令系统的互通	Q.600–Q.699
七号信令系统规范	Q.700–Q.799
Q3接口	Q.800–Q.849
一号数字用户信令系统	Q.850–Q.999
公众陆地移动网	Q.1000–Q.1099
与卫星移动系统的互通	Q.1100–Q.1199
智能网	Q.1200–Q.1699
IMT-2000的信令要求和协议	Q.1700–Q.1799
承载独立呼叫控制相关的信令规范（BICC）	Q.1900–Q.1999
宽带ISDN	Q.2000–Q.2999
下一代网络的信令要求和协议	Q.3000–Q.3999
软件定义宽带接入网的信令要求和协议	Q.3710–Q.3899
测试规范	Q.3900–Q.4099
IMT-2000的信令要求和协议	Q.5000–Q.5049
打击假冒和盗用信息通信技术（ICT）设备	**Q.5050–Q.5069**

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T Q.5050建议书

打击假冒信息通信技术（ICT）设备的解决方案框架

摘要

近年来，信息通信技术（ICT）设备在人们日常生活中的使用越来越普及，但假冒ICT设备在市场中销售、流通和使用的增加亦给此类设备造成了负面影响。

假冒ICT设备属于明目张胆侵犯原创产品或正品的商标、抄袭其硬件或软件设计、对品牌或包装侵权的产品，这些假冒设备通常不遵守适用的国家和/或国际技术标准、监管要求或一致性流程、制造许可协议或其他适用的法律要求。

当今使用的各类ICT设备中，智能电话和其他移动设备已为世界人民广泛使用并成为受到喜爱的产品，但副作用是这些产品亦引起了全球黑市/灰色市场的注意。

这给诸如用户、网络运营商、正品设备制造商、交易商和政府等利益攸关方造成了不良后果，其中包括降低了用户的安全防护水平和服务质量，同时给一系列利益攸关方带来了收入损失。

由于假冒ICT设备的供求经济使全球打假市场的操作变得更为复杂，因此没有一种方案能够单独解决问题，这就要求人们使用全面的手段广泛采用各种措施。

因此，ITU-T Q.5050建议书旨在阐述一种可应对高水平挑战和满足高水平要求的参考框架，供用户在部署打击假冒ICT设备的流通和使用解决方案时考虑。

历史沿革

版本	建议书	批准日期	研究组	唯一标识符*
1.0	ITU-T Q.5050	2019-03-15	11	11.1002/1000/13702

关键词

打击假冒ICT设备、合规、一致性、一致性评估、框架、要求、安全、标准、唯一标识符

* 要访问该建议书，请在万维网浏览器的地址栏中输入URL：http://handle.itu.int/，然后输入建议书的唯一标识符。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T Q.5050建议书案

打击假冒ICT设备的解决方案框架

1 范围

本建议书包含为部署打击假冒信息和通信技术（ICT）设备的流通和使用的解决方案应考虑的参考框架和要求。

2 参考文献

参考文献下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

无

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 一致性评估[b-ISO/IEC 17000]：显示与产品、流程、系统、个人或机构相关的具体要求是否得到满足。

3.1.2 一致性评估方案（或计划）[b-ISO/IEC 17000]：与具体对象相关的一致性评估系统，在此系统中，相同的具体要求、具体规则和程序适用。

3.1.3 市场监督[b-EC-Regulation]：公共机构开展的活动和采取的措施，目的是确保产品能够遵守相关立法规定的要求，不会在卫生、安全或保护公众利益的其他方面造成危害。

3.1.4 标准[b-WTO-TBT]：经认可机构批准的文件，其针对产品、相关流程和生产方法提供的公共和常用规则、导则或特性并不强制要求遵守。此外，此类标准亦包括或专门用于处理适用于产品、流程和生产方法的术语、符号、包装、商标或标识要求。

3.1.5 监督[b-ISO/IEC 17000]：一致性评估活动的系统性迭代，是维持一致性声明有效性的基础。

3.1.6 技术性贸易壁垒[b-WTO-TBT]：世界贸易组织（WTO）的技术性贸易壁垒协议旨在确保技术规则、标准和一致性评估程序不具歧视性且不会给贸易树立不必要的障碍。

3.1.7 技术规则[b-WTO-TBT]：对产品特性或相关流程以及生产方法做出规定的文件，其中包括必须遵守的适用行政规定。此外，此类技术规则亦包括或专门用于处理适用于产品、流程和生产方法的术语、符号、包装、商标或标识要求。

3.1.8 灰色市场[b-Gartner]：从原产商或相关政府规定的常规商业渠道之外进口和销售的设备，与授权分销渠道形成了一个并行的市场。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 假冒ICT设备：属于明目张胆侵犯原创产品或正品的商标、抄袭其硬件或软件设计、对品牌或包装侵权的信息通信技术（ICT）设备，这些假冒设备通常不遵守适用的国家和/或国际技术标准、监管要求或一致性流程、制造许可协议或其他适用的法律要求。

3.2.2 伪造ICT设备：是指其组件、软件、唯一标识、受知识产权保护的部件或商标，在未经制造商或制造商法律代表明示许可的情况下被试探性或实际更改的信息通信技术（ICT）设备。

3.2.3 唯一标识符：与单一设备相关的标识符，旨在对此设备进行独一无二地标识。

4 缩写词和首字母缩略语

本建议书使用了下述缩写词和首字母缩略语：

CAS 一致性评估方案

DevID 设备标识符

DIRBS 设备识别、注册和屏蔽系统

EAP 外部认证协议

EIR 设备身份注册

ICT 信息通信技术

IMEI 国际移动设备标识

IoT 物联网

IPR 知识产权

IVR 互动语音响应

PCB 印刷电路板

SIM 用户识别模块

TAC 型号划分代码

TBT 技术性贸易壁垒

TEE 值得信赖的执行环境

TPM 值得信赖的平台模块

TRIPS 知识产权的贸易相关方面

5 惯例

本建议书适用于以下描述方式表达的规定：

a) “需要”一词指的是必须严格遵守的要求，要声明与本建议书一致就不得偏离这种要求。

b) “应”这个词表示一种建议，但不是必须的要求。因此，因此在声明一致性时本建议书不用提及这种要求。

c) “可”字样表明一个可选的要求是被允许的，不意味着任何被建议的意思。该术语并不意味着供应商必须实施这一选项，是否启用这一特性可由网络运营商/服务提供商任选；而是指供应商可以视情选择提供这一特性，同时仍然声明与本建议书一致。

6 一般问题

近年来，ICT设备在人们日常生活中的使用越来越普及，但假冒ICT设备在市场中的销售、流通和使用的增加亦给此类设备造成了负面影响。这给诸如用户、网络运营商、正品设备制造商、交易商和政府等利益攸关方造成了不良后果，其中包括降低了用户的安全防护水平和服务质量，同时给一系列利益攸关方带来了收入损失。

人们认识到假冒伪劣电信/ICT产品经济学意义上的供需关系使得应对这一全球黑市/灰色市场的尝试变得更加复杂，因此没有一种万能的方案能够单独解决假冒伪劣问题。本建议书提出的框架由广泛的措施构成，可采取并应用全面的方法来解决此问题。应在产品销售地国的帮助下，尽可能在假冒产品的产地和出口地市场控制这些假冒产品的来源。

对所有从事产品检验或测试的人而言，区分正品与假冒ICT设备均非易事。因为造假者的目的就是制造与正品设备非常相似的产品，其使用的方法可能是提供虚假或偷窃的文件，有时是安装供从正品或其附件上拆下的硬件，有时甚至会复制合法软件或唯一标识符，所有这些做法的目标都是妨碍利益攸关方辨识产品。至关重要的是在部署解决方案时将这些因素及其他因素考虑进去，以避免在目前正在解决的问题之上，给用户和正品生产厂家造成更多的问题。

当今使用的各类ICT设备中，智能电话和其他移动设备已为世界人民广泛使用并成为受到喜爱的产品，但副作用是这些产品亦引起了全球黑市/灰色市场的注意。有些国家已为解决假冒ICT设备问题采取了措施并成功地为遏制假冒ICT设备的流通和使用部署了解决方案，而另一些国家的政府在这方面仍然面临挑战且尚不清楚应采取何种最佳战略。

为解决使用假冒设备的问题而采取的许多解决方案具有相似性，例如依靠唯一的设备标识符，借助于一致性评估方案，以及采用可阻止这些假冒设备入网的方法（见附件A针对移动设备提出的建议）。

但是，出于不同原因世界各国政府在打击假冒ICT设备方面仍然面临挑战，这些原因既包括 技术问题，假冒产品制造商为逃避检测而采取的措施，也包括纯粹的消费者对购买假冒产品的欲望，即消费者决定主动去购买假冒产品。

因此，选择打击假冒ICT的国家应考虑采用一种全面的、联合多个机构/利益攸关方的方法，和其他已处理过此类问题的国家部署的技术解决方案，以使能够获得指导和最佳做法实例。

7 有序电信设备市场的基本要素

创建有序的电信产品和服务市场需要多种因素。一项基本要求是对进入市场的产品提出严格的技术要求。此类要求涉及用户群体和网络服务提供商人员的安全以及为电信业务建立一个无干扰的环境等。

鉴于全球化的数字经济要通过一个强劲、安全且可靠的电信平台开展经济活动，因此社会经济的发展需要有不受干扰的 – 无线和有线 – 通信服务。此外，定义明确、管理良好、透明且无歧视的市场准入机制，可为设备供应商、服务提供商和普通人赢得信任与信心。得到适当立法和监管框架支撑的此类机制是满足国内外连通质量要求的基石，而连通对参与全球化数字经济而言至关重要。事实上，它切实反映出了社会需求的重点和价值[b-ITU-D-CI-Guidelines]。

8 在部署打击假冒ICT设备解决方案时的考量：

在部署打击假冒ICT设备解决方案的过程中，利益攸关方将面对若干挑战：

8.1 检测和识别假冒ICT设备

造假者的目的之一是使其产品能够行销全球市场。造假者会从产品的外观与感受，复制唯一标识符、软件甚至是ICT设备内部原件方面做文章，令假冒产品与正品尽可能相似。

这就提出了一些挑战。例如所有原厂生成的货物识别码能够并且正在被造假者滥用，以达到使消费者和管理部门相信其产品是正品的目的。任何身份识别机制及其安全措施均可能成为造假者和罪犯的目标。型号核准标志和图标以及电子识别码经常为躲避海关和执法机构在边界的检查而遭故意破坏，甚至是处于空白状态，等到当地市场后再行编造。[b-ITU-T TR-Counterfeit]

所有原厂生成的货物识别码能够被造假者伪造，以达到欺骗消费者和管理部门的目的 – 证明他们的产品是正品。不仅是在ICT产业，在很多产业中均存在这一问题。读者应当牢记任何身份识别机制及其安全措施均会成为造假者和罪犯的目标。

例如，造假者的一个常见做法是破坏部分设备用于网络鉴权的唯一标识符，从而使网络将这些ICT设备误认为是正品设备。另一做法是截获正品设备并通过篡改软件使其貌似正品升级后的版本（因此更加昂贵），或者是用假冒产品更换电池等正品的内部原件，以达到在市场上出售赝品的目的。

型号核准标志和图标以及电子识别码经常为躲避海关和执法机构在边界的检查而蓄故意破坏。对生产厂家、消费者和执法官员来说，难以将假冒设备的虚假识别标记同正品的识别标记区分开来，更不用提确认产品本身的真伪了。

8.2 跟踪假冒ICT设备的生产商和贩运者

一旦判定产品为非正规设备，相关机构应追踪生产该非法设备的经济体、生产商和贩运者，并将这些生产商和贩运者从市场上清除出去[b-OECD]。

如果无法在源头确定假冒产品的生产商和贩运者并对他们采取执法行动，则在目的地经济体采取的行动可能不会有效果。

8.3 取缔市场中正在使用的假冒ICT设备

控制上市后假冒ICT设备需等待对这些设备采取行动的机会。可能采取的行动包括 (i) 比照原厂产品的特性开展现场或远程检测和验证；(ii) 停止使用假冒设备和/或 (iii)没收假冒设备。

上述机会和行动存在若干挑战：

– 现场检验设备真伪存在几种情况： 在开展服务活动的过程中，在开展市场监督活动的过程中，或是在法律机构有权对设备进行检查的情况下。这方面的挑战在于如何创建所需的知识库并激发相关机构执行此类任务的兴趣。

– 可采取逻辑或远程的方式进行验证，例如在某类在线系统注册过程中，对唯一的标识符和产品指纹进行交叉校验。然而这通常需要与互联网连接，所以此做法在偏远地区和农村环境可能具有挑战性，特别是在发展中国家。尽管应采用电子程序，但仍有必要将设备的物理特性与产品数据库中的信息加以对比。

– 如果设备使用唯一标识符进行网络注册，则使用特定市场的授权设备数据库可拒绝假冒ICT设备入网。这方面的挑战在于如何建立并维持相关的注册系统和数据库，特别是在大量设备在尚无此类控制便已部署的情况下。

– 应注意避免滥用标识符和注册系统，尊重消息者权益且不要给ICT产品的用户造成负面影响。消费者也应得到保护，免受任意断开网络连接带来影响。

– 没收假冒ICT设备有赖于现场验证，在大多数情况下，需要法律框架下的执法机构为可能采取的司法行动提供支持。挑战在于如何在不同机构之间建立合作关系，制定法律框架以及确定假冒ICT设备应负的责任。

– 不应低估执法给用户造成的影响。要考虑到某些国家可能不允许断开任何设备且用户的生命可能存在风险。

8.4 限制新假冒ICT设备的进口及其在市场上的流通和销售

除采取行动消除库存或在用假冒ICT设备之外，应采取措施限制新假冒ICT设备的进口、走私以及在市场上的流通和销售。

此方法能在采取上述行动主管部门的财政和时间限制内，帮助减少市场内假冒ICT设备的总量，同时降低给用户造成的影响，使此影响低于为将假冒ICT设备从网络中断开而采取的行动。

正如第8.2段所述，这些措施亦应聚焦于假冒ICT产品的来源。

8.5 区分正品和假冒ICT设备

为保障消除市场中在用假冒ICT设备及阻止新假冒设备进入市场行动的有效性，有必要实施能够区分正品和假冒设备的解决方案和标准。即便是在考虑到克隆唯一标识符的情况下，此种方案的执行亦需要极高的精度，从而使ICT设备的断网行动最好通过自动化系统实施或针对少量ICT设备实施手动断网。

区分正品和假冒ICT设备时应考虑以下方面：

– 造假者的目标是生产一种与原厂正品十分相似的产品。

– 造假者可能会积极尝试通过为假冒产品提供虚假或偷窃的文件、硬件和软件，给检测造成困扰。

– 假冒产品的某些元件可能来自正品及其附件，其中包括但不限于：软件、唯一标识符、套管硬件、印刷电路板（PCB）的设计和芯片集。

– 正品会定期进行固件软件更新，这主要是出于安全原因。此更新同样适用于应用和部分附件。因此，确定正品的设备“手印”可能具有挑战性。

– 很多时候，视检可能不足以区分正品，因此可能需要更多的专业技术能力、支持或实验室测试。

8.6 限制给正品ICT设备厂商造成的影响

打击假冒设备的方案应尽量限制给正品ICT设备厂商造成影响，将精力侧重于假冒ICT设备、假冒设备的生产厂家及购买者。

应当避免采用会增加正品制造商制造和处理合法设备成本的方案，由于造假者通常依靠低廉的价格促使消费者主动选择购买假冒ICT设备，因此这种方案会在无意中使造假者受益。

8.7 考虑在清除假冒ICT设备过程中降低给最终用户造成的影响

为清除假冒ICT设备或将其从网络中断开采取的任何方案均应审慎考虑给最终用户造成的影响，且在实现同一目标存在多种途径时，应采用可降低给消费者造成的总体影响的那一种。

因此，应考虑以下挑战：

– 有些国家可能不允许中断ICT设备的网络连接。

– 在断网之前并非总能通过设备与用户取得联系（例如，仅使用数据或SMS的设备、呼叫前转、互动式语音应答（IVR）系统等不与用户联系的方式）。

– 屏蔽支持关键业务的假冒ICT设备可能存在风险（例如医疗应用、金融业务等）。

– 确保用户权利不受侵犯且此种行动是依据国家立法执行。

8.8 消费者教育

应在购买和继续使用假冒ICT产品的问题上开展消费者教育，其中包括但不限于可能的健康风险和/或服务水平低下。

必须考虑到，尽管消费者也知道后果，但经常会因为价格主动购买假冒产品，因此至关重要的是提高消费者对使用假冒ICT产品所产生的负面影响以及使用正品设备好处的认识。

8.9 规避技术性贸易壁垒（TBT）

应注意避免妨碍正品ICT设备的有效进口和使用，根据世界贸易组织（WTO）与贸易相关的知识产权（TRIPS）[b-TRIPS Agreement]定义，妨碍行为将构成技术性贸易壁垒（TBT）。

这方面的操作可能包括“白名单”的使用，因失误或决策不当，阻碍旅行者和游客等合法用户使用ICT产品。这种注册设备的要求可能会无意产生TBT。

9 框架要求

部署打击假冒ICT设备的方案时，各国应考虑以下要求：

9.1 确定假冒设备的制造商和贩运者并对其采取执法行动

在打击市场内已有假冒ICT设备和新进入相关国家的此类设备的过程中，必须制定一个流程，以跟踪其来源并从市场中清除提供此类产品的制造商和贩运者。

鉴于假冒ICT设备出售之前通常会跨越几个不同的国家，因此不仅要求此流程中涉及的利益攸关方密切协作，亦需在相关国家的对等方之间开展合作，以满足本节所述要求。

如第8.2段所述，需要在正品原产地确定假冒设备的制造商和贩运者并对其采取执法行动。

9.2 与行业和消费者团体磋商

采取任何补救行动前必须与网络运营商、行业及消费者团体等全体利益攸关方沟通，这样方能就行业举措开展磋商并就恰当合理的行动达成共识，从而尽量降低给最终用户造成的服务中断。

此外，消费者能够认识到他们在使用和购买ICT设备方面的义务和权利，因此会降低打击假冒ICT设备给所有利益攸关方造成的负面影响。应尽一切努力尽量降低并避免服务的中断与误解。提供的全部信息均应明确且易于最终用户理解。

此外亦要求落实以促进可用性、设备无障碍获取和消费者教育为重点的行动，展示使用合法设备的好处以及与使用假冒产品有关的负面影响。

9.3 可靠的唯一标识符

正品ICT设备须贴有安全、唯一且一致的标识符，即无法被未经授权的实体篡改，且由授权指定人指定的标识符对各设备均具有唯一性。

建议制造商将此唯一标识符置于设备的安全部件之内，同时在技术可行的范围内采取安全措施，对唯一标识符的篡改行为进行检测并在原标识符恢复之前禁止使用该设备。

建议发行标识符的实体实施可确保正确、安全使用这些唯一标识符的程序。

9.4 中心参考数据库

建议在唯一标识符的基础上，针对特定市场部署一个有关授权设备的中心数据库，以便有效地区分正品和假冒ICT设备。

建立此数据库时应考虑以下项目：

– 此中央数据库应与海关署、执法警察和监管机构等国内利益攸关方共享，使各机构能够了解商品的流通情况，在相应情况下阻止假冒ICT设备的进口以及在市场上的流通和销售，同时为追踪假冒生产商和贩卖者提供帮助。

– 此中央数据库应成为清除市场内在用假冒设备解决方案的基石。

– 特定市场的数据库可提供相关国家产品的信息，其中有些是全球数据库的子数据库或者甚至是与全球数据库存在链接。

9.5 部署一致性评估机制

为有效部署针对授权设备的国家中央参考数据库，须在正品制造商制定的型号核准标志、图标或其他唯一标识符的基础上，使用现有（或建立）强大的一致性评估机制（CAS），从而使所有利益攸关方（例如，海关署、客户和行业机构）能够区分原装和假冒ICT设备。

– 若干国家主管部门、区域和国际组织、私营公司和诸多ICT企业已经出台了有效的CAS。一般性情况下，在全球使用ICT方面，设备有必要遵守一套国际认可的标准并通过一致性评估程序。（例如，国际电联实验室的认可 – CASC、ISO/CASCO、IECEE CB、GSMA、FCC、加拿大创新科学与经济发展局、ANATEL、GCF、PTCRB、ARIB等）。

– 这些组织拥有和产品控制相关的大量数据，例如：负责制造和出售此类产品的实体；标准和国家法规集（例如，频谱划分）和产品原产地。

– 推动有序ICT市场的建设有几种方式。其中一个例子是：根据国际电联C&I项目支柱4，已经制定了不同的指导原则。C&I项目的门户网站链接为：（http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx）。

9.6 与海关署和恰当的国内机构密切协作

为有效地限制假冒设备的进口及其在市场上的流通和销售，负责国家中央参考数据库的机构有必要与海关署密切协作，且不同国家的海关之间亦要密切协作。

– 鉴于海关署和其他相关国内消费者机构在截获假冒产品方面发挥的关键作用，至关重要的是为他们提供识别假冒ICT设备的工具，例如：国家中央参考数据库；
– 如果相关国家法律法规允许，则可通过验证机制核对某设备的身份以确定该设备是否为正品的方式，打击假冒、走私和盗窃等非法ICT设备交易；
– 必须在不同组织之间建立起执法程序和通报手段，同时确保他们能够全面运行。这其中包括相关信息的交换，例如：关于ICT产品是否与国家、区域或国际标准一致的数据库；
– 建立海关采用分享产品信息并提供有助于识别假冒设备的报警信息在线跨政府平台，例如：世界海关组织的IPM[b-WCO-IPM]。

9.7 在采取任何救助行动前与最终用户分享相关信息

必须要让消费者了解购买假冒ICT设备的危险，即假冒产品可能无法安全使用，且性能不如正版商品。

此外，必须向消费者明确解释不允许使用假冒ICT设备原因（如安全风险、服务质量的下降和因此产生的投诉率上升、带来干扰的危险和侵犯知识产权（IPR）等），同时应澄清一切最终错误信息，这些信息涉及可能给市场造成影响的程序背后的原因。

在开发识别假冒ICT设备的技术解决方案时，建议为公众提供一种工具来检查产品是否为正品。

9.8 支持适用的国家法律和监管框架

在对假冒ICT设备实施任何限制行动前，需要取得适用国家法律和监管框架的支持，其中包括：

– 限制在电信网络中激活假冒设备；
– 限制进口、在市场中流通和销售不符合国家法律和监管框架的假冒ICT设备及附件；
– 为当局、消费者和销售渠道区分原装和假冒ICT设备提供必要的方案；
– 加强可防止制造假冒产品和其他违法产品的安全措施；
– 建立防止篡改唯一标识符的法律框架。

考虑这一要求时，应适当参考可能已经涉及上述各个方面的现有国家立法和监管框架。

9.9 考虑市场上在用的产品

在对市场中的假冒ICT设备采取干预行动之前，建议考虑为使用这些产品的用户提供保护的必要性。这将减轻对这些设备用户的负面影响，因为他们并不知晓与购买和使用这些假冒ICT设备相关的国家法律或法规条款或要求。

屏蔽可操作的ICT设备可能会给不同类型的网络、最终用户和基础设施造成严重和意想不到的影响。在这种情况下，一种可选方案是采用适当的过渡机制，如开始阶段仅屏蔽新的终端并允许已经在网的设备继续运行。但是，最终用户必须使用正品终端。

10 可能的假冒ICT解决方案

考虑到上文引述的要求并根据[b-ITU-T TR-Counterfeit]所载案例研究提供的信息以及从其他地方收集的信息，下文介绍了一些可能用于打击假冒ICT设备的方法以及在部署这些解决方案时应考虑的一些因素：

10.1 禁止许使用无效和假设备标识符

如果设备使用唯一标识符进行网络注册，则可使用载有已获在特定市场操作授权设备的数据库来拒绝假冒ICT设备注册。

在这些情况下，如果ICT设备实际上拥有可靠的唯一标识符，则人们可以部署解决方案。这些解决方案将：

– 在网络内屏蔽使用无效唯一标识符的设备；

– 屏蔽未获监管机构批准设备的使用；

– 阻止非法进口和销售这些设备。

如果选择了这条行动路线，则亦建议提高消费者对这些要求的认识。此外，如上文第9.8段所指出的，可能需要在国家层面通过适当的立法修改。

当采用的解决方案通过判定并阻止使用具有无效唯一识别码的设备来打击假冒ICT设备时，该解决方案亦有助于：

– 确保只进口或销售合法设备，从而增加关税和增值税收入；

– 通过应合法请求将被盗设备的唯一标识码登记在“黑名单”中的方式，打击设备盗窃；

– 确保消费者不使用低质量的设备，这些设备可能未经授权或对人体健康有危害，抑或不能充分确保服务质量（为确保用户得到保障，在用户购买设备之前使用工具对设备的合法性进行方便的验证）。

在标准的操作过程中应注意保护消费者个人信息，不让ICT设备的使用者遭受标识注册机制带来负面影响。消费者也应得到保护，免受网络任意断开网络连接带来的影响。

有关可能的移动设备解决方案实现方式的更多信息，见附件A。

10.2 ICT设备的认证和市场监督

正如上文第9.5段所指出的，部署一致性评估机制（CAS）可以帮助建立授权设备的国家参考数据库，该数据库包含设备的唯一标识符列表和附加信息（如批准标记、技术规范和物理特性），以便所有利益攸关方(如海关署、客户和行业用户)能够识别核准的设备。

此外，海关官员可利用此信息识别假冒产品，实施市场监管和其他可能会有需要的执法措施。此外，曾有无视进口管理规定纪录的进口者会被确认并登记进入特别名录。当ICT设备由走私者进口时，监管机构会收到通知并可作出决定开展检查，从而使执法得到保证。

作为CAS政策不可分割的组成部分，对已部署电信设备实施市场监督的目标是确保投放市场的产品不会造成电磁干扰，危害公共电信网络，或给公众的健康、安全或任何其他方面造成危害。

事实上，市场监督包括采取一切必要行动（例如，禁止、撤回、召回）停止不能完全符合相关法律和规定要求产品的流通，让产品合乎规定并采取制裁措施。

市场监督对电信市场的顺利运作至关重要。这对于保护消费者和工人免受不符合要求的产品带来的风险至关重要。此外，市场监督有助于保护负责任的企业免受无视规则或偷工减料的无良经营者的不公平竞争。

世界各地的许多监管机构对市场监督组织有具体的法律要求。法规给市场监督机构明确规定了有本国特色的义务，规定他们必须拥有正确履行职能所需的必要权力、资源和知识[b-ITU-T-CI-Portal]。该法规要求建立程序，以跟踪投诉、监测事故、核实是否已采取纠正措施并收集有关安全问题的科学技术知识。此外，国际电联成员国建立、实施和定期更新国家市场监督计划，并定期审查和评估其监控活动的运作情况（例如每隔几年）。[b-ITU-D-CI-Guidelines]

欧洲委员会（EC）第765/2008号条例规定市场监督包含“指定部门开展的活动和采取的措施，以确保产品符合相关法律规定的要求并且不危及健康、安全或其他涉及公共利益保护的方面”。[b-EC- Regulation]

因此为加强产品边检措施，建议在市场监督以外实施补充监管，以帮助相关机构识别假冒商品，从而保证出售给最终用户的产品与实际提交认证流程的产品相符。[b-ITU-D-Rep]

联合国欧洲经济委员会（UNECE）建议各国的市场监督与海关监管活动相互协调，并使知识产权所有者能将假冒商品上报市场监督部门[b-UNECE]。

10.3 设备生命周期管理

在不损害用户权利的情况下，辨别原厂ICT设备与克隆设备的能力备受欢迎。这些克隆设备通常滥用标识符或其他独一无二的标识要素以便称为原厂设备。

有一种解决方案或可帮助这些利益攸关方并保证产品的真实性，即应部署基于这些唯一标识符的设备生命周期管理系统，该系统能够对ICT设备进行跟踪，从产品的制造过程开始（包括部件的原产地、运输以及产品出售的零售商店）一直延伸至产品交付给最终用户。

所有利益攸关方均应可以获得这些信息，即使假冒产品可以克隆唯一标识符，但当局甚至最终用户将有能力验证这些信息的真实性。例如，如果用户在某国商店内通过核查唯一标识符的工具显示该产品假设由另一零售商甚至应在另一国家销售，则即使该唯一标识符有效，仍可作为该产品是假冒产品的有力证据。

在处理最终用户转售二手产品时，应小心谨慎的使用这种解决方案，因为国家立法应考虑在用户与受控设备之间建立联系给保护个人信息造成的影响。

应认为通过这种方法识别出的产品可能并非假冒产品而是在灰色市场上销售的正品，因此需要采取其他的行动来识别假冒产品。

11 参考框架

基于第10段中介绍的不同可行方法的共同点，图1阐述了一种解决假冒ICT设备生产、流通和使用的拟用框架：

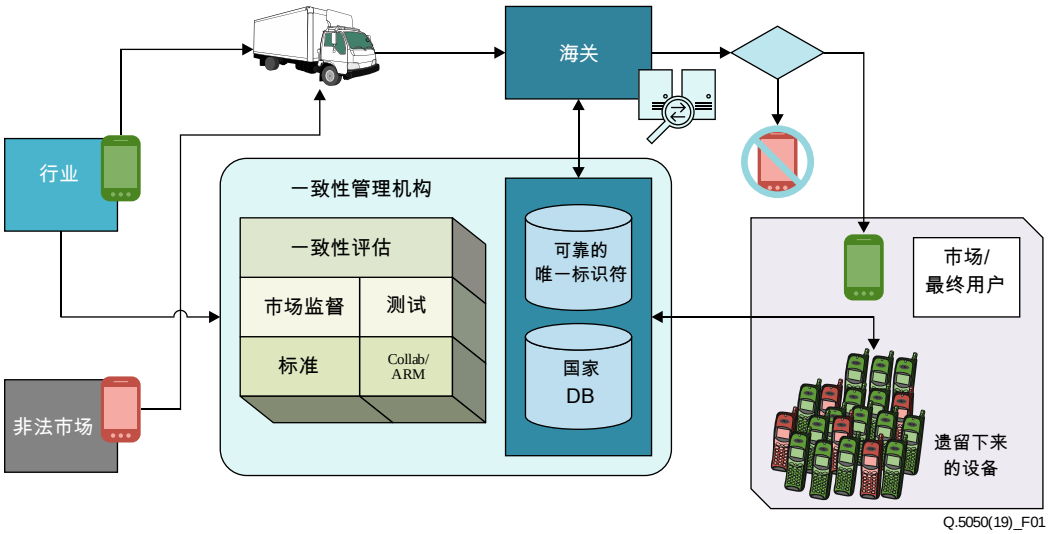

图1 – 拟用的一般性框架

不同组织运营开展的多种多样的活动及其运营的信息系统，应该共同为识别并打击使用假冒和遭篡改的设备提供关键信息并对这些信息加以控制。

合法商家允许对进入某国的产品是否合规进行检查，并指定了负责相关设备的代表/负责人。

当产品到达检查站时，相关实体（例如海关）会从各个法律角度验证这些设备，包括这些设备是否符合任何适用的监管和认证要求，如射频分配、安全性和互操作性等。亦可以对照设备白名单[1]进行检查，以验证进口设备标识符的分配是否合法，以及受检设备的品牌和型号是否与发布标识符时记录的细节相匹配。

在此阶段，假冒产品等未经授权的产品被挡在市场之外。相关实体的人员得到可能已出台的一致性评估机制和数据库的支持，该数据库存储了关于进口集装箱内货物的信息。

一旦设备（合法或非法）投放市场，此类库存数据库亦可为执法活动提供支持。

1 例如，GSMA全球TAC数据库或可用于为3GPP合规设备建立白名单提供帮助。

附件A

移动设备解决方案

（本附件构成本建议书中的一部分）

处理符合3GPP标准的移动设备时，部分识别正品和合法进口移动终端的解决方案是基于国际移动设备标识（IMEI）注册系统的使用。依靠IMEI阻止假冒移动设备扩散的解决方案是基于：

– 阻止使用无效IMEI号码的移动设备（例如，无IMEI、全零IMEI、非标准格式字符串、重复的IMEI、无授权组织分配的IMEI以及指定组织仍未分配的有效IMEI）入网；[2]

– 采取其他举措，例如提高消费者意识，强制执法措施，在国家层面上适当地修改法律。

为阻止使用假冒移动设备，该系统的部署可基于能够显示国家网络活动的，移动设备各有效IMEI代码（符合标准，由指定组织正式分配、合法进口、通过类型核准或确认的标识符）的注册。移动设备的IMEI注册可确保移动设备符合国家法规，且对一些国家而言，能够确保这些设备是合法进口的。

- **参考数据库**

IMEI代码用于创建包含设备“白名单”、“灰名单”和“黑名单”的数据库。“白名单”是获得授权在某国使用的设备注册表（例如该国合法进口或制造的设备），“灰名单”是未确认状态设备的注册表（未输入“白名单”或“黑名单”），而“黑名单”是电信网络必须拒绝为其提供服务设备的注册表。

应事先分析“白名单”、“灰名单”和“黑名单”的部署可能会影响哪些网络和用户，因为这可能会限制设备在国家之间的流动，并对外国来访用户和网络运营商产生影响。

“灰名单”和“黑名单”是通过处理来自“白名单”的数据以及来自运营商、进口商和海关当局的数据自动生成的。

- **与运营商网络的集成**

为了确保与注册系统的积极互动，电信运营商必须维护他们的设备识别登记表（EIR），确保EIR与IMEI代码数据库之间定期同步并自动交换数据（例如每天）。

终端一旦在某一运营商网络入网或注册，则该相关运营商将把终端的IMEI号转发至数据库。系统会披露不在“白”名单内的IMEI号，查出假冒的移动电话并将其IMEI号登入“灰”名单。相关终端的机主会收到一条短信通知，并必须在自进入“灰”名单之日起规定的时限内内确认终端的合法来源。

应当确保登记系统和相关程序的可靠性和安全性。该数据库通常按照不同接入权限，为监管机构、海关、网络运营商和普通大众提供接入。用户应该有权访问此数据库，以此检查该国是否允许某移动设备运行（通常采用发送短信或使用网页的方式）。

重要的是要注意，应视短信为可以与客户进行交流的不安全媒介，它可能会被欺诈者利用，因此可能有必要采取其他措施。

---

[2] GSMA全球TAC数据库或可用于验证符合3GPP规范设备的盗用或克隆IMEI。

- **检测克隆的IMEI**

鉴于某些设备的唯一标识符有可能遭篡改，且贩运者有可能开始通过克隆常规设备的IMEI避开此系统，因此应采取额外措施来识别和打击克隆合法IMEI的假冒设备。

一种可行的途径是采用带有产品附加信息的数据库，该数据库可用于验证使用标识符的产品是否与该品的其他属性相符。这些工具的使用可得到一致性评估机制的协助，此机制可在设备认证过程中收集相关信息并将这些信息存储在所有利益攸关方均可访问的数据库中。

- **其他考虑**

此外，还有一种方案通过判定并屏蔽无效或篡改IMEI代码的移动设备来打击假冒移动设备。该解决方案亦有助于：

– 阻止非法进口这些设备，以确保进口和销售移动设备的合法性，从而增加关税和增值税收入；

– 通过应合法请求将失窃终端的IMEI码录入“黑名单”从而使失窃终端无法使用的方式，对盗窃手机进行打击（应失窃移动设备机主的请求，可将同样的程序用于终端的锁机）；

– 阻止使用未经监管机构型号核准的设备，确保消费者不使用低质量的移动终端，这些终端可能未经授权或危及人类健康抑或无法充分保障移动通信服务的质量（采购前通过工具对移动电话的合法性进行简单验证，以便为用户提供保护）。

重要的是坚持使用全国一盘棋的方法，因为假冒设备可能存在于多个网络，因此检测程序应提高效率，以避免给多个用户造成影响、重复劳动或在不同移动运营商之间造成冲突。

为执行上述方案，应与全体利益攸关方探讨并开展早期诊断（评估无效标识符、克隆等问题的严重性），对检测与控制流程做出规划，评估所需资源（资金、人员、时间）并为降低给最终用户造成的影响进行后果分析。

亦可认为在某些情况下，这些机制可能会给旅行者和游客等合法用户带来问题，例如：

– 一位国外游客来到某国，将一张当地用户身份模块（SIM）卡放在自己的设备中，结果误入白名单陷阱，导致他无法使用手机。

– 持续使用设备数月的漫游来访用户在使用设备一段时间后亦可能遭到本地白名单不公平的惩罚。

– 可能会向使用本地SIM的某国来访用户发送注册信息，但这些来访用户不会说当地语言因此无法理解此信息。因此，他们不会进行注册从而使其设备列入黑名单。这可能会造成：i) 来访用户中断与本地网络的连接；ii) 尽管来访用户的设备完全合法，但由于信息共享，该用户的合法设备在他国被列入黑名单。

鉴于如果执行不好此类机制可能会引发问题，因此设计时就应避免采取这些方案。最后，不得出于其他原因任意使用此功能将用户断网。

附录I

其他行业解决方案

（本附录构成本建议书的组成部分）

业界已付出了多种努力来解决假冒设备问题，提升设备和公司的可信度。这些由行业推动的付出，旨在为提升供应链的安全性开发自愿采用的解决方案。假冒设备是这些努力针对的目标之一，但却不是唯一的目标。行业必须与政府合作，特别是在执法和海关领域。最好将这些努力取得的成果视作工具包，让公司根据的需求和具体环境（例如，产品、市场等）从中各取所需。

请注意，业界针对假冒产品开展的活动涵盖供应链各异、覆盖面广泛的多种产品，其中有些活动会有不同的需求。这是与各类参与者进行的复杂互动。除了这些外部活动之外，公司还为开发打击假冒的手段进行了高度敏感且保密的研发。

下文并不全面地概述了部分为提升设备安全是开展的工作，这些努力有助于增大造假的难度。

- **GSMA IMEI数据库**

IMEI是移动网络中用于识别设备的15位数字的号码。型号划分码– TAC 是识别具体型号的IMEI前8位数字。

全球移动通信系统协会（GSMA）维护的全球数据库包含为符合3GPP的设备指定的具体TAC。此数据库的名称为 IMEI数据库。

可通过下述方式使用此数据库：

– 与正品制造商协作识别假冒ICT设备，其中这些制造商可利用GSMA TAC数据库清单加以确定。

– GSMA TAC可向部委、监管机构、海关和执法部门等政府实体开放，作为移动设备来源和规范的信息来源。此信息可用于识别异常和无法确认设备是否为正品的设备制造厂家。

– 使用GSMA TAC 数据库验证移动设备制造商及其IMEI的真实性。海关和执法机构可使用GSMA服务台验证生产商提供的TAC证书序号。这是与TAC有关的第二个序号。这些标识符之间若存在不匹配，则意味存在着某种形式的标识符伪造行为。

– 监管机构可使用GSMA TAC数据库确保正在进行一致性评估检测的移动设备与数据库所列型号的说明匹配。

GSMA IMEI数据库：https://imeidb.gsma.com/imei/index。

GSMA IMEI服务：https://www.gsma.com/services/tac-allocation/the-imei-database/。

- **设备识别、注册和屏蔽系统（DIRBS）**

DIRBS是基于服务器的软件平台，旨在打击一个国家假冒、非法和盗窃移动设备的行为。DIRBS软件平台作为开放源用于帮助各国政府、监管机构和其他各方对蜂窝网中假冒、非法和盗用设备的非正当使用。该平台符合国际电联有关各国非法和非批准型号设备的建议书。

DIRBS由国家级设备数据库构成，在不同层面与运营商、本地制造商、进口商、消费者、海关、执法机构和全球GSMA IMEI数据库建立接口。DIRBS平台包括分析引擎和相关子系统，为屏蔽假冒和欺诈设备提供信息；实际的屏蔽是根据针对特定国家的管理规则加以判定并通过运营商设备识别注册表（EIR）实施。

更多信息请参见：www.qualcomm.com/dirbs。

- **值得信赖的计算组**

“值得信赖的计算组（TCG）是一个非赢利组织，旨在开发、制定并推行开放、中立于厂商的全球行业标准，支持根植于硬件的信任，用于可互操作、值得信任的计算平台。”

在其他领域，TCG为值得依赖的平台模块制定了与此主题相关的规范：

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

正如上述网站所述，TPM是一种能够安全存储平台（个人计算机或膝上电脑）认证要素的计算机芯片（微控制器）。这些要素包括口令、证书或加密密钥。

此机制允许通过本地和远程认证来建立对设备真实性的信任。

TCG亦为解决包括物联网（IoT）在内的嵌入式系统的安全问题建立了嵌入式系统工作组：

http://www.trustedcomputinggroup.org/developers/embedded_systems

- **全球平台**

全球平台已为值得信任的执行环境（TEE）制定了标准，现代移动设备已将其作为存储和使用敏感安全码和安全资产的方法。

更多信息请参见：https://www.globalplatform.org/specificationsdevice.asp。

- **ISO/IEC JTC1/SC27**

SC27的范围对行业活动很重要，这些活动涉及安全性，减少假冒产品以及为保护信息和ICT制定标准。此范围涵盖一般性方法、技术及处理安全和保护个人信息的导则。

SC27的众多工作就包括出版与打击假冒设备相关的标准，例如：

– [b-ISO/IEC 15408]：“信息技术 – 安全技术 – IT安全的评估标准”（共同标准）；

– [b-ISO/IEC 27034]：“信息技术 – 安全技术 – 应用安全”；

– [b-ISO/IEC 27036-3]：“信息技术 – 安全技术 – 供应商关系的信息安全 – 第3部分：信息通信技术供应链安全的指导原则”；

– [b-ISO/IEC 20243]：“信息技术 – 开放、值得依赖技术提供商的TM标准（O-TTPS）– 减少遭受恶意破坏的产品和假冒产品”。

更多信息请参见：http://www.din.de/en/meta/jtc1sc27。

- **公开组受信任技术的论坛**

公开组受信任技术的论坛（OTTF）主导开发了全球供应链完整性项目和框架，旨在为IT产品购买者提供一批经认证的技术伙伴和供应商供其选择。请注意，上文列出的 [b-ISO/IEC 20243]首先是该公开组制定的。

更多信息请参见：http://www.opengroup.org/getinvolved/forums/trusted。

- **电气和电子工程师学会**

电气和电子工程师学会（IEEE）为确保设备标识的安全制定了标准并为设备标识的加密绑定开发了方法，例如IEEE 802.1ar – “局域和城域网标准：安全设备标识”。

正如IEEE网站指出的：“此标准对安全设备标识符（DevIDs）做出规范，设计的目标是将这些标识符作为安全设备的认证证书，与扩展认证协议（EAP）、其他行业标准认证及配置协议互操作。标准化的设备标识可促进安全设备认证的互操作，并简化安全设备的部署和管理。”

更多信息请参见：http://www.ieee802.org/1/pages/802.1ar.html

- **其他与假冒产品有关的行业活动包括：**

ICC – 打假情报局

http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

ICC – 停止仿造和盗版商业行动（BASCAP）组

http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/

参考资料

[b-ITU-T-CI-Portal] ITU C&I Portal under Pillar 4 keeps updated information on country's C&I regulatory framework http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

[b-ITU-T TR-Counterfeit] Technical Report on Counterfeit ICT device (2015).

[b-IEEE 802.1] IEEE 802.1 (2009), *Standard for Local and Metropolitan Area Networks: Secure Device Identity*. – http://www.ieee802.org/1/pages/802.1ar.html

[b-ISO/IEC 15408-1] ISO/IEC 15408-1:2009, *Information technology - Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/IEC 17000] ISO/IEC 17000:2004, *Conformity assessment – Vocabulary and general principles*.

[b-ISO/IEC 20243] ISO/IEC 20243:2015, *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

[b-ISO/IEC 27034] ISO/IEC 27034:2011, *Information technology – Security techniques – Application security*.

[b-ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[b-EC-Regulation] Market Surveillance Regulation EC no. 765/2008.

[b-Gartner] https://www.gartner.com/it-glossary/gray-market

[b-ITU-D-CI-Guidelines] ITU Guidelines on Establishing conformity and interoperability regimes: Complete Guidelines (2015), ITU http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf

[b-ITU-D-Rep] Final Report for the Question 4/2 – Question 4/2: Assistance to developing countries for implementing conformance and interoperability programmes, ITU-D Study Groups, 2017, https://www.itu.int/pub/D-STG-SG02.04.1-2017

[b-OECD] 2017 OECD report "Trade in Counterfeit ICT Goods".

[b-TRIPS Agreement] Trade-Related Aspects of Intellectual Property Rights; annex of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.

[b-UNECE] Recommendation M. on the: Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[b-WCO-IPM] World Customs Organization IPM – http://www.wcoipm.org/

[b-WTO-TBT] World Trade Organization – WTO Agreement on Technical Barriers to Trade.

ITU-T 系列建议书

A 系列	ITU-T 工作的组织
D 系列	一般资费原则
E 系列	综合网络运行、电话业务、业务运行和人为因素
F 系列	非话电信业务
G 系列	传输系统和媒质、数字系统和网络
H 系列	视听及多媒体系统
I 系列	综合业务数字网
J 系列	有线网络和电视、声音节目及其它多媒体信号的传输
K 系列	干扰的防护
L 系列	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护。
M 系列	电信管理，包括 TMN 和网络维护
N 系列	维护：国际声音节目和电视传输电路
O 系列	测量设备的技术规范
P 系列	电话传输质量、电话设施及本地线路网络
Q 系列	**交换和信令**
R 系列	电报传输
S 系列	电报业务终端设备
T 系列	远程信息处理业务的终端设备
U 系列	电报交换
V 系列	电话网上的数据通信
X 系列	数据网、开放系统通信和安全性
Y 系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z 系列	用于电信系统的语言和一般软件问题

瑞士印刷
2019年，日内瓦