国 际 电 信 联 盟

ITU-T 技术报告

国际电联电信标准化部门

（2015年12月11日）

仿造信息通信技术（ICT）设备

ITU-T

International Telecommunication Union

摘要

仿造已被公认为日趋严重的社会经济问题。本技术报告就仿造信息通信技术（ICT）设备问题的性质提供了背景资料，回顾了涉及此类侵犯知识产权情况的国际公约以及各组织在执行知识产权过程中开展的活动并阐述了一系列旨在打击仿造产品贸易的措施。此外，附件A介绍了多项国家和区域性打击仿造移动设备的举措。

关键词

仿造、伪劣

参考号

QSTR-COUNTERFEIT.

修改日志

有关“仿造ICT设备”的ITU-T技术报告第2版是于2015年12月2-11日在日内瓦召开的ITU-T第11研究组会议上通过的。

编辑 Keith Mainwaring
UNIS

电话：+46 76 107 6877
电子邮件：
keith.mainwaring@ukrainesystems.com

目录

图表清单

页码

ITU-T技术报告

仿造ICT设备

摘要

仿造已被公认为日趋严重的社会经济问题。本技术报告就仿造信息通信技术（ICT）设备问题的性质提供了背景资料，回顾了涉及此类侵犯知识产权情况的国际公约以及各组织在执行知识产权过程中开展的活动并阐述了一系列旨在打击仿造产品贸易的措施。此外，附件A介绍了多项国家和区域性打击仿造移动设备的举措。

1 引言：仿造产品 – 日益严重的问题

虽然难以衡量，越来越多的证据表明，仿造产品泛滥的程度以及殃及的产品范围成为日益严重的问题。2008年，经合发组织（OECD）[1]发表了一份报告。根据海关的没收情况估计，2005年仿造和盗版货物（不包括数字产品以及本国制作和消费的产品）的国际贸易总额超过2000亿美元。这一估算以国际贸易从2000年1000亿美元至2007年2500亿美元的增长和构成变化为基础，占全球贸易的1.95% [2]。有些估计甚至更高，国际商会（ICC）仿造情报局估计，仿造在每年6000亿美元的世界贸易中占5-7% [3]。

ICC停止仿造和盗版商业行动（BASCAP）组授权开展一项研究[4]以充实OECD对仿造和盗版产生的经济和社会影响的描述。根据该报告的估算，全球仿造和盗版产品经济总额达每年6500亿美元，其中国际贸易占一半以上（2850亿至3600亿美元），国内生产和消费在1400亿至2150亿美元之间，数字内容（音乐、电影和软件）在300亿至750亿美元之间。此外，据估计，G20国家政府和消费者每年（因税收减少和反击措施执行与医疗支出的增加）为仿造和盗版付出的代价超过1250亿美元并因此损失约250万个可能的就业机会。

根据欧洲联盟（EU）各国海关当局的登记，进入欧盟的仿造货物在2005至2010年间增加了两倍。欧洲委员会于2011年7月发表的统计数据表明，侵犯知识产权（IPR）的可疑出货数量呈明显上升趋势。2010年海关登记了约80 000起案件，与2009年相比约增加了一倍。欧盟外部边界扣留的伪造产品多达1.03亿。
http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf

仿造商品范围之广可谓登峰造极 – 食品和饮料、医药产品、电子和汽车组件、各类消费产品，甚至整个商场。计算机组件（显示屏、机壳、硬驱）、计算机设备、路由器、网络摄像头、遥控器、移动电话、电视（TV）、光盘（CD）和数字通用磁盘（DVD）播放机、音箱、相机、耳机、通用串行总线（USB）适配器、软件、证书、认证标识和数据（生物特征数据）均在仿造之列。

种种因素使互联网成为令零售商亲睐的资源，特别是针对小规模市场的零售商（市场遍及全球，成立公司简便易行，为提高吸引力和说服力而移动并关闭网站，发送电子邮件无需成本）以及可以匿名的可能性使互联网成为销售仿造货物的最佳场所。然而，大量的互联网网站使知识产权所有者和执法机构难以分辨非法操作。推介性电子邮件、电子商务和拍卖网站都被仿造货物的销售所利用。

就ICT行业而言，KPMG和AGMA报告指出，在信息技术（IT）行业全球销售的所有货物中，8-10%为仿造货物，因仿造造成IT行业收入的损失在2007年达1 000亿美元。仅惠普通

过2005至2009年在55个国家开展的4 620项调查就没收了价值超过7.950亿美元[6]的仿造打印耗材。在2011年美国的海关罚没中，消费电子产品占22%，2010年产品价值增加16%。约三分之一的这类货物为移动电话[5]。

2011年，估计全球仿造移动电话多达2 504万部。http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline。相当于2011年销售的1.546亿部手机中的16% [8]。对移动电话市场仿造普及率的估计与2011年针对欧洲委员会开展的有关价值链和供货安全国际化及其分割情况的研究状况相辅相成。根据这项研究，仿造移动电话在全球售出设备市场中约占15-20%，收入为90亿美元。

除生产仿造设备外，仿造电子元器件亦混入合法产品供应链。2011年秋季有关仿造电子元器件用于美国军用设备的消息进入人们的视线，为此，参议院军事委员会就国防部供应链中仿造电子元器件的使用召开听证会[9]。根据商务部工业和安全局[10]开展的一项研究做出的估计，国防合同供应链中采用仿造电子元器件的事件约为1 800件，涉及100多万个元器件。事件的数量也从2005年的3 868起增加至2008年的9 356起。听证会后，出台的2012年国防授权法（NDAA）包含有关处理仿造元器件的指导原则，要求对进口电子元器件加强检查，让合同商全权负责发现假冒元器件并对可能假冒元器件进入产品的情况予以纠正[11]。

2008年OECD开展的研究发现，多数仿造产品源于亚洲的一个国家（占没收仿造产品的69.7%）。

本技术报告旨在就仿造问题以及该问题的解决提供背景资料，突出ICT设备的仿造以及可用来缓解该问题的ICT手段。

除仿造设备外，所谓“劣质”或“未经授权的”ICT设备和配件亦四处蔓延。尽管这些术语没有统一的标准化定义，但这些设备通常使用低质元器件，而且在多数情况下未遵守国家有关移动设备的认证、批准、分销和销售的现行法律要求。这些设备不一定都侵犯了设备制造商的知识产权，因此不在已被接受的“仿造”定义范畴之内，为此，不属于本技术报告涉及的范畴。因为该报告侧重于仿造设备。“劣质”设备属于另外一类问题。该问题的解决需要单独考虑。

2 何为仿造

世界贸易组织有关知识产权贸易方面的协议（TRIPS协议）将仿造商标货物定义为“包括包装在内的任何如下货物：未经许可而载有的商标与此类货物已有效注册的商标相同，或其基本特征不能与此种商标相区分并因此在进口国法律项下侵犯了所涉商标所有权人的权利”（第51条脚注14）。术语“仿造”因此在TRIPS协定中仅用于商标领域。它指比普通商标侵权定义更准确的侵权货物，前提是该商标与原商标相同或基本特征无法区分。这段案文未涉及使用仿造商标的意图。它从与注册产品使用商标的相似性角度定义仿造商品适用于与注册商标相同的货物情况。事实上，这种侵权货物通常包含商标雷同的情况，从而有意造成与原商品相同的印象。这种做法通常旨在以假乱真，因为故意要在原产品和复制品之间造成混淆。

TRIPS协定同一脚注还将盗版货物定义为任何如下货物：“未经所有权人同意或未经生产国所有权人充分授权的人同意而制造的复制品以及直接或间接由一物品制成的货物，如此种复制在进口国法律项下构成对版权和相关权利的侵犯”。因此，术语“盗版”涉及版权以及TRIPS协定中相关权利的侵犯。

3 仿造ICT设备和组件的影响

一些与仿造ICT设备相关的社会影响是独一无二的，与其他类侵权行为毫无相干。举例而言，仿造设备通常未经正式测试，也未按照任何适用的规则要求获得批准。使用仿造设备可能带来极大的风险。例如，曾有报告指出，仿造电池爆炸造成人员死亡，由于充电器造成的触电和火灾时有发生，还有一些文件谈及铅和镉等有害物质含量较高的设备。

2008年OECD的报告包含了有关社会经济效应和对所有权人、消费者和政府影响的评估：

- 考虑到社会经济影响，仿造可能会对创新、外国直接投资水平、经济增长以及就业水平产生不良影响，并有可能将资源转入有组织的犯罪网络。
- 仿造对所有权人可能产生经济影响，因为销售量和专利税、价格、品牌价值和声誉、运作成本和范围可能受到影响。
- 消费者会发现，仿造货物的品质不达标并可能产生严重的健康和安全隐患。
- 政府无法征收足够的税收并可能面临腐败问题，同时有必要为打击仿造行为增加资源。

3.1 仿造ICT设备实例

以下是仿造ICT设备影响的主要实例：

3.1.1 移动电话

仿造移动电话和配件通过以下方式对社会造成不良影响：[1]

- 降低移动电信业务的服务质量，因此影响用户和企业体验；
- 因使用不良或不当配件和材料为消费者带来安全隐患；
- 加大网络安全威胁；
- 影响消费者隐私；
- 危害数字交易的安全性；
- 逃避适用税收和关税，因此对政府税收收入造成不良影响；
- 因无法为消费者提供担保以及违背消费法律要求使财力最薄弱的消费者受到伤害；
- 因在这些设备的制造中使用危险物质为环境和消费者健康带来风险；
- 为毒品交易、恐怖和其它本地及国际犯罪行为起到推波助澜的作用；
- 因不公平竞争和欺骗行为造成的市场扭曲对经济产生危害；
- 破坏原产品生产公司的商标。

诺基亚技术研究院（INdT）是位于巴西的一家独立研发实体，它开展的一项研究确认指出，仿造电话质量低劣，对消费者、电信运营商和本地经济可能产生不良影响。研究审查了44种仿造和劣质蜂窝电话，将其与真品和同类设备进行比较。研究显示，仿造电话在呼叫尝试中失败率为26%，已建呼叫中掉话率为24%。此外，在正品电话运行顺利的地方，仿造电话无法使用，因为与正品电话相比，传输质量较低。此外，在蜂窝切换（在蜂窝之间移动

[1] 以下基于MMF仿造/劣质 – 政府资源指导，
http://spotafakephone.com//docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf

时保持呼叫的能力）中，比正品电话切换时间长41%，且切换中的掉话率为34%。见移动制造商论坛（MMF）仿造/劣质移动电话政府资源指导附件1中的图表：http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf。

仿造移动电话还具有严重的健康和安全风险。这些设备可能包含的化学元素超过所规定的安全标准，并难以通过电子废物管理计划进行搜集。这对于缺少或没有良好回收能力并拥有大量仿造移动设备的发展中国家的影响尤其深重。通过进一步抑制这些设备的运转来解决仿造设备的问题使发展中国家的情况更加复杂化。

组装不当并使用低质组件的仿造设备包含许多国家或各国法律限制的有害物质（RoHS）。

诺基亚位于巴西的技术研究院（INdT）最近就有害物质开展的另一项研究彰显仿造电话可能带来的危险。具体而言，研究的目的是评估仿造电话是否符合RoHS以及欧盟有关限制在电子和电器设备中使用某些有害物质的法令。该法令限制在各类电子和电器设备中使用六种有害物质。

这项研究利用IEC 62321 [75]标准测试方法测试了五种仿造电话和158个组件，其中包括机壳、显示器、集成电路（IC）、键盘和其它表装设备（SMD）组件。INdT的研究显示，内部和外部组件均包含浓度大大超过所允许的RoHS最大值的有害物质（铅和镉）。图A：MMF仿造/劣质移动电话有害物质的物理分析 – 面向政府的资源指导http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf表明，在所测试的移动电话的内部和外部组件中均发现了超量铅和镉。

在其它国家进行的其它研究也确认了仿造移动电话中有害物质的存在。印度海得拉巴电子技术材料中心（C-MET）为测试印度市场中移动手机是否符合RoHS开展了一项研究。在此研究中，C-MET选择了15种移动电话模式进行测试。电话的挑选基于其在印度市场的普及性和可用性，测试还使用了IEC 62321（2008）程序。

结果表明，所有仿造移动电话中包含的有害物质比例严重超标，尤其是铅（Pb）。在一些情况下，测试值比全球公认的Pb限值超出35-40倍。许多重要的组件，如存储卡槽、用户身份模块（SIM）槽、相机等消费者直接接触的组件在有害物质方面含量最高，与设备内组件相比，为消费者带来了的风险明显加大。相反，对全球和其它公认品牌的移动电话的测试结果却符合RoHS限值，因此消费者的使用是安全的。图B为MMF仿造/劣质移动电话 – 面向政府的资源指导http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf，概括了这项研究结果；图C为MMF仿造劣质移动电话 – 面向政府的资源指导http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf，用图表显示出高铅含量的领域。

此外，使用复制/假冒/丢失的国际移动设备身份（IMEI）号码的电话可对国家和个人安全造成威胁，因为这些电话难以在网上跟踪。

最后，谈到仿造移动设备贸易可能造成的收入损失，肯尼亚仿造机构宣称，该国因仿造手机市场造成的损失达3 850万美元[39]。乌克兰于2009年安装了移动终端自动注册信息系统（AISMTRU）后自2010年到2012年因移动终端海关进口关税付款增加收入5亿美元。在2009年实施该系统之前，乌克兰使用的移动设备中只有5-7%是通过合法渠道进口的，而今天92-95%的设备是合法进口的[40]。

3.1.2 ICT产品的配件和组件

仿造已出售的ICT产品配件司空见惯。对于移动电话以及其它ICT产品，配件指电池、充电器和耳机。对于打印机，通常墨盒是仿造的。而数字相机中，与机身登记匹配的假冒镜头和其它诸如接线和记忆卡等假冒配件比比皆是。这些假冒组件甚至进入到芯片级层面。偶然或有意使用假冒电子组件可为医疗设备或其它重要的用于安全的ICT产品用户带来严重问题。2013年，在巴黎CarteS大会上未经授权的MIFARE无接触仿造卡被当场没收：http://www.mifare.net/files/6114/2295/3702/NXP_Whitepaper_Protect_your_reputation_with_genuine_MIFARE_products_2015.pdf

仿造电池遍及世界各地，尤其令人担忧。仿造电池已引发多场大火。仿造电池的类型从碱性AA电池到包含在许多类产品，特别是移动电话中的充电锂电池。

有报道称，仿造电池导致死亡：http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aLWvmmrHx9F0。与此报道相关的是，这些仿造电池多发现在贫困地区，因为这些地方手机利用率较高，因此需要经常更换电池。

这类事件在世界各国屡见不鲜。经过多次报道后，人们对在飞机上造成问题的这类电池万分忧虑。2014年2月，英国民用航空局的Geoff Leach说：“在网上可疑地点购买的廉价、仿造电池令其忧心忡忡，这类电池一旦出现问题，可产生不可估量的后果”。http://www.bbc.co.uk/news/business-25733346 。

2004年，在美国参议院司法委员会听证中，Gillette代表解释道，通过一星期的努力，他们抓获了100万假冒Duracell电池和其它仿造产品：http://www.judiciary.senate.gov/meetings/counterfeiting-and-theft-of-tangible-intellectual-property-challenges-and-solutions &
http://www.judiciary.senate.gov/imo/media/doc/Willard%20Testimony%20032304.pdf

耳机亦令人堪忧，劣质的仿造产品不仅可能损伤耳朵，还能造成火灾风险。2013年曾有报告指出，官方没收的假冒耳机价值1 500万英镑：http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods

3.1.3 对讲机

Motorola Solutions公司提醒用户谨防购买2013年在越南发现的仿造对讲机。这些仿造对讲机危害用户，它们不仅复制了摩托罗拉对讲机设计，还使用未经授权的摩托罗拉徽标型号号码，使客户难以辨别真伪：http://uk.reuters.com/article/2013/07/09/motorola-solutions-idUSnBw085384a+100+BSW20130709

3.1.4 数字相机

数字相机是多种仿造ICT产品中的一员。与其它产品一样，数字相机难以区分厂商、零售商。热心的使用者有时会为帮助消费者辨别假货提供指导：http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html

诸如网络摄像头这类的仿造设备对于用户具有极高的安全和隐私风险。这些产品中的软件不仅质量低下或从根本上存在缺陷，而且，用户也无法获得安全升级或售后支持，从而使自己陷入网络风险。

3.1.5 个人计算机和平板电脑

一些类型的计算机和平板电脑的风靡导致仿造产品铺天盖地而来。有时这些产品只是“诱饵”，甚至没有电路板。http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/。对于包含电子部分的产品，一些已预置了包含在仿造操作系统中的恶意软件。http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware

3.1.6 电子儿童玩具

2014年，多数儿童玩具包含某种电子成分。从假冒游戏机和手持游戏机到婴儿玩具都可能对儿童造成身体伤害。安全风险包括未接地电源带来的触电风险：http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys

4 知识产权（IPR）公约

许多国际协议和公约为按照国家法律保护IPR确定了实质性标准，同时包含可允许的例外和限制并确定了政府为所有权人提供的针对违规行为采取有效行动而必须遵循的程序。

4.1 《保护工业产权巴黎公约》和《保护文学和艺术作品伯尔尼公约》

世界知识产权组织（WIPO）管理涉及知识产权的多项条约。基本条约包括《保护工业产权巴黎公约》和《保护文学和艺术作品伯尔尼公约》。

《巴黎公约》是在1883年达成的，之后经过多次修改。该公约旨在保护“专利、工业外观设计、商标、服务商标、商号、产地标记或原产地名称以及制止不正当竞争”[18]。有关仿造，该公约要求各签字国采取措施打击直接或间接使用商品原产地的虚假标记或生产者、制造者或商人身份的虚假标记。

4.2 世界贸易组织（WTO）《与贸易有关的知识产权协定》（TRIPS）

世界贸易组织（WTO）管理着TRIPS协定。该协定确定了所有WTO成员在保护和执行IPR过程中将实施的起码标准。因此，TRIPS协定首次全面地将一套完整的执行条款引入多边协议。WTO成员之间在此方面出现的任何争议将按照WTO争议解决谅解予以处理。

TRIPS有关执法的条款具有两项基本目标，即为所有权人提供有效的执法手段并确保执法程序的平衡和相关，从而不对合法贸易造成影响。该协定分为五个章节。第一节为所有执法程序必须满足的一般性义务做出规定。这些规定主要确保程序的有效性，使一些基本程序原则得到满足。以下章节涉及民事和行政程序及救济、临时措施、与边界措施相关的特殊要求和刑法程序。

该协议对一般性侵权行为和仿造或盗版做出区分。前者必须配备民事和行政程序以及救济措施，而后者是更为明目张胆、厚颜无耻的侵权行为，为此必须施加某些附加程序和救济方式，如边界措施和刑法程序。为此，仿造货物从根本上被定义为涉及商标原样复制的货物，而盗版货物被定义为按照版权或相关权利规定违背复制权利的货物。

具体而言，WTO成员具有以下义务：

(a) 民事和行政程序：所有权人必须能够启动针对知识产权侵权者的民事司法或在任选的基础上启动行政程序。这些程序必须公平平等。制定有关证据的规则。此外，成员需要司法机构授予进行三类救济的权利：禁止、损坏和其它救济。作为防止滥用的保障，这些义务还扩展到所有权人滥用执法程序时对被告人的赔偿。

(b) 暂行措施：临时禁令构成法庭争议解决过程中的一个重要手段。因此，司法机构必须有权利发出立即采取有效暂行措施的指令，以便对声称的侵权行为采取行动。这些措施旨在防止IPR侵权的发生并保护有关侵权行为的相关证据。与有关执法的其它章节相同，一些程序要求和防止滥用的保障措施也有所规定。

(c) 边界措施：使所有权人能够获得海关管理部门的合作，从而在边界截获侵权货物并防止这些货物进入流通领域。这些是对仿造商标和盗版货物的强制性规定，而成员还可将其用于出口的侵权货物、过境货物、**微量**进口和并行进口。边界措施与暂行措施一样，必须符合一些程序要求并具备防止滥用保障。有关救济，相关管理机构必须有权命令在侵权货物的商务渠道以外进行销毁或处理。

(d) 刑事程序：必须对恶意仿造商标或商用盗版情况予以处理。是否将其用于其它IPR侵权案件是可以选择的。从救济角度，协定规定，制裁必须包括监禁和/或罚款并在适当的情况下包括对侵权货物和材料以及用来生产的设备的没收、扣留和销毁。

WTO最不发达国家成员目前受益于过渡安排，在2021年7月之前免于遵从TRIPS一般性协定规定的保护和执法标准并在2016年1月之前免于遵守医药行业有关专利和未披露数据保护和执行的规定。这种做法的旨在为他们奠定可行的技术基础提供机遇。

5 IPR执法

尽管有关保护知识产权的国际公约已存在了100多年，国际论坛仅在近期才开始探讨执法问题。这主要是因为TRIPS协定奠定的基础以及IPR侵权日益加大的社会经济影响。IPR执法现已列入许多国际组织的议事日程，如WIPO、世界海关组织（WCO）和国际刑警组织以及欧盟和许多国家。

5.1 世界产权组织（WIPO）

世界产权组织（WIPO）于2002年建立了执法顾问委员会（ACE），其宗旨是与其它国际组织和私营部门开展协调以打击伪造和盗版。该组织提供培训项目和技术援助。

WIPO还与联合国环境署（UNEP）和诸如联合国亚太经社委员会（UNESCAP）等其它组织合作以提高人们对与日俱增的仿造产品的回收和处理挑战的认识：
http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html

http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx

http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods

5.2 世界贸易组织 – TRIPS理事会

TRIPS理事会是在WTO总理事会下的三个行业理事会之一，它负责管理TRIPS协定，尤其负责监督协定的操作和成员履行协定义务的情况。理事会每年在日内瓦召开三次正式会议并按需要组织情况通报会议。会议构成有关TRIPS协定任何相关问题的讨论和磋商论坛并用来澄清或解释协定条款。IPR执法问题曾多次在TRIPS理事会上作为专门话题讨论，最近一次是在2012年。

5.3 联合国毒品和犯罪问题办公室（UNODC）

UNODC是《联合国打击跨国有组织犯罪公约》的管理机构。这是全球范围内打击各类有组织犯罪的合作平台。目前，已有167个国家加入该公约并致力于通过合作打击有组织的犯罪并确保制定相应的国内法律。

UNODC每两年组织《联合国打击跨国有组织犯罪公约》各方会议。这些会议将来自世界各地的政府汇聚一堂以推动并审议公约的实施，从而确保以更好的手段应对跨国有组织的犯罪。最后一次会议于2012年10月举行。

联合国毒品和犯罪办公室侧重于仿造货物贸易与跨国有组织犯罪之间的关联 http://www.unodc.org/counterfeit/。UNODC于2014年1月推出了“远离仿造，以防陷入有组织的犯罪”的宣传活动，从而提高消费者对每年非法走私价值高达2500亿美元的仿造货物的认识。有关远离仿造以防误入“有组织的犯罪”的宣传活动让消费者了解，购买仿造货物可能为有组织的犯罪团伙慷慨解囊，置消费者健康和安全于风险之中并助纣为虐，招致其它道德和环境忧患。

UNODC还努力打击非法货物的流动，如通过技术援助项目提供仿造产品和毒品。UNODC和世界海关组织于2006年发起了集装箱控制项目（CCP）。该项目共抓获487个欺诈性集装箱和走私货物以及195箱毒品：

https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html

https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html

5.4 世界海关组织（WCO）

WCO是由179个海关主管部门组成的政府间组织，为其成员保障并推动合法贸易、实现收入、保护社会提供引导、指导和支持。由于海关主管部门负责防止国家边界非法流入仿造和盗版货物，WCO牵头了全球为打击这类犯罪所开展的工作的讨论。这包括完善执法方法和促进海关之间以及海关与私营部门之间的交流，从而为打击仿造和盗版加大工作力度。

引起海关官员和全球业界的关注并确保他们提高对仿造产品的警惕性是WCO IPR和健康与安全项目的核心。WCO将保护消费者健康和安全作为首要任务，特别积极地开展能力建设活动并开发各类执法工具。

WCO认识到与私营部门合作的重要性，因此与业界成员及协会密切合作，评估其需求和处理问题时遇到的困难。WCO定期邀请所有权人参加各类反仿造活动，如现场作业、区域或国家研讨会，并开发了在线工具、公共成员界面（IPM），使海关人员配备检测仿造和盗版产品的手段并与各方经济力量进行实时沟通。

大规模作业对于WCO反仿造举措发挥着重要的作用。大量海关主管部门同步提高打击仿造产品的执法能力，以便对全球仿造活动进行量化并确定性质。仅2013年海关主管部门在非洲区域的作业和拉丁美洲区域的作业就截获了11亿项仿造产品。

WCO还开发了全球在线检测工具IPM，旨在让前线海关人员方便区分真品及伪造复制。自2010年面世以来，IPM已成为现场海关人员和私营部门之间开展实时通信的核心手段，使他们得以实时传递重要信息，从而截获仿造货物。

在移动IPM最近推出后，现场海关人员可以通过移动装置访问IPM，并接收数据库中包含的所有相关信息。新的版本使他们能够利用移动设备扫描数百万产品之上符合行业标准的

GSI条形码，并以更高效的方式搜索产品数据库。此外，扫描条形码将自动连接至与所控制产品相关的认证部门。新的功能被称为IPM Connected – 与IPM相连的全球安全功能提供方网络（SFP）。随着SFP网络的扩大，大量所有权人已加盟IPM，使系统中的品牌数量超过700个，涉及从医药、食品、杀虫剂到快速移动的货物和奢侈品等多个行业[16]。

5.5 欧盟

在欧盟层面，自2011年以来便就有关知识产权执法的2004/48/EC 法令开展了公共磋商。上期有关欧盟成员国知识产权民事强制执行制度效率的公共磋商于2013年3月结束。欧盟于2013年7月发布了一份回复摘要。

欧盟委员会于7月1日通过了一份通报“向重就知识产权执法达成共识迈进：欧盟行动计划” – COM (2014)932。

该行动计划中所列十项行动聚焦于商业性侵权（即所谓“货币跟踪”法），旨在加强预防，提高成员国之间的跨境合作，在目标数据的基础上确定知识产权强制执行政策的优先级。

欧洲假冒盗版观察机构作为欧盟下设机构于2009年成立。欧洲议会和理事会第386/2012号法规，将该机构更名为欧洲侵犯知识产权观察机构，并于2012年6月5日完全将其归入内部市场协调局。 作为公共和私营参与方的一个平台，该机构允许这些参与方分享有关IPR执法的最佳做法和经验，提升公众意识并就数据的采集与监测开展协作。

欧洲委员会在欧盟层面通过互联网宣传有关假冒产品销售的备忘录（MoU）。互联网平台、品牌所有者和贸易协会共同于2011年5月签署了此项备忘录。该备忘录为打击网上销售假冒商品建立了一套做法规则，并提高了缔约国间的合作水平。

海关

2003年7月22日，海关针对某些产品疑似违反某些知识产权所采取行动的理事会第1383/2003号法规被608/2013号法规取代。

5.6 国际刑警组织

国际刑警组织由190个成员国组成，于2002年成立了知识产权行动组。该组对在区域和全球层面抓获仿造货物的工作提供支持，通过国际IP犯罪调查学院（IIPCIC）组织培训课程并已创建了国际知识产权犯罪数据库。

5.7 欧洲经济委员会（UNECE）

UNECE有关监管协调和标准化政策的工作组（WP.6）成立了市场监督顾问组（MARS小组），旨在鼓励成员国开展协调以遏制仿造货物问题。他们制定了有关“将市场监督基础设施作为保护消费者和用户不受仿造货物侵害的辅助手段”的建议书[18]。

5.8 国家举措（若干实例）

5.8.1 法国

CNAC（**国家反仿造委员会**）是法国国家反仿造委员会

http://www.industrie.gouv.fr/enjeux/pi/cnac.php，而INPI（**国家知识产权局**）是国家有关工业财产的机构http://www.inpi.fr/fr/accueil.html 。财政部（**经济和财务部**）亦参加反仿造活动：

http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet

5.8.2 英国知识产权局

英国政府知识产权局于2004年成立了知识产权（IP）犯罪小组。该局每年发布IP犯罪报告并公布了供应链工具包[19]。英国还设立了知识产权部长。

5.8.3 肯尼亚反仿造局

肯尼亚议会于2008年通过了反仿造法（第13款）。该法案禁止仿造货物贸易，同时成立了反仿造局[20]。

5.8.4 中美商务和贸易委员会

美国和中国成立了联合商务贸易委员会。在其2013年12月召开的第24次会议上，中国打击知识产权侵权和假冒伪劣货物制造和销售国家领导小组致力于在2014年通过一项行动计划，其中包括提高公众认识，要求所有IPR保护和执法行动符合各项法律和规定：www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet

6 工业打假论坛

企业已对假冒问题做出反应，通过成立论坛体现其利益诉求。这些论坛提供有关问题严重程度的信息，就缓解假冒造成的影响提出建议方法，说服各国政府和国际组织就打击假冒现象采取行动。

6.1 国际商会（ICC）

ICC是国际商业的组织，其成员包括约120个国家数以千计的公司和协会。ICC作为商界代表参与政府和政府间组织的活动。ICC成立于1919年并于1923年成立了国际商会仲裁法院。

ICC于1985年成立了打假情报局。最近又成立了“禁止假冒与盗版商业行动（BASCAP）组”。

ICC打假情报局在维护案例分析数据库的同时也提供调查服务。

BASCAP继续开展最初由经济合作发展组织发起的有关假冒和盗版对经济和社会所产生影响的研究，并成立了按国家、行业、品牌保护和全球联系方式对信息加以分门别类的信息交流中心。

ICC同时发布了知识产权路线图[25]。

6.2 国际打假联盟（IACC）

IACC [26]成立于1979年，其成员来自各产业部门。其目标是通过推进反假冒法规打击假冒和盗版现象。

6.3 手机制造商论坛（MMF）

手机制造商论坛负责维护提供假冒手机和假电池信息的网站（spotafakephone.com）。

6.4 国际服务和计算机交易商协会和北美电信交易商协会（AscdiNatd）

AscdiNatd制定了一项打假计划，向成员公司提供打假政策和假冒产品信息的来源，其中包括来自HP和Cisco的信息[27]。

6.5 清除灰色市场和假冒产品联盟（AGMA）

AGMA于2001年由3Com、Cisco系统、惠普、Nortel和Xerox组建，其目的是打击假冒高科技产品。

6.6 英国电工和制造者同盟协会（BEAMA）打假工作组

BEAMA是为英国和全欧洲电工产业服务的独立专家知识库和论坛。作为300多家电工产业制造商的代言人，BEAMA对全球和英国的政治、标准化和商业政策有显著影响力。

BEAMA打假工作组（ACWG）于2000年组建。其目标是对造假者制造的假冒电子产品采取行动，打击那些将这些产品分到欧洲、中东和非洲等诸多国际市场的分销商。该工作组由引领行业潮流的装备、分销、测试、认证和执法产业协会，以及BEAMA的成员组成。该工作组积极的工作赢得了全球认可，并且同全世界的贸易协会和执法机构开展合作。

现已经建立了供电子装备产业使用的造假者数据库，该数据库已移交给世界各地的监管机构供其实施本地市场监测之使用。

工作组的活动通过贸易杂志文章、演示、会议、指南和海报进行公开宣传，以提高对这项不但日益凸显，而且对消费者的安全和商业道德的具有破坏性的潜在威胁的认识。

工作组负责管理打假行动项目，收集和传播有关知识产权问题的信息，并代表协会对政府和其他机构作出响应。

目前的活动包括在中国、阿拉伯联合酋长国、英国、尼日利亚和伊拉克的项目，以及所部署的全面网络和港口监督计划。

在英国，BEAMA同许多领先的产业机构一道，致力于提高公众认识，打击假冒和不合规产品。专门为此建立的产业门户网站www.counterfeit-kills.co.uk已经上线。

6.7 UKEA（英国电子联盟）

在英国，UKEA是由各贸易协会组成的代表电子产业的联盟。其目标是协调业内问题的讨论并同政府沟通。UKEA建立了打假论坛[28]，藉此公布假冒电子零件问题、解决方案提供商和最佳做法等信息。

6.8 打假组（ACG）

ACG是英国的贸易协会，成立于1980年，当时其成员主要集中在汽车产业，但现在代表大多数产业部门。

6.9 UNIFAB – 制造商联盟

制造商联盟是一个法国组织，致力于通过提高公众意识（通过建立假冒产品博物馆以及其他活动）、向企业提供信息及游说活动的方式打假。http://www.unifab.com/en/

6.10 国际电子制造举措（iNEMI）

iNEMI确定了一项有关“假冒零件—评估方法和指标发展”的计划。
http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf

7 打击假冒设备的措施

7.1 引言

可以通过以在产品上作某种标记的方式打击假冒设备，亦可通过对产品生命周期的严格控制对其进行认证。难以伪造的标签可贴于产品之上，分配的序列号可用于认证商品是否为正品（例如通过访问数据库的方式）。

可为独立的商品分配唯一的识别码。如mPedigree就是用于打假系统的一例，它被用于打击非洲的药物假冒现象。该系统允许消费者通过向医药产品的记录系统发送（免费）短信（SMS），检验药品的真伪。

需通过测试、评估和认证等措施对供应链或对产品的整个生命周期进行严格控制，以保证产品的安全，维护其应有的质量。此外，需为海关官员辨别假冒产品提供工具，但也可以使用市场监控机制。

识别码可以用清晰的文字印制在物体上，或通过编码印制在“身份（ID）标签”上，如条形码、射频识别（RFID）标签、智能卡或红外标签，便于自动读取。对物体的识别可以分为三层。首先是纯识别层面，在该层对物体作唯一识别，例如通过电子产品编码（EPC）。第二层是编码层，纯识别码可以被编码为不同的格式。最后是物理实现，例如将完成的身份编码写在RFID标签上。

为保证识别码在全球对于特定应用的唯一性，必须以有组织的方式通过某种形式的分配程序对其进行管理。GSM协会（GSMA）负责管理用于全球移动通信系统（GSM）、通用移动通信系统（UMTS）和长期演进（LTE）设备的移动设备国际识别码（IMEI）；电信行业协会负责为CDMA设备分配移动设备识别码（MEID），GS1负责管理条形码识别码。ISO负责管理若干识别码领域，同时作为最高层机关将诸如GS1等其他组织的识别码机制纳入。

另一个示例是通过对设备进行标记指出其在某国已获得上市许可。例如，Anatel要求移动电话充电器和电池附带一个通过其决议481/2007[2]定义的安全标签。见图1。

[2] https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=

图1 – Anatel要求按照其决议481/2007定义的安全标签示例

这种方式多年来已被用于电信设备产业，并成功在部分国家/区域实施[3]（例如FCC[4]、Anatel[5]和EU[6]）。

海关官员需要能够确认假冒产品，可以使用市场监管和其他执法措施。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设备由不良进口者输入时，监管机构会收到通知并可作出决定开展检查，由此执法得到保证。见图2。

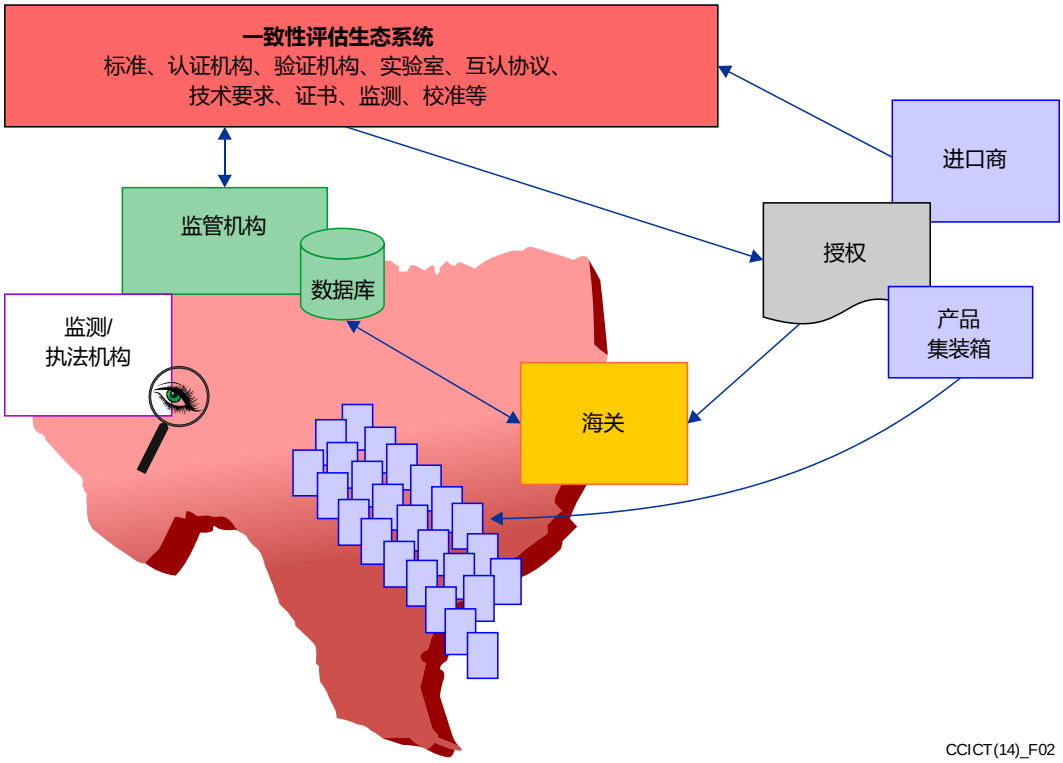


图2 – 一致性评估生态系统

应当注意假冒产品实际上有可能符合特定的要求，可同真品实现互操作，能够通过一致性测试和互操作测试。于是，可能需要通过商标持有人的产品评估准确地确定假冒产品并与真品相区分。

ICT产业的特点是存在大量的国际竞争者，他们推动持续创新。尽管这一局面令人满意，市场同时要面对那些不按照国际、区域或国家规定行事的制造商/销售商。

信息的不对称在发展中国家特别突出，在那里几乎没有或完全没有技术开发和一致性评估程序。管理一致性测试系统典型的常见问题是缺乏可信赖和可追溯的信息，如以下情况所示：i）确认产品的来源或法律责任机构；ii）生产工厂地址；iii）认证机构；以及iv）合格的具有合法认证资质的实验室。在有些情况下，已将其工程和制造能力移至其他国家的外国

[3] 通过使用一致性评估系统，有可能需要认证、一致性声明和/或受益于互认协议（MRA）。

[4] https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P

[5] http://www.anatel.gov.br/grandeseventos/en/frequently-asked-questions-faqs

[6] http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en

公司代表可能是不具备任何技术知识和提供帮助能力的进口商。尽管这种处理可以节省生产过程的成本，制造电信/ICT设备的质量和可信度则被削弱。

也许有人主张认为利益、贪婪、消费者需求、缺少标准和/或执法不力导致了设备质量低下。在有些情况下，同样的品牌或型号，由于缺少适当的、针对特定市场的一致性测试过程，安装了不同的电子部件，其质量或优或劣。产品按照目的地质量管理的严格程度，被有选择地运至不同地方。被称为热带化的程序给人们留下的印象就是为了向赤道以南地区销售而篡改设备。

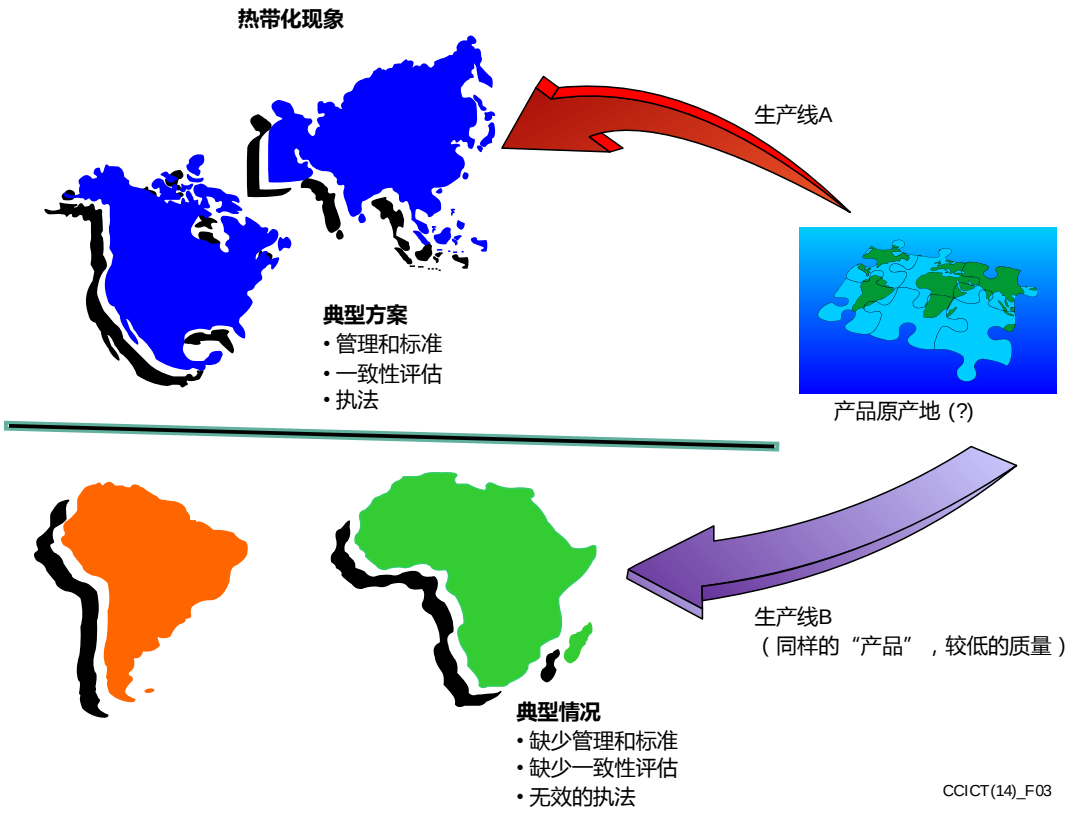


图3 – 被称为热带化的程序

7.2 识别码和型号核准标志的滥用

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。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。对生产厂家、消费者和执法官员来说，难以将假冒的识别标记同真品的识别标记区分开来，更不用提确认产品本身的真伪了。

7.3 国际移动设备标识（IMEI）

如前所述，移动电话对于造假者是特别诱人的目标，为应对这一情况，移动制造商论坛（MMF）建立了一个网站，向消费者介绍如何识别假冒的电话和电池 http://spotafakephone.com。他们建议消费者应当了解真品的外观、能力、是否在售和价格，并检查移动设备国际识别码（IMEI）。对每部移动电话来说，IMEI是其唯一的识别码。假冒产品常常没有IMEI或标印假冒的IMEI。对生产厂家、网络运营商和管理机构来

说，造假者的生产已经日益进化，从现有生产厂家窃取合法的IMEI号码范围，是其造假策略的一部分。这可以作为逃避IMEI检查系统的一种方法。

为了保证IMEI的唯一性，其分配由GSMA负责管理。分配方案是分层次的，GSMA向分配机构分配2位识别码，分配机构则向设备分配IMEI。目前获得分配授权的分配机构是无线协会（CTIA）、英国通信认证管理委员会（BABT）、电信终端测试技术协会（TAF）（中国）和印度移动标准联盟（MSAI）。

2003年1月1日生效的IMEI的格式见图4如下[37]：

型号分配码（TAC）	序列号	校验位
NNXXXX YY	ZZZZZZ	A

TAC	型号分配码，之前称为型号核准码。
NN	分配机构识别码。
XXXXYY	由分配机构定义的移动设备（ME）型号识别码。
ZZZZZZ	由分配机构分配但由生产厂家分配给每个ME。
A	校验位，由其他IMEI位共同确定。

图4 – IMEI的格式

GSMA还记录每部由IMEI确定设备的其他信息，如生产厂家名称、型号编码和技术能力（例如支持的频段和功率等级等）。

GSMA负责维护之前被称为中心设备标识登记表（CEIR）的IMEI数据库（IMEI DB）[38]，IMEI DB包含一份设备的“白名单”，这些设备被认为适合在全球使用；IMEI DB还包含一份设备的“黑名单”，其中的IMEI由于丢失、失窃或因故障而对网络完整性带来威胁而不宜使用。应当注意IMEI DB白名单是一份TAC的名单，并非完整的IMEI号名单，其数据向符合条件方免费开放，如国家监管部门、执法机构和海关机构。除IMEI DB外，独立的网络运营商可以实施其自有的设备识别登记表（EIR），可将“白名单”下载至该登记表，这使得运营商能够控制访问其网络的设备。http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/

IMEI DB的首要用途是使运营商能够识别在其网络上使用的设备及其特性，并封锁被盗手持设备。IMEI DB亦可用于侦测假冒设备、漂白的非法设备、震慑犯罪以及协助执法。

然而，在IMEI的使用中曾出现若干问题。据报道，有的设备没有IMEI、IMEI全为零、使用复制的IMEI或未经授权组织分配的IMEI等。有些带有非法或非唯一IMEI的设备是假冒产品，其他的虽然是真品，但由于生产厂家方面理解有误，并未遵守GSMA的IMEI分配程序。例如：据估计在印度有3000万没有IMEI码的GSM手持终端，GSMA授权MSAI提供一项临时赦免计划，其中包括为识别每台设备而为其植入真的IMEI码（真IMEI植入（GII）计划）。

举一个复制IMEI的例子，澳大利亚被侦测到6500部带有135790246811220这一IMEI码的手持终端。至于未注册IMEI，乌干达一网络运营商声称：其网络内未在IMEI DB上注册的TAC数量大于由GSMA分配并已在IMEI DB上注册的TAC数量。

因此，有足够理由保证IMEI的使用得到授权，并按照GSMA的分配程序分配IMEI码。IMEI DB是探测假冒手机的工具之一，举例来说，由于存在230万使用假冒移动终端的用户，肯尼亚自2012年9月起拒绝非法IMEI手机接入。有关这些案例的更多信息和其他使用IMEI确认假冒手机的案例可参见附件A。由于若干国家的努力均依赖于使用IMEI解决假冒手机问题，保证IMEI分配程序和数据库的安全可靠并使IMEI在手机中安全编码至关重要。

一种方案是要求运营商屏蔽经复制和非法的IMEI，这些设备必须在网络上认证才能工作。当这些设备第一次接入时对其进行屏蔽或许是目前解决这些问题最有效的工具。

然而，屏蔽IMEI尚有若干限制。其中之一是GSMA维护的仅是TAC码的白名单而并非完整IMEI的白名单。第二，从合法设备上得到的IMEI被克隆到假冒伪劣产品使得屏蔽过程变得更为复杂。最后，任何屏蔽方案必须防止或禁止其他克隆IMEI复制到该设备。

尽管屏蔽面临挑战，但市场上仍有可用的解决方案。同时，应避免简单地将各国的方案拼凑在一起，它会将问题转移到邻国，这一点非常重要。考虑到IMEI由GSMA分配且IMEI数据库由GSMA维护，GSMA以某种方式参与国家举措，以利用其全面的可用名录和其他技术措施是符合逻辑的。

然而，考虑到预计假冒设备的数量巨大，仅屏蔽正在使用的终端就会给网络和最终用户带来沉重和难以预估的冲击，这一事实不容忽视。

在这方面很重要的是，需要考虑发展中国家较低的社会经济水平，移动电话是交流和参与信息社会的主要门户[7]。不幸的是，这里充斥着大量更为廉价的假冒设备。

因此，整个社会不得不做好准备面对改变。必须研究、考虑和计划更好的方式。例如，必须向消费者解释清楚不允许使用假冒设备的动机（安全风险、服务质量差以及随之而来的投诉增加、干扰危害和知识产权侵权等）。

有鉴于此，如果监管部门和政府选择实施终端屏蔽行动，重要的是要采用过渡性政策，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，最终用户必须转而使用真品终端，因为移动终端的生命周期是18个月[8]。

7.4 唯一标识符

电子产品代码（EPC）最早由麻省理工学院自动识别中心于1999年研制，现今由EPCglobal公司管理，该公司是国际标准组织（GS1）的附属公司。该组织确定了全球供应链系统最广泛使用的规范。国际标准化组织（ISO）和泛在ID中心（日本）亦确定了多种应用的标识符。

GS1为识别物品、位置、海运集装箱、资产、服务、文件类型、货运、托运定义了九个识别关键字，如下：

---

[7] 国际电联的移动促发展举措：http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx

[8] http://www3.epa.gov/epawaste/education/quest/pdfs/unit1/chap2/u1-2_product-life.pdf：“蜂窝电话在平均仅使用18个月后被更换—尽管仍可使用的时间长得多。”

- GTIN – 全球贸易物品代码
- GLN – 全球位置代码
- SSCC –货运包装箱序列代码
- GRAI – 全球可回收资产标识
- GIAI – 全球单项资产标识
- GSRN – 全球服务关系代码
- GDTI – 全球文件类型标识
- GSIN – 全球货运识别代码
- GINC – 全球托运识别代码

全球贸易物品代码用于识别多个对象类别，而全球位置代码，货运包装箱序列代码，全球单个资产标识和全球服务关系代码识别单个对象；全球可回收资产标识和全球文件类型根据序列号识别对象的分类或者单个物品。全球托运识别代码和全球装运识别代码识别逻辑分组而不是物理对象。这些识别关键字为使用条形码而设计。这些代码和EPCglobal定义的使用射频识别电子产品代码具有相关性。全球贸易物品代码通过附加序列号扩展了电子产品代码结构，以通过唯一代码识别物体。其他的用于识别单个对象的关键字具有一个等效的直接电子产品代码。下面的电子产品代码定义为：

- 一般标识符
  - urn:epc:id:gid:管理者编号.对象类.序列号
- 全球贸易物品序列代码
  - urn:epc:id:sgtin:公司前缀.项目参考.序列号
- 海运集装箱序列代码
  - urn:epc:id:sscc:公司前缀.序列化参考
- 带有或者不带扩展的全球位置代码
  - urn:epc:id:sgln:公司前缀.位置参考.扩展
- 全球可回收资产标识
  - urn:epc:id:grai:公司前缀.资产类型.序列号
- 全球单个资产标识
  - urn:epc:id:giai:公司前缀.单个资产参考
- 全球文件类型标识
  - urn:epc:id:gdti:公司前缀.文件类型.序列号
- 全球服务关系代码
  - urn:epc:id:gsrn:公司前缀.服务代码
- 美国国防部
  - urn:epc:id:usdod:CAGEOrDODAAC.序列号
- 航空航天和国防标识
  - urn:epc:id:adi:CAGEOrDODAAC.原始部分代码.顺序排列

国际标准化组织/国际电工委员会15459[42]为供应链追踪定义了特殊的标识符，这些标识符可表示为自动识别和数据获取的媒介，例如条形码和射频识别。

国际标准化组织/国际电工委员会（ISO/IEC）15459[42]的第1、4、5、6和8部分详细说明了特殊字符串分别用来识别运输工具、个别项目、可回收运输工具、产品分组和运输工具。在各种情况下，唯一标识符均实施了结构化分类，以方便有效的管理此类对象的标识符。

第2部分详细说明了为物品管理应用划分特殊标识符的程序要求，阐述注册机构和出版机构的责任。这些程序不适用于那些国际标准化组织已经指定维护机构或者注册机构提供识别方案的项目。因此不适用于：

- 货运集装箱，因为它们的特殊代码在ISO 6346[43]中有详细说明；
- 车辆，因为它们它们的特殊标识在ISO 3779[44]中有详细说明；
- 车载无线电，因为它们的特殊识别在ISO 10486[45]中有详细说明；和
- 国际标准书号[ISBN][46]和国际标准连续出版物编号[ISSN] [47]方案。

第3部分详细说明了适用于物品管理特殊标识符的一般规则，这些规则要求确保在那些特殊标识符各类别间完全兼容。

ISO的246技术委员会得到特许制定防伪工具标准。该委员会正在制定用性能准则作为授权方案的标准，以便同假冒伪劣商品的生产做斗争[48]。

除ISO和EPCglobal之外，日本的泛在ID中心已经定义了名为“ucode”[49]的通用标识符，该标识符不仅希望识别物理对象而且可能用于识别地点和数字信息，见图5。基本的ucode长度为128比特（但是可以扩展至多个128比特）且可以内置其他标识符，例如国际标准书号，互联网协议地址或者ITU-T E.164电话号码[76]。Ucode是一种基础的需要在关系型数据库中指定含义的数字。任何个人或者组织都能够从泛在ID中心获取ucode，泛在ID中心充当了登记机构发放这些编号。

版本 （4比特）	TLDc （16比特）	cc （4比特）	SLDc （可变）	ic （可变）
TLDc：	顶级域代码（由泛在ID中心指配）			
cc：	类代码(指明次级域代码和单个对象识别代码之间的边界)			
SLDc：	次级域代码			
ic：	单个对象识别代码			

图5 – ucode格式

ITU-T在开展获取与物体标签识别相关的多媒体信息系统的工作。作为这项工作的一部分，正在制定可用于识别的不同ID方案的描述。泛在ID中心提交了它们的ucode方案，以便将这些ucode指配给按照ITU-T X.668建议书[50]注册于分支{joint-iso-itu-t(2) tag-based(27)}的对象标识符（OID）。之前描述的ISO/IEC特殊ID方案被指配给对象标识符下边的分支{iso(1)}。结果是ISO/IEC（包括EPCglobal）和泛在ID中心的标识符方案的对象标识符不仅指配给**{iso}**分支（ISO和EPCglobal）也指配给**{joint-iso-itu-t}**分支（泛在ID中心），因而不同注册机构的不同识别方案共存。对于射频识别标签，对象标识符和ID将按照ISO/IEC 15962[77进行]编码。

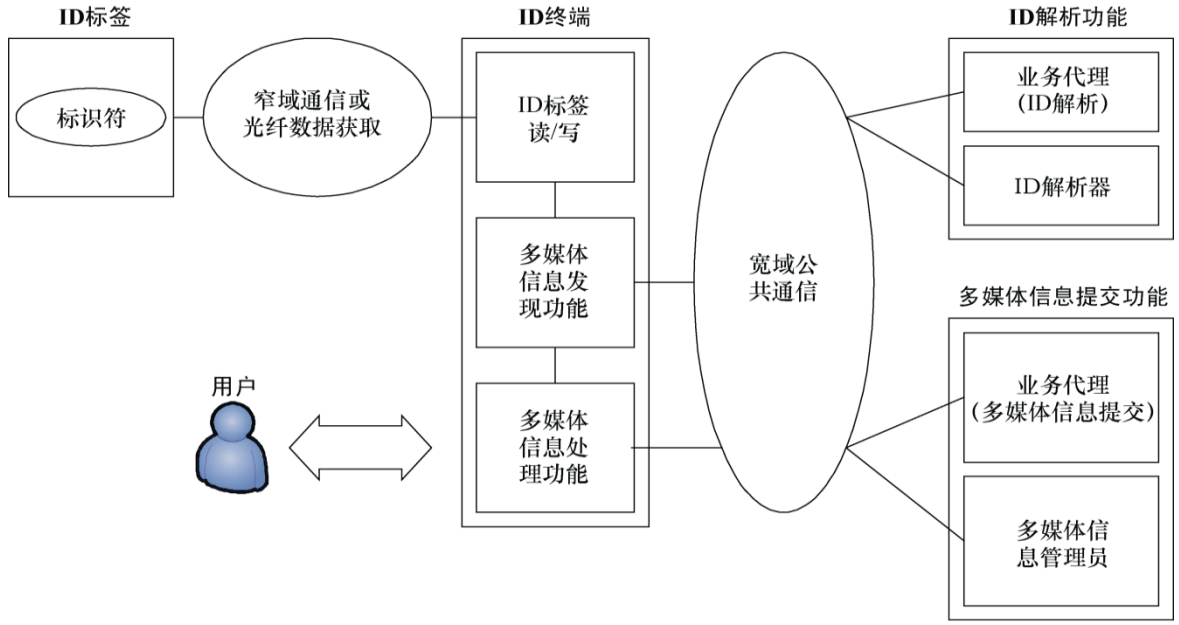
注：“对象标示符”中的词汇“对象”一词这里并不是指一个通常的“物体”，而是指根据ISO/IEC 15961 [78]中的定义：定义明确的一条信息、定义、或规范，它们需要一个名称以识别其在一通信中的使用。一个对象标识符明确识别此类对象。对象标识符分层组织为树形图的根或者顶部的弧，注明负责定义相关信息的组织。顶部的弧代表ITU-T、国际标准化组织和ISO – ITU-T的结合。它们分别得到数值0、1和2。在ISO – ITU-T结合的树形图中，“基于标签”的弧的数值是27。

与一物体相关的数据可连同标识符存储到标签中，如果标签有足够存储记忆的话。然而，另一种寻找一标识符相关信息的可能方法是使用标识符解析机制。

射频识别的众多业务与应用可以想象为能够以不同的形式（文本、音频或图像）提供与标签标识符相关联的信息。例如，在博物馆，贴在一幅油画的标签上的标识符可以用来获得关于该油画和艺术家的更多信息。在杂货店，食品包装袋上的标识符可以用来检查食品是否可以安全食用，而不是已被发现经某种污染的样品。在其它领域如药品/医药、农业、图书馆、零售贸易、旅游业、物流和供应链管理等各个领域，标识符获取的信息可极具价值。ITU-T F.771 [55]建议书描述了可利用已贴标签物品的信息提供的服务以及这些服务的要求。

ITU-T H.621 [52]建议书中介绍了一种用于获取贴了标签的物品的信息的模型（参见图6）。在该模型中，多媒体信息发现功能可以向ID解析功能发送从ID标签读取器处获得的标识符，从而获得一个指示符（如URL等统一资源定位符），指向适当的多媒体信息管理器。这样，就有可能访问到与标签ID相关的信息。由于标识符的数量可能极多，因此，ID解析功能有可能在一种树状结构中分布。

ID解析功能可基于互联网域名系统（DNS）的使用，该系统通常用于提供与统一资源定位符（URL）相对应的IP地址。在EPCglobal中描述的的对象命名服务（ONS）使用DNS机制寻找于电子产品代码相关的信息。



CCICT（14）F06

图6 – 由基于标签的识别触发的、用于多媒体信息接入的功能性架构
（建议书ITU-T H.621）

此外，ITU-T X.1255 [79]建议书https://www.itu.int/rec/T-REC-X.1255-201309-I/en提供了一个发现身份管理信息的框架，该身份管理信息在国际电联全权代表大会打击假冒伪劣电信/信息和通信技术设备的决议中有说明。

7.5 自动身份识别和数据获取

7.5.1 条形码

条形码往往被用于识别产品。它们具有多种形式，从超市里人们非常熟悉的通用商品码（UPC）到二维码（2D）。条形码容易被造假者伪造和复制。

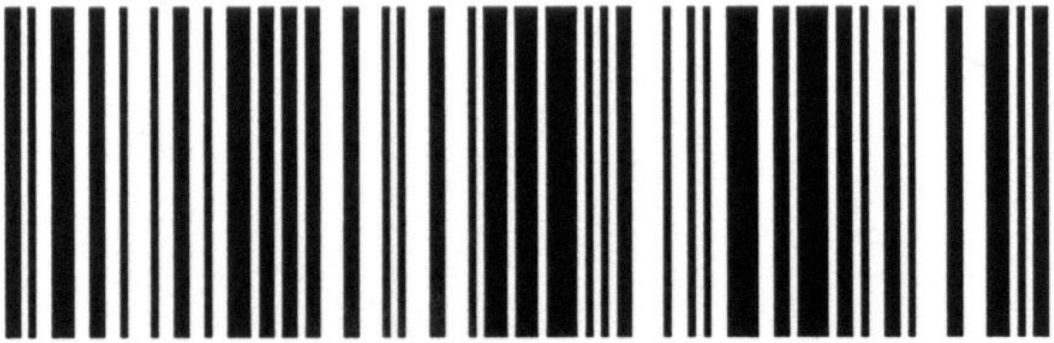


图7 – 线性条形码之例

线性条形码之例见图7：

通用商品码ISO/IEC 15420 [80]

条形码39 ISO/IEC 16388 [81]

条形码128 ISO/IEC 15417 [82]

图8 – 矩阵（二维）条形码之例

矩阵（二维）条形码之例，见图8：

CodablockF ISO/IEC 15417+

PDF 417 ISO/IEC 15438 [83]

Maxicode ISO/IEC 16023 [84]

QR code ISO/IEC 18004 [85]

数据矩阵ISO/IEC 16022 [86]

条形码可以用于序列号编码。例如，DIN 66401 [87]定义了包含一个矩阵符（ISO/IEC 16022或ISO/IEC 18004）的独一无二的识别标记（UIM）和独一无二的数据标识符（按照ANSI MH10.8.2 [88]和“+”按照ANSI/HIBC 2.3 [89]的符号）。这是在电子和卫生保健领域对小件物品做标记的应用标准。它们特别适用于使用喷墨或者激光的直接标记和打印标签。

给物品贴标签和用线性和二维条码直接对产品做标记的要求在ISO 28219 [53]中有详细说明。为产品包装设计线性和二维条码标签的要求在ISO 22742 [54]中有详细说明，而那些用于船运、运输和接收的标签在ISO 15394 [55]中有说明。

7.5.2 射频识别

射频识别能够使用短距离无线技术读取贴标签的物品和存储在标签上的信息。射频识别的参数包括对象身份识别、空中接口参数以及数据通信协议。

ISO/IEC 15963 [56]详细说明无线电频率（RF）标签如何指配特殊的标识符。RF标签拥有一个集成电路制造商划分的标识符 – 标签ID。标签ID（TID）在标签被贴到某些物品或者特殊物品标识符被存储到标签单独的内存部分时可以用作特殊物品标识符（UII）。UII在这种情况下可以是一个由EPCglobal详细说明的电子产品代码。

图9展示了ISO/IEC 15963标签ID格式。

划分等级（AC）	TID发布注册号码	序列号
8比特	大小由划分等级至确定	大小由划分等级和TID发布值确定

图9 – ISO/IEC 15963标签ID格式

划分等级注明了指配号码的机构 – TID发布方。集成电路卡制造商可以按照ISO/IEC 7816-6 [90]的方案或者美国国家标准学会INCITS（信息技术标准国际委员会）的方案注册指配唯一的标识符，货运集装箱和运输应用的的标签制造商也可以采用ISO 14816 [91]的程序。EPCglobal标识则作为GSI等级采用ISO/IEC 15963方案。

五个等级的TID发布方如图10所示：

AC值	等级	TID发布方标识符大小	序列号大小	注册机构（TID发布方注册码）
000xxxxx	INCITS 256	见ANSI INCITS 256 [92] & 371.1 [93]	见ANSI INCITS 256和371.1	autoid.org
11100000	ISO/IEC 7816-6	8 bits	48 bits	APACS（英国付费主管部门）
11100001	ISO 14816	见NEN	见NEN	NEN（荷兰标准化所）
11100010	GS1	见ISO/IEC 18000-6 Type C [94] & ISO/IEC 18000-3 Mode 3 [95]	见ISO/IEC 18000-6 Type C & 18000-3 Mode 3	GS1
11100011	ISO/IEC 7816-6	8比特	48比特	APACS（包括内存大小和扩展TID字头）
所有其他数值	保留			保留

图10 – 唯一TID发布方的等级

早期的RFID用于识别动物。ISO在1994年完成了定义动物RFID识别码结构的标准（ISO 11784 [96]）。强制性标准ISO 11785 [97]描述了如何读取此类标签信息。

ISO已经在定义一整套物品管理的规范：ISO/IEC标准15961到15963描述了通用数据协议和标识符格式，它们适用于描述大量不同频率空中接口的ISO/IEC 18000系列标准[98]。不同频段需要单独的规范，因为工作的频率决定了通信兼容性的参数，例如：工作范围或者是否发射收到周边水体的影响。

ISO/IEC 29167-1 [57]定义了安全体系结构和ISO/IEC 18000空中结构标准的文件管理。依赖于应用的安全机制被定义，标签可以支持该机制的全部或者子集。一个RFID标签询问器可获取得到标签支持的安全机制信息及进一步的信息，例如加密算法和密钥长度应用方面的信息。

ISO/IEC TR 24729-4 [58]提供了有关评估标签上数据安全和标签到读取器通信安全的潜在威胁的系统设计者实施导则，同时还有关于确保标签数据安全的恰当对策的描述。

RFID的供应链应用（有适用于运输集装箱，可回收运输项目，运输工具，产品包装和产品标签的各个部分）在ISO 17363到17367 [99]到[103]中有详细说明。ISO 18185 [104]描述了如何利用RFID追踪运输集装箱的情况。ISO还制定了性能和一致性测试规范。

ISO/IEC 29160 [105]中详细描述的RFID标记可以用作产品上的标签以表明它有RFID标签，见图11。

图11 – ISO/IEC 29160中详细说明的RFID标记之例

EPCglobal是GS1的下属开发机构，为使用RFID的电子产品代码制定规范。EPCglobal已经制定了一系列标准，包括标签数据编码、空中接口协议，读取器协议，以及信息和对象名称服务的规范。EPCglobal系列标准的概览如图12所示。

EPCglobal系列标准的主要组成部分如下：

- 电子产品代码标签数据标准（TDS）定义了若干识别方案并描述了如何将数据编码到标签以及如何将其编码成为适合电子产品代码系统网络使用的形式。
- 电子产品代码标签数据翻译标准提供了机器可读版的电子产品代码数据格式。该标准可用于确认电子产品代码标识符和在多个数据表示之间的翻译。
- 标签协议是RFID空中接口。在“Gen 2”接口，读取器通过调制860-960 MHz频段范围的无线电频率信号发送信息到标签。从接收读取器发射信号的能量的角度看，标签是无源的。这种空中接口协议包含在ISO/IEC18000系列规范中作为第六部分中的C类型。短波空中接口在13.65 MHz工作。这种规范向下兼容ISO/IEC 15693 [106]。
- 客户使用低层的读取器协议（LIRP）在操作空中协议层面控制读取器，该协议在应用软件和读取器（读取器协议（RP））之间提供接口。
- 读取器发现客户使用在发现、配置以及初始化（DCI）标准中详细说明的程序。
- 读取器管理（RM）标准用于监测RFID读取器的运行状态。它基于互联网工程任务组（IETF）定义的简单网络管理协议（SNMP）的使用。
- 应用层事件（ALE）标准为用户获取过滤后的电子产品代码数据提供了方法。这种接口在基础设施组件之间提供了独立性，这些组件获取原始电子产品代码信息，并且处理这些数据和使用这些数据的应用。
- 电子产品代码信息服务（EPCIS）标准允许在企业内部或者之间分享电子产品代码数据。
- 核心业务词汇（CBV）旨在确保交换EPCIS数据的所有各方均能对一数据的含义有同样的理解。
- 对象命名服务标准描述了域名系统（DNS）如何用于获取于特定电子产品代码有关的信息。

- EPCglobal证书简介标准描述了电子产品代码全球网络内的实体如何得到授权。采用了ITU-T X.509 [60]认证框架和IETF RFC 3280 [61]与IETF RFC 3279 [62]中定义的互联网公钥基础设施描述。
- 电子履历（Pedigree）标准详细说明了处理电子药品“履历”文件的方法，用于制药业供货链应用。

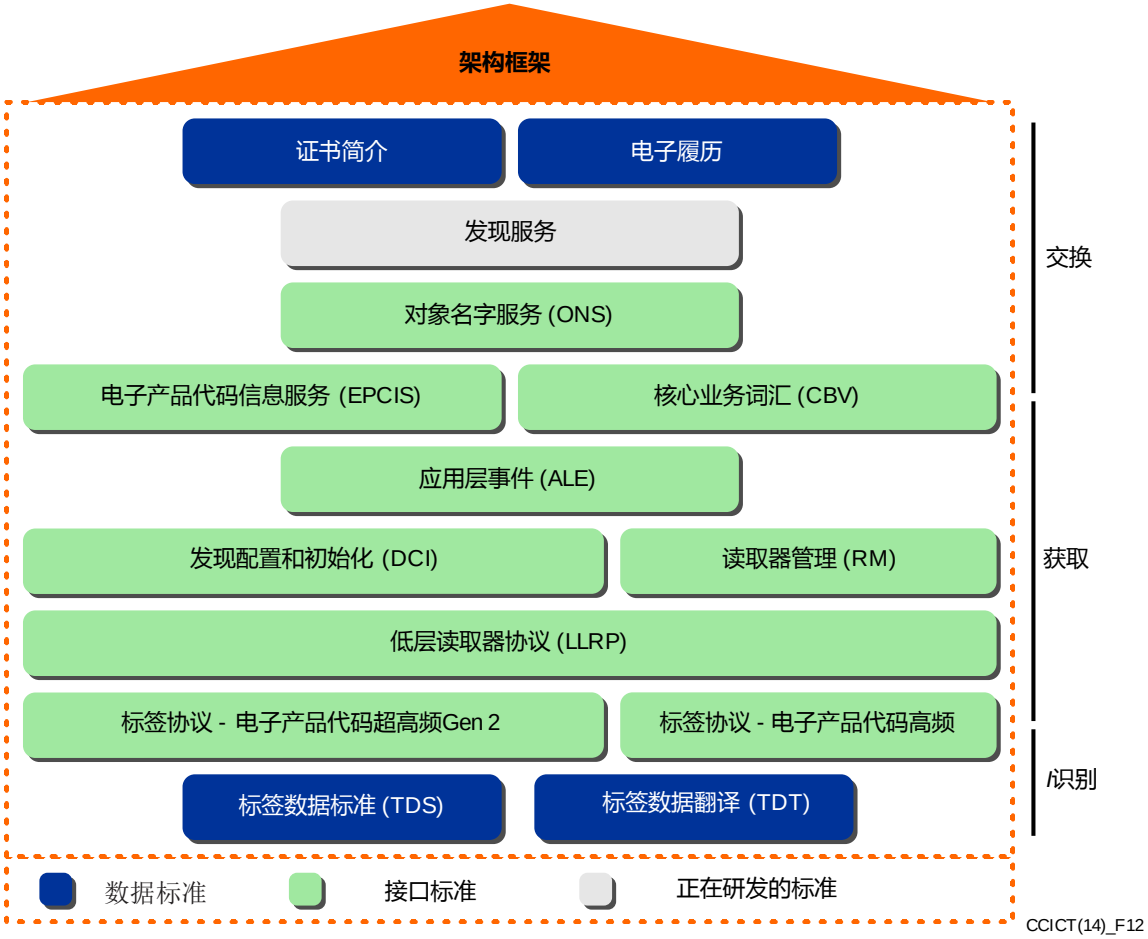


图12 – EPCglobal标准概览[59]

7.6 安全打印和全息标签

安全打印技术用于生成防篡改标签，标签也可以补充不容易伪造的全息图像。然而应当指出，这种机制被广泛滥用并被造假者复制。

7.7 供应链管理

维持供应链的安全性对于打击假冒伪劣行为而言非常重要。ISO28000系列国际标准详细说明了供应链安全管理的要求。这些标准适用于在生产或者供应过程的任何阶段涉及制造业、服务业、存储、或者空中、铁路、陆路和海洋运输的任何规模的组织。现已有下列标准：

- ISO 28000:2007，**供应链的安全管理系统规范**[107]

- ISO 28001:2007，供应链安全管理系统供应链安全管理系统 – 执行供应链安全、评估和计划的最佳规程--要求和指南[108]
- ISO 28003:2007，供应链安全管理系统 – 对实体提供供应链安全管理系统的审核和认证。[109]
- ISO 28004-1:2007，供应链安全管理系统 – 实施ISO 28000指南 – 第一部分 – 一般准则。[110]
- ISO 28005-2:2011，供应链安全管理系统 – 电子口岸通关（EPC） – 第二部分：核心数据组成。[111]

ISO 28000要求各组织进入安全环境，在其中工作并判断是否实施了恰当的安全措施。一个安全管理系统的组成如图13所示。

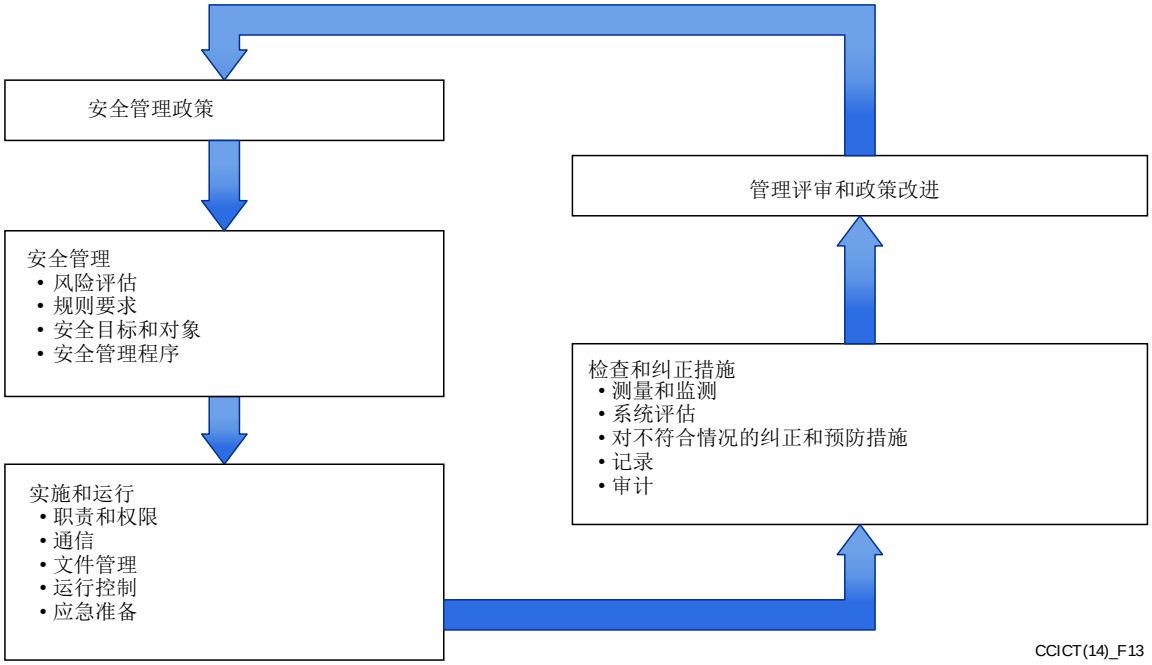


图13 – ISO 28000 安全管理系统组成

世界海关组织（WCO）安全框架标准旨在确保全球供应链的安全，同时包括一本列出水运具有假冒伪劣货物高风险因素的手册。安全框架基于海关到海关的协议以及海关到企业的合作伙伴关系，企业会因履行供应链安全标准而受益。

IEC的107技术委员会，其活动领域是对航空工业过程管理，制定了与避免使用假冒伪劣的、欺诈的和再生的电子元器件[64]相关的规范。该委员会目前正在制定有关管理来自非特许渠道的电子元器件的规范，并阻止假冒伪劣元器件进入供应链[65]。

国际自动机工程师学会（SAE International）(原为汽车工程师学会)已经制定了一些专门避免假冒伪劣电子元器件进入航空和汽车工业的供应链的规范，这些规范在电子产工业中被广泛引用。SAE已经制定了两份文件，旨在将其用于采购决定：

SAE AS5553 [112]：“假冒伪劣电子产品部件：避免，检测，减少”；和

SAE ARP6178 [113]：“假冒伪劣电子产品部件：经销商的风险评估工具”；以及供经销商使用的规范：SAE AS6081 [114]：“假冒伪劣电子产品部件：避免协议，经销商”。SAE还制定了一项有关测试的规范：SAE AS6171 [115]：“测试方法标准：假冒伪劣电子产品部件。”

IEC的107技术委员会与SAE在SAE AS5553方面通过联络安排开展紧密合作。

大多数涉及之前所提及的假冒商品问题的论坛均对供应链管理提出建议和指导。总体来说，对产品可追溯性、检查和试验（由第一、二、三方来完成）均有一定的要求。英国知识产权犯罪问题报告小组在2011年研发了供应链工具箱。

7.8 测试

国际电工委员会（IEC）按以下一致性评估方案操作 http://www.iec.ch/about/activities/conformity.htm：

- IECEE – IEC系统电工设备和元件的一致性评估方案；
- IECEx – IEC系统有关设备在爆燃性环境使用的标准认证；
- IECQ – IEC系统电子元件质量评估系统。

这些IEC CA方案基于第三方认证并采用在线系统提供鉴别假冒产品的认证信息。

国际电工委员会电工产品合格测试与认证组织（IECEE）运作一个认证机构（CB）体系，该体系基于其成员对测试结果相互认可的原则，获取国家层面的认证或批准。CB公告为该体系的用户提供数据库 http://members.iecee.org/iecee/ieceemembers.nsf/cb_bulletin?OpenForm，其中提供以下方面的信息：

- 该体系接受采用的标准；
- 参与的国家认证机构，其中包括产品类别及其得到认可的标准；以及
- 每个成员国在每项标准方面的差异。

IECEE CBTC Online是国家认证机构的在线测试证书登记系统，并且允许公众访问。

IECEE设立了一个研究打击假冒措施的任务组（CMC-WG 23）。

国际电工委员会防爆电气产品认证体系（IECEx）国际认证系统由以下部分组成：

IECEx认证设备体系；

IECEx认证服务设施体系；

IECEx一致性标志许可证制度；

IECEx人员能力资格认证。

The IECEx在线合格证书（CoC）提供依据上述体系颁发相关证书和许可证信息。

国际电工委员会电子元器件质量评定体系（IECQ）对航空电子设备系统执行IECQ电子元器件管理计划（ECMP）和IECQ有害物质过程管理体系（HSPM），可以在线获得证书。

7.9 数据库

已知的假冒商品数据库供执法部门使用，例如世界海关组织（WCO）和国际刑警组织的数据库，也包括消费者的数据库。国际商业假冒调查局（ICC CIB）也有个案例研究数据库。

7.10 市场监督

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”[66]。

假冒商品可以在市场监督活动中甄别出来，市场监督部门应该积极参与打击假冒商品贸易。联合国欧洲经济委员会（UNECE）建议各国的市场监督和海关监管活动相互协调，而且给予版权所有者机会报告市场监督部门假冒商品问题[67]。

一些国家要求产品在登记后再销售。例如，尼日利亚标准组织最近推出了电子产品登记制度，以限制假冒产品的出售。

8 标准组织

涉及打击假冒商品相关议题的主要国际标准化组织有国际标准化组织（ISO）和国际电工委员会（IEC）。

2009年，ISO创建了一个技术委员会，制定防伪工具（ISO TC 246）的规范。该委员会为打击假冒物品的认证方案制定了性能标准规范（ISO 12931）[48]。此规范的目的在于树立消费者信心，使供应链更安全，同时协助政府当局制定防范性、有威慑力的惩罚性政策。ISO TC 246不再有效，但此领域的工作将在规范ISO TC 247下开展。

检测和防控身份、财务、产品及其他形式的社会经济诈骗等领域的标准化属于规范ISO TC 247的范围：“应对诈骗的对策及控制”。该委员会还制定了防伪可用的互操作对象标识的ISO指南标准 – ISO 16678 [116]：“用于防止假冒和非法贸易的互操作对象标识和相关认证系统指南”。这个新项目涉及在数据库中用大量序列号来辨别产品以确定其真实性。此项国际标准旨在确保利用可靠和安全的物品识别，防止非法物品流入市场。序列编号的产品从制造链到销售链，包括消费者，均可验证出其真实性。

ISO认识到伪造和盗版对分门别类的各种消费品影响极大，其中包括电子设备和鞋类产品，药品，汽车和汽车部件，食品和饮料，化妆品，电影和音乐制品，电子产品，安全装置和飞机部件。消费者具体关注的领域包括安全与健康风险，性能问题，相关可用性和适用性，无障碍获取性，数据保护，失业，经济危害以及与有组织犯罪的关系等。
http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf

ISO/IEC联合技术委员会ISO/IEC JTC 1/ SC 31正在开展自动识别和数据捕获技术的研究。该委员会由7个工作组组成，每个组的议题如下：

- WG1数据载体；
- WG2数据结构；
- WG4物品管理的射频识别；
- WG5实时定位系统；
- WG6移动物品的识别和管理（MIIM）；
- WG7物品管理安全。

欧洲标准化委员会（CEN）也在研究规范TC 225的自动识别与数据采集技术（AIDC）。

许多国家级标准化组织已成立了类似于ISO/IEC的委员会。例如，德国标准化协会（DIN）创建德标DIN NA 043-01-31研究自动识别和数据捕获技术[68]以及DIN NA 043-01-31-04 UA研究射频识别项目管理。

关于航空电子设备过程管理规范的IEC TC 107正在研究如何防伪。

此外，国际汽车工程师学会（SAE）正在制定规范，防止在高科技行业使用假冒电子元器件，GS1已组织制定了一套关于物品识别和供应链管理的规范。

9 打击假冒的指南

若干组织从制造商和经销商、政府和他们的执法机构以及消费者等不同视角推出打击假冒的指南。

防伪论坛向原始设备制造商（OEMs）、经销商和零部件制造商推荐最佳做法[69]。这些指南包括：

- 直接从制造商或授权经销商采购，如不能实现，则从当地的灰色市场采购；
- 如果从灰色市场采购，则坚持要求其提供真实性的书面证据；
- 加强协调产品和组件的使用周期管理；
- 确保报废和劣质产品予以丢弃处理；以及
- 使用唯一标识，加强文档管理以提高产品的可追溯性。

组件技术研究院有限公司（CTI）为进行电子元器件独立经销商认证而研制出防范假冒组件方案（CCAP-101）[70]。已明确对经销商提出要求，要求他们检测电子元器件，避免假冒产品流向消费者。可进行电子检测。采用这种认证方案是为了达到规范SAE AS5553的目标。

同样，独立电子经销商协会（IDEA）制定了有关减少假冒产品并检验的规范（IDEA-STD-1010A）[117]和质量管理规范（IDEA-QMS-9090）[118]。

ICC知识产权路线图包含有关各方面知识产权保护的商业和政府行为建议，包括打击假冒和盗版行为。特别是，ICC呼吁政府在执行知识产权（IPR）规定方面应当做的更多，因为“政府在打击盗版行为和假冒产品方面的资源与该问题的规模相比严重不足”。

OECD观察到，假冒和盗版产品的交易市场可以被划分为两类：“初级市场”，消费者认为那里的产品是正品；和二级市场，购买者在那里为了廉价而有意购买假冒和盗版产品。对购买冒牌衬衫或手提包没有顾忌的人，也许并不愿意购买假药或者冒牌电子产品。打击这两类市场的假冒产品需要采取不同的策略，因此有必要了解在某类市场某个特定产品的交易量。

可能在初级市场打击假冒产品会更有效，例如，可以展开宣传攻势指出购买假货的危险，而对于二级市场的产品，也许有必要施加更为严厉的惩罚。

英国知识产权犯罪问题报告小组的供应链工具箱[71]旨在提高对假货进入合法商业供应链问题的认识，并对如何保护知识产权资产提供指导。说明 – 公司如何降低假货进入其供应链的风险流程图如下图14所示。

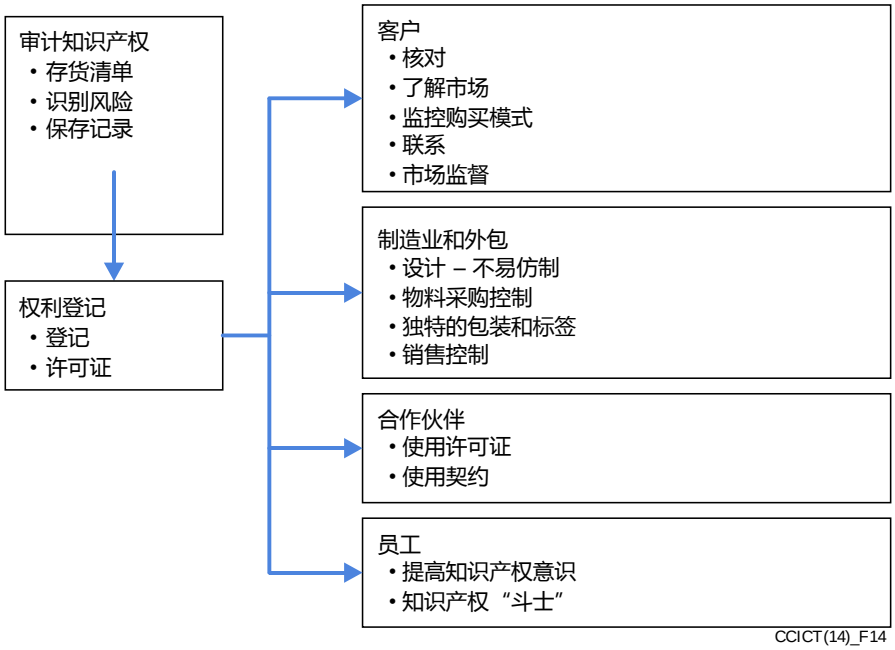


图14 – 保护知识产权
（改编自英国知识产权犯罪集团工具箱[75]）

MMF为政府研制了资源指南，提出一系列措施，其中包括：

- 在法律和监管框架方面做出改变，限制在电信网络中激活假冒设备；
- 限制进口不符合工业标准或未经批准的/不符合国家立法和监管框架的移动设备及其附件；
- 建立必要的全球行业和主管机构联盟并为当局、消费者和销售渠道验证原装产品提供方案；
- 研发统一的创新型技术方案，限制假冒移动设备在电信网络中使用的可能性，以及
- 支持可加强安全功能（例如唯一独立的识别码）的标准，以防止制造假冒产品和其他违法产品。

此方法超越了对传统强制手段的依赖，而是阻止这些设备在网络上的运行。尽管如此，强制执行、公共宣传和市场监督依然很重要，只要有可能，移动电话制造商仍将继续与国家当局保持合作。

10 结论

假冒这个日益严重的问题正在影响着更多种类的产品。在ICT领域，手机尤其容易成为仿制的目标，每年大约有2.5亿的假货出售量，大约占全球市场的15%-20%，除了对正版产品制造厂家有明显的经济影响（品牌贬值，收入减少，版权和商标侵权，不正当竞争）以外，对授权经销商和政府部门也有影响（如避税，需支付额外费用以确保国家法律得到遵守，应对公共安全危险，失去劳动机会），此外，对消费者的健康、安全和隐私以及公众安全也带来危险，对网络运营商也有负面影响（因服务质量低（QoS）、潜在干扰、电磁兼容问题（EMC）和网络中断导致）。大多数冒牌手机都产自一个亚洲国家，美国参议院军事委员会在有关防御系统供应链中假冒电子部件的听证会上，已经证实这个国家大量假冒的电

子元器件源自发达国家非正式部门回收的电子垃圾[9]。很显然，在假冒设备远销世界各地之前还需要做更多的工作来识别并查处其源头。

打击假冒的法律文书已基本完成，但执法力量仍然薄弱。2008年OECD报告认为，“假冒和盗版行为的规模和影响过于严重，它们迫使政府、企业和消费者采取强有力且持久的行动。在这一方面，更有效的执法显得至关重要，即获得公众支持打击假冒和盗版。加强政府和企业之间的合作无疑是有益的，而且还能更好地收集数据”。

政府越来越积极地参与这个问题，大量开展宣传活动，提供咨询，更严厉地追究罪犯的法律责任，就像最近中国政府的做法。政府不仅要加强知识产权规范，并且还要执行巴塞尔公约，以确保在无害于环境的方式下处理用过的和报废的设备，而不是促进非正规的假冒经济。应在全球范围内采用环保的道德规范。

政府可能也希望将市场监管活动与海关当局联系起来，以提高检测假冒产品的能力。查获的假冒ICT设备应被视为电子废弃物，并按照无害于环境的废弃物管理方案处理。

受假冒产品影响的公司和行业已经开始组织宣传和游说活动，以维护其利益。然而，可能需要在更大范围开展关于假冒的宣传。在美国，2012年国防授权法案（NDAA）全权委托承包商检测假冒部件，并对所有在产品中使用假冒部件的情况予以处理。

消费者也需要了解购买假冒设备的危险，即假冒产品可能无法安全使用，且性能不如正版商品。显然，许多国家和国际组织，以及制造商、零售商和媒体，定期向消费者强调假冒商品带来的问题。但是，消费者往往不管任何潜在的后果，仍然选择购买假冒商品，他们似乎只看重价格。

假冒也可能受到设备使用周期管理的影响，这不仅涉及供应链，还涉及包括返回、再利用和回收环节在内的整个周期。使用周期管理需要手段识别和验证物品并安全地追踪它们。然而追踪应适当且恰当，应采用自动识别和数据采集技术（AIDC），如RFID，因为这可能涉及重要的隐私问题，物品可能会与其所有者产生联系。在标准过程中应注意尊重消费者的隐私权，不让ICT产品的使用者遭受因标识注册机制带来的困扰。消费者也应得到保护，免受网络任意断开连接带来问题的影响。

综上所述，AIDC技术和供应链管理标准可以用来打击假冒行为。

打击假冒还需要跨行业合作。海关当局之类的执法者可以采用一些常用工具（例如用于检测假护照和假支票的工具），以及大批行业和产品的具体机制，并有针对性地与公有和私营部门开展合作。

在今天的手机行业，也有一些基于IMEI登记制度的系统用来识别正版和合法进口的移动终端，这类系统由独立的行政机构和管理部门计划建造或管理运行。也有一些区域性方案交换非法来源的移动终端设备的信息。这种机制可能也会影响到合法用户。例如，一个国外用户来到一个国家，然后将一张当地SIM卡放在自己的设备中，结果误入白名单的陷阱，导致他们无法使用手机。这种机制可能给商品的自由流通带来阻力。在其他信息和通信技术领域，由于产品的自然属性和行业结构，这样的机制并不存在。

尽管有些国家依靠IMEI登记制度已经成功部署解决方案来抵制假冒手机的传播，然而，其他国家，尤其是发展中国家，在寻找有效的解决方案来打击假冒设备方面，仍然面临着严峻的挑战。目前，一些国家采用的可行解决方案是基于阻止无效IMEI号码的手机联网，阻止使用未被管理部门批准的设备类型，阻止非法进口这些设备；或者采取其他举措，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。

主要的国际标准化组织针对打击假冒提出了一些议题。目前还没有国际电联建议书，进行现有打击假冒产品系统的差异比较，描述相应的框架，同时考虑性能以及在全球范围内的互操作性，等等。国际电联和其他利益相关者在促进各方关于找出处理假冒设备方法的国际和区域性协调方面起到重要的作用。此外，国际电联需要协助成员采取必要的措施，以防止或检测篡改唯一设备标识符或其复本的行为。

本技术报告仅提出了有关打击假冒的议题，诸如什么是假冒，它的影响，知识产权公约及其实施，行业打假论坛，打假措施及参与打假的组织机构。为了协助监管部门保护消费者、经营者和政府免受假冒设备的消极影响，国际电联应对此议题展开深入研究。

11 国际电联协定

国际电联2010年全权代表大会（PP-10）第177号决议“请各成员国和部门成员注意其他国家有关对基础通信设施质量产生负面影响的设备方面的法律规章制度，尤其要认识到发展中国家对假冒设备的意见”[72]。

WTDC-14第79号决议：“电信/信息和通信技术在打击处理假冒电信/信息和通信设备的作用”和国际电联2014年全权代表大会（PP-14）第COM5/4号决议“打击假冒电信/信息和通信技术”授权国际电联解决这类假冒ICT设备带来的问题。

第11研究组的第8个课题研究该项问题，2014年11月，国际电联在日内瓦举办了关于“打击假冒伪劣的ICT设备”的研讨会。http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx

ITU-T第16和17研究组提交了有关物品识别和认证的建议书。

ITU-T第5研究组负责研究设计减少循环使用ICT对环境产生影响的方法。

电信标准化局（TSB）主任已成立一个知识产权特设小组（AHG）：http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx，该小组研究专利政策、软件著作权、商标指南以及其他相关议题。该小组自1998年就已开始活动了。国际电联和WIPO多次联合组织召开研讨会，例如2001年召开的关于多语种域名的研讨会以及2009年召开的关于“解决信息通信技术和知识产权的争议”议题的研讨会：http://www.wipo.int/amc/en/events/workshops/2009/itu/index.html。2012年，国际电联还举办了关于专利的圆桌讨论会，为各行业标准机构和监管部门提供一个中立的场地来探讨现行的专利政策和现有的行业实践是否能够充分满足各利益相关方的需求http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx。迄今为止，该小组还没有解决打假方面的问题。

国际电联在解决假冒ICT设备问题方面起到一定作用。

在国际电联世界电信发展大会的第64号决议（海得拉巴，2010年）的框架中拟定了国际电联电信发展部门（ITU-D）第1研究组关于融合环境中的监管与消费者保护的报告（2013年3月），援引与网上商品和服务（更多的是跨国）相关的保护，使革新者、创造者和消费者免受假冒和盗版的影响，将此作为监管部门应面对的挑战。

国际电联电信发展部门2012年5月公布，根据发展中国家在不同区域建立合格性评估实验室的指导方案，各成员国表示，假冒设备加剧了一致性和互操作性方面的问题 http://www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf。据称，“对在市场上倾销其他国家没有通过检测的不符合标准的产品持有怀疑是另一个值得关注的问题，正如假冒产品的进口和流通。解决这个问题的一

个关键要素是拥有一个强有力的型号审批制度，一个测试技术标准的实验室，测试制度和测试能力，去批准和监督市场上应用的通信技术，同时还需要监管、审计和执法部门的支持。如果没有给一个国家或地区提供建全的技术需求，型号审批制度以及可以使用的测试实验室，那么市场将在很大程度上不能得到保护。”当不同机构的多种标准在一个产品中实现时，测试和互操作性都会受到严重制约。应该承认，独立测试制度虽然看似诱人，但在解决假冒产品这一问题上，它是不可能带来任何真正改变的。

应当指出的是，制假者变得日益复杂，假冒产品能够做到符合规定的技术要求以及与正品的互操作。因此，假冒产品可以符合一系列相关的技术标准，并通过了一致性和互操作性检验。在这种情况下，只有商标持有人通过执行产品评估才能准确地从正版产品中识别出假冒产品。

关于缩小阿拉伯和非洲地区标准化工作差距（BSG）的国际电联区域研讨会提出了假冒ICT设备的问题（阿尔及利亚，2011年9月26日-9月28日），会议指出应当鼓励这些区域通过建立已列入黑名单的假冒产品数据库，在区域层面上实现信息共享。http://www.itu.int/ITU-T/newslog/ITU+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx

在ITU-T电信标准化顾问组（TSAG）说明会在一致性评估和互操作性方面（日内瓦，2012年1月13日）以及ITU论坛在阿拉伯和非洲地区的一致性和互操作性方面（突尼斯，2012年11月5日-11月7日），均强调阿拉伯地区的结论，即假冒设备是一个令人厌烦的问题，特别是在手机市场，以及是否需要在这方面开展全球性合作。http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf], [http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00000E0005PPTE.pptx

ITU电信发展部门组织的监管协会会议考虑了关于手机防盗、灰色市场和假冒设备及其对行业、运营商、各国政府和用户的影响这一问题（斯里兰卡，科伦坡，2012年10月1日），按照第48号决议（启海得拉巴，2010年）“加强电信监管部门之间的合作”，呼吁国际电联组织、协调和促进各项活动以推动监管机构和监管协会在主要监管问题上实现国际及区域层面上的信息共享。10个区域监管协会的代表，包括ARCTEL-CPLP，AREGNET，ARTAC，EMERG，FRATEL，REGULATEL，OCCUR，FTRA，SATRC和APT，概述了区域活动是非常有益的，例如：

- 共享通过双边或多边协定签署的GSM和CDMA黑名单数据库；
- 业界遵守防止对IMEI复本或制造商的电子序列标识号进行重新编程的安全建议；
- 建立监管财政和/或关税机制以确保更好地控制手机进口，防止被盗的移动终端设备和/或其部件出口或再出口；
- 组织宣传来提高公共对于报告他们的移动终端设备被盗和遗失的重要性的认识。

许多地区的协会介绍了他们处理此问题的经验，并且意识到协调行业和运营商的合作是一个关键问题。监管机构协会会议采纳了一项建议，ITU与GSM协会开展关于研究手机防盗、灰色市场和假冒设备的合作并提供指导和建议http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf。

12 参考文献

[1] *The Economic Impact of Counterfeiting and Piracy*, OECD, June 2008.

[2] http://www.oecd.org/sti/ind/44088872.pdf

[3] http://www.icc-ccs.org/icc/cib

[4] *Estimating the global economic and social impacts of counterfeiting and piracy*. http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[5] Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf

[6] http://www.havocscope.com/counterfeit-hp-printing-supplies

[7] http://www.spotafakephone.com/

[8] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412

[9] http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

[10] *Defence Industrial Base Assessment: Counterfeit Electronics*, January 2010 http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-count

[11] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818

[12] In *WIPO Intellectual Property Handbook* http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

[13] UK IP Toolkit 2009.

[14] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[15] http://www.wipo.int/treaties/en/ip/washington

[16] www.wcoipm.org and http://ipmpromo.wcoomdpublications.org/

[17] void

[18] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html

[19] https://www.gov.uk/government/publications/annual-ip-crime-report-2013-to-2014

[20] http://www.aca.go.ke

[21] http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/

[22] http://www.iccwbo.org/bascap/id7608/index.html

[23] http://www.pasdirectory.com

[24] http://www.iccwbo.org/bascap/id42204/index.html

[25] http://www.iccwbo.org/policy/ip/id2950/index.html

[26] http://www.iacc.org/

[27] http://www.ascdi.com/

[28] http://www.anticounterfeitingforum.org.uk

[29] http://archive.basel.int/convention/basics.html

[30] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf

[31] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm

[32] http://www.bbc.co.uk/news/world-europe-10846395

[33] *Recycling – From E-Waste to Resources*, UNEP, 2009.

[34] Directive 2002/96/EC.

[35] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE and WEEE). Process Management Specification (March 2011)
http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346

[36] http://www.numberingplans.com/?page=analysis&sub=imeinr

[37] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 October 2013.

[38] http://www.gsma.com/imei-database

[39] http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/VAT-Report_TKO.pdf

[40] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012.
http://www.nkrzi.gov.ua/images/upload/142/3963/4b2c475b68c147860c36a6e1fc2a3e47.pdf

[41] GS1 EPC Tag Data Standard 1.6, 9 September 2011.

http://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf

[42] ISO/IEC 15459, *Unique identifiers*.

Part 1:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units*.

Part 2:2006, *Information technology – Unique identifiers – Registration procedures*.

Part 3:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules*.

Part 4:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual products and product packages*.

Part 5:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Individual returnable transport items (RTIs)*.

Part 6:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 6: Groupings*.

Part 8:2009, *Information technology – Part 8: Grouping of transport units*.

[43] ISO 6346:1995, *Freight containers – Coding, identification and marking*.

[44] ISO 3779:2009, *Road vehicles – Vehicle identification number (VIN) – Content and structure*.

[45] ISO 10486:1992, *Passenger cars – Car radio identification number (CRIN)*.

[46] ISO 2108:2005, *Information and documentation – International standard book number (ISBN)*.

[47] ISO 3297:2007, *Information and documentation – International standard serial number (ISSN)*.

[48] ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.

[49] http://www.uidcenter.org/learning-about-ucode

[50] Recommendation ITU-T X.668 (2008) | ISO/IEC 9834-9:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*.

[51] Recommendation ITU-T F.771 (2008), *Service description and requirements for multimedia information access triggered by tag-based identification*.

[52] Recommendation ITU-T H.621 (2008), *Architecture of a system for multimedia information access triggered by tag-based identification*.

[53] ISO 28219:2009, *Packaging – Labelling and direct product marking with linear bar code and two-dimensional symbols*.

[54] ISO 22742:2010, *Packaging – Linear bar code and two-dimensional symbols for product packaging*.

[55] ISO 15394:2009, *Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels*.

[56] ISO/IEC 15963:2009, *Information technology – Radio frequency identification for item management – Unique identification for RF tags*.

[57] ISO/IEC 29167-1:2014, *Information technology – Automatic identification and data capture techniques – Part 1: Security services for RFID air interfaces*.

[58] ISO/IEC TR 24729-4:2009, *Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security*.

[59] http://www.gs1.org/gsmp/kc/epcglobal

[60] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[61] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[62] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[63] http://www.wcoomd.org

[64] IEC/TS 62668-1 ed2.0 (2014), *Process management for avionics – Counterfeiting prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*.

[65] IEC/TS 62668-2 ed1.0 (2014), *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*.

[66] Adapted from Market Surveillance Regulation EC no 765/2008, art 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf

[67] 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

[68] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html

[69] http://www.anticounterfeitingforum.org.uk/best_practice.aspx

[70] http://www.cti-us.com/CCAP.htm]

[71] http://www.ipo.gov.uk/ipctoolkit.pdf

[72] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf

[73] Establishing Conformity and Interoperability Regimes – Basic Guidelines (ITU, 2014).

[74] *Guidelines for developing countries on establishing conformity assessment test labs in different regions*, ITU, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf

[75] IEC 62321:2008, *Electrotechnical products – Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers)*.

[76] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[77] ISO/IEC 15962:2013, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions*.

[78] ISO/IEC 15961:2004, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface*.

[79] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[80] ISO/IEC 15420:2009, *Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification*.

[81] ISO/IEC 16388:2007, *Information technology – Automatic identification and data capture techniques – Code 39 bar code symbology specification*.

[82] ISO/IEC 15417:2007, *Information technology -- Automatic identification and data capture techniques – Code 128 bar code symbology specification*.

[83] ISO/IEC 15438:2006, *Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification*.

[84] ISO/IEC 16023:2000, *Information technology – International symbology specification – MaxiCode*.

[85] ISO/IEC 18004:2006, *Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification*.

[86] ISO/IEC 16022:2006, *Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification*.

[87] DIN 66401 (2010), *Unique Identification Mark (UIM)***.**

[88] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard***.**

[89] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier*.

[90] ISO/IEC 7816-6:2004, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange*.

[91] ISO 14816:2005, *Road transport and traffic telematics – Automatic vehicle and equipment identification – Numbering and data structure*.

[92] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID)*.

[93] ANSI INCITS 371.1-2003, *Information technology - Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol*.

[94] ISO/IEC 18000-6:2013, *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*.

[95] ISO/IEC 18000-3:2010, *Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz*.

[96] ISO 11784:1996, *Radio frequency identification of animals – Code structure*.

[97] ISO 11785:1996, *Radio frequency identification of animals – Technical concept*.

[98] ISO/IEC 18000 (All Parts), *Information technology – Radio frequency identification for item management*.

[99] ISO 17363:2013, *Supply chain applications of RFID – Freight containers*.

[100] ISO 17364:2013, *Supply chain applications of RFID – Returnable transport items (RTIs) and returnable packaging items (RPIs).*
[101] ISO 17365:2013, *Supply chain applications of RFID – Transport units.*
[102] ISO 17366:20`3, *Supply chain applications of RFID – Product packaging*.
[103] ISO 17367:2013, *Supply chain applications of RFID – Product packaging*.
[104] ISO 18185 (All Parts), *Freight containers – Electronic seals*.
[105] ISO/IEC 29160:2012, *Information technology – Radio frequency identification for item management – RFID Emblem*.
[106] ISO/IEC 15693, *Identification cards – Contactless integrated circuit cards – Vicinity cards*.
[107] ISO 28000:2007, *Specification for security management systems for the supply chain*.
[108] ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance.*
[109] ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*.
[110] ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*.
[111] ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements.*
[112] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.
[113] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.
[114] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors.*
[115] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.
[116] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.
[117] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.
[118] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

术语表

AC	划分等级
ADI	航空航天和国防标识
AIDC	自动识别和数据获取
ALE	应用层事件
AWP	自动化工作场所
CB	认证机构
CBV	核心业务词汇
cc	类代码
CD	光盘
CDMA	码分多址
CDR	呼叫细节记录
CEIR	中央设备标识注册
CIPS	综合信息保护系统
CoPC	人员能力资格认证
DB	数据库
DCI	发现、配置以及初始化
DNS	域名系统
DVD	数字通用光盘
EIR	设备标识注册
EMC	电磁兼容性
EPC	电子产品编码
EPCIS	电子产品代码信息服务
GDTI	全球文件类型标识
GIAI	全球单个资产标识
GID	一般标识符
GII	真 IMEI 植入计划
GINC	全球托运识别代码
GLN	全球位置代码
GRAI	全球可回收资产标识
GSIN	全球货运识别代码
GSM	全球移动通信系统

GSRN	全球服务关系代码
GTIN	全球贸易物品代码
HF	高频
ic	识别代码
IC	集成电路
ICT	信息通信技术
ID	识别
IMEI	国际移动设备识别码
IP	知识产权
IP	互联网协议
IPM	公共成员界面
IPR	知识产权
ISBN	国际标准书号
ISSN	国际标准连续出版物编号
IT	信息技术
LLRP	低层读取器协议
LTE	长期演进
ME	移动设备
MEID	移动设备标识
MIIM	移动物品识别和管理
MRA	相互认可协议
MSC	移动交换中心
MSISDN	移动用户综合服务数字网
NIR	非电离辐射
OID	对象标识符
ONS	对象命名服务
QoS	服务质量
RF	射频
RFID	射频识别
RM	读取器管理
RoHS	限制的有害物质
RP	读取器协议

RUIM	可移动用户识别模块
SFP	安全功能提供方
SGLN	带有或者不带扩展的全球位置代码
SGTIN	全球贸易物品序列代码
SIM	用户标识模块
SLDc	次级域代码
SMD	表装设备
SMS	短信
SNMP	简单网络管理协议
SS7	7 号信令系统
SSCC	货运包装箱序列代码
TAC	型号分配码
TC	技术委员会
TDS	标签数据标准
TDT	标签数据翻译
TID	标签 ID
TLDc	顶级域代码
TV	电视
UHF	特高频
UII	特殊物品标识符
UIM	独一无二的识别标记
UMTS	通用移动通信系统
UPC	通用商品码
URL	统一资源定位符
USB	通用串行总线
WG	工作组

附件A
假冒移动设备识别系统

如上文技术报告所述，假冒移动设备一直为人们所关注，且各国已就遏制假冒移动设备的泛滥采取了一系列举措。这些举措有些最初意在确保移动设备能够依法进口（即不进口违禁设备），随后的评估认为这些举措可保障设备不为假冒产品。这些方案与专门解决假冒问题的举措有许多相似特征，例如都是基于唯一标识（IMEI）的认证。

下文各节介绍了国家和区域性机构的措施示例。

A.1 各国主管部门和监管机构的措施示例

A.1.1 阿塞拜疆

根据2011年12月28日阿塞拜疆共和国内阁部长会议第212号决定批准的“移动终端注册规则”，通信和信息技术部信息计算机中心（ICC）建立了移动设备注册系统（MDRS）http://www.rabita.az/en/c-media/news/details/134。

移动终端注册旨在防止进口产地不详且无法满足有害电磁辐射限制等强制性技术标准的低质终端，同时提高制造厂商的知名度与竞争力。注册系统可防止用户使用丢失/失窃的移动终端以及非法进口至该国的终端。

自2013年3月1日起，移动运营商每天均会将阿塞拜疆境内移动终端的IMEI号输入中央数据库系统。通信和信息技术部报告称自MDRS启动以来，共有1.2亿GSM终端进行了注册。约有300,000终端不达标，但仍可继续使用当前的移动电话号码工作，但不达标的新终端不得在该国使用http://www.mincom.gov.az/media-en/news-2/details/1840。

2013年5月1日前在网内使用的所有移动终端IMEI号均被视为已注册，因此可在网内自由使用。注册系统启用后，所有私人用（使用该国某一移动运营商的SIM卡）进口移动终端的IMEI号均应在入网后30天内注册。此规则不适用于使用外国运营商SIM卡的漫游移动终端。

用户可通过专用网页（imei.az）或发送短信，使用IMEI号码确定其终端的合法性。中央数据库系统位于通信和信息技术部信息计算机中心（ICC）。与此同时，移动运营商已安装了与中央数据库同步的相应设备。MDRS软件由本地专家开发。

A.1.2 巴西

SIGA – 综合终端管理系统

巴西国家电信管理局 – Anatel的《移动服务法规》要求，运营商只允许经Anatel认证的终端在其网内使用（《移动服务法规》第8条第IV款，第10条第V款，经第477/2007号决议批准[9]）。因此，Anatel强制要求巴西移动运营商联合采用一种技术方案，遏制使用未经认证的移动终端，或IMEI被篡改或克隆的终端。

运营商为履行此义务而提交的既定行动计划确定了技术解决方案的行动纲领，为尽量减少对用户的影响而在真实用户基础上提出的标准，该方案实施后为确保仅符合Anatel法规的

[9] http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477

终端能够入网而针对新用户施行的标准，为避免给国内外用户造成不便而针对移动用户实施的标准，面向移动网络用户开展的树立意识活动等内容。

2012年Anatel在考虑到技术和监管等方面的前提下，批准了该行动计划。此解决方案称为SIGA – 即“综合终端管理系统”，其开发是基于以下技术前提：

- 所有巴西移动运营商共同推出集中解决方案；
- 与移动平台运营商推出集成方案；
- 推出可实现低人工干预信息输入的自动化解决方案；
- 可扩容且复杂度可升级并提高；
- 充满活力且灵活，规则可随时调整；
- 由诸如呼叫细节记录（CDR）和管理系统操作员等多个信息源构成，其中包括可酌情使用国际数据库；
- 可高效地采取行动，抑制非法终端的使用；
- 可尽量降低对常规最终用户的潜在影响；
- 可靠且安全。

如今，SIGA的技术运营由ABR电信[10]实施，该电信协会是由绝大多数电信运营商合资创建的技术协会，旨在为巴西电信市场开发、部署和运营提供集中化的技术解决方案。

为确保SIGA取得成功，此项目与所有其它各方开展了充分互动，其中包括Anatel、海关署、运营商协会（SindiTelebrasil）、运营商、设备制造商、制造商联盟（ABINEE）和ABR电信公司。此外，该问题的复杂性在于涉及运营商的方方面面，以及多个市场参与方和最终用户；因此必须就所有行动进行详细的讨论。

SIGA自2014年3月以来便积极参与运营商网络的工作，收集分析不符合巴西监管要求的终端市场规模所需的必要信息，这样所有相关方便可确定需采取的必要行动，确保在尽量降低对消费者所造成影响的前提下将假冒伪劣和未经授权的终端从网络中清除出去。

目前正在探讨的可满足此前提的一项做法是，创建包含各种情况的可继续使用终端的数据库（终端与用户间存在唯一对应关系），说明哪些终端仍可继续在网络中使用，但任何新的非正常终端均不得入网。这样，对用户的影响可明显降低，而该数据库将随着手机的更新而消亡。

另一重要做法是邀请将代表用户的实体加入探讨，在采取会给用户造成直接影响的任何行动（例如屏蔽或暂停终端的使用）前与其进行充分沟通。

为此，运营商、Anatel与制造商联盟共同制定及沟通计划；该计划的实施应由上述实体执行，协调与消费者沟通的各个渠道（如公益广告、运营商的账单和呼叫中心），向用户展示购买合法并经认证的终端的益处，以及在巴西使用假冒伪劣和未经授权终端的风险。

有关此项目技术的更多详细信息可直接从国家电信局 – 巴西主管部门Anatel获取。[11]

[10] http://www.abrtelecom.com.br

[11] prre@anatel.gov.br

A.1.3 哥伦比亚

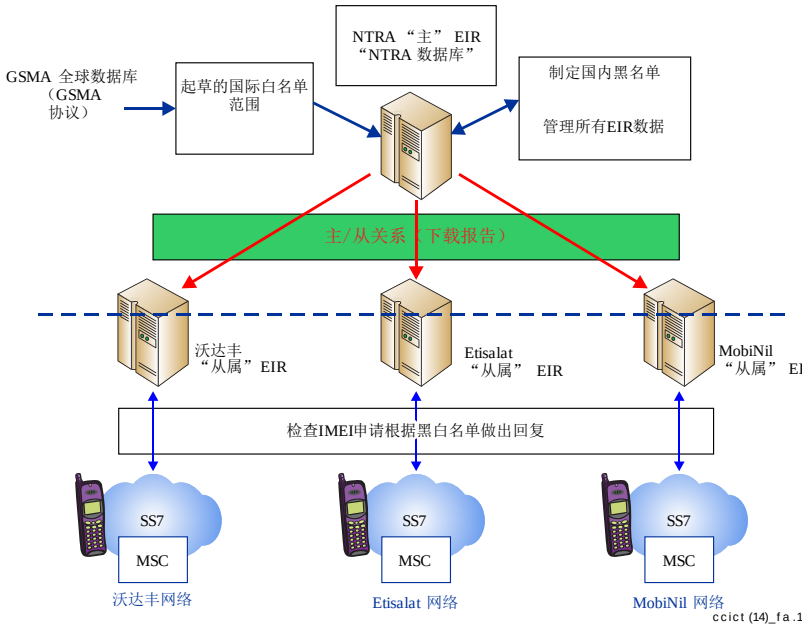
2011年，信息和通信技术部发布了第1630号法令，旨在建立一种管控新移动终端与二手移动终端营销与销售的机制，同时建立两类集中数据库：一类数据库中记录有已上报失窃或丢失的终端设备的IMEI号并禁止使用或激活这些终端；另一数据库记录有合法进口或在该国使用的终端设备的IMEI号，及与之相对应的机主或用户的识别码。

2011年6月颁布的有关公民安全的1453号法案规定，对移动终端IMEI进行篡改、重新编程、重新贴标或修改者以及启用失窃终端者可判入狱6-8年。此外，还将没收改动后的设备 http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf。

这些举措旨在控制失窃移动终端的销售与使用，但很可能会对假冒产品的使用产生影响。

A.1.4 埃及

2008年，国家电信监管局（NTRA）成立了市场监管部，为型号核准提供支持。2010年埃及建立了打击使用假冒移动终端设备的系统。此系统使用GSMA IMEI DB每周更新IMEI TAC白名单和中央设备标识注册（EIR）工具 – IMEI数据库。此方案旨在遏制使用非法、假冒手机、内容为空或克隆的IMEI，打击手机盗窃、解决卫生和安全方面的问题。



图A.1 – 埃及的中央EIR IMEI数据库解决方案

根据NTRA的统计，共有350万部手机使用非法IMEI号13579024681122，250,000部手机使用克隆IMEI，500,000部手机使用假IMEI、350,000部手机使用全零IMEI，另有100,000部手机无IMEI号http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf。

2010年2月，NTRA宣布该国的三家运营商将联合在埃及市场拒绝向任何匿名用户和无IMEI手机提供服务http://www.cellular-news.com/story/42911.php。

A.1.5 印度尼西亚

印尼于2013年1月提高了蜂窝电话进口的条件，同时提出了技术程序和标准要求，施加了分销与港口限制，实施启运前监控，并规定了进口前预注册IMEI号的义务。第81/2012号工业部长令和第82/2012号贸易部长令对此做出了详细的阐述 http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf。

A.1.6 肯尼亚

A.1.6.1 简介

据肯尼亚打假局（ACA）称，真假产品间的不公平竞争估计每年会给企业界（本地制造商、投资者和创新者）带来500亿先令（约5.96亿美元）的收入损失，因此给诸多厂家造成了关闭和/或搬迁的威胁。假冒产品通过逃税每年给政府和经济造成的损失估计超过190亿先令（约2.27亿美元） http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471。受影响最大的行业包括制药、电子、CD 与盗版软件、酒精饮料、手机和农业用品。

根据肯尼亚信息通信法 Cap 411A 成立的肯尼亚通信委员会负责颁发信息和通信业务许可并对其实施监管。该法第25节授权该委员会依据相关前提条件，分别为电信系统和电信业务的运营与提供颁发许可。其中一项许可要求对通信设备进行型号审核，以确保其与公共通信网兼容。在此背景下，2010年的肯尼亚信息通信法规第3条（进口、型号核准、通信设备分销），要求所有手机在与公共网络连接之前均必须进行型号核准 http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf。

型号核准程序的核心目标是保障公众不受伪劣和/或假冒移动电话终端造成的不良影响，这些危害涉及技术、经济、卫生和安全等方面。ICT 产业内假冒手机方面挑战的更多信息请参见下文第 A.1.6.2节。没有相应国际移动设备标识（IMEI）的手机无法通过型号核准。

鉴于上述原因，必须逐渐放弃使用假冒移动电话终端。但这需要考虑所有利益攸关方的利益，因此退出工作的最终截止日期为2012年9月30日。

为保障利益攸关方的利益和关注得到考虑，该委员会自2011年10月起便与 ICT 产业参与方，各类政府机构以及其它与假冒移动电话问题相关的各方开展了公开磋商，以应对这些仿制电话给该产业和整体经济带来的挑战。通过这些磋商，各方已就针对该主题事宜采取的具体行动方案达成了一致。

已达成共识的行动包括，由该委员会开展树立公众意识活动，确保用户意识到假冒设备造成的负面影响；建立一个供公众使用的系统，用于判定所用手机的真伪；在移动网络内建立屏蔽假冒手机的系统；为客户提供相关的支持服务。

另一项重大行动是所有相关政府机构加强对假冒移动设备的监督和打击。目前建立的可访问 GSMA 数据库的手机认证系统，能够通过提交 IMEI 验证手机的有效性。此外，还在移动网络内建立了一个屏蔽假冒手机的系统。

由于开展了以上活动，2012年9月30日后共有189万部假冒移动电话退出了肯尼亚市场。

A.1.6.2 假冒移动电话的逐步清退

1) 背景

a) 实施设备标识注册（EIR）系统

如今，手机在肯尼亚已是必须品而非奢侈品。该国不断增长的手机用户目前已接近2,920万。但移动通信业务的推广面临的挑战之一是手机盗窃以及给安全造成巨大风险的手机协助犯罪。

在上述威胁出现后，该委员会于2011年与当时持有牌照的移动运营商进行了一系列磋商，力求为此问题找到一个长久的解决方案。与此同时，东非通信组织（EACO）采用了一项方案，要求该区域的监管机构和运营商通过磋商寻找遏制该区域手机盗窃的最佳办法。

在磋商过程中，移动网内有一种名为设备标识注册（EIR）的内置功能可为解决手机盗窃问题提供机制。EIR可核查接入移动网络的各手机的唯一国际移动设备标识（IMEI）并将其记录下来。此类信息将在相关机构提出要求的情况下，尽量提供给这些机构。

为此，所有移动运营商为实施EIR系统达成了一份备忘录（MoU），这将为在区域层面落实此系统铺平道路。此外，就多数使用复制和/或假冒IMEI的仿造手机和非法获得的手机而言，可使用EIR系统对其进行跟踪并屏蔽其使用。其它一些使用类似IMEI的手机亦将被停用。

在此背景下，如果在EIR系统全面实施前要成功地解决假冒手机问题，则必须响应国际号召，彻底清除这些伪劣产品。

b) 落实手机方面的法律/监管框架

i) 法律/监管框架

从通信产业角度来看，肯尼亚信息通信法Cap 411A第25节规定了有关手机的法律/监管框架。根据此法案颁发的许可要求仅为经过型号核准的手机提供服务。

此外，2010年的肯尼亚信息通信法规第3条（进口、型号核准、通信设备分销），明确要求所有手机在与公共网络连接之前均必须进行型号核准。请务必注意，根据该委员会的型号核准要求，没有相应IMEI或IMEI被篡改的GSM手机无法获得型号核准。因此，所有不具备合法IMEI或IMEI被克隆的手机本质上均为非法手机，因此其使用违反了上述法案。

ii) 该委员会近期的指令和运营商的响应

2011年5月，该委员会通知所有移动网络运营商于2011年9月30日前逐步清除假冒手机。此指令是对通信行业“管理章程函”精神的响应。

2) 行业磋商

在收到该指令后，移动业参与方再次请求重新审议此指令，指出有大量用户在使用IMEI相同或IMEI存在问题的手机。此外，运营商停用约200多万部假冒手机可能会给其收入带来不利影响。

为确保尽量降低该指令的实施给业务中断造成的影响，该委员会成立了一个开放的分委员会，其代表主要来自移动运营商、相关政府部委、设备制造商、销售商和民间团体。

ICT参与方与各类政府机构开展的一系列磋商旨在应对产业和经济因假冒手机而面临的挑战。GSM协会（GSMA）指出，肯尼亚是为欧洲失窃手机和直接仿造手机提供巨大市场的国家之一。根据处理此类问题的国际经验，GSMA也通过各种技术干预为支持肯尼亚的相关进程提供了大量的咨询服务。磋商现已决定为支持该举措采取具体和行动。

这些行动主要包括由该委员会开展树立公众意识活动，确保用户意识到假冒设备造成的负面影响，手机厂商承诺建立一个供公众判定手机真伪的系统。此外，网络运营商还应在移动网络内建立屏蔽假冒手机的系统，并为客户提供相关的支持服务，与此同时政府机构应监督并打击假冒手机。

在开展树立公众意识活动的同时，建立一个可访问GSMA数据库的手机认证系统，通过提交IMEI验证手机的有效性http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf。

A.1.7 卢旺达

卢旺达公用设施监管署（RURA）于2013年宣布禁止向该国进口假冒移动设备，同时屏蔽那些已经在用的假冒手机 http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print。卢旺达面临的另一挑战是，假冒手机将拨打EACO统一短码100（客户服务）、101（坦桑尼亚的缴费服务）和102（坦桑尼亚的余额查询服务）至112（应急、警务）。这迫使RURA临时为客户信息服务重新指配一个不同的短码http://www.eaco.int/docs/19_congress_report.pdf。

A.1.8 斯里兰卡

2013年3月，斯里兰卡电信监管委员会（TRCSL）就“设计、开发和安装斯里兰卡移动网络设备标识注册（CEIR）系统”公开招标 http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf。

为消灭假冒移动电话市场，阻止移动电话盗窃并保护消费者的利益，TRCSL有意建立一个与所有移动运营商EIR相连接的中央设备标识注册（CEIR）系统。CEIR作为所有移动运营商的中央系统，可分享已列入黑名单的移动终端信息，这使在一个网络内被列入黑名单的终端即便更换了用户标识模块（SIM）也无法在另一网络使用。

根据TRCSL的要求，CEIR须确保以下功能：

i) CEIR须能够维护移动网注册终端所在的IMEI数据库。

ii) CEIR须能够确定以下IMEI：

a) 未分配的IMEI；

b) 内容为空、复制或全零的IMEI。

iii) CEIR数据库须包含在斯里兰卡所有移动网注册的终端的下述信息：

a) IMEI；

b) IMEI的状态（白、灰、黑）；

c) 创建记录的日期；

d) 上次记录更新的日期；

e) 设备型号；

f) 处于当前IMEI状态的原因（无效、失窃、克隆、有效）。

iv) CEIR须能够禁止为IMEI无效或被列入黑名单的用户提供服务。

v) CEIR须能够确定终端型号、版本和其它信息。

vi) 当新用户账号激活时，CEIR须能够在IMEI数据库中创建新记录。

vii) CEIR须提供运营商更新的本地黑/白/灰数据库信息，以防止跨网络克隆，保持数据库信息的更新。

viii) CEIR须使用最有效的方法定期使用最新信息更新IMEI数据库。

ix) CEIR须能够通过对比GSMA提供的IMEI辨别假冒IMEI。

x) CEIR须能够与所有相应网元和移动运营商的接口进行互操作。

xi) CEIR数据库须支持灵活的输入方法（通过手动输入数据，存有IMEI范围更新的无相对关系结构记录文件）。

xii) CEIR须检查IMEI格式以验证其格式和范围是否有效。

A.1.9 土耳其

2006年，土耳其信息通信技术局（ICTA）建立了中央设备标识注册（CEIR）系统，以防止使用未经注册的移动电话、税收损失、不公平行业竞争、劫持、消除和人工干预进口流程。该基础设施的建立旨在减少非法进口终端，终止为走私、丢失和失窃的终端以及克隆IMEI号的终端提供无线网络服务。

https://www.icta.mu/mediaoffice/publi.htm

图A.2 – 中央设备标识注册系统的结构

《无线电通信法》的IMEI号分类如下：

- 白名单：包含已注册且其电子标识信息未曾变更的终端的IMEI号。
- 黑名单：包含属于丢失或失窃类别且电子标识信息已经变更的IMEI号。电信运营商有权终止此类终端的无线通信。
- 灰名单：包含即不属于白名单也不属于黑名单的IMEI号，且允许为其提供无线通信服务。电信运营商必须分析此类终端呼叫的详情，并通知ICTA。电信运营商还须使用消息通知此类终端用户其终端不在白名单内。
- 匹配的白名单：包含的IMEI号是缴纳过注册费用户的IMEI号在移动用户综合服务数字网（MSISDN）内号码的克隆。它还包含与某电信运营商签约并在土耳其临时使用过MSISDN号的终端。

根据ICTA2010年年报，截止2010年底，共有131,836,847个合法注册的IMEI号和14,308,239个由于丢失、走私、失窃和克隆等原因被纳入黑名单的IMEI号 https://www.icta.mu/mediaoffice/publi.htm。

A.1.10 乌干达

乌干达通信委员会（UCC）开展了一项旨在逐渐消灭乌干达市场内假冒手机的项目 http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html。一项经UCC认证的研究指出，乌干达市场有30%的手机为假冒产品。调查还指出该国政府因假冒仿制手机，约损失了150亿先令（~5.4亿美元，截至2014年11月）http://www.monitor.co.ug/Business/Commodities/Survey+finds+30++of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html。

2012年12月，UCC公布了一份磋商文件“消灭假冒手机的时间表和任务分配”http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf，将此项目定义为四个实施阶段：

阶段1：移动电话认证：

在此阶段，消费者可使用互联网和短信应用查询其手机的状态。

建议消费者立即用上述两个渠道验证其移动电话的合法性。

阶段2：拒绝为新增假冒手机提供服务

在此阶段，以前未在任何网络注册的新假冒手机不得入网。执行此阶段任务的拟定日期为2013年1月31日。

阶段3：终断为所有假冒移动电话提供服务：

在此阶段，所有假冒移动电话，包括以前进行过网络签约的电话，均须退网。执行此阶段任务的拟定日期为2013年7月1日。

阶段4：项目的巩固：

在此阶段，该委员会须审议与项目落实相关的成果，以及与电子废弃物和IMEI克隆相关的问题。目前仍在考虑如何处理此阶段各类问题的建议。

A.1.11 乌克兰

A.1.11.1 简介

2008年，急需迫切解决的问题是违禁终端的进口问题，此类终端占领了乌克兰93%-95%的市场。从技术和安全角度来看这些来源未知的手机中大部分无法满足乌克兰的标准。乌克兰“无线电频率资源”法授权国家通信和信息化监管委员会（NCCIR）采取更多措施保护乌克兰市场免受低质、无授权或非法移动终端的冲击。

NCCIR为移动终端的进程定义了监管程序。作为进口程序的一种技术手段，乌克兰国家无线电频率中心（UCRF）于2009年创建了乌克兰国家无线电频率中心（AISMTRU）。因此移动终端的非法进口大幅下降，2010年仅占市场的5%-7%，且在此后几年持续下降。

乌克兰使用IMEI为合法进口的终端建立了一个数据库。数据库中包括如下清单：针对合法进口终端的“白名单”，针对地位不确定终端的“灰名单”及拒绝为其提供服务终端的“黑名单”。该数据库按照不同接入权限，为监管机构、海关、网络运营商和普通大众提供接入。

AISMTRU执行以下职能：

- 自动处理进口商的在电信网内使用相关终端设备的申请，完成注册监管程序；

- 阻止非法向乌克兰境内进口“灰色”终端；
- 打击手机盗窃；
- 实现UCRF工作流程自动化，提高UCRF与终端市场参与方相互协作的效率；
- 判定“克隆”的IMEI号并屏蔽使用“克隆”IMEI号的终端。

有关AISMTRU的详细信息请参见第A.1.11.2节。

乌克兰立法禁止销售IMEI号未在AISMTRU注册的移动终端。AISMTRU的主体部分为通用数据库，该数据库负责保存移动终端IMEI号的“白”、“灰”和“黑”名单。终端一旦在某一运营商网络入网或注册，则该相关运营商将自动把终端的IMEI号转发至通用数据库。AISMTRU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”名单之日起的90天内确认终端的合法来源。

失窃终端的IMEI号将应执法机构的请求在“黑”名单中登记，此做法使手机盗窃失去了意义。同样的程序亦适用于根据手机失主请求锁定终端的操作。网络运营商不为“黑”名单中的终端提供服务。

为消费者在购买手机前提供验证移动终端合法性的便捷工具，可实现保护消费者的目标。所有消费者均可通过将SMS发送至全国通用号码“307”或访问UCRF的互联网门户，验证终端IMEI号的状态。验证所需时间不超过10秒。

AISMTRU的实施为乌克兰的合法终端市场提供了保障，并大幅减少了该国“灰色”（非法）移动终端的进口。非法进口移动终端的份额已从2008年的93%-95%下降至2010年的5%-7%，且随后几年也始终保持这一比例。2010-2012年，上缴乌克兰国家预算的移动终端进口关税为5亿美元，而此前三年的这一金额为3亿美元。乌克兰移动终端市场主要由符合该国技术特性要求的移动终端构成。

A.1.11.2 在乌克兰注册的移动终端自动信息系统（AISMTRU）

A.1.11.2.1背景

由运营商提供的移动（蜂窝）通信业务的迅猛发展以及此类电信业务在乌克兰的迅速普及，导致移动终端市场在乌克兰快速膨胀，从而也导致了此类产品进口的增加。

“移动终端”是指移动手机或其它电信网终端用户设备，这些设备有国际标识号且可使用该号确定网络中的身份。

2008年，乌克兰移动终端市场出现了严重问题：市场上93%-95%的产品为“灰色进口”终端，换言之，为走私产品。此外，这些产品中的大部分为产地不名的品牌手机仿制品，无论从技术还是安全角度均无法满足乌克兰的标准。各种市场监管措施都无济于事，且这些终端并非乌克兰制造。

此后，出现了一个独立的监管机构 – 国家通信和信息化监管委员会（NCCIR）。乌克兰“无线电频率资源”法授权该委员会采取更多措施保护乌克兰市场免受低质、无授权或非法移动终端的冲击。

A.1.11.2.2目标

为控制终端的进口、制造和使用NCCIR定义了如下目标：

1) 将低质移动终端逐出乌克兰市场，这些终端可能未经授权且对人体健康有害。

2) 保障移动通信服务具备相当的质量。

3) 解决手机失窃这一社会问题，尤其是会对儿童。

4) 打击乌克兰市场内非法进口和非法使用的移动终端。

考虑到上述目标，如今已为移动设备的进口和使用制定了程序。这些程序以官方法案的形式存在 – 乌克兰无线电子设施和辐射装置进口规程和电子设施和发射设备使用规程。

A.1.11.2.3进口程序

乌克兰的无线电设备进口由海关署根据以下条件进行监控：

- 是否有符合无线设备技术规则的文件；
- 是否符合无线电子设施和辐射装置进口规程（这些装置可在乌克兰的公共频段使用）；
- 是否在无线电电子设施和发射设备注册系统中注册（不注册不得在乌克兰的公共频段使用）。

进口商向UCRF提交的IMEI号，在处理后将进入IMEI通用数据库的“白名单”。为注册合法进口的国际终端设备标识，乌克兰国家海关署将向UCRF提供海关申报摘要（电子形式），用于无线电电子设施每日的进口。

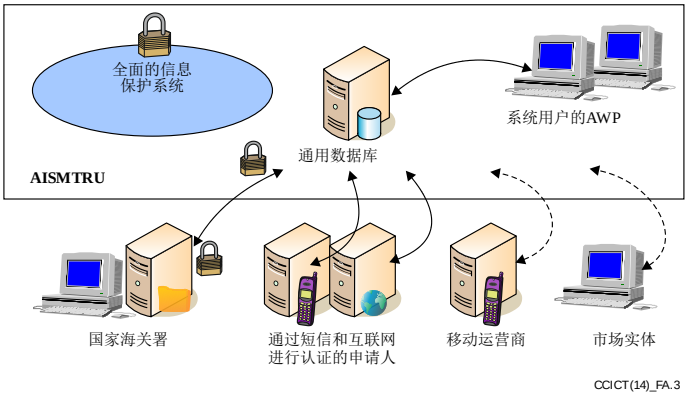
作为上述监管进程程序的技术实施方式之一，2009年7月1日UCRF创建了乌克兰移动终端注册自动信息系统（AISMTRU）并将其投入使用。

根据乌克兰有关“一致性确认”的法律，终端设备一致性的确认必须得到监管机构（NCCIR）认可的机构的认证。

A.1.11.2.4AISMTRU的职能

AISMTRU的职能请参见第A.1.11.1款：

- 自动处理进口商的申请；
- 防止向乌克兰境内进口“灰色”终端；
- 打击手机盗窃；
- 实现UCRF工作流程自动化，提高UCRF与终端市场参与方相互协作的效率；
- 判定“克隆”的IMEI号并屏蔽使用“克隆”IMEI号的终端。



图A.3 – AISMTRU的职能

A.1.11.2.5授权

根据当前的立法，以下实体被授权使用AISMTRU：

- 乌克兰国家无线电频率中心；
- 国家通信和信息化监管委员会；
- 移动运营商；
- 国家海关署；
- 内务部；
- 移动终端的采购者和用户；及
- 进口商。

A.1.11.2.6IMEI通用数据库

AISMTRU主要由IMEI通用数据库构成，其中包括三个常规组成部分：

- “白名单”：合法进口或在乌克兰合法制造的终端IMEI号记录。
- “灰名单”：首次进入电信网注册时未被录入“白名单”或“黑名单”的终端IMEI号在通用数据库中的记录。
- “黑名单”：禁止运营商为其提供服务的终端的IMEI号记录（进入“灰名单”后90天仍未确认其合法来源的失窃或丢失手机）。

IMEI通用数据库的维护子系统为UCRF授权用户提供了一种工具，供其将数据录入“白名单”。“灰”和“黑”名单均自动生成。UCRF授权的用户拥有有限的权限，可更改特定IMEI号在“灰”和“黑”名单中的状态。

UCRF授权用户的行动均通过单个用户的电子数字签名确认。

子系统具有数据导入功能，能够将终端进口商和移动运营商的数据发送至IMEI记录。

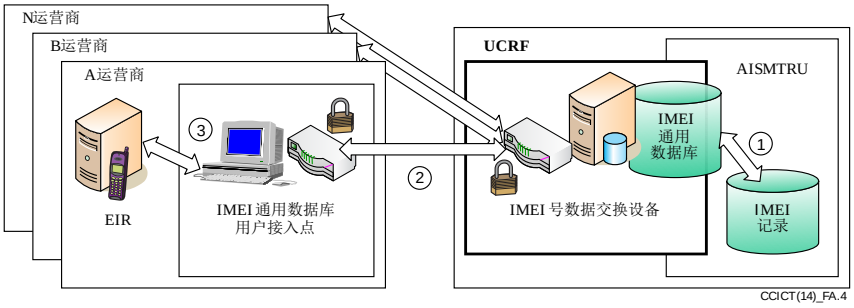
通过处理“白名单”数据和运营商数据以及进口商和海关的数据，可生成并保持“灰”和“黑”名单记录。

将系统投入运营的第一阶段可实现两个目标：

1) 保护乌克兰市场免受可能会危及用户健康的无授权低质移动终端的侵害。

2) 阻止非法进口移动终端及其在乌克兰的使用。

随后为实现所有目标建立了一个系统，以达到停止使用失窃移动终端等目的，尤其是针对儿童。



图A.4 – EIR和IMEI通用数据库

在第二阶段，为在AISMTRU与国内移动运营商间交换“白”、“灰”和“黑”名单中的IMEI号，设立了一个子系统。在此阶段，IMEI号的交换使用“手动”模式。

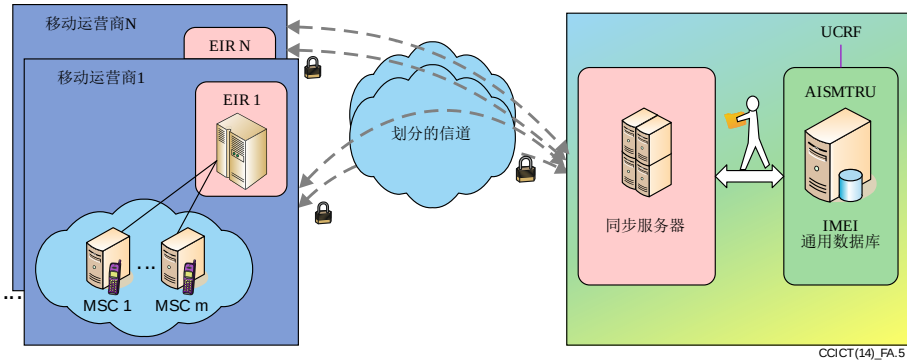
此外，数据交换子系统被用于通知内务部有关失窃/丢失终端的信息，并可供海关交换进口终端的信息。

为确保与AISMTRU积极互动，运营商和UCRF已提供了：

- 设备标识注册（EIR）的维护服务；
- IMEI通用数据库用户接入点（用户点）；
- 用户点与EIR互动的渠道；
- 针对授权用户应用数字签名证书的服务。

AISMTRU内置系统，实现了蜂窝（移动）运营商与IMEI通用数据库的同步。藉此可实施移动运营商EIR与IMEI通用数据库间IMEI号名单的自动交换。这样，各终端的IMEI号在运营商网络中注册后，将出现在AISMTRU中并可在IMEI通用数据库内查询。

同步服务器同时支持使用手动和自动模式与运营商的EIR连接。



图A.5 – 同步服务器

A.1.11.2.7特性

系统的特性包括：

- 使用工业标准进行数据存储与传输（数据交换）；
- 确保数据和整个系统的安全；
- 使用数字签名国家标准确保系统内数据处理各阶段的完整性和不可否认性；
- 系统的模块结构；
- 运营模式为24x7。

A.1.11.2.8数据安全

AISMTRU的全面信息保护系统（CIPS）可满足当前的立法要求，且依据具有相关权能的政府机构审查结果做出的肯定结论证实了这一点。

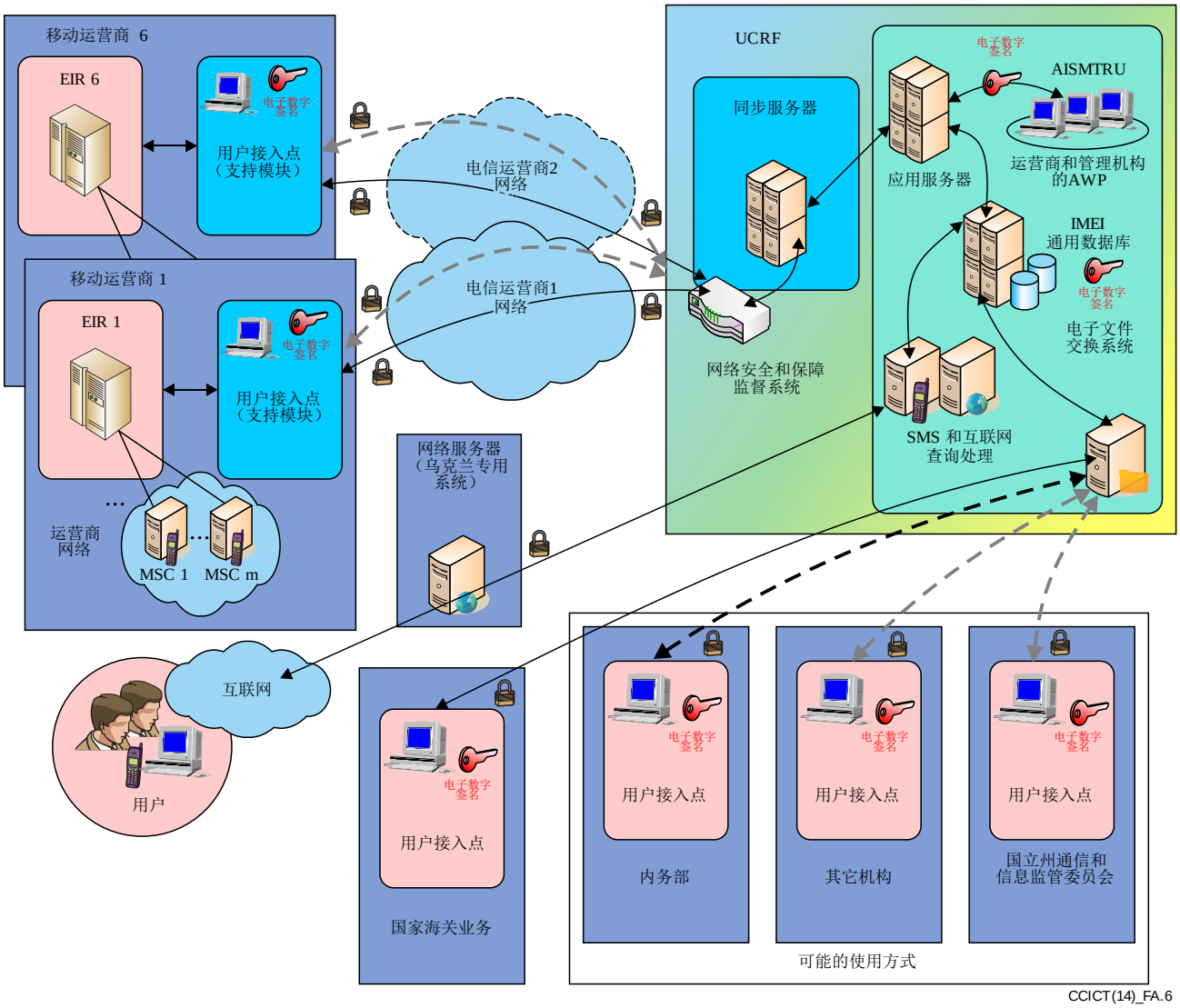
CIPS可确保：

- 控制对保密信息的有限访问；
- 能够识别在该系统内传输、处理和存储的访问受限信息所面临的安全威胁；
- 防止未经授权访问受限信息，保障其保密性、完整性和可用性；

- 在不安全的环境内防止信息泄露；
- 防止技术信息遭受未经授权的访问、破坏、修改和屏蔽。

通过下述方式保障安全性与可靠性：

- 将电子数据签名作为确保信息、授权以及授权用户认证真实性与完整性的可靠方式；
- 根据乌克兰的国家标准实施电子数字签名；
- 备份与恢复系统的可用性；
- 安全日志的维护（在系统中记录所有用户操作或事件）。



图A.6 – AISMTRU全面信息保护系统（CIPS）

A.1.11.2.9实施效果

1) 消费者保护

乌克兰的消费者可在购买移动终端前验证终端的合法性。方式是访问UCRF的官方网站或将验证后的终端IMEI码通过SMS发送至移动运营商通用号码“307”。几秒后，回复将给出所发IMEI码在IMEI通用数据库中的状态。

此做法可确保乌克兰市场内不存在无法满足该国使用要求的终端。

乌克兰当前的立法禁止使用IMEI码未在IMEI通用数据库中注册的移动终端。

2) 打击终端盗窃

可应执法机构的请求将被盗终端的IMEI号列入“黑名单”，使终端盗窃失去意义。

同样的程序亦适用于应手机失主请求锁定终端的操作。

3) 抑制非法进口

首先，所有终端与运营商网络的连接要立即在相关网络中注册。所有运营商网络（国际漫游的终端除外）的终端IMEI号，均会由移动运营商按规定时间自动发送至AISMTRU IMEI通用数据库。

AISMTRU将披露IMEI通用数据库“白名单”中不存在的IMEI号。这些IMEI号使用“灰名单”注册。相关终端的机主将收到一条短信，警告该机可能会在90天内被锁定。

在这90天结束后，该IMEI号将从“灰名单”转入“黑名单”。“黑名单”中的终端不能享受运营商的服务（拒绝其在网络注册，但拨打紧急呼叫号码“112”除外）。与其它运营商网络的连接不会改变终端的“灰”“黑”状态。

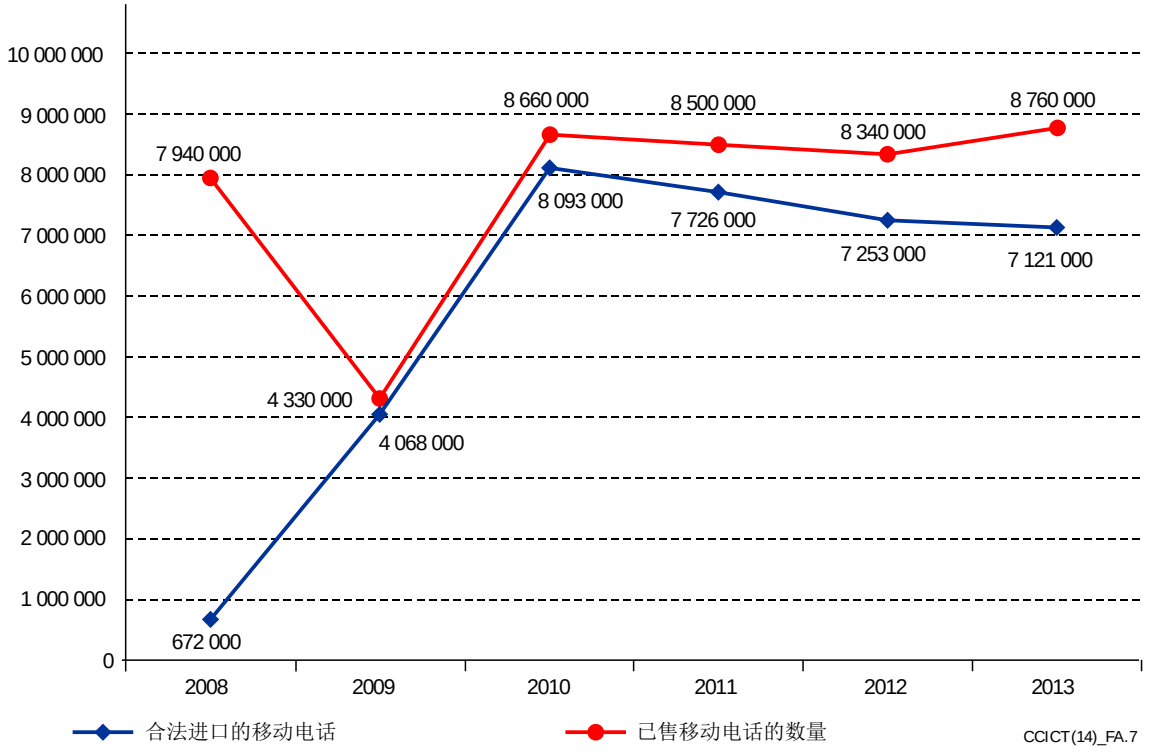
收到已进入“灰名单”和还剩90天服务期的短信警告后，机主可向UCRF申请提供该终端的合法进口确认。UCRF员工对机主的申请进行审核，如果进口的合法性得到确认，则将IMEI号从“灰名单”移至“白名单”。此程序结束后，移动运营商开始为该终端提供无限时服务。

但是，由于缺乏所需法律文件，目前并未中断为“黑名单”中的终端提供服务。

UCRF通过呼叫中心处理移动终端用户有关IMEI号状态和终端进口情况查询的呼叫。

4) 乌克兰终端市场的法制化

- 乌克兰的移动终端“灰色”（非法）进口已经急剧下降。2010年，合法进口的移动终端数量上升了93%-95%（2008年的增长率为7.5%）。
- 2010-2012年，上缴乌克兰国家预算的移动终端进口关税为5亿美元，而此前三年的这一金额为3亿美元。
- 乌克兰移动终端市场的主要由符合该国技术特性要求的移动终端构成 。
- 截至2013年4月30日，AISMTRU IMEI通用数据库中共有140,865,260个注册移动终端IMEI码。
- AISMTRU仅使用UCRF收到的进口商付费作为其七个月开支的经费来源。



图A.7 – 乌克兰实施AISMTRU的影响

A.1.12 阿拉伯联合酋长国（UAE）

阿联酋电信法禁止使用、销售、购买、分销和宣传假冒移动设备。该国电信管理机构（TRA）采取一切必要步骤确保禁止在阿联酋出售和使用此类设备。涉嫌销售假冒手机者将受到警告或罚款，在有些情况下不遵守法规将被吊销牌照。

2011年，为提高认识并劝阻人们使用假冒移动电话，TRA发起了一项新活动 http://www.uaeinteract.com/docs/TRA_urges_against_use_of_fake_cell_phones/47437.htm，

并宣布自2012年1月1日起，所有使用假冒IMEI号码的移动电话设备均不得在阿联酋移动电信网内使用。TRA在各大日报发布公告，警示人们假冒伪劣手机即将被禁用。

此措施意在废止假冒伪劣移动电话设备，但相关用户若使用正规移动电话，则签约服务不受影响，可继续正常工作。通过短信将移动设备的IMEI号码发至“8877”，则用户可收到服务提供商返回的移动设备状态信息。服务提供商会立即与假冒伪劣设备用户联系，所有未经型号认证的手机均将无法使用任何电信服务，其中包括呼叫、短信和互联网服务。

TRA宣布，假冒伪劣移动电话设备可能会给用户的健康造成损害，并鼓励所有用户在购买移动终端和设备时保持适当的警惕。根据TRA的调查，假冒伪劣移动电话尤其容易出现电池泄露和爆炸，释放出具有高度腐蚀性或毒性的化学物质。低质量的组装还意味着辐射水平未经检查，电池消耗更快且接收到的信号通常更弱。

TRA的最终目标是消灭阿联酋境内的假冒伪劣移动电话，让普通民众和零售商都了解使用此类电话的风险。TRA认识到假冒和盗版问题不仅对经济和知识产权有重大影响，而且假冒伪劣的移动电话还是劣质产品，其生产未经相应的测试和检查。

A.2 区域联合措施示例

A.2.1 美洲国家电信委员会（CITEL）

CITEL是美洲国家组织（OAS）大会于1994年成立的机构，旨在推动美洲电信/ICT的发展。美洲全部35个国家均是该组织的成员，另外还有100多个来自ICT产业的准成员。

CITEL第1常设顾问委员会（电信）于2009年建议各成员国“将创建数据库作为打假计划的组成部分”（CITEL PCC.I第15次会议的最后报告，2009年10月2日）。2011年12月，CITEL PCC.II（包括广播在内的无线电通信）着手开始研究电信主管部门就假冒伪劣手机的使用所采取的措施。

PCC.II决定请各主管部门提供“有关就假冒伪劣手机已经或拟采取的行动、监管与行政措施，及其给用户和运营商带来的负面影响，其中包括干扰、NIR水平、危险或违禁化学元件的使用”的信息（CCITEL PCC.II第18次会议的最后报告，2011年12月22日，第121号决议）。

CITEL还审议了移动电话盗窃问题，两个常设顾问委员会均同意与此问题相关的一系列决议。

PCC.II同意2011年9月的第73号决议中有关“为打击移动设备盗窃建立区域合作伙伴关系”的内容。此决议请PCC.I审议“由CITEL推动其成员国制定联合措施，限制该地区的任何国家，激活失窃的移动终端设备，并请CITEL通过针对运营商的具体建议，使这些运营商能够使用其提供的技术且不允许任何来源尚未彻底探明的设备入网，为打击此类设备建立一个区域性合作伙伴关系”（PCC.II第17次会议的最后报告，2011年9月6日，第73号决议）。

PCC.I几乎立即便做出回应，同意了一项有关“采取区域措施打击移动终端设备盗窃”的决议（CCITEL PCC.I第19次会议的最后报告，2011年9月20日，第189号决议）。此项决议注意到该问题的国际属性，当一国采取打击设备盗窃的措施后，移动设备就会被发送到另一国家，因此有必要在区域层面采取措施。除与丢失/被盗手机相关的措施外，第189号决议亦请成员国“考虑在监管框架中要求禁止启用已上报失窃、丢失或在区域或国际数据库中被标为**来源非法**的设备的IMEI或生产厂家电子序列号”（楷体为编辑标出）。

第189号决议的附件包括一系列补充措施，例如“研究控制本地移动终端设备的营销及其入网的可行性”以及“推动建立可确保移动终端设备和/或其零售来源合法并依据各成员国监管框架对其进行验证的监管财政和/或海关机制，同时建立海关监控机制阻止失窃移动终端设备和/或其零件离境或再出口”。

PCC.I同意了于2012年提出的有关“就上报失窃、丢失或找回的移动终端设备交换信息而采取区域性措施”的建议（CCITEL PCC.I第20次会议的最后报告，2012年6月10日，第16号建议），该建议中亦包括“来源非法”的终端。请各成员国“在国家、区域和国际层面采取措施，利用针对不同接入技术的现有在用平台，就失窃、丢失或非法移动终端设备交换信息，以打击黑市并促进各国开展合作，维护保障公民安全的各项原则和最终用户的权利。此外，还建议各成员国“考虑为就失窃、丢失或非法移动终端设备交换信息创建一个数据库，在码分多址（CDMA）、EV-DO和双模CDMA/4G的情况下可使用移动设备标识符（MEID）且在任何网络中都可使用可移动用户识别模块（RUIM）”。

PCC.I亦认可了有关“失窃和/或丢失移动终端”的“技术说明书”（CCITEL PCC.I第23次会议的最后报告，2013年10月10日，第217号决议）。

2014年5月，CITEL批准了第222号决议（XXIV-14） – **“强化遏制假冒伪劣及未经核准的移动设备扩散的区域性措施”**。

因此，成立了信函工作组负责探讨遏制假冒伪劣和未经核准的移动设备扩散的区域性措施，以实现与成员国分享有关此问题的信息、经验和技术以及监管最佳做法的目的，并为美洲区起草相关建议和导则。

2014年8月，信函工作组的工作计划获得批准并被纳入“欺诈管控及电信业不合规做法与打击移动终端盗窃的区域性措施报告人机制”，其职责范围如下：

1) 定义假冒伪劣以及未经核准的移动设备的含义。
2) 评估假冒伪劣以及未经核准的移动设备的范围与本质特征。
3) 就打击假冒伪劣以及未经核准的移动设备的销售与使用，促进在CITEL成员国间分享信息、交流经验。
4) 将全球在打击假冒伪劣以及未经核准的移动设备的销售与使用方面的最佳做法记录在案。
5) 提议起草技术说明书、建议和/或CITEL决议，制定技术和监管措施，用以打击美洲地区假冒伪劣以及未经核准的移动设备的销售与使用。
6) 完成相关工作并向“电信业不合规做法与欺诈管控报告人机制”汇报取得的成果。

A.2.2 东非社区（EAC）

东非每年因仿制造成的收入损失超过5亿美元：http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products/。国外和本地贸易商以及厂商提供的廉价低劣的产品，在包装上非法复制了知名品牌及其设计。

根据2010年通过的共同市场协议，只有协作方能击垮假冒产品及相关贸易。

东非通信组织（EACO）是一家区域性机构，汇聚了东非五个成员国（肯尼亚、坦桑尼亚、卢旺达、布隆迪和乌干达）的监管、邮政、电信和广播机构。EACO审议了该地区假冒移动电话泛滥的问题，并于2012年就一项共同举措达成了共识。

EACO编号任务组（CCK-肯尼亚、TCRA-坦桑尼亚、RURA-卢旺达、ARCT-布隆迪和UCC-乌干达）于2012年5月建议，建立一个国家数据库并采用手机认证程序，保护消费者、企业和网络免受假冒产品的影响（EACO编号任务组2011-2012年报告）。

2012年召开的第19届EACO大会得知了该地区设备标识注册（EIR）的实施情况，当前面临的部分挑战请参见：http://www.eaco.int/docs/19_congress_report.pdf。其中包括：

- 重复使用或缺少国际移动设备标识（IMEI）；
- 消费者未树立假冒产品的危害意识，不了解如何验证设备的合法性；
- 本地销售商/分销商缺乏抵制出售廉价伪劣设备的意识；和
- 实施成本高昂。

为应对这些挑战，建议采用以下解决方案：

- 开展针对消费者和本地销售商的树立意识活动；
- 所有销售商/经销商均必须拥有销售许可；
- 改进型号核准程序；

- 建立设备数据库；及
- 要求SIM注册。

A.2.3 葡萄牙语国家通信和电信监管机构协会（ARCTEL-CPLP）

葡萄牙语国家通信和电信监管机构协会（ARCTEL-CPLP）的成员来自安哥拉、巴西、佛得角、几内亚比绍、莫桑比克、葡萄牙、圣多美和普林西比和东帝汶（http://www.arctel-cplp.org）。ARCTEL-CPLP在2012年国际电联全球监管机构专题研讨会上，就手机盗窃、灰色市场和假冒设备问题发表了演讲。https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf

ARCTEL-CPLP提议将传统解决方案（即国家黑名单数据库系统）推广到整个区域，建议：

- 通过双边或多边协议分享GSM和CDMA黑名单数据库；
- 建立监管财政和/或海关机制，确保更好的控制手机进口并防止再出口；
- 相关方行为应遵守安全建议，防止重新编程、复制IMEI或生产厂家的电子序列识别号；
- 开展树立意识活动，让人们了解报告移动终端设备失窃或丢失的重要性。