国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Q.5051

(03/2020)

Q系列：交换和信令，以及相关的测量和测试

打击假冒和被盗ICT设备

打击使用被盗移动设备的框架

ITU-T Q.5051 建议书

国际电信联盟

ITU-T Q系列建议书

交换和信令，以及相关的测量和测试

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
数字交换机	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
NGN的信令要求和协议	Q.3000–Q.3709
SDN的信令要求和协议	Q.3710–Q.3899
测试规范	Q.3900–Q.4099
IMT-2020的信令要求和协议	Q.5000–Q.5049
打击假冒和被盗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.5051 建议书

打击使用被盗移动设备的框架

摘要

ITU-T Q.5051建议书提议了一个框架，包含了有关要求和涉及众多方面的值得推荐的综合性措施，可采纳并应用于打击盗窃移动设备的行为以及被盗移动设备的再次使用。

近年来，随着移动设备上可用功能和作用的不断增长，这些设备在人们日常生活中的重要性和用途与日俱增。这也带来了副作用，我们看到，在有些国家，旨在窃取这些设备并借以牟利的事情增多了，不仅是通过转卖设备本身，还通过非法使用设备所含的信息来牟利。

为了应对这种情况，需要采取措施阻断盗窃移动设备的行为和被盗移动设备的再次使用，并保护存储在这些设备上的消费者数据免遭非法使用。此外，当设备在某个国家内被盗，可能在这个国家已经部署了减少被盗设备被使用的解决方案，很常见的情况就是把这些设备销往那些可能还未部署类似的减少再次使用方案的其他国家或地区，因此，为了在全球范围内打击盗窃移动设备和再次使用被盗移动设备的行为，各国政府和运营商之间采取协调行动并共享信息对于这些举措取得成功就至关重要。否则，就会产生跨境非法贸易被盗设备的风险。

值得注意的是，由于当今部署的大多数用于解决设备被盗和再次使用问题的解决方案都依赖于唯一标识符列表，因此，违法者采取的绕过这些措施的常见方法是篡改设备以修改其唯一标识符，有时选择使用一个已在合法设备上使用的标识符，以使设备重返市场并连接到移动网络。

为了应对这种情况，世界上许多国家不仅参与打击使用被盗移动设备，而且还参与防止带有未经授权的重新编程的唯一标识符（通常称为篡改标识符）的设备重返网络。同时，其他国家的政府也面临挑战，不清楚应采取的最佳策略，这主要是由于缺乏知识或专门技能，无法了解问题和可能的解决办法，也无法做出知情选择，以部署适合本国国情的、可能有效的解决办法。因此，正如WTSA第97号决议（2016年，Hammamet）所指出的那样，必须有指导方针来应对这一挑战。

历史沿革

版本	建议书名称	批准日期	研究组	唯一识别码*
1.0	ITU-T Q.5051	2020-03-13	11	11.1002/1000/14140

关键词

打击被盗移动设备，一致性，框架，要求，安全性。

* 获取此建议书，请在网络浏览器地址栏输入网址：http://handle.itu.int/，后接建议书的唯一识别码。例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是联合国负责信息通信技术（ICT）事务的专门机构。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）协作制定的。

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

页码

ITU-T Q.5051 建议书

打击使用被盗移动设备的框架

1 范围

本建议书阐述了在部署为打击使用被盗移动设备的解决方案时应考虑的参考框架和要求。

2 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建议书目录定期出版。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。

[ITU-T Q.5050] ITU-T Q.5050建议书 (2019)：打击假冒ICT设备的解决方案框架。

[ITU-T X.1058] ITU-T X.1058建议书 (2017)：信息技术 – 安全技术 – 个人可识别信息保护行为准则。

[ITU-T X.1127] ITU-T X.1127建议书 (2017)：手机防盗措施的功能安全性要求和架构。

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 设备用户[ITU-T X.1127]：有权使用移动设备的用户。

3.1.2 终止开关[b-GSMA]：“终止开关”指一种用于对移动设备的关键功能进行禁用的方式。终止开关实质上是移动设备装置中的一种功能，因此，当该功能被激发，例如设备接收到一条某种格式的信息时，移动设备便会按照要求停止运行，且仅能在设备所有者授权对设备进行再次激活的情况下该设备才能得以激活或再次使用。

3.1.3 移动电话 [b-ITU-T X-Sup.19]：用于通过无线电跨越大的地理区域接入公共移动网络来发起电话呼叫和传递文本信息、同时允许用户处于移动状态的电子设备。

3.1.4 智能电话[b-ITU-T X-Sup.19]：拥有强大计算能力、异质连接性和为第三方应用程序提供平台的先进操作系统的移动电话。

3.1.5 被篡改的ICT设备[ITU-T Q.5050]：包含有下述内容的信息通信技术（ICT）设备，即未经制造商或其法定代表人的明确同意，对其组件、软件、唯一标识符、受知识产权或商标保护的项目进行了暂时或有效的更改。

3.1.6 唯一标识符[ITU-T Q.5050]：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。

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 无效的标识符：如果某个唯一标识符不符合技术标准中规定的格式，或者不在负责管理的实体分发的设备标识符参考数据库中，则此唯一标识符为无效的标识符。

3.2.2 克隆的标识符：指由负责管理的实体合法地分配到某个设备的有效的设备标识符，但该标识符正被其他的不同设备所使用。

3.2.3 可靠的唯一标识符：仅为单个设备所唯一使用的标识符，只能由负责管理的实体分配，且未获授权方不得修改。

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：

EIR 设备标识寄存器

IMEI 国际移动设备标识

IMSI 国际移动用户识别码

PII 个人可识别信息

RUI 可靠的唯一识别码

TAC 型号分配码

5 惯例

本建议书适用于以下描述方式表达的规定：

a) 关键词“要求”（is required to）表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

b) 关键词“应该”（should）和“建议”（is recommended）指的是建议性的、并非绝对需遵守的要求，因此，声称遵守本建议书时无需提及此要求。

c) 关键词“可以”（may）表示允许作为选项但并非建议遵守的要求。该措辞无意暗示供应商在实施时必须提供这一选项，以便网络运营商/服务提供商拥有启用该功能的选项。相反，它是指供应商可选择是否提供该功能，并仍声称遵守本建议书。

6 一般问题

近年来，随着移动设备上提供的功能性和能力的不断增长，这些设备在人们日常生活中的重要性和用途与日俱增。同时也有副作用，我们看到，在有些国家，旨在窃取这些设备并以之牟利的事情增多了，不仅是通过转卖设备本身，还通过非法使用设备所含的信息来牟利。

为了应对这种情况，需要采取措施阻断盗窃和被盗移动设备的再次使用，并保护存储在这些设备上的消费者数据免遭非法使用。此外，当设备在某个国家内被盗，可能在这个国家已经部署了减少被盗设备被使用的解决方案，很常见的情况就是把这些设备销往那些可能还未部署类似的减少再次使用方案的其他国家或地区。因此，为了在全球范围内打击盗窃移动设备和再次使用被盗移动设备的行为，各国政府与运营商之间采取协调行动并共享信息对于这些举措取得成功就至关重要。否则，就会无意间促进了被盗设备国际跨境非法贸易的风险。

为了应对这种情况，许多国家不仅参与打击使用被盗移动设备，而且还参与防止带有未经授权的重新编程的唯一标识符（通常称为篡改标识符）的设备重返网络。同时，其他国家的政府也面临挑战，不清楚应采取的最佳策略，这主要是由于缺乏知识或专门技能，无法了解问题和可能的解决办法，也无法做出知情选择，以部署适合本国国情的、可能有效的解决办法。因此，正如世界电信标准化全会（WTSA）第97号决议（2016年，哈马马特）所指出的那样，必须通过一些建议来应对这一挑战。

因此，本建议书描述了一个框架，包含了有关需求和涉及众多方面的值得推荐的综合性措施，可采纳并应用于打击盗窃移动设备的行为以及被盗移动设备的再次使用。

7 高层面要求

在部署针对使用被盗移动设备的解决方案的过程中，各利益攸关方将面对若干挑战。在部署打击使用被盗移动设备的解决方案时，各国应考虑本节中的要求。

7.1 防止未授权用户使用被盗的移动设备

当设备被窃或丢失后，需要有解决方案能锁死设备，使未经授权的用户无法再操作该设备。

要求在未经授权的用户尝试访问设备一定次数后（例如，经过一定次数的尝试后，未经授权的用户仍未能输入正确的用户密码或个人识别号码（PIN），此进程应自动进行。

建议当设备的授权用户有此要求时，可以远程激活此进程（例如，激活丢失/被盗设备上的终止开关功能）。

要求设置能逆转设备不可操作的选项，以便设备的授权用户找回设备时操作，并在可行的最大范围内恢复用户的数据。

[ITU-T X.1127]涉及到手机防盗措施的功能安全要求和体系结构。该建议介绍了在智能手机丢失或被盗时可以使用的终止开关工具的实施情况。此类工具应该提供以下能力：

– 远程删除智能手机上授权用户的数据；
– 使智能手机无法被未经授权的用户使用；
– 在技术上可行的范围内，防范未经授权用户的允许而重新激活手机；
– 如果是授权用户找回了智能手机，扭转不可操作性，并在可行的最大范围内恢复用户的数据。
– 提供丢失或被盗移动设备的位置跟踪信息。

此外，建议教育移动设备用户如何配置和使用这一功能，并向其服务提供商、相关警察或司法机构报告丢失/被盗的移动设备，以便防止该设备访问移动网络和便于执法机构采取适当的行动。

7.2 防止被盗的移动设备接入网络

需要实施解决方案以防止被盗的移动设备接入移动网络，最好是通过可审核的自动化系统来实施。

要求只有得到授权的人员（例如，设备的合法所有者）才能请求在该国的所有网络中纳入或移除被盗的移动设备。

建议制定防止被盗设备在网络上使用的政策框架。

值得注意的是，在移动网络上被阻断的设备使用其唯一标识符仍可以接入不查验这些唯一标识符的网络，例如Wi-Fi网络。因此，诸如第7.1节中提到的用于补充这个方法的措施就很重要了。

7.3 防止使用带有篡改和/或克隆的唯一标识符的移动设备

要求实施可以识别带有篡改和/或克隆的标识符的移动设备的解决方案，这种方案应具有极大的精确性，可以将带有篡改和/或克隆的标识符的移动设备与正版设备区分开来，以便可以采取破坏性行动，这个进程最好通过自动化系统进行，且不会对正版设备产生影响。

建议解决方案中包括参考数据库，以便识别正版设备中的信息及其合法来源。国家的注册数据库用于识别合法进口和购买的设备，与分配给制造商的标识符和设备的其他特征有关的数据库可作为参考数据库的信息来源，以便有助于区分正版设备和被篡改过的设备。

要求在此解决方案中考虑，在检测和控制过程中需要解决各种不同类型被篡改过的信息，例如：无效的标识符、克隆的标识符、（若适用）未经类型核准或未在国家参考数据库中注册的标识符。

7.4 防止其他国家的被盗移动设备接入网络

建议当地法律法规促进各国政府和运营商之间的协调和信息共享，以防止被盗设备（无论在何处被盗）的再次使用。

如果不鼓励、不促进国际上的数据共享，就是允许被盗设备的非法国际贸易继续不受遏制地进行，从而导致在某个国家被盗的设备被出口到其他国家或地区并销售。

为研究解决这一问题，建议建立一个世界各地的服务对象均可访问的全球被盗设备数据库，以便报告被盗设备和检查被盗设备的状态。

各国的国内设备黑名单应该与国际社会交换并向其提供，可以通过将本地的被盗设备数据与全球被盗设备数据库连接和交换来实现。

7.5 减轻对消费者的影响

在采取任何打击使用被盗移动设备的解决方案时，应该考虑对消费者的影响。当可以采用多种与消费者有关的方法来实现同样的目标时，采用能并减轻对合法消费者总体影响的方法。

建议对在网络中新激活的带有无效的标识符的设备进行控制，并事先通知用户，为他们提供充分适当的时间，使其可以提供合法购买的证据，并减轻或避免设备突然被拒绝服务产生的影响。

建议对于标识符被篡改和/或克隆的设备，在采取控制措施时，避免阻止用户的订阅服务。

建议以各种方式公开传播教育和宣传运动，以说明应采取的措施和目的、收益，以及用户在手机丢失或被盗、或当购买了被篡改或克隆的标识符的设备时可以选择的选项和行动。

建议在对被篡改和/或克隆的标识符的设备采取措施时，应考虑赦免或过渡期措施，因为这些已在使用的设备也有可能是用户出于善意而购买的，而用户并不知道这些设备的风险。如果决定不阻断这些已使用的设备，则应采取其他额外措施以避免这些设备被新用户激活。

建议确定有效的方法，接受用户的举报和信息，并采取暂停服务和阻断设备标识符的行动。

建议在不要求用户记住或寻找标识符的情况下，为确定要被阻断的设备标识符提供便利。例如，可以在运营商的网络中查找设备的通话记录活动，以确定丢失/被盗的标识符。

建议暂停服务和阻断丢失/被盗设备的标识符要尽量迅速。例如，负责阻断设备的利益攸关方只要确认了请求，就立即阻断设备。

要求为所有的利益攸关方提供检查和验证设备是否已被阻断的工具。

建议负责阻断设备的利益攸关方在阻断设备时要回应用户的问询，或者在拒绝一个请求时，向用户提供原因，解释为什么不会阻断已举报的设备。

7.6 保护消费者私人数据

如果设备丢失或被盗，消费者的私人数据应该得到保护。作为主要措施，建议实施一些机制以禁止设备的运行，包括禁止未经授权的用户获取设备上保存的私人数据。

建议教育消费者提高对保护和备份其个人数据重要性的认识，并学会如何使用设备上的功能使他们能远程删除被盗设备上的个人可识别信息（PII）。

建议制造商在所有的新设备上默认包括[ITU-T X.1127]建议书中的功能。

建议利益攸关方对消费者进行有关如何配置和使用此功能的教育。

7.7 防止被盗的移动设备进入市场

建议国家电信监管机构与其他有关国家机构（例如海关）开展协作，以改进对在本国和其他国家报告丢失的或被盗的设备的控制。

作为此项协作的一部分，应酌情考虑以下内容：

1) 访问被盗设备数据库，但是由于可以通过修改唯一标识符绕过国内和国际被盗设备数据库，还需要更多信息（例如无效的、非型号核准的设备）。
2) 访问分配给合法制造商的全球标识符数据库，以验证标识符的结构是否属于要进口的设备。
3) 根据相关国家法规，访问已获型号核准的设备品牌和型号列表，以便允许仅进口获得型号核准的设备型号。

4) 访问国家参考数据库，其中记录了合法进口和购买的设备的标识符（如果适用）。

5) 访问全球被盗设备数据库以及访问能提供用于确认设备合法性的设备特定信息的数据库。特定信息数据库的意义在于，当被盗设备的唯一标识符可能被代表另一台设备的标识符进行了修改和重新编程的情况下，其能发挥识别作用。

建议仔细查验国家设备数据库内全部的标识符，以避免登记一台设备的标识符时，该标识符属于已进入该国的另一台设备。

建议对出售被盗设备的销售点采取法律行动。

7.8 解决篡改被盗移动设备唯一标识符的其他考虑因素

解决篡改被盗移动设备的其他考虑因素包括：

– 考虑制定政策框架，防止被篡改的被盗移动设备在市场上使用或出售。

– 提供与盗窃和篡改移动设备唯一标识符有关的技术方面的教育和培训。

– 考虑对用于篡改移动设备标识符的硬件和/或软件的使用进行控制。

建议制定法律依据和支持，以允许执法机构对那些改变、修改、更改、擦除或篡改移动设备标识符的人进行处罚，以防止其绕过阻断被盗设备进入市场的行为。

建议这种法律框架还应涵盖可对提供、拥有、进口或出售用于篡改移动设备标识符的硬件和/或软件的人员采取的行动。

建议对执法机构进行有关盗窃和篡改移动设备唯一标识符的技术方面的教育和培训，以及起诉相关罪行的法律框架的教育和培训。

建议移动设备制造商纳入确保移动设备唯一标识符可靠性和完整性的机制。

8 框架要求

部署解决方案以解决被盗的移动设备时，各国应考虑以下要求：

8.1 集中式参考数据库

建议使用集中式参考数据库来存储丢失和被盗设备的信息。因此，所有运营商都应使用此数据库来防止被盗设备接入任何移动网络。该数据库至少应该包含被盗设备的唯一标识符、事件的日期以及将信息录入数据库的实体。

建议这种数据库还包括其他类型的标识符和信息，以帮助识别和处理篡改过标识符的被盗设备。

建议在此参考数据库中包含与合法进口和/或购买的设备有关的信息。

建议授权实体可以访问所有相关数据库。

建议实施强制性设备注册。在实施强制性设备注册时，在将设备与个人可识别信息关联时应格外小心，并注意对合法移动设备的贸易和移动市场竞争产生副作用。

建议实施审核程序，以验证举报的被盗设备是否已被阻断，以及所有利益攸关方是否都采用了正确的程序。

8.2 网络支持阻断设备

要求移动网络应包含能够阻断有效标识符被列入黑名单中的被盗设备接入的元素，以及那些传输标识符格式不符合唯一标识符[1]标准的设备的元素。

建议在移动网络中使用的阻断解决方案应支持避免使用带有克隆的唯一标识符的设备的功能，从而鉴别出正版设备来[2]。

8.3 可靠的唯一标识符

建议用于防止被盗移动设备接入移动网络的参考数据库应基于可靠的唯一标识符（RUI），因为篡改设备唯一标识符可能会对旨在从市场上清除被盗设备的解决方案的效率产生负面影响。

建议移动设备将此唯一标识符存储[3]在设备内的安全元素中，并且设备应在技术上可行的范围内实施安全措施，以检测对安全元素或存储在其中的信息的篡改，以便设备在恢复原始数据之前，无法使用。

建议负责这些唯一标识符的管理实体实施一项程序，以鼓励已向其分配了标识符的合法设备制造商正确、安全地使用唯一标识符。

建议唯一标识符遵循完整性原则（任何制造商都必须从指定实体分配标识符范围）和行业定义的安全原则（所有设置的旨在以无法篡改的方式实施标识符的措施或这些措施的组合）[4]。

建议行业实施这些原则的过程应得到政府或国家法规框架的支持。

即使在维护服务期间，也要求唯一标识符不可重新编程。在制造过程之后允许更改标识符可能会降低唯一标识符的安全性，从而使其受到未经授权的第三方的篡改。

8.4 与执法机构及其他国内机构的紧密协作

为有效地限制被盗设备在市场上的流通，要求在负责维护和提供参考数据库的实体、国家海关机构之间以及在来自不同国家的这些实体和相关利益攸关方之间建立紧密的协作。请考虑以下做法：

---

1 见关于符合3GPP/3GPP2标准的设备的[b-3GPP TS 122.016]和[b-3GPP TS 123.003]标准。

2 对于符合3GPP/3GPP标准的设备，但使用IMEI作为唯一标识符时，从无线接入网到核心网的IMEI-IMSI的检查有助于满足此要求。

3 例如，3GPP TS 122.016规定IMEI不得被改变。

4 例如，请见3GPP兼容设备的IMEI安全设计原则[b-IMEI-SEC]。

– 鉴于海关机构和其他相关的国家授权机构在监视和拦截被盗、丢失、被篡改的产品中发挥着关键作用，因此重要的是给他们提供工具来识别被盗、丢失、被篡改甚至是合法的设备，例如集中式参考数据库。
– 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：与国家、区域或国际标准一致的移动设备数据库；
– 可以通过采用机制来验证单个设备的身份，以检查该设备是否为正版设备以及该国的法律和法规是否允许使用该设备，来打击被盗移动设备的非法交易。
– 执法机构根据国家法律框架，出于调查目的，可以选择不立即阻断设备，以识别在市场上出售的被盗设备的来源，尽管应优先考虑尽快阻断所有设备，除非在个别情况下，有这样做的有效和特殊理由。

建议高层领导战略来自政府高层，以推动联盟和全面措施的实施，以促进业界以外的不同部门和管理机构（例如执法、海关、商务等）的承诺和执行活动。

8.5 检查移动设备状态的工具

要求为消费者和其他利益攸关方提供一个公共工具，以检查移动设备的状态。消费者和其他利益攸关方应该能够（最好使用互联网）检查某些设备是否被标记为被盗或丢失。

建议在对设备检查的答复中列出负责阻断设备的实体（包括实施阻断的国家/地区），避免消费者有可能采购到或购买到被盗设备，如果由具有相同标识符的克隆设备导致不正确的阻断或第三方阻断，还需解决投诉。而且，这是消费者进行购买前检查的重要工具。

建议零售商和参与处理设备的实体对其购买的设备进行检查，以确保这些设备没有被报告丢失、被盗或具有重复的唯一标识符。应保存记录，以证明已进行尽职调查，以降低对被报告丢失、被盗或具有重复的唯一标识符的设备进行交易的可能性。

8.6 支持适用的国家法律和监管框架

建议在具备技术能力的情况下，开发各种机制在移动网络中识别和阻断丢失和被盗的设备以及被篡改了独特标识符的设备。应该与本地移动网络运营商进行核查。

建议在对具有篡改和重复的唯一标识符的被盗设备采取任何限制性措施之前，先获得适用的国家法律和监管框架的支持，其中包括：

– 限制在国内或其他国家报告被盗设备在电信网络上的网络接入；
– 限制标识符被篡改的设备在电信网络上的网络接入；

– 限制篡改移动设备唯一标识符以及篡改的后果；
– 确立必要的解决方案，帮助管理机构、消费者和销售渠道区分正版设备和被盗篡改设备；
– 拥有负责执行上述要点的机构。

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 参考框架

根据第8条概述的框架要求，图1描述了打击移动设备盗窃和使用被盗移动设备的建议参考框架。必须指出的是，图1中描述的功能要素并非都是必需的，每个国家可根据其需要实施这些要素。

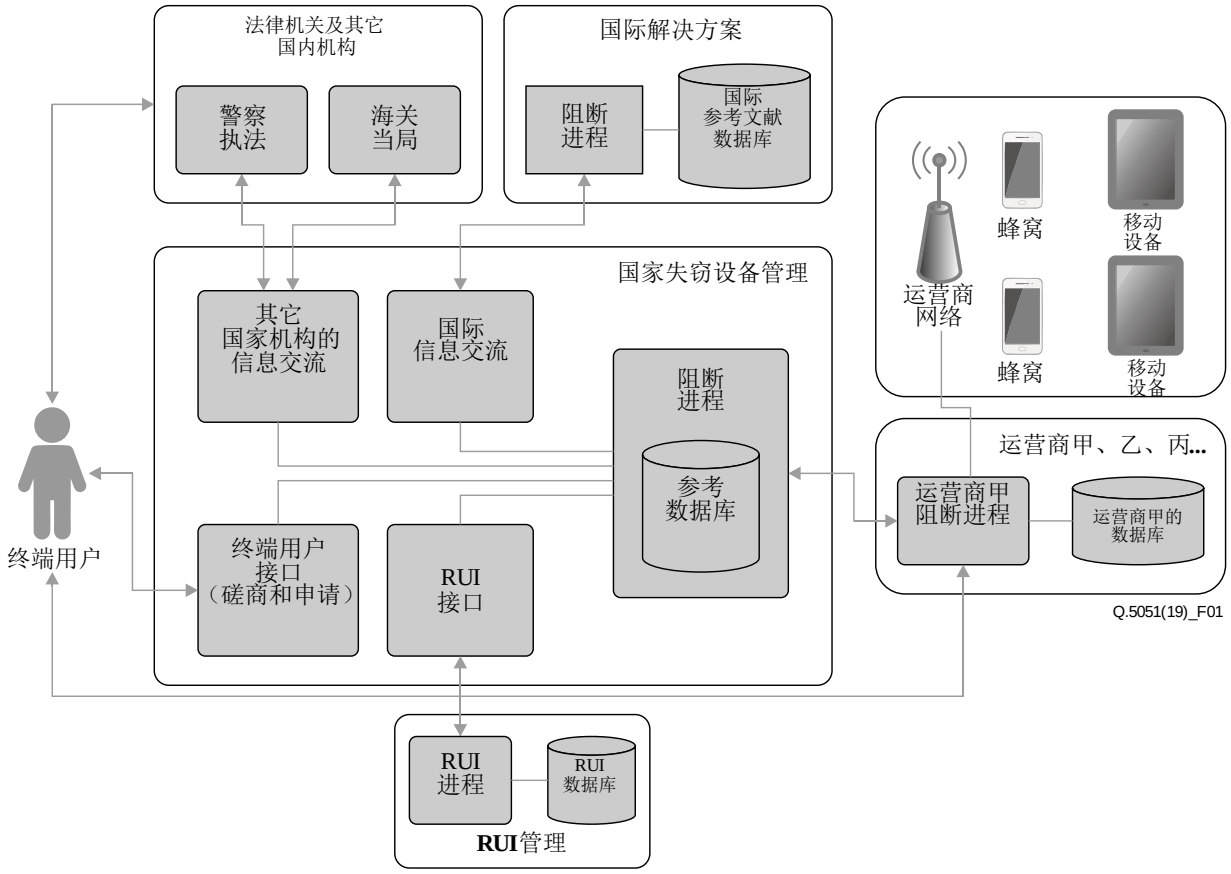

图1 – 建议的一般性框架

由不同组织开展的各种各样的活动和运营的信息系统，应共同控制和产生关键信息，以识别和打击丢失、被盗的移动设备以及带有无效的标识符的移动设备的使用。

消费者和其他利益攸关方应该能够检查某个设备是否标记有任何限制（被盗、丢失或带有无效的标识符）。

可以通过不同的利益攸关方（消费者、执法机构、移动运营商或直接向中央系统）提交阻断被盗设备的请求。无论在何处提交阻断使用设备的请求，都应采取措施来验证用户身份以及设备所有权。对于那些尚未出售给消费者的设备，例如那些在运输途中、从零售店等地方被盗的设备，在请求阻断该设备的同时，应附上法律声明。

为了限制被盗设备在市场上的流通，其他相关的国家机构（例如，执法和海关机构）应具有使用所有可用参考数据库和来源检查设备状态的能力。

与国际实体的交流也很重要，可以在双边基础上或通过全球参考数据库进行。

为了确保有效阻断国家移动网络上的被盗设备，所有运营商都应与国家和全球参考数据库同步。

要求将RUI管理与被盗的移动设备阻断进程整合在一起，因为存在通过篡改某些设备的唯一标识符绕过阻断进程的可能。

要求实施一种进程，以识别和控制网络上具有无效的标识符的移动设备，这可能是由于被盗设备被阻断后对其进行篡改而导致的。

10 期望的特性

在部署解决方案以打击被盗移动设备的使用时，各国应考虑以下期望的特性：

10.1 丢失和被盗设备全球参考数据库

由于被阻断的设备可以运输或甚至出售给不同国家的消费者，因此建议使用全球参考数据库来共享和阻断丢失和被盗的设备标识符，以便在单个信息点中将被盗的设备列入黑名单，有助于共享并减少阻断时间。

建议不管运营商的规模如何，都应阻断具有此全球参考数据库中的标识符的所有设备连接到本地网络，但是，可以根据每种实现方式的特定环境考虑替代方法（例如，比照全球参考数据库，对激活的唯一标识符进行批处理）。

要求全球参考数据库可用于执法机构和其他政府机构，以报告和查询标识符组，以促进其在打击移动设备盗窃中的法律行动。

建议针对要报告的被盗设备的准确性，对要报告给全球数据库的信息进行验证。仅在进行此类验证之后，才应提供由上述各方汇编的被盗设备列表，以将其包含在此全球被盗设备数据库中。

该全球数据库应该可供世界各地的所有利益攸关方使用，以验证某设备是否为已报告被盗的设备。可以在系统级别（可以阻断设备的组织）以及在消费者级别（来自任何国家的消费者都应能够检查该设备是否为被盗设备），都可以访问数据库。

如果可以，全球数据库应提供适当的信息（例如，设备特征、设备被盗的国家/地区，事件日期等）。如果在多个国家/地区找到被盗的设备标识符，则全球数据库应在其结果中提供该信息。

应实施程序，以便全球数据库的参与者可以解决意外阻止（例如，错误阻断、与重复和克隆的设备标识符相关的阻断）。

10.2 针对销售丢失、被盗或被篡改的设备的机构所采取的措施

建议各国考虑一个框架，确立销售点仅仅出售经型号核准的设备的责任以及提供被盗设备或标识符被篡改的设备的后果。这将使执法机构获得法律支持，以打击对这些设备的买卖。

可以在国家参考数据库中包含合法进口和出售设备的标识符。该数据库可以协助各种国家执法行动和活动，例如进口、销售、在网络中使用以及执法机构的行动等。

因此，这可以帮助执法机构访问授权设备的数据库，以对向公众提供被盗、被篡改或克隆的设备的企业采取行动，甚至可以识别和拦截非法进口的产品。

附录一

GSMA打击移动设备盗窃的方法

（本附录不构成此建议书的组成部分）

在越来越多的国家/地区，运营商允许消费者报告移动设备丢失或被盗的情况。运营商可以建立设备的唯一标识符，即国际移动设备标识（IMEI），继而移动网络运营商可以阻断电话接入其移动网络。这被称为列入IMEI黑名单[5]。

作为使用全球数据库的示例，在移动运营商社区中，列入黑名单的IMEI被提供给GSMA的全球IMEI数据库，使运营商可以在国内和国际上交换数据并在多个网络上阻断设备。

GSMA IMEI数据库维护一个全球黑名单，该黑名单是根据参与的运营者提供的数据进行整理的。GSMA将全天候地将黑名单信息提供给已建立与IMEI数据库连接的运营商，供他们下载并在自己的网络中用于设备阻断的目的。参与的运营商选择一个运营商列表，从中获取黑名单数据，这决定了数据共享覆盖范围的实现程度。

对于用户来说，向服务提供商报告设备失踪，无法分清楚设备是丢失或被盗，因此通常在这些状态之间没有区别。如果所有者找到了该设备并将其报告给其服务提供商，则可以解除对设备的阻断，并从IMEI数据库中删除IMEI。然后，GSMA将从黑名单移出的指令发送给已下载原始黑名单记录的已连接的运营商。

由于该全球数据库的性质以及市场上不同利益攸关方对防止设备盗窃的承诺，GSMA开发了一种功能，可以检查IMEI的状态。这称为设备检查，它支持与批准的合作伙伴（包括零售商、保险公司、回收商和执法机构）共享数据和设备状态信息。

使用此系统，感兴趣的利益攸关方可以支持查明设备是否已被报告丢失或被盗，并提供设备历史记录以及设备型号信息和功能。这种检查能力可带来许多好处：i）帮助经销商在被盗设备进入供应链之前识别并排除这些设备；ii）确认真实设备型号的真伪并帮助计算设备价值；iii）通过降低被盗设备的价值来防止设备被盗；iv）确认报告该设备被盗或丢失的网络运营商，这有助于将其归还给合法所有者。

除了网络运营商外，移动设备生态系统中的许多其他组织都可以使用设备检查服务，其中包括：i）设备回收商、零售商和经销商，它们使用这些数据来减少被报告为被盗、丢失的设备进入回收、转售渠道的可能性；ii）保险公司依靠数据库减少丢失/被盗设备的虚假或夸大的保险索赔；iii）执法机构使用它来识别和协助调查和/或遣返被盗或丢失的货物[6]。

可以通过诸如提供本地语言的国家主管部门和允许执行IMEI查找的托管门户等实体提供服务的方式，向包括消费者在内的一系列其他利益攸关方提供查询全球IMEI数据库中的单个标识符的权限。当前仅向能够明确为其客户标识和证明IMEI数据的网络运营商授予向黑名单提交条目和/或从黑名单中移出标识符的访问权限，从而维护黑名单的完整性。正在考虑将对编写黑名单的访问权限扩展到可以证明并担保其将阻断IMEI的其他方，例如设备制造商、零售商等。

---

[5] 请见[b-GSMA-IMEI-Blklst]

[6] 请见[b-GSMA-IMEI-DevChk]

与国家数据库相比，上述相关系统（GSMA IMEI数据库和IMEI设备检查）为利益攸关方带来了一系列优势，国家数据库虽然分散，但可以通过交换和阻止报告为丢失或被盗标识符的双边或多边努力来建设。这些优势包括：a）减少实施和微调的时间；b）减少资本支出（CAPEX）和运营支出（OPEX）成本；c）降低复杂性和更高有效（一个共同的交换点，而不是几个起点和终点）；和d）减少信息复制。这些项目基于所引用系统的以下特征：a）模块化，b）运营商/政府无连接费；c）IMEI数据库是自1996年以来一直存在的成熟且稳定的技术平台。

参考资料

[b-ITU-T X.Sup.19] ITU-T X-系列建议书 – 补充19（2013年），智能手机安全方面的补充。

[b-IMEI-SEC] GSMA（2016年），IMEI安全涉及原则 – 支持被盗移动设备阻断功能（4.0版）
<https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01)，数字蜂窝电信系统（第二阶段+）（GSM）；通用移动电信系统（UMTS）；国际移动设备标识（IMEI）（*3G TS 22.016 version 3.1.0 Release 1999*）。

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04)，数字蜂窝电信系统（第二阶段+）；通用移动电信系统（UMTS）；编号、寻址和识别（*3GPP TS 23.003 version 10.5.0 Release 10*）。

[b-GSMA] GSMA，正式文件SG.24（2016年），防盗设备功能要求（3.0版）。

[b-GSMA-IMEI-Blklst] GSMA服务，IMEI黑名单
<https://www.gsma.com/services/gsma-imei/imei-blacklisting/>（2020年4月13日最后一次访问）

[b-GSMA-IMEI-DevChk] GSMA服务，设备检查。
<https://www.gsma.com/services/gsma-imei/about-device-check/>（2020年4月13日最后一次访问）

ITU-T 系列建议书

A 系列	ITU-T 工作的组织
D 系列	资费及结算原则和国际电信/ICT 的经济和政策问题
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	视听和多媒体系统
I 系列	综合业务数字网
J 系列	有线网和电视、声音节目及其他多媒体信号的传输
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	测量设备技术规程
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，以及相关联的测量和测试**
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
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	电信系统中使用的语言和一般性软件情况

瑞士印刷
2020年，日内瓦