国 际 电 信 联 盟

ITU-T X.1812

(05/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

IMT-2020安全

基于信任关系的IMT-2020生态系统安全框架

ITU-T X.1812 建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
网页安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	**X.1800–X.1819**

ITU-T X.1812 建议书

基于信任关系的IMT-2020生态系统安全框架

概要

ITU-T X.1812建议书确定了国际移动通信-2020（IMT-2020；亦称第五代移动通信）生态系统的利益攸关方，分析他们之间的信任关系，识别威胁并明确各利益攸关方的安全责任，规范了利益攸关方之间的安全边界，并基于这些信任关系建立安全框架。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1812	2022-05-20	17	11.1002/1000/14808

关键词

生态系统、框架、IMT-2020、信任

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，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、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已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

1 范围 1
2 参考文献 1
3 定义 1
3.1 其他地方定义的术语 1
3.2 本建议书定义的术语 2
4 缩写和首字母缩略词 2
5 惯例 3
6 概述 4
7 可信任模型支持的安全框架 5
8 利益攸关方在IMT-2020生态系统场景中的角色 6
8.1 总述 6
8.2 场景1：网络运营商域中的虚拟化网络部署 6
8.3 场景2：互联和漫游 8
8.4 场景3：提供远程操作能力的汽车租赁 9
8.5 场景4：向行业开放网络能力 10
8.6 场景5：供应链 11
8.7 IMT-2020生态系统中的利益攸关方 13
9 信任级别、信任标准和信任模型 14
9.1 总述 14
9.2 信任级别 14
9.3 信任的标准 16
9.4 基于信任关系映射的信任模型 17
10 信任关系基础上的信任模型支持安全要求 18
10.1 总述 18
10.2 信任级别的安全要求 18
10.3 将信任解释为详细的保证要求 21
参考资料 23

引言

国际移动通信-2020（IMT-2020；亦称第五代移动通信（5G））系统中的利益攸关方数量比以往通信系统更庞大，也更多样。在第二、第三和第四代（2G、3G和4G）通信系统中，主要利益攸关方可以概括为服务提供商、网络运营商、设备供应商和用户。然而，在IMT-2020生态系统中，工商企业等垂直用户也参与其中。此外，服务提供商可以细分为云平台运营商、数据分析公司、应用提供商等。另外，终端侧用户不像以前那样只是最终用户。签约用户可以包括一系列不同类型的利益攸关方，特别是在商业终端领域，例如在共享车辆通信的使用情景下。这些变化在各利益攸关方之间建立了复杂的关系，并为IMT-2020生态系统提出了一系列新的安全问题。

IMT-2020网络还引入了新功能。例如，在IMT-2020中引入网络虚拟化打破了网络实体之间的固定连接，实现了软件定义的网络。基于服务的架构提供了另一示例。有了这样的架构，IMT-2020网络便可以构建更多与云相关的功能。此外，切片功能可以实现IMT-2020网络与服务之间更有效的合作。

随着时间的推移，越来越多的信息技术（IT）将应用于IMT-2020系统，不仅应用于其服务，还将应用于其网络。IMT-2020网络完全基于互联网协议。该网络的架构规范是基于服务而非参考点，与以前的网络架构一样。信号越来越多地通过互联网而不是专用网络传输。IMT-2020网络中的传输协议由Diameter [b-IETF RFC 6733]变化而来，其受欢迎的程度不如全球广泛使用的超文本传输协议。所有这些变化都将惠及IMT-2020网络和服务的部署和运营。

然而，使用流行的协议和开放的连接环境也会给攻击者带来便利。攻击者不需要花费那么多时间来研究复杂的电信协议，在网络中寻找入侵点可能会更简单。因此，在IMT-2020网络中，假设内部通信可信已不再合理。由此可见，从4G到IMT-2020的变化，打破了网络运营商之间的信任关系。

此外，IMT-2020网络设计更加灵活，可以满足各种服务需求。特别是切片功能已引入IMT-2020网络。IMT-2020网络也可以将一些功能向服务开放。这种能力开放将使IMT-2020服务能够控制一些网络功能。这些新功能将使IMT-2020网络和服务之间的安全边界更加模糊。

本建议书确定了IMT-2020生态系统的利益攸关方，分析了他们之间的信任关系，确定了威胁并明确了每个利益攸关方的安全责任，规范了利益攸关方之间的安全边界，并基于这些信任关系建立了安全框架。

ITU-T X.1812建议书

基于信任关系的IMT-2020生态系统安全框架

1 范围

本建议书为国际移动通信-2020（IMT-2020）生态系统指定了一个基于信任关系的安全框架，描述了实现以下目标的一般方法：

– 确定提供IMT-2020业务的方案；

– 确定IMT-2020生态系统中的利益攸关方；

– 分析利益攸关方之间的信任关系；

– 确定适用于每个利益攸关方的威胁；

– 澄清每个利益相攸关方的安全责任；

– 规范利益攸关方之间的安全界限；

– 规范基于信任模型的安全需求；和

– 建立基于利益攸关方之间信任关系的安全框架。

2 参考文献

下列ITU-T建议书和其他参考文献包含的条款，通过本文的引用构成本建议书的条款。在出版时，所指示的版本有效。所有建议书和其他参考文献均可能进行修订；因此，鼓励本建议书的用户研究应用建议书最新版本和下面列出的其他参考文献的可能性。定期发布当前有效的ITU-T建议书清单。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

无。

3 定义

3.1 其他地方定义的术语

本建议书使用了其他地方定义的以下术语：

3.1.1 业务单位[b- ISO/TS 21089]：组织内独立且可问责的职能或子职能部门

注 – 业务单位可以包括卫生医疗提供组织内的部门、服务或专业。

3.1.2 部署[b-ISO/IEC/IEEE 24765]：项目过程中系统投入运行并解决切换问题的阶段。

3.1.3 开发者[b-NIST SP800-53]：一个实体，其内部包括：(i)信息系统、系统组件或信息系统服务的开发者或制造商；(ii)系统集成商；(iii)供应商；以及(iv)产品经销商。

3.1.4 域[b-ISO/IEC 14888-1]：在单一安全策略下运行的一组实体。

示例：由一个受权机构或一组受权机构使用相同安全策略创建的公钥证书。

3.1.5 信息系统[b-ISO/IEC 27000]：应用、服务、信息技术资产或其他信息处理组件。

3.1.6 周期[b- ISO/IEC/IEEE 15288]：系统、产品、服务、项目或其他人造实体从构思到退役的演变过程。

3.1.7 网络功能[b-ITU-T Y.3100]：IMT-2020背景下网络中的一种处理功能。

注1 – 网络功能包括但不限于网络节点功能，例如会话管理、移动性管理和传输功能，其功能行为和接口已定义。

注2 – 网络功能可以在专用硬件上实现，也可以作为虚拟化软件功能实现。

注3 – 网络功能不是资源，而是可以使用资源进行实例化的任何网络功能。

3.1.8 利益攸关方[b-ISO/PAS 19450]：对正在设计、开发或部署的系统感兴趣或可能受其影响的个人、组织或群体。

3.1.9 供应商[b-ISO 10393]：提供产品或服务的组织或个人。

3.1.10 系统开发[b-ISO/IEC 2382]：通常由需求分析、系统设计、实施、文件和质量保证构成的过程。

3.1.11 信任度[b-ISO/IEC 25010]：用户或其他利益攸关方对产品或系统将按预期运行的信心水平。

3.1.12 信任级别[b-ISO 28598-1]：客户对供应商满足特定质量要求所提供的事先、补充和间接证据权重的估计。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 外部服务提供商：一组实体，其内部包括a) 组织信息系统所建立安全授权边界之外的组织内实体； b) 该组织以外的公共部门（如联邦机构）或私营部门（如商业服务提供商）实体；或者c)公共和私营部门的某种组合。

注：改编自[b-NIST SP800-53]。

3.2.2 供应链：通过上下游的联系，参与以产品和服务的形式为最终消费者创造价值的过程和活动的组织网络。

3.2.3 系统开发生命周期：规划、创建、测试、部署和维护信息系统的结构化方法。

3.2.4 信任模型：由描述利益攸关方之间信任关系和链的组件构成的模型。

4 缩写和首字母缩略词

本建议书使用以下缩写和首字母缩略词：

2G 第二代

3G 第三代

4G 第四代

5G 第五代

5GC 第五代的核心

BS 基站

CAB 一致性评估机构

E2E 端到端

HO 归属运营商

ICP 互联网内容提供商

ICT 信息通信技术

IMT-2020 国际移动通信-2020

IoT 物联网

IoV 车联网

IPX 互联网络分组交换

ISP 互联网服务提供商

IT 信息技术

NE 网元

NESAS 网络设备安全保证方案

NF 网络功能

NFV 网络功能虚拟化

NPN 非公共网络

PII 个人可识别信息

PLMN 公共陆地移动网络

SCAS 安全保证规范

SDL 安全开发生命周期

UICC 通用集成电路卡

VNF 虚拟化网络功能

VO 被访运营商

5 惯例

在本建议书中：

短语“**建议**”（is recommended）指的是一项建议性的、并非绝对需遵守的要求，因此，宣称遵循本建议书时无需提及该项要求。

短语“**可选**”（can optionally）指的是一项允许的可选要求，不隐含任何建议的意味。本术语无意暗示供应商的实施方案必须提供选项，以及网络运营商/服务提供商可以选择启用该功能。相反地，本术语意味着供应商可以选择提供该功能，并仍宣称遵循本建议书。

6 概述

5G时代前，电信系统主要用于提供电话、互联网接入和相关服务。由于这些系统的能力和速率限制，相关使用案例通常很简单，特别是通信系统中只涉及少量角色。呼叫业务涉及的参与方为主叫方、被叫方和移动网络。数据业务的参与方为终端、移动网络和服务或应用提供商。此外，为支持网络和应用系统的构建，供应商也参与其中。终端制造商和通用集成电路卡（UICC）提供商与终端息息相关。这些是2G,、3G和4G电信系统中涉及的主要参与方。

然而，IMT-2020生态系统的情况有所不同。生态系统不仅包含电信系统在终端、网络和服务领域的所有利益攸关方，还包含其他利益攸关方。在终端方面，由于移动设备可以是多方共享的诸多不同类型设备之一，而不仅仅是电话，因此签约用户不像以前一样仅仅是终端用户。在网络方面，IMT-2020引入了一系列新功能。例如，IMT-2020中的网络虚拟化打破了网络实体之间的固定连接，实现了软件定义的网络，突破了网络部署的安全边界。越来越多的信息技术（IT）手段被应用于IMT-2020网络，这些技术亦可能被攻击者利用。网络开放业务在控制平面而不是用户平面为攻击者打开了接口。网络服务涉及垂直参与方，比如工商企业，将服务提供商分为云平台运营商、数据分析公司、应用提供商等（如图1所示）。

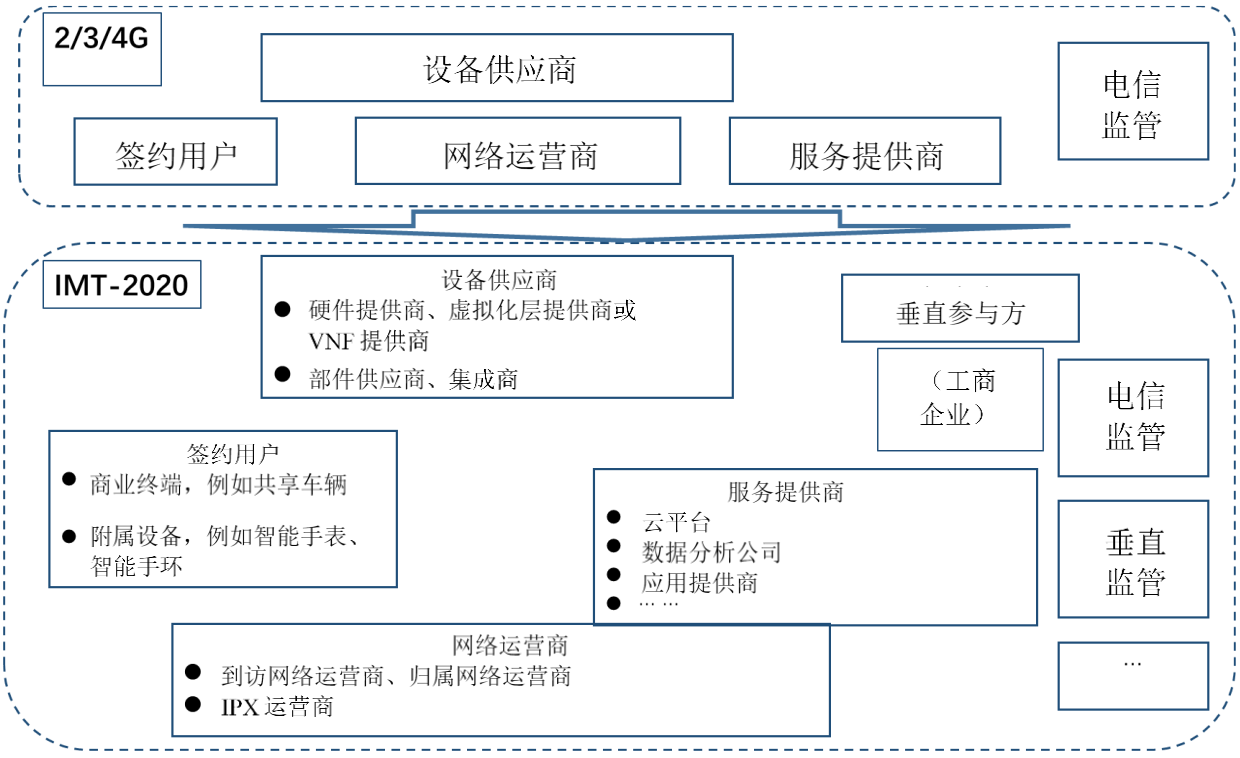


图1 – 从2G、3G、4G到IMT-2020的生态系统演变

在这种情况下，IMT-2020系统的信任关系是不同的。用户或签约用户和网络或业务系统之间的关系比以前更加紧密。复杂的长尾供应链推动运营商更多地考虑对供应商的评价。业务和网络之间的紧密联系使得垂直行业对网络的依赖性很强，需要更严格的信任和安全性要求。相关方需要考虑为IMT-2020生态系统提供一个新的信任模型，以确定利益主体之间的明确安全要求和安全边界。这样，在保证数据安全的情况下，可以尽可能地提高通信效率。

共有五种属性，即快速恢复能力、通信安全、身份管理、个人可识别信息（PII）保护和安全保证，会对IMT-2020系统的可信度产生影响。

- 快速恢复能力：快速恢复能力是指某组织抵御网络中断所产生影响的能力。IMT-2020中各种互补和部分重叠的功能，有助于实现IMT-2020系统对网络攻击和非恶意事件的快速恢复能力。
- 通信安全：通信安全在IMT-2020中应用于数据通信。在IMT-2020系统中，设备及其自身基础设施的安全通信至关重要。
- 身份管理：身份管理系统由管理组成IMT-2020系统实体身份属性的生命周期、值、类型和可选元数据的过程及策略组成。无论是否漫游，均应为识别和验证用户提供安全的身份管理，建议确保只有真正的用户才能获取网络服务。此类系统是建立在强大的加密原语和安全特性之上。
- PII保护：数据隐私在[b-ISO/TS 21719-2]中定义为个人和组织在收集、使用、保留、披露和处置个人信息方面的权利和义务。PII的保护职能包括保护PII不被未经授权方用于识别用户。
- 安全保证：安全保证为相信已经或将满足安全目标的理由提供了依据。安全保证是确保网络设备满足安全要求的一种手段，通过安全开发和产品生命周期流程实现。

7 可信任模型支持的安全框架

本建议书通过剖析几个典型场景，分析并确定利益攸关方在IMT-2020生态系统中的角色以及角色之间的信任关系。然后，尝试确定要考虑的关键因素的信任级别。在此基础上，本建议书给出了如何基于信任级别确定安全需求的建议，并形成了基于信任关系的安全框架，如图2所示。

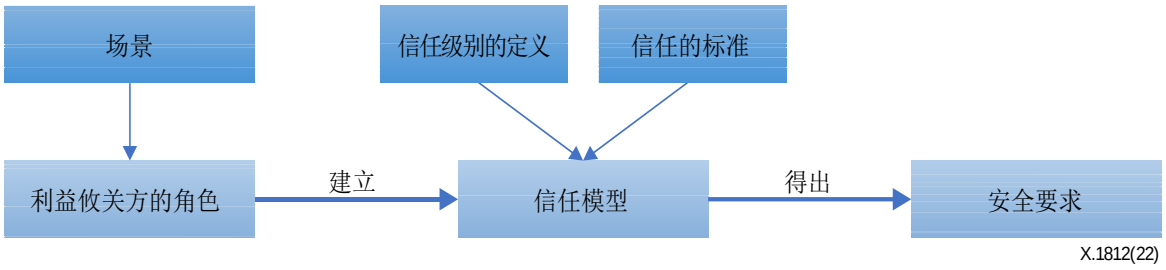
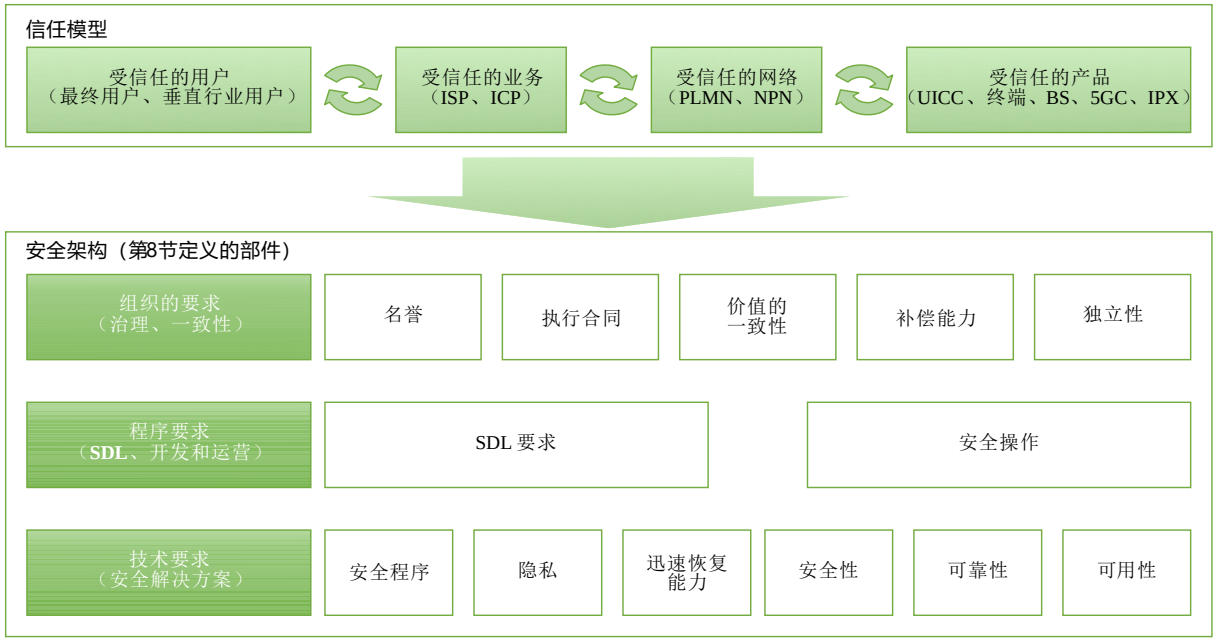


图2–为IMT-2020生态系统构建基于信任关系的安全框架的途径

基于所有利益攸关方的角色和关系、信任模型和安全要求，本建议书中建立的信任模型所支持的安全框架如图3所示。框架中的所有组成部分均在以下章节中进行了描述：第8节利益相关方的角色；第9节信任模式；以及第10节安全要求。



X.1812(22)

图3 -基于利益攸关方之间信任关系的受信任模型支持的安全框架

5GC：第五代通信的核心；BS：基站；ICP：互联网内容提供商；ISP：互联网服务提供商；NPN：非公共网络；SDL：安全开发生命周期

8 利益攸关方在IMT-2020生态系统场景中的角色

8.1 总述

当前的电信系统可细分为三个子系统：终端、网络和服务。有必要考虑每个子系统之间以及子系统内部可能存在的关系。由于第三代合作伙伴项目（3GPP）等其他标准组织已研究过终端 - 网络关系，所以本节中不再进一步阐述。

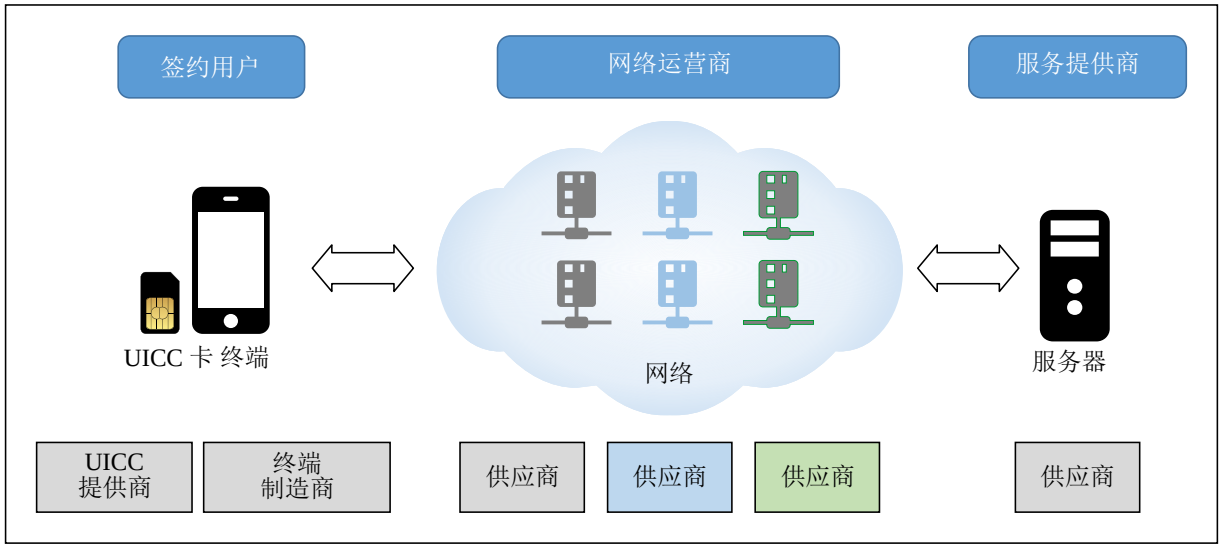
总体而言，本节涉及的五个场景涵盖了除终端-网络关系之外的所有可能存在的系统间关系。

8.2 场景1：网络运营商域中的虚拟化网络部署

8.2.1 总述

此场景主要关注内部网络的关系。

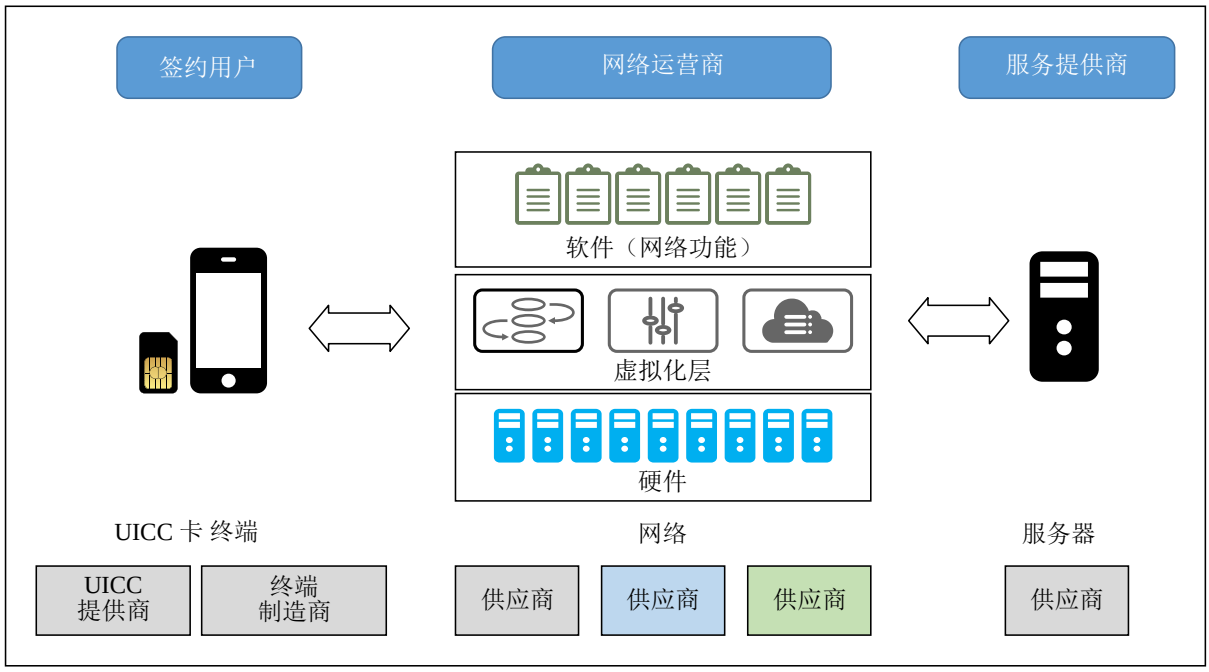
在当前的电信网络中，部署在网络中的网元（NE）通常作为专用物理设备。每个网元根据其能力，作为一个或多个物理实体服务器。电缆、光纤、交换机和路由器用于通过物理接口连接这些网络设备。在这种情况下，主要利益攸关方为：用户或签约用户；移动终端制造商；UICC提供商；网络设备供应商和运营商。如图4所示。



X.1812(22)

图4 - 网络运营商域的主要利益攸关方

在IMT-2020中，软件定义网络/网络功能虚拟化技术得到了显著发展，并已逐步开始在网络中部署。随着信息技术使用的增加，电信网络也在发展。在设计IMT-2020网络架构时，引入了一种新颖的基于服务的架构，以便更好地利用IT进行部署和维护。网元被操作和维护更加灵活的网络功能（NF）取代。NF可以作为虚拟化网络功能（VNF）实现，甚至可以通过运行在虚拟机上的软件应用程序的形式来实现。这表明网络虚拟化将广泛应用于IMT-2020网络的部署。因此，网络的实现就从原来的软硬件设备集成变成了硬件、虚拟层和NFV的三层组合。所以，该场景中涉及的主要利益攸关方是：用户或签约用户；移动终端制造商；UICC提供商；NE供应商（硬件提供商、虚拟化层提供商、VNF提供商）和网络运营商。图5对此进行了归纳。



X.1812(22)

图5 - 网络运营商域虚拟化网络部署的主要利益攸关方

8.2.2 利益攸关方在此场景中的角色

这些利益攸关方在此场景中扮演以下角色：

- 用户或签约用户：用户或签约用户是电信服务的最终用户，即客户。用户设备由制造商提供的移动终端和卡供应商提供的UICC组成。
- 移动终端制造商：此实体提供与网络通信的用户或签约用户使用的终端。
- UICC提供商：此实体提供可用于表示签约用户身份的UICC。
- NE供应商：此实体提供设备或设备中的组件，这些组件可以组成电信系统或服务平台/系统。

  注 – 如果提供组件，以实体可以进一步分为硬件提供商、虚拟化层提供商或VNF提供商。
- 网络运营商：此实体拥有或控制向用户和服务提供商销售和交付电信服务所需的所有要素。

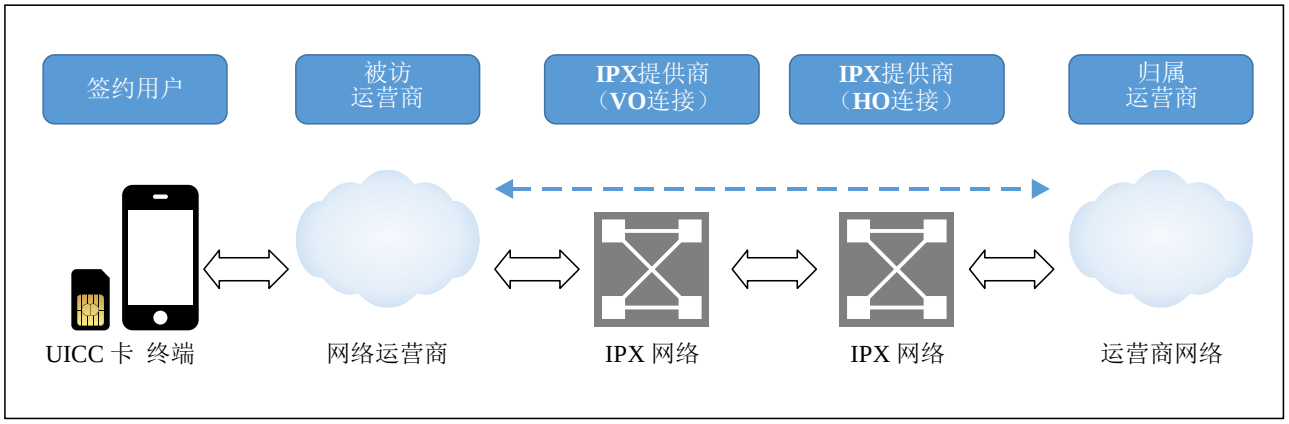
8.3 场景2：互联和漫游

8.3.1 总述

此场景主要关注内部网络的关系。

移动电信网络可在全球运营商间互连和协调的基础上为全球用户提供服务。运营商之间的这种互连和协调涉及服务层和传输层的协调与合作。

到目前为止，公共陆地移动网（PLMN）运营商之间互连的设计原则假设运营商（在服务水平方面）可以完全相互信任，且亦可信任信令和用户数据的传输。为确保向特定运营商正确转发信令消息，引入了网间分组交换（IPX）提供商。然而，随着网络的增长和互联网的使用，IPX的连接变得越来越复杂，也可能受到通过互联网实施的攻击。因此，运营商只能保证与其直接相连的IPX连接的安全性，而不能保证运营商之间的链路以及运营商所有其他链路的安全性。见图6所示。



X.1812(22)

图6 -互联和漫游场景中的主要利益攸关方

HO：归属运营商；VO：被访问运营商

此外，运营商中的许多漏洞也被攻击者发现和利用，使攻击者能够以被攻击设备为跳板对其他运营商发起攻击。因此，运营商也不再信任服务层的消息 [b-3GPP TS 33.501]。

此场景涉及的主要参与方是用户或签约用户、被访运营商、归属运营商和IPX运营商（包括连接被访运营商的IPX和连接归属运营商的IPX）。

8.3.2 利益攸关方在此场景中的角色

这些利益攸关方在此场景中扮演以下角色：

- 用户或签约用户：电信服务的最终用户，即客户。
- 被访运营商：当签约用户在其归属网络运营商的覆盖范围之外时，这些运营商向用户提供接入服务。
- 归属运营商：此运营商拥有签约用户并向他们提供服务。
- IPX运营商（连接被访运营商的IPX，或连接本地运营商的IPX）：此实体提供运营商之间的互联网分组交换服务。

8.4 场景3：提供远程操作能力的汽车租赁

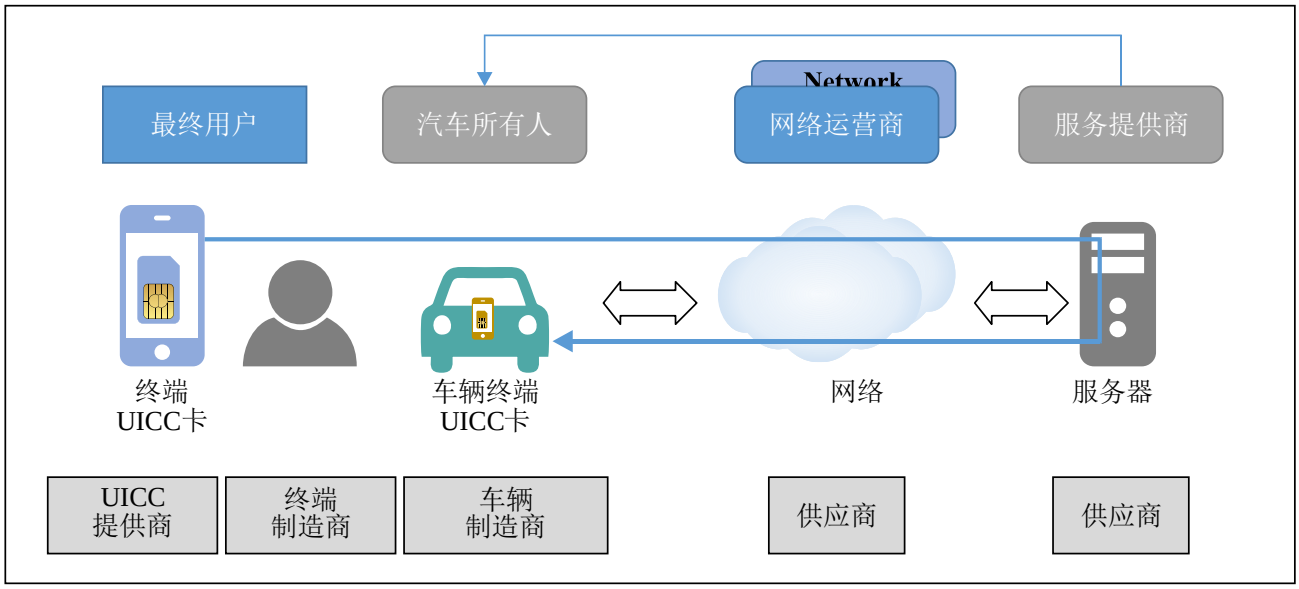
8.4.1 总述

此场景主要关注内部终端之间以及终端与服务的关系。

如今，越来越多的车辆使用内置或后期安装的通信模块与远程平台通信。此类车辆可以将车辆的具体状态上传到远程平台或从远程平台获取指令。在这种情况下，车辆由两部分构成：一部分与电信相关，由终端制造商提供；另一部分是车辆本身，在车辆工厂制造。

传统移动通信网络主要向用户提供语音、短消息或数据网络接入服务。用户是终端的最终用户。对汽车租赁服务而言，使用提供通信终端车辆的司机并非签约用户。另一方面，租车者通常需要使用其移动终端上的应用程序通过通信网络与平台互动，以便远程获取车辆信息或远程操作租赁车辆，例如对车辆进行定位、不用钥匙打开或关闭车门、启动或关闭空调。

因此，在这种情况下，如图7所示，此场景涉及的主要利益攸关方为汽车租赁商、车辆（作为移动终端）、移动终端制造商、UICC提供商、汽车制造商、NE供应商、网络运营商和应用提供商。



X.1812(22)

图7 – 提供远程操作能力情况下的汽车租赁主要利益攸关方

8.4.2 利益攸关方在此场景中的角色

这些利益攸关方在此场景中扮演以下角色：

- 租车方：某用户从租车公司租车，且租车人也是拥有移动终端的移动网络签约用户。
- 车辆：车辆属于特定配置嵌入式移动终端的汽车租赁公司，可将车辆视为网络签约用户。
- 移动终端制造商：此实体提供网络通信用户使用的终端。
- UICC提供商：此实体提供可用于表示签约用户身份的UICC。
- 汽车制造商：此实体生产的车辆可能包含也可能不包含移动终端。
- NE供应商：此实体提供可组成电信系统或服务平台或系统的设备或设备组件。
- 网络运营商：此实体拥有或控制向用户和服务提供商销售和交付电信服务所需的一切要素。
- 应用提供商：此实体为用户提供租车服务应用。

8.5 场景4：向行业开放网络能力

8.5.1 总述

此场景主要关注网络与服务以及内部服务之间的关系。

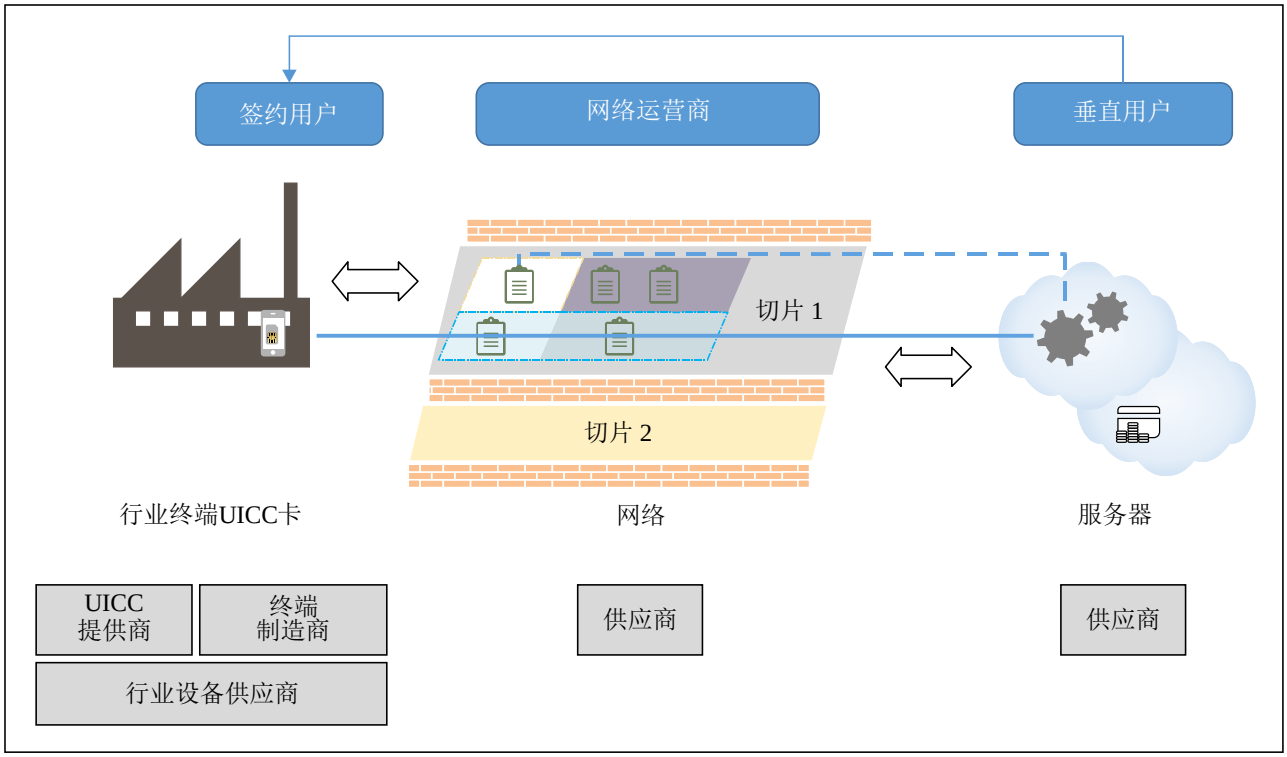
IMT-2020拥有增强移动宽带、海量物联网（IoT）连接、超可靠低延迟通信等新功能。有了这些功能，IMT-2020网络便可以为不同行业等垂直领域提供更好的网络连接支持。

与个人通信相比，垂直行业的传播需求有所不同，如服务多样性、功能差异化、技术异质性等。应用层的垂直通信通常有严格的安全要求，例如与其他行业用户的通信隔离、更多的管理能力或与拥有能力开放等特征的网络运营商协作。

与传统服务相比，垂直行业的服务可能会与网络运营商合作，因此引入了应用提供商，相关的应用服务器提供商或云平台提供商也参与其中。

与场景3一样，终端侧设备也可以包含两部分：一部分与通信相关，由终端制造商提供，另一部分与专门的垂直应用相关，由其他工业终端制造商提供。

在图8所示情况下，场景涉及的主要利益攸关方为：垂直行业用户；通信终端制造商；UICC提供商；工业终端制造商；NE厂商、应用服务器提供商或云平台服务提供商；应用提供商和网络运营商。



X.1812(22)

图8 – 开放网络能力场景中的主要利益攸关方

8.5.2 利益攸关方在此场景中的角色

这些主要利益攸关方在此场景中扮演以下角色：

- 垂直行业用户：垂直行业用户使用在应用服务器或公共或私有云平台上运行的专用应用程序，通过电信网络远程控制行业终端。
- 通信终端制造商：此实体提供网络通信用户使用的终端。
- UICC提供商：此实体提供可用于表示签约用户身份的UICC。
- 行业终端制造商：此实体为工厂或企业交付工业机器、网络或系统。
- NE供应商：此实体提供可组成电信系统或服务平台或系统的设备或设备组件。
- 应用服务器提供商或云平台服务提供商：此实体拥有为上层应用程序提供存储和计算资源服务的基础架构和平台。
- 应用提供商：工厂或企业收集信息或向行业终端提供控制信号。
- 网络运营商：此实体拥有或控制向用户和服务提供商销售和交付电信服务所需的一切要素。

8.6 场景5：供应链

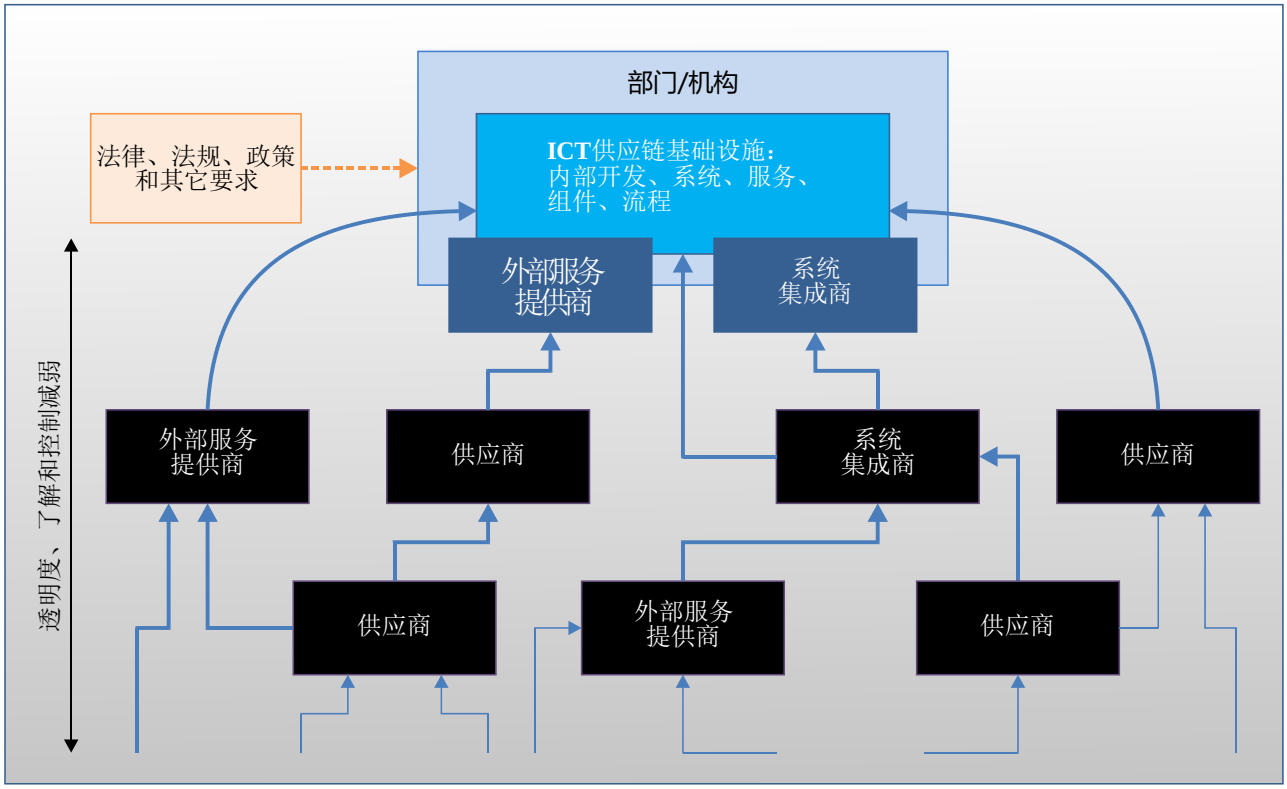
8.6.1 总述

IMT-2020生态系统是指由许多组织组成的社区，这些组织为IMT-2020服务和应用发挥作用贡献了大量的技术和专业知识。

供应链是将产品或服务从供应商转移到客户过程中涉及的组织、人员、活动、信息和资源系统。供应链风险管理是指组织通过协调努力，确定、监控、检测和减轻供应链连续性和盈利能力受到的威胁。IMT-2020生态系统的供应链风险管理有如下四大安全支柱：

- 安全方面：安全涉及信息的保密性、完整性和可用性，这些信息：a) 描述了供应链（例如，关于IMT-2020产品和服务的横向路径信息，包括逻辑和物理路径）；或b) 遍历供应链（例如，IMT-2020产品和服务中包含的知识产权），以及参与供应链的利益攸关方的信息（在整个生命周期中接触IMT-2020产品或服务的任何人）；
- 完整性方面：完整性旨在确保IMT-2020产品或服务在供应链中是真实、未被改变，且产品和服务将按照采购方的规范执行，没有额外不需要的功能。
- 快速恢复能力方面：确保供应链在受到压力和出现失败的情况下提供所需的产品和服务；
- 质量方面：减少可能限制组件预期功能、导致组件出现故障或提供可乘之机的漏洞。

此场景主要关注供应链和相应关系。图9展示了供应链场景中的主要参与方。



X.1812(22)

ICT：信息通信技术

图9 – 供应链场景中的主要利益攸关方

8.6.2 利益攸关方在此场景中的角色

供应链存在几个利益攸关方：开发商或制造商；系统集成商；供应商；产品经销商；提供商和外部服务提供商。

开发者或制造商指：i) 信息系统、系统组件或信息系统服务的开发者或制造商；ii) 系统集成商；iii) 供应商；或iv) 产品经销商。

系统集成商可以是一个人或一家公司，负责将组件子系统整合成一个整体，并确保这些子系统共同运行。此做法称为系统集成。

生产商是向公司或个人提供商品或服务的任何人。生产商通常制造产品，然后将这些产品卖给客户。企业是独立于承包咨询或软件开发等服务公司的法律实体。

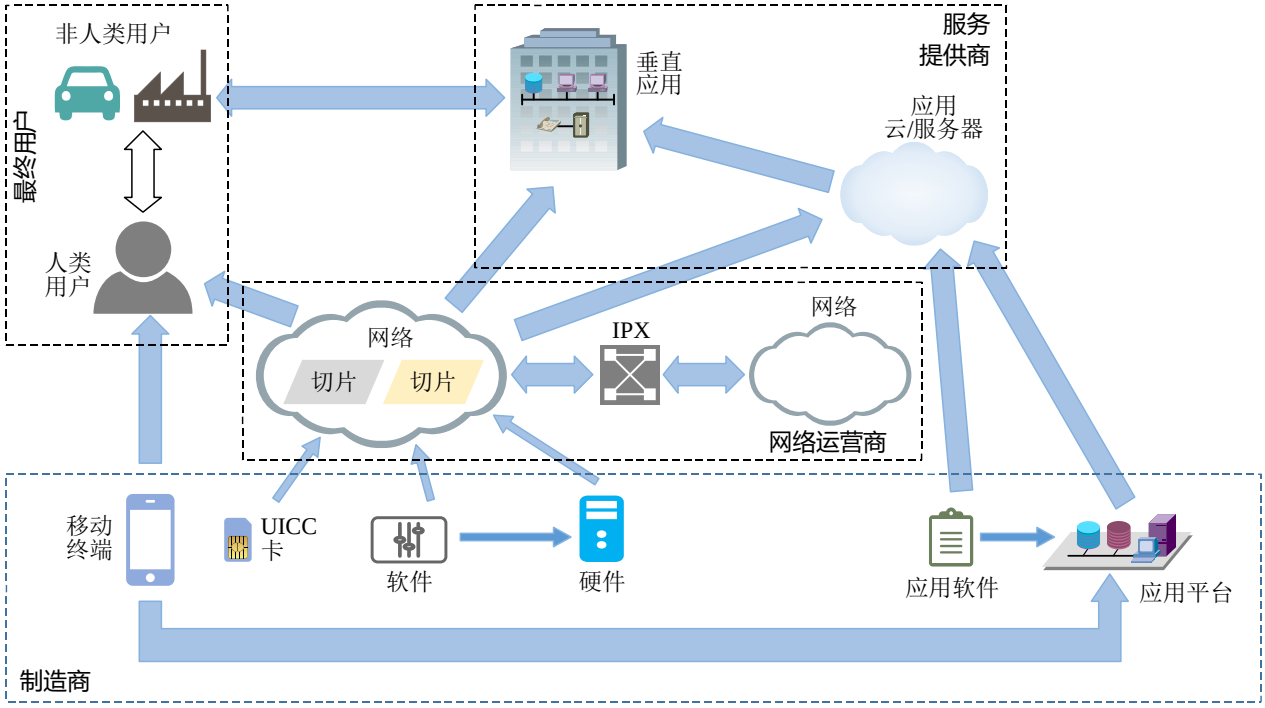
产品经销商是指购买商品或服务的公司或个人，目的是销售商品或服务，而不是消费或使用商品或服务。

供应商是向另一方提供商品和服务的实体。

外部服务提供商是指：i) 组织内为组织信息系统建立的安全授权边界之外的实体；ii) 该组织以外的公共部门（如联邦机构）或私营部门（如商业服务提供商）的实体；或者iii) 公共和私营部门选择的某种组合。

8.7 IMT-2020生态系统中的利益攸关方

基于第8.2到8.6节描述的使用案例，IMT-2020生态系统可以分类为图10中的四种利益攸关方：制造商；网络运营商、服务提供商和最终用户。



X.1812(22)

图10 - IMT-2020生态系统中的利益攸关方

一个利益相关方可能与另一利益相关方有直接关系，例如，作为供应链的一部分。

对于IMT-2020生态系统，制造商可以看作是一组开发人员或制造商、系统集成商和供应商。网络运营商子系统可视为产品经销商和网络服务供应商。服务提供商可视为外部机构。

组件制造商为无线设备制造商和网络设备制造商提供技术构件。此类组件制造商也可以直接向网络运营商提供这种构件。无线设备制造商为最终用户或作为各行业机器的组件提供设备，而网络设备制造商生产支持网络基础设施（包括无线和有线）的设备。网络运营商通过IPX将这些设备、网络组件、网络设备和来自其他运营商的网络结合成一个全球运营网络，为最终用户服务。最终用户通过网络进行语音通话、发送短信和运行应用程序。网络运营商还通过其网络能力开放服务或其他特定服务，为外部服务提供商提供通信和相关服务。

9 信任级别、信任标准和信任模型

9.1 总述

按照第3.1.11节的定义，信任是指用户或其他利益攸关方对产品或系统的预期行为的信心程度。信任在IMT-2020生态系统中也发挥着重要作用。本建议书制定了一个IMT-2020生态系统信任模型，使利益攸关方能够就信任和安全做出合理决策。

这种IMT-2020生态系统信任模型分为三个层次。

- 第一级信任涵盖政府和监管机构提出的信任要求。管理信任的关键因素包括国际标准的采用以及认证的公开透明。
- 第二级信任是满足行业组织的信任要求。此类机构的关键因素包括利益相关方的定义、端到端（E2E）解决方案的所有者、最终市场用户、业务模式、信任级别和信任关系。
- 第三级信任是通过提供基于第一和第二级关键因素的技术解决方案来确保信任。

本建议书侧重于第二和第三个层面，即行业组织和技术解决方案。

IMT-2020网络运营商需要依靠制造商提供的设备或器材建立其网络系统。因此，网络运营商需要相信制造商提供的设备能够满足网络运营商的要求。

服务提供商依靠网络传输信息，因此需要信任网络运营商，以确保数据及时正确地传输。服务提供商还需要依赖制造商提供的设备建立服务，因此亦需信任制造商可提供能满足服务提供商要求的设备。

终端用户需要依赖网络传输和服务应用，因此需要信任网络运营商提供的网络接入合法有效。他们对服务提供商的信任要求相似。

9.2 信任级别

以有意义的方式量化信任本质上很困难。本建议书建立的信任模型引入了信任级别的定性概念，能够对不同信任程度的含义进行推理。

支持IMT-2020的服务在一系列环境中运行，因此有不同的信任要求。例如，不同的垂直行业承载着不同业务，在不同场景下运营，因此信任定位也不相同。此外，有些行业被归为国家关键基础设施的组成部分，如智能电网，而其他行业仅用于汽车租赁等不太关键的日常场景。

如果某特定垂直行业被认为是关键基础设施的组成部分，则显然此行业需要更加相信IMT-2020系统将按照预期运行。换言之，需要为这个行业设定更高的信任度，因为任何损害都会影响国家稳定。另一方面，对于那些失败所产生影响相对较小的行业，只需要级别较低的信任。

例如，窄带物联网IoT服务，如车联网（IoV）、工业互联网、智能电网和自动浇花，每个网络都有不同的信任级别，因为对这些行业遭受的损害对社会或用户有不同的影响。

具体用例的信任级别主要取决于对相关垂直领域的损害对社会和国家的影响程度。这最好由垂直组织决定，因为垂直组织拥有来自多个领域的代表和开展必要分析的专业知识；规范信任级别也是其尽职调查工作的一部分。因此，对于更高信任级别的用例，所涉利益攸关方承担的责任应该更高；换言之，还需要为这些利益攸关方设置更高的信任级别。

对于这里建立的信任模型，建议假设各方的信任级别可以设置为三个定性级别之一：高、中或低。做出这一假设有两个主要原因：

- 首先，给信任级别分配定量数值很可能存在巨大问题，因为没有明显的信任指标（例如，与风险分析不同，该指标可基于发生概率和影响成本评估的年化组合）；
- 其次，这种三级标准已经够用，可覆盖许多现有的用例且在其他地方也被采用，例如，网络设备安全保证方案（NESAS）[b-GSMA FS.13]，[b-GSMA FS.14]，[b-GSMA FS.15]，[b-GSMA FS.16]用于衡量信任要求。

现在问题仍然是确定这三个信任级别的含义，以便可以一致地使用本文中建立的模型。第9.3节给出了旨在确定信任级别的信任标准。

考虑到资产的多样性和特定垂直领域中广泛的部署场景，实际上需要根据背景进一步完善一般信任级别。例如，自动驾驶所需的信任级别显然会因特定的车联网、校园网或宏观网络而异。

以下示例进一步说明了对复杂的、基于特定背景的信任级别规范需求。假设运营商根据定义的信任级别选择网络设备制造商。如果仅规定一个级别，则需根据单个信任级别选择所有网络设备制造商。然而，核心网络比天线等更加敏感、更有价值、更具影响力，因此在典型情况下，核心网络制造商的信任级别需要高于天线制造商。

作为进一步的细化，信任级别是针对业务单元和业务场景分别规范。针对垂直行业，这意味着整个垂直行业的信任级别和特定垂直行业场景的单独规范。两种情况下可能的信任级别组合如表1所示。

表1 – 业务部门以及业务场景的信任级别和关系

业务部门的信任级别	业务场景的信任级别
高	高
	中
	低
中	中
	低
低	低

为了使级别定义更实用、更通用，建议灵活规范组件的信任级别。例如，组件信任级别可以根据资产价值或部署区域加以定义。

具体举例而言，尽管整个智能电网的信任度很高，但在电网内部电缆和电杆不如IMT-2020网络传感器和信号传输基础设施有价值。即使对于传感器和信号传输基础设施，部署在小城市的智能电网网络也不如部署在大都市的电网网络敏感。

表2描述了垂直行业和利益攸关方之间关系可能的信任级别。

表2 – 垂直行业和利益攸关方之间可能的信任级别

系统的信任级别	组件的信任级别	利益攸关方的信任级别
高	高	高
	中	中
	低	低
中	中	中
	低	低
低	低	低

9.3 信任的标准

将信任级别确定为高、中或低需要评估利益攸关方之间的信任关系。任何两个利益攸关方之间的信任关系都受到很多因素的影响，一类利益攸关方与另一类不同利益攸关方之间的信任度也会有所不同。因此，评价标准需要单独规范。

鉴于选择信任级别是为了最大限度地减少潜在威胁和这些威胁风险造成的伤害，此类标准可涉及资产价值、影响范围、影响严重程度和发生风险的可能性，基于风险管理标准，如[b-NIST SP800-30]、[b-ISO ISO 31000]和[b-ISO/IEC 27005]。

- 资产：这一因素的重要性显而易见。资产越重要，就越需要将资产置于利益攸关方的完全控制之下，必要的信任级别也就越高。
- 影响的规模：对于影响大的利益攸关方，范围越大，则失败的影响就越大。因此，如果利益攸关方影响范围较大，则需要较高的信任级别。例如，与销售覆盖广大区域的核心NE供应商相比，运营商应赋予销售覆盖微小区域的小规模小区设备供应商更低的信任度。
- 影响的严重性：对作为关键基础设施组成部分的利益攸关方而言，其损害后果更加严重，因此需要付出更大的努力防止这种损害。这导致在与其他各方互动时需要更仔细评估。因此，关系失败报造成的影响越严重，必要的信任级别就应越高。
- 发生风险的可能性：如果发生的概率较高，更有可能发生风险。

IMT-2020的生态系统非常复杂。不同类别的利益攸关方，例如最终用户、设备制造商、网络运营商和服务提供商，都包含各种具体实例。由于信任是一个主观概念，信任很难衡量和标准化，两个实例之间的信任程度亦有所不同。然而，有必要定义一套涵盖大多数情况的一般信任级别，即：低、中、高，以便为IMT-2020生态系统中的每个实体提供指导。

表3提供了如何基于各种信任标准确定总体信任级别的示例。

表3 – 信任级别标准

总体信任级别	信任级别标准			
	资产价值	影响规模	影响的严重性	发生风险的可能性
高	高	高	高	高
中	中	中	中	中
低	低	低	低	低

使用表3中的映射时，重要的是信任标准风险级别要考虑已经实施或将要实施的风险缓解措施。例如，现有用于高价值互联网的服务均可评估为高价值，如资产价值、影响规模和影响严重程度；此外，从表面上看，鉴于互联网通信协议不包含强大的安全功能，受攻击的可能性也将非常高。表3表明为满足电子商务的需求，互联网中的信任级别需要很高。然而，尽管由于互联网不能保证通信渠道的保密性、完整性或可用性，事实上真实世界的互联网信任度实际不高，但电子商务仍被非常广泛和成功地用于大量交易。

事实上，这种方案之所以可行，是因为数据传输的机密性和完整性风险是通过常规使用传输层安全性[b-IETF RFC 5246]保护通信端点间通信加以解决，因此可被视为第10.2节中规定的安全要求的一部分。

总之，所需信任级别的计算须考虑应用具体风险缓解措施后的实际威胁级别。否则，可能会对设备和服务提供商的信任度提出不切实际的要求，导致成本大幅增加。

9.4 基于信任关系映射的信任模型

为以可互操作的标准化方式建立IMT-2020安全边界和安全措施，有必要适当开发和利用信任模型。为使信任模型有效，需要分析信任关系。

基于第9.2节中确定的因素，双方之间的整体信任关系也是单向而非双向的。各种利益攸关方之间的信任关系分析示例如表4所示。

表4 – 利益攸关方之间的信任关系

主观	客观			
	最终用户	制造商	网络运营商	服务提供商
最终用户		中/低	高/中/低	高/中/低
制造商	–		高	高
网络运营商	低	高/中/低		高/中/低
服务提供商	高/中/低	高/中/低	高/中/低	

IMT-2020生态系统中不同合作伙伴之间的信任关系通常非常复杂。因此，有必要建立一个能够反映这种复杂性的信任模型。换言之，可以细化整体信任关系，以给出子系统级别的信任值。表5给出了一个在子系统级别分析信任关系的示例。

表5 – 制造商子域内的子系统级信任关系

主观	客观			
	芯片组/调制解调器	模块	设备提供商	软件提供商
芯片组/调制解调器		–	–	–
模块	高/中		–	–
设备提供商	高/中	高/中		–
软件提供商	高/中	高/中	高/中	

使用表6中的模型提供一个汽车租赁场景作为E2E示例。

表6 – 租车场景中基于信任关系的信任模型

主观		客观						
		服务提供商（车辆）	租车人	制造商			网络运营商	服务提供商
				终端/UICC	汽车（不包括终端和UICC）	网络设备		
车辆			中/低	中	高/中	–	高/中/低	高
租车人		高/中		中/低	中/低	–	高/中/低	高/中/低
制造商	终端/UICC	–	–		–	–	高	高
	汽车	–	–	–		–	–	高
	网络设备	–	–	–	–		高	–
网络运营商		低	低	高/中/低	–	高/中/低		高/中/低
服务提供商		高	中/低	高/中/低	高/中	–	高/中/低	

10 信任关系基础上的信任模型支持安全要求

10.1 总述

在某特定场景下，系统是由一系列利益攸关方建立的，他们通过提供不同的服务和功能确保系统按照预期的方式运行和工作，给利益攸关方带来益处。这些利益攸关方共同构成了生态系统。

在生态系统运行过程中，可能会出现潜在的威胁和危险，阻碍业务运行。为防止威胁造成伤害，所有利益攸关方都需要以遵守法律和提供采用安全开发程序的安全产品、服务和解决方案的方式，帮助保证生态系统持续运行。

第9节建立的信任模型可以帮助利益攸关方确定基于信任的安全需求。

10.2 信任级别的安全要求

10.2.1 概述

利益攸关方的信任级别可以用于评估利益攸关方是否能够提供适当的损害防御能力。可以通过制定安全要求减轻这种损害。因此，安全要求可以基于组织的能力，包括人员的专业水平、安全开发流程（如安全开发周期）的使用或安全操作程序能力以及与值得信赖的解决方案相关的技术能力。更多详细信息，请参见[b-NIST FICIC]、[b-BSIMM]等标准和实践。见表7。

表7 – 信任级别和安全要求类别

信任级别	安全要求类别		
主观	客观		
	相关组织的能力 （信用良好）	系统开发和产品生命周期安全或安全运营能力 （良好的程序）	与可信解决方案相关的技术能力 （优秀的解决方案）
高	√	√	√
中	√	√	–
低	√	–	–

10.2.2 组织的要求

10.2.2.1 引言

某一组织与信任相关的安全能力可以细分为：声誉、执行合同的能力、价值的一致性、对违反合同的可能补偿及其独立性。

10.2.2.2 声誉

声誉反映了产品或系统一直以来对实现特定目标的遵守程度。声誉是一种衡量标准，可以从对利益攸关方早期互动的直接或间接了解中获悉，用以评估对利益攸关方的信任程度。作为信任的一种表现形式，信任度通常依靠历史信息来推断未来可信的概率。因此，当某特定利益攸关方先前在遵循协议方面表现良好时，其在业内的声誉也会增加，从而可以提升另一方对该利益攸关方的信心。声誉管理的数据可以从基于证据的各种可靠和得到广泛接受的资源中获得，例如证书或官方年度和财务报告。然而，特定利益攸关方在不同的领域可能声誉不同。例如，设备制造商和网络运营商或服务提供商之间的关系是供应商-客户关系，而不同制造商之间的关系可能是竞争关系。因此，设备制造商可以在网络运营商或服务提供商那里拥有良好的声誉，但同一设备制造商在竞争对手那里可能会有不良声誉。因此，当审查外部提供的信誉信息时，网络运营商或服务提供商不能将从竞争制造商处获得的信誉信息作为主要来源。

10.2.2.3 合同的执行

在连续合作执行合同或多次间歇合作履行合同的情况下，执行合同的质量会对双方的信心产生影响，也会对当事人之间的信任关系产生影响。如果合同执行得好，相互的信心就会上升，信任关系就会紧密。相反，如果合同执行不好，相互的信任就会下降，信任关系也会下降。对于持续性的多次合作，例如用户多次访问服务提供商，用户的历史体验将直接影响其对服务系统的信任。在此情况下，建议将用户的历史体验信息归类为合同执行问题，而非信誉问题。

10.2.2.4 价值的一致性

当利益攸关方分享相同的价值时，他们之间的关系更加紧密，对未来长期的期望也更加一致。这样一来，双方的互信会更高，彼此之间也会存在更好的信任关系。

10.2.2.5 补偿能力

补偿能力是指承诺未得到履行时，对补偿的期望。对补偿的期望可视作利益攸关方即使在异常情况下也会寻求履行合同的另一种保证。一般来说，补偿越慷慨，同行受到的损失就越小。这样的能力会增加对方的信心和信任。例如，区域性网络法案可以规定对各利益攸关方的处罚/赔偿水平及严重程度，以提高可信度。

10.2.2.6 独立性

利益攸关方的独立性反映了其在执行合同时的自主权。独立性包括母公司控制子公司的能力，也包括管理部门对企业实体的影响。独立性涉及的利益攸关方越多，则从他们那里获得的影响力就越大，他们之间的信任关系也会受到更大的影响。

10.2.2.7 摘要

表8展示了信任级别与组织能力相关的一个示例。实际上，中低信任级别需要哪些方面的精确选择根据应用程序域而有所不同。例如，在某些情况下，可能仍然需要适当的供应商信誉来提供低级别信任，而在其他情况下，即使需要中等信任级别，供应商信誉可能也并不重要。

表8 – 与组织能力相关的信任级别和安全要求

信任级别	组织能力方面的安全需求				
	声誉	合同的执行	价值的一致性	补偿能力	独立性
高	√	√	√	√	√
中	（√）	√	–	√	（√）
低	–	√	–	（√）	–

10.2.3 程序要求

10.2.3.1 引言

安全运营能力可以通过以下能力实现：开发和产品生命周期的安全以及安全运营能力。

10.2.3.2 开发和产品生命周期的安全性

在NESAS中，开发和产品生命周期涵盖了可能影响网络产品生命周期的所有方面，包括网络产品的规划、设计、实施、交付、更新以及最终的退出。目前，对于IMT-2020网络，由全球移动通信系统协会（GSMA）和3GPP联合开发的NESAS确定了面向IMT-2020网络设备的开发和产品生命周期安全，涵盖了网络产品在其整个开发过程中的各个阶段，其中包括规划、设计、实施、测试、发布、生产和交付和产品生命周期（涵盖了所开发网络产品生命周期的各个阶段，其中包括维护和版本更新）。建议将其作为供应商开发和产品生命周期评估的参考。

10.2.3.3 安全运营能力

安全运营能力意味着产品或网络在商用时需要得到良好的管理，包括安全部署、强化和受限访问控制等。

10.2.3.4 摘要

因此，关于安全操作能力，建议采用表9所示的安全要求。

表9 –安全操作能力的信任级别和安全要求

信任级别	安全操作能力的安全要求	
	系统开发和产品生命周期安全	安全操作
高	√	√
中	（√）	√
低	–	√

10.2.4 技术要求

可信度可通过满足以下方面的相应级别满足：安全程序、隐私、弹性、安全性、可靠性和可用性。从可信度的角度看，建议这些是利益攸关方提供的产品和安全解决方案具备的关键属性，见[b-BSI 10754-1]和[b NIST SP800-160v1]系列文件所述。

表10展示了信任级别与某组织的可信度建立关联的方法示例。如上文所述，在实践中，中低信任级别需要哪些精确的选择根据应用域而变化。例如，在某些情况下，可能仍然需要适当级别的数据隐私保护实现低信任级别，而在其他情况下，即使需要中等信任级别，数据隐私保护可能也不重要。

表10 – 可信度的信任级别和安全要求

信任级别	可信度的安全要求					
	安全程序	隐私	快速恢复能力	安全性	可靠性	可用性
高	√	√	√	√	√	√
中	√	（√）	（√）	（√）	（√）	√
低	√	–	–	（√）	（√）	–

在现实世界的实现过程中，精确需求取决于服务场景，需要允许具有灵活性。如上所述，如果信任级别低，尽管安全要求可能相对较低，但可能需要制定更高的特定要求，例如在隐私方面。

10.3 将信任解释为详细的保证要求

一旦为特定用例确定了所需信任级别，则有必要为实施和做操作决策对此信任级别加以解释。

这可以通过将所需信任级别与第10.2节所列特定要求相对照的方式加以实现，且这些要求可通过产品和系统保障实现。目前存在一系列历史悠久的标准化技术，通过测试和评估，例如由专业第三方进行的测试和评估，确保产品和系统的可信度。这些可以用作第9.4节所述类型分析产生的必要信任级别，与设备和服务获取以及所用精确保证要求相互对照基础。

表11中的示例旨在使信任需求级别能够体现到基于产品和系统评估，并以信任为基础的业务和运营决策。

表11 – 所需信任级别与保证要求的对照关系示例

所需信任级别	保证实体的类型	安全保障方案示例
高	由认可的公共机构进行评估	共同标准[b-ISO/IEC 15408（所有部分）] 国家监管机构[b-ISO/IEC 27001] NESAS 安全保障规范（SCAS）[b-3GPP TS33.511] [b-3GPP TS33.512] [b-3GPP TS33.513] [b-3GPP TS33.514] [b-3GPP TS33.515] [b-3GPP TS33.516] [b-3GPP TS33.517] [b-3GPP TS33.518] [b-3GPP TS33.519]
中	由经认可的合格评定机构进行评估（CAB）	共同标准 [b-ISA/IEC 62443（所有部分）] [b-ISO/IEC 27001] NESAS/SCAS
低	CAB评估或自我评估	共同标准 NESAS/SCAS

即使在特定的保障方案内，不同程度或类型的保障也可能适用于不同的信任级别。

- 有些技术，特别是 [b-ISO/IEC 15408（所有部分）]规范的技术，允许指定多种保障级别，因此不同的信任级别可选择要求不同水平的 [b-ISO/IEC 15408（所有部分）]评估。然而，其他方案，如[b-ISO/IEC 27001]，只允许单一水平的评估。
- 可从评估中获得的保障程度可能会因执行评估机构而异（如表11中间一栏所示）。例如，对照[b-ISO/IEC 27001]的要求进行自我评估可能适合低信任级别。

此外，给予评估的权重可以通过其他因素来加强，例如：

- 设备或服务是否对任务交付至关重要，或者只是提供特定功能的多种方式之一（例如通过冗余）；
- 针对特定产品、系统或服务的不同方面是否开展了多重保障评估。

参考资料

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 28598-1] ISO 28598-1:2017, *Acceptance sampling procedures based on the allocation of priorities principle (APP) – Part 1: Guidelines for the APP approach*.

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. Available [viewed 2022-07-18] at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en .

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

[b-ISO/IEC/IEEE 15288] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*.

[b-ISO/IEC 15408(all parts)] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*.

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27005] ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*.

[b-ISO/PAS 19450] Publicly Available Specification ISO/PAS 19450:2015, *Automation systems and integration – Object-process methodology*.

[b-ISO/TS 21089] Technical Specification ISO/TS 21089:2018, *Health informatics – Trusted end-to-end information flows.*

[b-ISO/TS 21719-2] Technical Specification ISO/TS 21719-2:2018, *Electronic fee collection – Personalization of on-board equipment (OBE) Part 2: Using dedicated short-range communication*.

[b-ISO/TS 22318] Technical Specification ISO/TS 22318:2021, *Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management*.

[b-ISA/IEC 62443] ISA/IEC 62443 (all parts) [series of automation and control systems cybersecurity standards].

[b-GSMA FS.13] GSM Association (2022). *Network equipment security assurance scheme – Overview*, Official Document FS.13, version 2.1. London:

GSM Association. 29 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf

[b-GSMA FS.14] GSM Association (2022). *Network equipment security assurance scheme –Security test laboratory accreditation*, Official Document FS.14, version 2.1. London: GSM Association. 15 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf .

[b-GSMA FS.15] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology*, Official Document FS.15, version 2.1. London: GSM Association. 33 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf .

[b-GSMA FS.16] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements*, Official Document FS.16, version 2.1. London: GSM Association. 22 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf .

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol*.

[b-3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system*.

[b-3GPP TS 33.511] Technical Specification 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*.

[b-3GPP TS 33.512] Technical Specification 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF)*.

[b-3GPP TS 33.513] Technical Specification 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF)*.

[b-3GPP TS 33.514] Technical Specification 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class*.

[b-3GPP TS 33.515] Technical Specification 3GPP TS33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class*.

[b-3GPP TS 33.516] Technical Specification 3PGP TS33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Technical Specification 3GPP TS33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*.

[b-3GPP TS 33.518] Technical Specification 3GPP TS33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class*.

[b-3GPP TS 33.519] Technical Specification 3GPP TS33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*.

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification*.

[b-BSIMM] British Standards Institution (2021). *Building security in maturity model,* BSIMM 12. London: British Standards Institution.

[b-NIST FICIC] NIST (2018). *Framework for improving critical infrastructure cybersecurity*, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. 48 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments,* NIST Special Publication, NIST SP800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology. 95 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf .

[b-NIST SP 800-53] NIST SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organizations*.

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1,* NIST Special Publication, NIST SP800-160v1. Gaithersburg, MD: National Institute of Standards and Technology. 243 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf .

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	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
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	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
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦