国际电信联盟
电信标准化部门

建议书

ITU-T X.1816 (03/2023)

X系列：数据网、开放系统通信和安全性

IMT-2020安全

有关IMT-2020网络切片中安全能力分类的导则和要求

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
万维网安全（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
万维网安全（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**

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1816建议书

有关IMT-2020网络切片中安全能力分类的导则和要求

摘要

基本网络切片技术功能和流程的定义为网络切片业务的第一波IMT-2020部署和商用奠定了坚实的基础。作为按需定制的端到端逻辑网络，切片可以提供差异化安全能力。首先，IMT-2020网络切片为差异化网络实施方案提供了支持性安全措施。其次，IMT-2020网络在切片层面支持一些可选的安全措施。一些安全措施还可以提供多种安全选项，运营商可能拥有不同的安全资源，这可能带来不同程度的安全保证或非安全性能。切片客户也有具体的安全需求，可能会向切片运营商请求具有不同安全保护级别的定制网络切片。对于切片客户或切片运营商而言，选择其切片的安全能力存在一些挑战，例如管理成本和定义不一致等。ITU-T X.1816建议书旨在对差异化IMT-2020网络切片安全能力进行描述，并提供有关IMT-2020网络切片安全能力和IMT-2020网络切片安全的分类导则，以帮助生态系统更清楚地理解和选择切片安全能力。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1816	2023-03-03	17	11.1002/1000/15114

关键词

分类、IMT-2020、网络切片、安全能力

* 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识别码，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”等其他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他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，国际电联未收到实施本建议书可能需要的受专利/软件版权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ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1816建议书

有关IMT-2020网络切片中安全能力分类的导则和要求

1 范围

本建议书旨在提供有关IMT-2020网络切片安全分类的导则和要求。本建议书规定：

- 差异化IMT-2020网络切片安全能力的定义；
- 确定IMT-2020网络切片安全能力分类的原则和方法。

2 参引

下列ITU-T建议书及含有本建议书引用条款的其他参引构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参引均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参引的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.805] ITU-T X.805 (2003)建议书，提供端到端通信的系统的安全架构。

[ITU-T X.1047] ITU-T X.1047 (2021)建议书，网络切片管理和编排的安全要求和架构。

[3GPP TS 33.501] 3GPP TS 33.501 V17.1.0 (2021)技术规范，第三代合作伙伴项目；技术规范组业务和系统问题；5G系统的安全架构和流程（第17版）。

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 网络切片（network slice） [b-ITU-T Y.3100]：提供具体网络能力和网络特性的一个逻辑网络。

注1 – 网络切片能够创建定制的网络，从而为不同的市场场景提供灵活的解决方案，这些市场场景在功能、性能和资源分配方面有不同的要求。

注2 – 网络切片可以有展示其能力的能力。

注3 – 网络切片的行为通过网络切片实例来实现。

3.1.2 网络切片实例（network slice instance） [b-ITU-T Y.3100]：基于网络切片蓝图创建的、网络切片的一个实例。

3.1.3 网络切片子网（network slice subnet） [b-ETSI TS 128 530]：有关一组托管功能和所需资源（例如，计算、存储和网络资源）管理问题的一种表示。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

AAA 认证、授权和结算

ACL 访问控制清单

AMF 访问和移动管理功能

CN 核心网

CU 中央单元

DDoS 分布式拒绝服务

DU 分布式单元

EAP 可扩展认证协议

ENSI 外部网络切片信息

gNB NR节点B

IMT-2020 国际移动通信-2020

NAT 网络地址转换

NFV 网络功能虚拟化

ng-eNB 下一代演进的节点-B

NSSAI 网络切片选择辅助信息

NSSAI 单一网络切片选择辅助信息

PDU 协议数据单元

PNF 物理网络功能

RAN 无线接入网

RB 无线承载

TLS 传输层安全

UE 用户设备

URL 统一资源定位符

VNF 虚拟网络功能

WAF 万维网应用防火墙

5 惯例

在本建议书中：

关键词“**建议**”（**is recommended**）指的是一项必须严格遵守的要求，如果宣称遵循本建议书，则不得违反。指的是一项建议的、但不绝对要求的要求。因此，宣称遵循本建议书并不需要存在本要求。

关键词“**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/业务提供商可以选

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 IMT-2020网络切片安全能力分类介绍

保证网络切片安全是引入网络切片的前提。对于使用切片通信业务的切片客户而言，需要一个为其切片实施方案定制的相应的安全保证，并且还可能基于其使用切片的业务有具体的安全要求。故其可能会向运营商请求具有不同安全保护的定制网络切片。对于设计、建设和运营网络并提供网络切片的切片运营商而言，切片涉及多个领域（例如，无线、传输、核心网、管理），并可提供差异化安全能力：首先，IMT-2020网络切片为差异化网络实施方案提供了安全措施。其次，IMT-2020网络在切片级支持一些可选的安全措施。一些安全措施还可以提供多种安全选项，并且运营商可能拥有不同的安全资源。这些都可能带来不同程度的安全保障或非安全性能。因此，需要基于客户的要求和网络能够提供的安全能力来决定一个切片的安全能力。切片客户或切片运营商在选择其切片的安全能力时面临一些挑战：

- 客户的安全要求可能模糊不清，数量很少，不足以映射安全能力。
- 客户可能有太多超出网络能力的安全要求。

  利益攸关方在安全能力和差异方面的知识成本可以不同，其选择的能力组合可能不合理。例如，所选能力提供的保护对于多个领域或利益攸关方来说可能是不一致的。
- 切片安全能力的组合数量可能非常多，运营商的管理和编排成本可能会比较高。

将对差异化IMT-2020网络切片安全能力以及对其进行分类和组合的方法提出建议，这具有以下意义：

- 有助于行业对切片的安全能力以及切片安全能力之间的差异（如性能）达成统一的理解。
- 提供IMT-2020网络切片安全能力的通用基本分类，以使行业清楚地了解切片安全能力并更好地匹配大多数行业应用。
- 有助于实现不同切片之间的漫游，也有助于切片的再利用。
- 为行业用户选择符合要求的适当切片提供参考。
- 为行业监管者制定切片的发展规划和战略提供参考。
- 为业务提供商在适当切片部署业务提供参考。
- 为运营商制定切片发展规划、评估切片价值和价格提供参考。
- 为设备商规划切片的技术路线图和产品路线图提供参考。

该方法包括以下几个方面：

- 以结构化的形式列出通用差异化切片安全能力，包括名称、描述、安全维度和选项。这在第7节中提供。
- 对于每个安全维度，可以通过基于一些原则列出具有不同选项的相应切片安全能力的组合，来形成有关一个安全维度的多个水平。这在第8节中提供。
- 此外，可以通过基于一些原则为每个安全维度选择一个水平，来形成由不同安全维度组成的基本切片安全类型。这在第9节中提供。
- 利益攸关方可以使用分类原则、方法和结果来决定一个切片的安全能力。这在第10节中提供。

7 IMT-2020网络切片安全能力

7.1 网络切片安全能力描述模板

第7节提供了一般IMT-2020网络安全能力的清单，这些网络安全能力在网络切片之间可有所不同。安全功能描述应清晰、简洁、明了。每个描述应包括：

- 能力描述：差异化IMT-2020网络切片安全能力的详细描述。
- 能力名称：指配给每个安全能力的唯一名称和首字母缩略语。
- 能力安全维度：安全能力旨在解决的一个特定的安全方面问题。有八（8）个安全维度，包括访问控制、认证、不可否认性、数据机密性、通信安全性、数据完整性、可用性和私密性[ITU-T X.805]。
- 能力选项：每个安全能力有多种选择，在不同的切片之间可有所不同。在本建议书中，每个选项都被称为“能力首字母缩略语序列号”。注：这些选项是通用的，不依赖于特定的网络实施方案。它们可以被进一步细分，以便与特定的实施方案相一致。

7.2 差异化IMT-2020切片安全能力

7.2.1 网络切片特定的认证和授权能力

- 能力描述：IMT-2020系统在用户设备（UE）与可能由外部第三方企业拥有的认证、授权和结算服务器（AAA-S）之间提供可选使用的网络切片特定的认证和授权[3GPP TS 33.501]。网络切片特定的认证和授权可以在初次认证之后基于单个网络切片选择辅助信息（S-NSSAI）来触发。AAA服务器还可以触发切片特定的授权撤销、重新认证和重新授权。
- 能力名称：网络切片特定的认证和授权（NSSAA）
- 能力安全维度：认证，访问控制
- 能力选项：
  - NSSAA.0：关
  - NSSAA.1：开

7.2.2 网络资源的网络切片隔离能力

- 能力描述：IMT-2020网络切片运行在运营商的统一基础设施资源上。有多种隔离解决方案来防止切片网元通过共享基础设施资源访问或影响不同切片中的网元；从切片子网领域来看：
  - 对于接入网（AN）：对于无线接口，动态无线承载（RB）资源共享和静态RB资源保留可用于资源分配。前者具有更好、更灵活的覆盖效果和资源利用率，而后者具有更高的可靠性和成本。对于基站，不同切片的中央单元（CU）和（DU）分布式单元可以是相同的。对于更高的隔离水平，可以通过分配专用硬件对其进行物理隔离，或者通过使用网络功能虚拟化（NFV）（即虚拟机/容器）共享硬件来对其进行逻辑隔离。
  - 对于传输网（TN）：传输网上的隔离可以是无隔离、物理隔离（例如，物理网络功能隔离、物理网络链路隔离等）、逻辑隔离（例如，逻辑网络功能隔离、逻辑/虚拟网络链路隔离等）[ITU-T X.1047]。
  - 对于核心网（CN）：核心网资源物理隔离包括一个或多个专用物理网络功能（PNF）隔离、专用物理网络链路隔离、地理位置隔离、计算隔离、内存隔离、

存储隔离、PNF、基于安全的隔离等。核心网资源逻辑隔离包括一个或多个虚拟网络功能（VNF）隔离、虚拟链路隔离、虚拟化技术隔离、虚拟计算隔离、虚拟内存隔离、虚拟存储隔离、被虚拟化以提供虚拟资源的硬件（HW）的地理位置隔离以及基于VNF安全的隔离等[ITU-T X.1047]。

从资源类型和隔离技术角度来看：

- 对于无线接口资源：RB共享或RB保留
- 对于AN/TN/CN的网络功能资源：物理隔离、逻辑隔离或无隔离

- 能力名称：网络资源的切片隔离（SIR）
- 能力安全维度：访问控制，可用性，私密性
- 能力选项和相应的性能：
  - SIR.0：无隔离
  - SIR.1：逻辑隔离+RB共享
  - SIR.2：逻辑+物理隔离+RB共享
  - SIR.3：物理隔离+RB共享
  - SIR.4：逻辑隔离+RB保留
  - SIR.5：逻辑+物理隔离+RB保留
  - SIR.6：物理隔离+RB保留

7.2.3 用户平面数据保护能力

- 能力描述：IMT-2020系统可以在切片层面上提供差异化用户面数据保护能力。下一代演进节点B（ng-eNB）/NR节点B（gNB）可以根据接收到的用户平面安全策略，决定是否激活每个PDU会话的用户平面机密性和/或用户平面完整性保护。用户平面安全策略可以被配置为指示“需要”或“不需要”。存在可选的加密算法[3GPP TS 33.501]。
- 能力名称：用户平面数据保护（UPDP）
- 能力安全维度：数据机密性，数据完整性
- 能力选项：
  - UPDP.0：不激活用户平面机密性和/或用户平面完整性保护
  - UPDP.1：利用可选的加密算法激活用户平面机密性和/或用户平面完整性保护

7.2.4 边界保护能力

- 能力描述：重要的是通过在边界、尤其是在CN边界部署安全控制功能/特征（例如，有关N6接口的N6保护配置）[b-3GPP TS 28.541]，来保护网络切片免受网络攻击。对于不同的网络片消费者，安全控制功能/特征可能不同，并且可以根据要求动态地来改变。安全控制功能可以是防火墙、网络地址转换（NAT）、反恶意软件、家长控制、分布式拒绝服务（DDoS）保护功能等[b-3GPP TS 28.541]。特征指的是转发规则、过滤规则、参数配置等。这些要求可以是对数据网络和隧道机制的访问控制。
- 能力名称：边界保护（BP）
- 能力安全维度：访问控制，可用性，通信安全性

- 能力选项：
  - BP.0：无安全控制功能
  - BP.1：部署有安全控制功能/特征

7.2.5 应用业务保护能力

- 能力描述：运营商可以在网络侧部署安全设备或安全模块，来为使用切片的应用业务和使用应用业务的用户提供不同的安全保护。例如，运营商网络可以提供异常终端检测、网络流量清理、恶意统一资源定位符（URL）检测、万维网应用防火墙（WAF）、防DDoS等。
- 能力名称：应用业务保护（ASP）
- 能力安全维度：通信安全性，访问控制，可用性
- 能力选项：
  - ASP.0：无应用业务保护
  - ASP.1：部署有应用业务保护

7.2.6 NSSAA期间EAP ID的私密性保护能力

- 能力描述：有多种可扩展认证协议（EAP）方法[b-IETF RFC 3748]可用于切片特定的认证。可以选择具备隐私保护能力的EAP方法，例如，EAP-传输层安全性（TLS）[b-IETF RFC 5216]、EAP-TTLS [b-IETF RFC 5281]，来保护用于基于EAP的NSSAA [3GPP TS 33.501]的EAP ID的私密性。
- 能力名称：NSSAA期间EAP ID的私密性保护（PPEAP）
- 能力安全维度：私密性
- 能力选项：
  - PPEAP.0：不使用具备私密性保护的EAP方法
  - PPEAP.1：使用具备私密性保护的EAP方法

7.2.7 (S-)NSSAI的私密性保护能力

- 能力描述：NSSAI用于确定网络切片/业务类型。关于运营商网络和客户的一些信息可以从NSSAI及其使用中获得。IMT-2020网络通过允许不使用NSSAI或使用运营商领域外的替代信息来提供用于保护(S-)NSSAI私密性的能力。在注册过程期间，访问和移动管理功能（AMF）可以在注册接受消息中向UE提供接入层连接建立NSSAI包含模式参数，指明UE是否以及何时须根据不同模式在接入层连接建立中纳入NSSAI信息。UE须默认不在3GPP访问的接入层中提供NSSAI，除非已经向其提供了在其他模式下操作的指示[b-3GPP TS 23.502]。在NSSAA期间，如果所使用的AAA服务器属于第三方，即作为内部IMT-2020核心的S-NSSAI，则该信息可以可选地在运营商的网络中映射于在运营商领域外传输和使用的外部网络切片信息（ENSI）[3GPP TS 33.501]。
- 能力名称：(S-)NSSAI的私密性保护（PPSI）
- 能力安全维度：私密性
- 能力选项：
  - PPSI.0：在运营商领域外使用NSSAI
  - PPSI.1：不使用NSSAI或在运营商领域外使用替代信息

7.3 IMT-2020切片安全能力分类

IMT-2020切片安全能力可以根据其安全维度进行分类，如表7-1所示。

表7-1 – 基于安全维度的IMT-2020切片安全能力分类

安全维度 切片安全能力	网络切片特定的认证和授权（NSSAA）	资源的切片隔离（SIR）	用户平面数据保护（UPDP）	边界保护（BP）	应用业务保护（ASP）	NSSAA 期间 EAP ID 的私密性保护（PPEAP）	(S-)NSSAI 的私密性保护（PPSI）
访问控制	√	√		√	√		
认证	√						
不可否认性							
数据机密性			√				
通信安全性				√	√		
数据完整性			√				
可用性		√		√	√		
私密性		√				√	√

8 通过切片安全能力实现的安全维度分类

8.1 基于切片安全能力的安全维度分类的方法和原则

每个安全维度的分类方法如下：

1) 建议列出属于安全维度的安全能力和相关选项。如果某项安全能力影响某个安全维度的可能性很小，则该安全能力可以选择不在该安全维度中列出，而只在主要受影响的其他安全维度中列出。

2) 建议列出不同能力选项的组合，并形成不同水平的安全维度。如果一个安全维度是通过多项安全能力实现的，则在组合安全能力选项时，每个保护效果水平对多个领域或利益攸关方都应保持一致。xx.nn（例如，AC.1，…，DI.0）是指安全维度xx的水平名称。

第8.2节给出了八个安全维度的通用清单，其水平基于第7节中列出的安全能力和选项。

8.2 基于IMT-2020切片安全能力的安全维度和水平

8.2.1 基于IMT-2020切片安全能力的访问控制

访问控制可以通过具有选项的能力来实现，这些选项包括但不限于：网络切片特定的认证和授权、网络资源的切片隔离、边界保护和应用业务保护。为实现不同水平的访问控制，有各种具有不同选项的能力组合。基于第7节，如下所示：

表8-1 – 访问控制水平

安全维度：访问控制（AC）														
能力	**网络切片特定的认证和授权（NSSAA)**		**应用业务保护(ASP)**		**资源的切片隔离 (SIR)**							**边界保护(BP)**		**水平名称**
选项	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
组合	NSSAA.0		ASP.0		SIR.0							BP.0		AC.0000
					SIR.0							BP.1		AC.0001
					SIR.1 SIR.4							BP.0		AC.0010 AC.0040
					SIR.1 SIR.4							BP.1		AC.0011 AC.0041
					SIR.2 SIR.5							BP.0		AC.0020 AC.0050
					SIR.2 SIR.5							BP.1		AC.0021 AC.0051
					SIR.3 SIR.6							BP.1		AC.0031 AC.0061
			ASP.1		SIR.0							BP.0		AC.0100
					SIR.0							BP.1		AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140
					SIR.1 SIR.4							BP.1		AC.0111 AC.0141
					SIR.2 SIR.5							BP.0		AC.0120 AC.0150
					SIR.2 SIR.5							BP.1		AC.0121 AC.0151
					SIR.3 SIR.6							BP.1		AC.0131 AC.0161
	NSSAA.1		ASP.0		SIR.0							BP.0		AC.1000
					SIR.0							BP.1		AC.1001
					SIR.1 SIR.4							BP.0		AC.1010 AC.1040
					SIR.1 SIR.4							BP.1		AC.1011 AC.1041
					SIR.2 SIR.5							BP.0		AC.1020 AC.1050
					SIR.2 SIR.5							BP.1		AC.1021 AC.1051
					SIR.3 SIR.6							BP.1		AC.1031 AC.1061

表8-1 – 访问控制水平

<table>
<tr><td colspan="13">安全维度：访问控制（AC）</td></tr>
<tr><td>能力</td><td colspan="2">网络切片特定的认证和授权（NSSAA)</td><td colspan="2">应用业务保护(ASP)</td><td colspan="7">资源的切片隔离 (SIR)</td><td colspan="2">边界保护(BP)</td><td>水平名称</td></tr>
<tr><td>选项</td><td>NSSAA.0</td><td>NSSAA.1</td><td>ASP.0</td><td>ASP.1</td><td>SIR.0</td><td>SIR.1</td><td>SIR.2</td><td>SIR.3</td><td>SIR.4</td><td>SIR.5</td><td>SIR.6</td><td>BP.0</td><td>BP.1</td><td></td></tr>
<tr><td rowspan="8"></td><td colspan="2" rowspan="8"></td><td colspan="2" rowspan="8">ASP.1</td><td colspan="7">SIR.0</td><td colspan="2">BP.0</td><td>AC.1100</td></tr>
<tr><td colspan="7">SIR.0</td><td colspan="2">BP.1</td><td>AC.1101</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.0</td><td>AC.1110
AC.1140</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.1</td><td>AC.1111
AC.1141</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.0</td><td>AC.1120
AC.1150</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.1</td><td>AC.1121
AC.1151</td></tr>
<tr><td colspan="7">SIR.3
SIR.6</td><td colspan="2">BP.1</td><td>AC.1131
AC.1161</td></tr>
</table>

8.2.2 基于IMT-2020切片安全能力的认证

认证可以通过包括网络切片特定的认证和授权在内的能力来实现。有两种水平的认证。如下所示：

表8-2 – 认证水平

安全维度：认证（Au）			
能力	**网络切片特定的认证和授权（NSSAA）**		**水平名称**
选项	**NSSAA.0**	**NSSAA.1**	
组合	NSSAA.0		Au.0
	NSSAA.1		Au.1

8.2.3 基于IMT-2020切片安全能力的不可否认性

第7节中没有实现不可否认性的能力。

8.2.4 基于IMT-2020切片安全能力的数据机密性

数据机密性可以通过包括用户平面数据保护在内的能力来实现。有两种级别的认证。如下所示：

表8-3 – 数据机密性水平

安全维度：数据机密性（DC）			
能力	**用户平面数据保护（UPDP）**		**水平名称**
选项	**UPDP.0**	**UPDP.1**	
组合	UPDP.0		DC.0
	UPDP.1		DC.1

8.2.5 基于IMT-2020切片安全能力的通信安全性

通信安全性可以通过包括边界保护、应用业务保护在内的能力来实现。这些能力有多种组合，不同的选项可以实现不同的通信安全性水平。如下所示：

表8-4 – 通信安全性水平

安全维度：通信安全性（CS）					
能力	**边界保护（BP）**		**应用业务保护（ASP）**		**水平名称**
选项	**BP.0**	**BP.1**	**ASP.0**	**ASP.1**	
组合	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

8.2.6 基于IMT-2020切片安全能力的数据完整性

数据完整性可以通过包括用户平面数据保护能力在内的能力来实现。有两种水平的数据完整性。如下所示：

表8-5 – 数据完整性水平

安全维度：数据完整性（DI）			
能力	**用户平面数据保护（UPDP）**		**水平名称**
选项	**UPDP.0**	**UPDP.1**	
组合	UPDP.0		DI.0
	UPDP.1		DI.1

8.2.7 基于IMT-2020切片安全能力的可用性

可用性可以通过包括网络资源的切片隔离、边界保护和应用业务保护在内的能力来实现。这些能力有多种组合，不同的选项可以实现不同的可用性水平。如下所示：

表8-6 – 可用性水平

安全维度：可用性（Av）							
能力	**应用业务保护（ASP）**		**资源的切片隔离（SIR）**		**边界保护（BP）**		**水平名称**
选项	**ASP.0**	**ASP.1**	**SIR.1/SIR.2/SIR.3**	**SIR.4/SIR.5/SIR.6**	**BP.0**	**BP.1**	
组合	ASP.0		SIR.1/SIR.2/SIR.3		BP.0		Av.000
					BP.1		Av.001
			SIR.4/SIR.5/SIR.6		BP.0		Av.010
					BP.1		Av.011
	ASP.1		SIR.1/SIR.2/SIR.3		BP.0		Av.100
					BP.1		Av.101
			SIR.4/SIR.5/SIR.6		BP.0		Av.110
					BP.1		Av.111

8.2.8 基于IMT-2020切片安全能力的私密性

私密性可以通过包括NSSAA期间EAP ID的私密性保护、(S-)NSSAI的私密性保护在内的能力来实现。这些能力有多种组合，不同的选项可以实现不同的私密性水平。如下所示：

表8-7 – 私密性水平

安全维度：私密性（Pr）					
能力	**NSSAA期间EAP ID的私密性保护（PPEAP）**		**(S-)NSSAI的私密性保护（PPSI）**		**水平名称**
选项	**PPEAP.0**	**PPEAP.1**	**PPSI.0**	**PPSI.1**	
组合	PPEAP.0		PPSI.0		Pr.00
	PPEAP.0		PPSI.1		Pr.01
	PPEAP.1		PPSI.0		Pr.10
	PPEAP.1		PPSI.1		Pr.11

9 有关切片安全类型的导则和要求

一组安全维度可以表征网络切片的一种安全类型，并且可以通过业务类别来区分。通过组合不同水平的安全维度，将会有多种切片安全类型。但并不是所有的组合都是合理的。

形成切片安全类型的方法和原则是：

1) 建议根据各水平的业务需求和性能，先确定优先级较高的安全维度的水平。

2) 建议根据各水平的业务要求和性能，确定剩余安全维度的水平。

3) 建议检查每个安全维度之间是否存在冲突，以便进行协调。在一个切片中，对于包含相同安全能力的不同安全维度，安全能力的选项应该保持一致。

4) 当更新一种切片安全类型的某些能力的选项或某些安全维度的水平时，建议更改相关的能力和安全维度，以保持一致。

10 有关网络切片安全能力分类的利益攸关方的导则和要求

建议切片运营商基于第7节中的通用切片安全能力清单及其私密性安全能力，准备其自身的切片安全能力清单。

建议切片运营商根据第8节中的方法，基于具有不同水平的安全维度及其私密性安全能力或其他维度的通用清单，准备其自身的具有不同水平的安全维度清单。

建议切片运营商根据第9节中的方法准备其自身的切片安全类型清单。

建议切片运营商通过从不同水平的安全维度或切片安全类型的映射，基于其切片安全能力清单或其具有不同水平的安全维度清单或其切片安全类型清单，来决定某个切片实例的安全能力和选项（例如，在供应[b-ETSI TS 128 531]期间）。

如果客户清楚地了解其安全要求和所映射的安全能力，则建议切片客户从通用切片安全能力清单或运营商切片安全能力清单中选择安全能力和选项的组合。

如果客户了解其想要实现的某个安全维度的效果，则建议切片客户根据不同水平的性能，从具有不同水平的安全维度的通用清单或具有不同水平的安全维度的运营商清单中选择相关安全维度的水平。

如果客户几乎不了解详细的安全内容，则建议切片客户从运营商的切片安全类型清单中选择一种类型。

附录I

IMT-2020网络切片安全能力选项的性能

（此附件非本建议书不可分割的组成部分）

注 – 性能取决于具体的实施细节，并可能随技术的发展而变化。

- NSSAA选项的性能：
  - NSSAA.0：基础水平。
  - NSSAA.1：更多自主权（针对垂直行业）。
- SIR选项的性能：
  - SIR.0：无隔离：基础水平。
  - SIR.1：逻辑隔离+RB共享：SIR.1比SIR.2和SIR.3更灵活，成本可能更低。
  - SIR.2：逻辑+物理隔离+RB共享：SIR.2比SIR.3更灵活，成本可能更低。SIR.2比SIR.1可靠性更高。
  - SIR.3：物理隔离+RB共享：SIR.3比SIR.1和SIR.2可靠性更高，资源成本更高。
  - SIR.4：逻辑隔离+RB保留：SIR.4比SIR.5和SIR.6更灵活，成本可能更低。
  - SIR.5：逻辑+物理隔离+RB保留：SIR.5比SIR.6更灵活，成本可能更低。SIR.2比SIR.4可靠性更高。
  - SIR.6：物理隔离+RB保留：SIR.6比其他的延迟更低，可靠性更高，成本更高。

逻辑隔离选项在服务器资源上的成本可能低于物理隔离选项，而前者在安全措施上的成本可能高于后者，以实现类似的保护效果。

与逻辑隔离选项相比，物理隔离选项可实现更高水平的访问控制。

RB共享选项比RB保留选项具有更好和更灵活的覆盖效果和资源利用率。

- UPDP选项的性能：
  - UPDP.0：无线接口中没有数据保护，延迟低于UPDP.1。
  - UPDP.1：根据可选的加密算法，无线接口中存在具有不同保护效果的数据保护。
- BP选项的性能：
  - BP.0：基础水平。
  - BP.1：根据部署的可选的安全控制功能/特征，存在具有不同保护效果的边界保护。
- ASP选项的性能：
  - ASP.0：基础水平。
  - ASP.1：根据可选的应用业务保护，存在具有不同保护效果的应用业务保护。
- PPEAP选项的性能：
  - PPEAP.0：UE身份被暴露。
  - PPEAP.1：UE身份是匿名的。

- PPSI选项的性能：
  - PPSI.0：(S-)NSSAI被暴露。
  - PPSI.1：(S-)NSSAI未被披露。

附录II

基本IMT-2020切片安全类型示例

（此附件非本建议书不可分割的组成部分）

下面的基本切片安全类型表是基于第9节的方法形成的，各利益攸关方可以直接使用该表，或者在此基础上进行调整以形成其自身的基本切片安全类型。

表II.1 – 基本切片安全类型示例

切片安全类型	访问控制	认证	可用性	通信安全性	数据机密性	数据完整性	不可否认性	私密性	判断	适当的业务
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	-	Pr.0	基本安全	公共网络
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	-	Pr.11	高安全性，最高成本	高安全类型，如政府、金融、证券和电网客户的专线
2	AC.0000	Autor.0	Av.0	CS.0	-	-	-	-	低成本	低成本类型，互联网接入和OTT视频
3	AC.xx61	-	Av.x11	-	-	-	-	Pr.xx4 Pr.xx6	高隔离、高成本	高隔离类型
4	-	-	Av.x1x	-	DC.0	DI.0	-	-	低延迟	低延迟类型，如云游戏

注 – 级别名称序列号中的x可指任何值。

参考文献

[b-ITU-T Y.3100] ITU-T Y.3100建议书（2017年），IMT-2020网络的术语和定义。

[b-3GPP TS 23.502] 3GPP TS 23.502，5G系统（5GS）的程序。
<https://www.3gpp.org/ftp/Specs/archive/23_series/23.502>

[b-3GPP TS 28.541] 3GPP TS 28.541，管理和协调；5G网络资源模型（NRM）；第2阶段和第3阶段。
<https://www.3gpp.org/ftp/Specs/archive/28_series/28.541>

[b-IETF RFC 3748] IETF RFC 3748，可扩展认证协议（EAP）。
<https://tools.ietf.org/html/rfc3748>

[b-IETF RFC 5216] IETF RFC 5216，EAP-TLS认证协议。
<https://www.rfc-editor.org/rfc/rfc5216.html>

[b-IETF RFC 5281] IETF RFC 5281，可扩展认证协议隧道传输层安全认证协议版本0（EAP-TTLSv0）。
<https://datatracker.ietf.org/doc/html/rfc5281>

[b-ETSI TS 128 530] ETSI TS 128 530 V17.1.0技术规范（2022年），5G；管理和协调；概念、用例和要求（3GPP TS 28.530第17版的版本17.2.0）。
<https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf>

[b-ETSI TS 128 531] ETSI TS 128 531 V16.9.0技术规范（2021年），5G；管理和协调；调配；（3GPP TS 28.531第16版的版本16.6.0）。

ITU-T 建议书系列

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，以及相关联的测量和测试
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
2023年，日内瓦