

5G 安全架构白皮书

2017-11





5G

目录

前言

- 1 ○ **5G 安全挑战和需求** ————— 1
 - 1.1 5G 多样化商业需求
 - 1.2 5G 网络支撑广连接、高覆盖的物联网接入
 - 1.3 5G 引入 IT 新技术、新架构带来的安全挑战

- 2 ○ **业务和网络架构的变化驱动 5G 安全架构变革** ————— 5
 - 2.1 5G 安全新特性
 - 2.2 对 4G 安全特性的延续和增强
 - 2.3 面向业务构建可扩展、可编排的智能 5G 安全架构框架
 - 2.4 5G 安全全球标准化进展

- 3 ○ **华为积极推动 5G 安全标准化，共建 5G 安全生态** ————— 16
 - 3.1 端到端安全评估体系

总结

A blue padlock is the central focus, set against a dark blue background filled with glowing binary code (0s and 1s) and hexadecimal characters (A-F, 0-9). The padlock is open, with the shackle raised. The overall aesthetic is high-tech and digital.

前言

我们已经看到了业界 5G 技术的初步实现。它提供了许多功能，使其成为数字化世界的首选平台。和 4G 一样，健全稳固的安全将是 5G 网络的优势之一。然而，仅仅用 4G 的安全特性来构造 5G 安全是远远不够的，因为 5G 的全方位业务不仅仅是基于 4G 的扩展。除了增强的 4G 安全功能之外，5G 还需要全新的安全功能和服务。

现代世界的潮流是数字化和全球化，网络安全是其关键特色之一。提高网络安全水平意味着促进一个更安全、更繁荣的社会。为了提供更好的网络安全，需要使用所有必要的工具和手段，而 5G 技术在其中承担了很大的责任。将移动网络的强大的安全功能开放给垂直行业，也有利于满足垂直行业的网络及业务的安全需求。当然，需要以受控的方式进行网络安全能力开放，这样才不会危及运营商，确保运营商网络自身的运营能力。

我们将展示 5G 安全如何实现两个不同的目标。第一个目标是保护 5G 平台本身。第二个同样重要的目标，是提供方法和机制来保护那些建立在 5G 平台之上的服务。

01

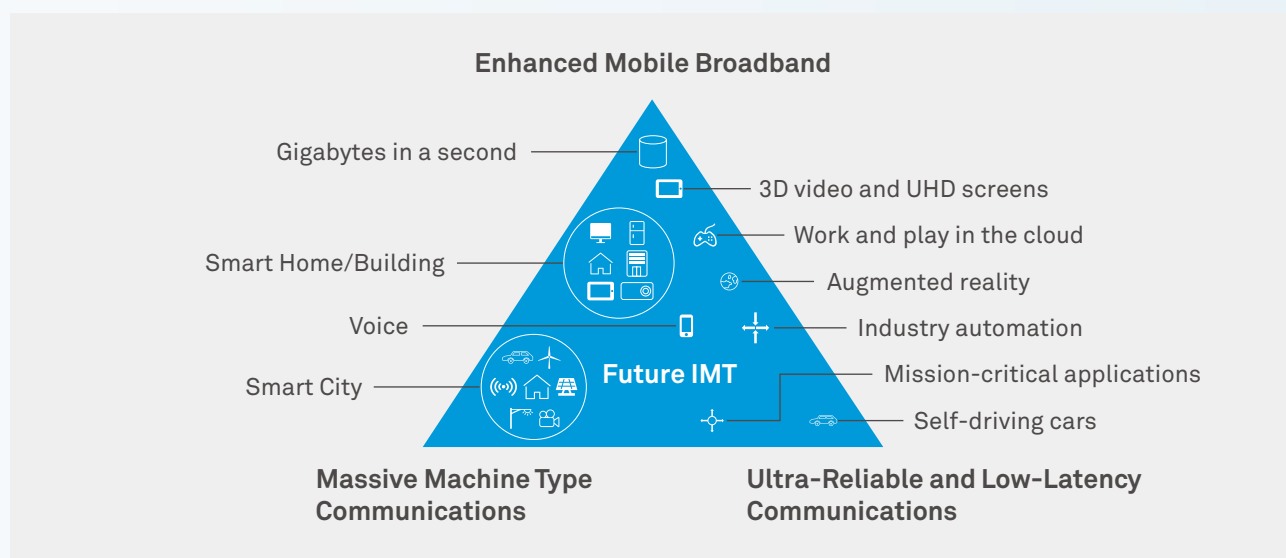
5G 安全挑战和需求

ITU-T 定义的 5G 用例广泛的支持垂直行业（如交通、物流、自动驾驶、健康、制造业、能源行业、媒体及娱乐业）的数字化，以及公共事业（智慧城市、公共安全和教育产业）的发展。随着高带宽、低时延、多连接的 5G 网络逐渐普及，将会形成一个普适性的网络平台，催化各行各业的技术与服务的发展。

移动网络业务范畴的扩展，丰富了电信网络的生态环境，也对移动网络的安全带来了新的需求和挑战。

1.1 5G 多样化商业需求

5G 不仅是下一代移动通信网络基础设施，而且是未来数字世界的使能者。5G 并不是一个单一的无线接入技术，也不是几个全新的无线接入技术，5G 是一个真正意义上的融合网络，无缝支持各种新的网络部署。



- eMBB 聚焦对带宽有极高需求的业务，例如高清视频，虚拟现实 / 增强现实等，满足人们对于数字化生活的需求
- mMTC 则覆盖对于联接密度要求较高的场景例如智能交通、智能电网、智能制造，满足人们对于数字化社会的需求
- uRLLC 聚焦对时延极其敏感的业务，例如自动驾驶 / 辅助驾驶、远程控制等，满足人们对于数字化工业的需求

业务多样化需要差异化安全保护机制

为了用一张物理网络满足不同的业务需求，网络在统一的底层物理设施基础上通过虚拟化技术生成相应的网络拓扑以及网络功能，为每一个特定业务类型生成一个网络切片。每一个网络切片在物理上是源自统一的网络基础设施，这样大大降低了运营商运营多个不同业务类型的建网成本；而在逻辑上切片又是隔离的，逻辑的独立性满足了每一类业务功能定制、独立运维的需求。

不同的业务会有差异化的安全需求。5G 系统支持多种业务并行发展，以满足个人用户、行业客户的多样性需求。从网络架构来看，基于原生云化架构的端到端切片满足这样的多样性需求。同样的，5G 安全设计也需支持业务的多样性，满足差异化安全需求。

网络切片本身也需要安全机制，保证切片的安全运营，用户的正常接入。

多元信任模型和可扩展的身份管理机制

3G 和 4G 时代，主要业务是语音，短信和移动宽带，业务类型相对比较单一。在传统移动通信网络中，网络对用户入网认证，并作为管道承载用户与服务间的业务认证，用户与网络构成二元信任模型。

5G 时代，移动通信网络不仅仅服务于个人消费者，更重要的是将服务于垂直行业，衍生出丰富的业务。5G 时代不仅仅是更快的移动网络或更强大的智能手机，而是链接世界的新型业务，如 mMTC 和 URLLC。在 5G 网络中，将融合传统二元信任模型，构建多元信任模型。网络和垂直行业可结合进行业务身份管理，使得业务运行更加高效，用户的个性化需求得以满足。

4G 网络身份管理的主要对象是移动宽带用户，采用以设备为单位的对称密钥管理体制，很好的满足了运营商的要求。而 5G 网络面临大量新增的 IOT 设备及其可穿戴设备，传统的用户管理机制在开户，认证等方面成本高昂，已经不能完全满足 5G 用户管理的需求，因此需要进一步扩展的身份管理机制，根据业务特征及其新的安全威胁进行优化。

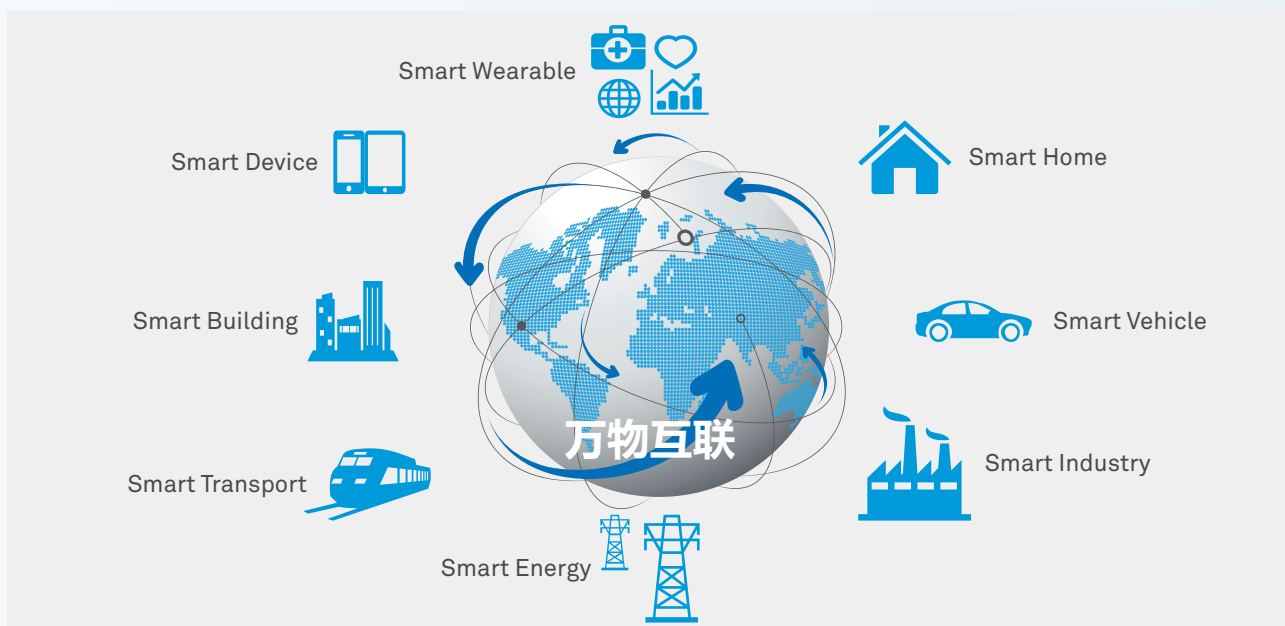
安全能力开放

业务开放带来安全挑战的同时，也给运营商安全业务带来了更广泛的机会。作为 5G 连接基础设施平台的提供者和运营者，电信运营商是业务提供商的最佳使能者，是行业客户可信任的商业伙伴。

垂直行业可以直接使用运营商开放的安全能力，降低了一些新型垂直行业的业务门槛和成本，并缩短上市时间。通过安全能力开放，运营商可以盘活网络资产和基础设施，开创新的利益增长点；可以打破管道化运营和封闭网络模式，以电信网络为中心构建安全生态系统；提升差异化竞争力，并形成运营商、垂直行业、安全厂商、个人用户的生态链，合作共赢共创商业价值。

1.2 5G 网络支撑广连接、高覆盖的物联网接入

5G 网络需要为物联网提供可靠的网络通信服务，海量的物联网设备传感器对连接管理提出了很高要求。例如车联网系统中的车车通信、车人通信、车路通信和车网通信涉及上亿传感设备的连接，对于保障交通安全、提高城市交通运行效率、降低污染排放都具有重要意义。大型城市的智能电表装机量过千万，每天从大量电表向电网数据中心上传大量的计量数据。智能制造要求永久在线、广覆盖、大连接，为连续运转的机器、数量庞大的产品和工人提供随时随地、无处不在的连接，保证生产各个环节任何位置间的物的连接。



物联网设备数量庞大，无人值守，对网络安全管理和安全防御都带来新的挑战。因此，5G 网络需要为海量的物联网设备提供安全可靠、成本可控的网络接入模式。

统一安全管理

5G 系统中存在不同的接入技术和终端，从安全管理的角度考虑，一个包含通用安全核心功能的统一安全框架能够更好的覆盖 5G 网络的整体安全需求。

异构接入网络将是下一代接入网络的主要技术特征之一。多制式、多接入、多站点的接入网络，需要协同 5G、LTE、WiFi 共存的多制式接入，以及宏站、小站、微站的不同站点形态的并发连接。安全管理需要具备灵活处理异构接入技术的安全能力。

智能化的安全防御

5G 是个开放的网络，海量物联网设备暴露在户外、硬件资源受限、无人值守，易受黑客攻击和控制，因此网络将会面临大量的网络攻击。如果采用现有的人工防御机制，不仅响应速度慢，还将导致防御成本急剧增加，所以需要考虑采用智能化的手段防御海量物联网设备的安全威胁。此外，网络攻击日趋自动化，0day 攻击的可能性越来越大，5G 中需要考虑被动变主动的安全防御机制。

垂直行业的 IoT 设备，和传统终端相比存在数量众多的特点。在 5G 中需考虑如何应对海量终端被劫持并对网络发起 (D) DoS 攻击。和单个终端发起 DoS 攻击相比，联合海量终端向单一网络节点发起 (D) DoS 攻击危害性更大。例如目前 3GPP 正在讨论引入公钥验证终端的永久标识，目的是增强隐私保护，但同时增加了网络节点的运算负荷，如果攻击者滥用这个功能，利用海量终端同时对网络发起验证请求，(D) DoS 风险将急剧增加

1.3 5G 引入 IT 新技术、新架构带来的安全挑战

为提高通信系统的灵活性、可扩展性和部署速度，5G 网络将引入 IT 新技术、新架构，包括 NFV/SDN 以及服务化架构。IT 新技术、新架构在使能网络功能的灵活性、可扩展性和快速部署的基础上，也给 5G 安全带来了新的挑战。

系统级的安全保护和访问授权机制

5G 网络中 NFV 虚拟化技术的应用，可进一步简化网络功能的部署和更新，使得部分功能网元以虚拟功能的形式部署在云化的基础设施上。5G 需要考虑基础设施的安全机制，从而保障 5G 业务在虚拟化环境下能够安全运行；同时定义更好的安全隔离手段，增强虚拟功能网元之间的安全管理。基于虚拟网络的切片也需要安全机制，保证切片的安全运营，用户的正常接入。

5G 服务化架构将网络功能进行解耦，并定义通用的服务化接口，支持各网络独立扩容、独立演进、按需部署，支持在被授权的情况下灵活调用各服务化网络功能。因此 5G 需从整体安全架构的角度考虑网络功能发现、授权和调用的安全。

全新的端到端安全评估

考虑到运营商网络的系统开放性和设备的多样性需，在软硬件解耦、虚拟化的环境中部署网络功能，要进行谨慎的安全评估。虽然 4G 也提出了端到端安全评估的概念，但是 4G 安全评估标准不适用虚拟化网络功能设施，以及系统级的评估。因此，5G 安全需要全新的端到端安全评估机制，来保障引入 IT 新技术后 5G 网络的安全部署。

02

业务和网络架构的变化驱动 5G 安全架构变革

5G 安全架构需进行以下变革，来支持 5G 拓展行业用户，应对 5G 海量物联网终端带来的安全挑战，在网络 IT 化环境中提供端到端的安全保护和防御手段。

2.1 5G 安全新特性

2.1.1 可扩展的身份管理机制

5G 需要多元化的身份管理机制和可扩展的身份管理框架，来应对垂直行业和海量物联网终端带来的安全管理需求。

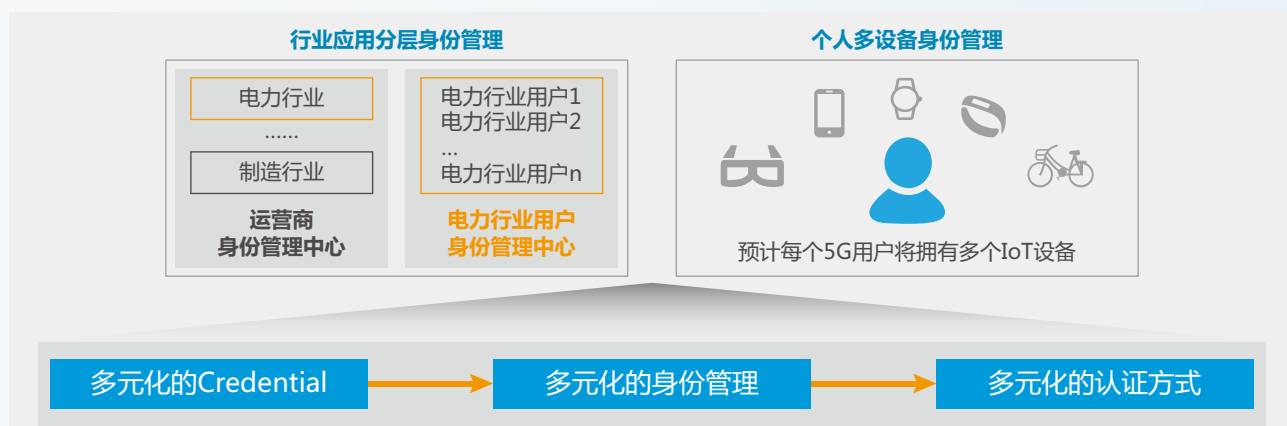
多元化的身份管理机制

为行业用户提供分层身份管理机制

未来运营商可以对行业用户的大量 IoT 终端采用分层的身份管理方式，即运营商管理行业用户身份，而行业用户管理终端用户身份，行业用户与运营商协作共担用户管理责任。这样，对于同一个行业用户的海量终端，网络的认证和授权都可以关联到同一个行业用户，从而方便的进行计费管理。行业用户可以在运营商许可的范围内，灵活的增加、减少终端，满足自身行业拓展的需要。

为个人用户提供以用户为单位的身份管理机制

未来个人用户可能同时拥有多个 IoT 设备，允许用户对自身的多个设备（如可穿戴设备）在一定范围内进行灵活的管理，包括设备的入网和服务属性等，如允许流量以在线和离线的方式在用户的不同设备之间共享。同一个用户的不同设备所使用的身份应该是相互关联的，他们的认证和授权也可以通过这个用户的身份标识进行关联，统一管理。



基于 (U)SIM 的可扩展身份管理框架

面向传统 eMBB 设备，基于对称钥的身份管理机制将得以延续

5G 中 eMBB 业务的主要服务对象仍然是移动宽带用户，4G 中采用的基于对称钥的身份管理方式可以满足这种业务需求。对称钥身份也可以帮助运营商管理设备，以及进行其他类型的身份信任状的发放。因此，即使 5G 需要多元化的身份信任状和身份管理，基于 (U)SIM 卡以及对称钥的身份管理方式在 5G 时代将得以延续并将发挥重要作用。

面向海量物联网设备，需要扩展基于对称钥的身份管理机制

物联网是 5G 网络最重要的场景，包括 mMTC 和 uRLLC。基于对称密钥的身份管理方式，存在认证链条长，身份管理成本高等问题，不利于运营商网络与垂直行业的融合，也不利于对海量物联网设备时有效支持。因此，面对 5G 物联网海量设备，我们需要引入基于非对称钥的身份管理机制，让运营商能够灵活高效的管理行业用户的 IoT 终端和可穿戴设备，缩短认证链条，提高海量设备网络接入认证效率。

对称钥和非对称钥的身份管理功能在网络侧可能会根据不同的业务切片进行部署，但运营商需要建立统一的身份管理体系。

2.1.2 安全功能的灵活调用和编排

如果 5G 网络具备保证各项业务安全的安全机制，并将其分解为模块化的、可调用的、可组合的安全能力，则在创建新业务时可以通过部署编排相应的安全能力，构建满足该业务安全需求的安全机制和防护措施。

在网络安全能力模块化的、可调用的、可组合的基础之上，垂直行业也可以灵活的调用所需的安全功能，满足特殊的安全需求。



安全功能的快速部署和调用

基于服务化架构，可以将网络具体安全功能或者能力进行独立的服务化定义，使得其他功能在授权的基础上，可以调用此安全功能或能力。这里安全功能或能力可以包括用户身份管理、认证鉴权，密钥管理及安全上下文的管理等等。安全功能的服务化定义增强了安全功能的精细灵活化管理，支持灵活调用，同时支持对调用安全功能的授权。

5G 业务安全需求的多样性也使得安全配置和管理变得复杂，如果还依靠人工来配置、管理和响应，会导致低效率和高成本。所以，在网络功能自动化管理的基础上，也需要安全能力管理自动化，包括安全功能的部署、编排、配置、调用等。

安全能力开放

作为普适性的全连接网络，5G 将比上一代网络更加开放，而网络能力开放需要相应安全保障。更进一步，可以将安全能力同网络能力一样开放给垂直行业使用。

安全能力开放要求 5G 网络内的安全功能以模块化的方式部署，并能够通过相应接口方便调用。通过组合不同的安全功能，可以快速提供安全能力以满足多种业务的端到端安全需求。通过安全能力开放，垂直行业可以直接安全地部署业务，从而降低了业务门槛并缩短部署时间。运营商则可以充分利用网络安全基础设施，丰富业务体验，与垂直行业一起共同创造和分享价值。这里安全功能或能力可以包括用户身份管理、认证鉴权，密钥管理及安全上下文的管理等等。

2.1.3 敏捷高效的分布式安全部署

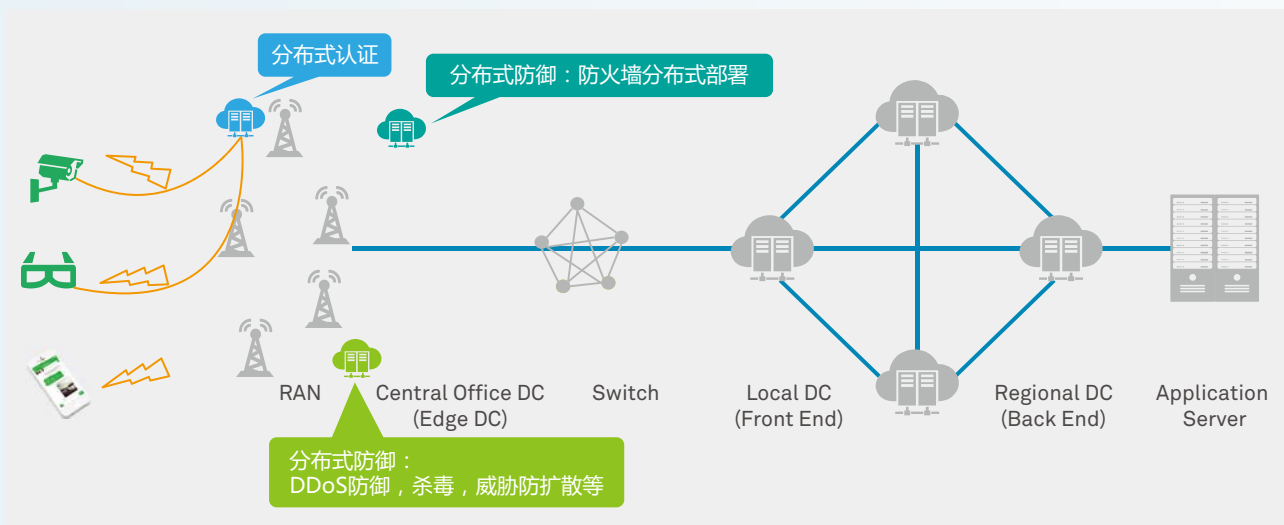
海量物联网设备对 5G 安全带来了新的威胁和挑战，包括大规模的网络攻击行为，海量设备认证信令风暴等。为了应对上述安全威胁和挑战，5G 安全架构需考虑支持分布式安全机制，即根据防御、安全管理等需求部署分布式安全功能。分布式安全功能包括分布式认证和分布式防御。

分布式认证机制

作为 5G 重要业务场景，海量物联网设备同时接入认证将会对网络的数据处理提出更高的要求。而传统集中式的认证机制中，每次设备的认证都需要调用核心身份管理节点，从而造成针对此节点的信令冲击。因此，5G 安全架构需要分布式的认证机制，应对海量设备的认证需求。分布式认证机制具体体现在，对于设备的认证可以通过多个分布式的认证节点并行执行，从而减少对于核心身份管理节点的访问，支撑海量设备的高效认证。分布式认证节点的部署可以根据海量物联网设备的分布情况进行灵活化的部署，降低网络的认证成本和复杂度。分布式认证机制可以采用基于证书的安全机制，也可以采用基于身份的安全机制。

分布式安全防御

分布式安全防御技术的理念是通过在网络边缘节点部署安全防御能力，从更靠近源头的地方扼制攻击行为，实现更敏捷的安全防御。具体体现在，为满足海量物联网设备的接入防御机制，5G 安全可将安全防御能力部署在更靠近 IoT 设备的接入点，如 RAN 或者 Edge DC。防御能力包括 DDoS 防御机制，分布式杀毒防御技术等。此方式可及时的应对设备的攻击行为，降低海量设备的接入攻击威胁。



2.1.4 切片安全机制

网络切片是 5G 及未来通信网络中的一项重要使能技术，其面向业务配置网络的特性可以有效地助力垂直行业进行数字化转型。切片安全同样是可配置、可裁剪的。切片安全本身可以为网络提供快速、差异化的、可裁剪的安全功能、性能、安全保护机制，从而用一套网络设施满足千差万别的应用、行业的需求，使能垂直行业快速推出安全新业务、使能客户简化安全运维、降低运营成本。

切片网络中的基础设施是共享的，除了共享带来的巨大优越性以外，同时带来一些潜在安全风险，网络切片是一个打通了各个子域的一组网络功能，资源，及连接关系构成的有机整体。各个子域都会有各自的安全风险及防护需要考量，如切片的终端部分安全、接入网安全、核心网切片安全和承载传输网切片安全等。端到端切片安全更重要的也应该是横向整体的考虑。

切片安全的差异化机制

不同终端的安全功能、性能、安全保护的需求在不同的应用场景可以是完全不同的。例如，用于视频播放的 eMBB 终端，对终端认证、加解密的安全需求同 LTE 类似；而传感器式的终端，由于计算能力有限、安全需求不高及成本敏感，需要有轻量级的认证、加解密算法；对于可靠安全通信，终端则需要快速接入认证、强加密算法的支持。因此，切片安全首先需要提供不同终端的安全差异化保护。

切片的安全隔离

切片的特征是切片和切片之间在逻辑功能上是分离的，但在物理资源上是共享的。因而切片安全的首要问题是如何做到网络切片之间的安全隔离。如果没有隔离，拥有某个切片访问权限的攻击者，可以以此切片为跳板，攻击其他的目标切片。比如，攻击者可以利用其合法接入的某个切片来非法占用目标切片的资源，导致目标切片不能正常对其合法用户提供服务。另外，在一个终端同时接入不同切片的场景，没有切片的隔离可能导致数据机密性（数据泄露）和完整性遭到攻击。

切片的隔离最先要考虑的是在切片的生成阶段。一个切片可以横跨多个子域：如终端、接入网、核心网、承载网等，各个子域的隔离都需要考虑，并进行资源的统筹安排，以达到一致的、端到端的隔离要求。其次，在实际业务运行时，终端与

切片网络的网元交互、安全协议、流程，都需要考虑到相应的隔离。

终端访问切片控制

端到端切片的主要目的之一是支持多样化的商业模式、满足不同行业、不同应用的需求。由于切片以及终端的多样性，终端访问切片的控制方式也将是多种多样的，保证用户设备能适时接入切片，同时得到应有的访问安全防护，防止受到外界的攻击。

切片管理面安全

切片管理面安全主要是保护切片在整个生命周期的安全。切片的生命周期包括四个阶段：准备、配置与激活、运行、撤销。在切片生命周期每个阶段都存在安全风险。比如，攻击者可以通过恶意软件攻陷切片模板，从而威胁到其生成的所有网络切片实例；攻击者也可以通过配置接口在配置或运行阶段攻击切片；切片在撤销阶段，如果不恰当处理，攻击者可以获得机密数据。因此，管理面的安全对整个切片网络至关重要。

在面向垂直行业的切片中，一些垂直行业有自行管理切片及切片安全能力的诉求。切片网络需要具备为不同切片提供不同安全特性的能力并对管理接口提供有效的安全保护。

2.1.5 主动智能的联动安全防御机制

5G 网络的复杂性和开放性、海量物联网设备的接入、行业用户安全需求的多样性使得安全管理的复杂度和工作量大增。依赖人工进行安全管理可能会导致响应慢、成本高等问题。因此，我们建议 5G 网络需要考虑引入基于智能化的主动防御技术，结合 IT 网络防御机制，形成一个基于统一情报威胁分析的，支持 ICT 联动的网络智能防御系统。

智能的异常检测、综合的威胁分析

5G 网络的复杂性和开放性使得安全威胁的种类大大增加，引入人工智能来检测未知攻击、复杂攻击的需求更为强烈。在网络的软件化、虚拟化背景下，复杂攻击的检测溯源需要使用机器学习的方法将虚拟机异常监控、恶意代码检测与核心网流量异常检测结合起来。智能的检测、综合的分析系统、代码、流量的异常。

ICT 安全情报协同

为了快速应对安全威胁，运营商之间、运营商与厂商之间、运营商与行业用户之间需要联动，实时交换安全情报，实现安全协同的自动化、智能化。例如，在运营商网络检测到异常终端时，可以将终端异常状态及时通知行业用户，行业用户来打补丁或清除恶意代码；运营商和行业用户之间通过人工智能直接交换异常信息，联合分析异常，定位攻击，可以提高效率，减少人工介入操作带来的响应时延。

建立自动化防御

网络的各层各域将会部署漏洞扫描、安全加固、防火墙、恶意代码检测、流量异常检测等多种安全功能。多种安全功能之间的协同会变得异常复杂，人工智能的引入可以大大提高效率，提高从安全监控，到安全检测分析、攻击阻止、攻击隔离、攻击预防等各环节的自动化程度，实现敏捷的安全管理。

2.2 对 4G 安全特性的延续和增强

eMBB 是 5G 网络的主要形态之一。它也是 4G 网络的直接扩展。因此，基于 4G 安全特性，可以构建 eMBB 的安全功能是很自然的。5G 的标准分阶段开发，eMBB 在第一阶段占主导地位。因此，eMBB 安全性在第一版 5G 安全标准中起着重要作用。综上所述，一种构建 5G 安全性的自然方式是从 4G 安全性开始，并根据新的 5G 安全需求进行扩展。从身份管理、终端安全、网络设备安全、密码算法和服务化角度，对 4G 安全及 5G 安全机制做了对比，如下表所示。

	4G	5G
身份管理机制	(U)SIM 身份管理机制	多元化的身份管理机制 eMBB 延续 (USIM) 身份管理机制
终端安全	终端中密钥存储、安全参数传递和安全运算的保护	延续 4G 终端安全，同时支持低成本 IoT 等设备安全
网络设备安全	4G 基站等网络设备保护机制	延续 4G 基站等保护机制，同时支持 NFV 部署环境下安全功能保护
数据保护算法	4G 安全密码算法	延续 4G 安全密码算法保护机制，同时考虑支持抗击未来更强算法攻击的保护算法
网络域安全	安全端到端的隧道建立机制 信任关系建立机制	延续 4G 网络域安全，同时支持基于服务化架构下网络域安全

基于 (U)SIM 卡的可信根可在 eMBB 场景下继续沿用

用户永久身份 ID 和根密钥是身份管理和认证的基础。针对 4G 的终端应用，基于 (U)SIM 的身份管理机制可提供根密钥安全存储保护和互操作的安全环境。同时基于 (U)SIM 的认证机制，可建立设备与网络的双向认证。因此，针对 5G 中 eMBB 等业务类型，4G (U)SIM 身份管理和认证机制可以延续使用。

需要考虑新的终端形态

4G 用户终端在密钥存储、安全参数传递和安全运算等都支持在安全保护的状态下执行，5G 用户终端可延续这些已有 4G 用户终端的成熟安全机制。同时，可预见 5G 将引入各种硬件资源受限、低成本、低功耗的 IOT 终端，继续沿用传统移动终端的安全机制已不可取，需要设计出更轻量化的数据保护和安全传输机制。

建议增强网络设备安全

4G 网络环境下基站处在相对不安全的位置，要求基站支持在安全的环境下进行设备启动、密钥存储、安全运算，以应对来自网络的攻击。5G 需延续 4G 基站设备安全环境的能力。另外，5G 中也包括其他海量网络设备的参与，以及 NFV 的部署。因此对于网络设备的基础安全能力，5G 需延续并根据网络设备部署方式的不同进一步增强。

需考虑应对未来的密码算法攻击

网络接入安全，可应对来自空口的攻击包括 UE 到 AN 的空口信令和用户数据的安全保护，UE 到 CN 的信令保护，以及 UE 的流动性管理安全。此类保护属于移动通信的基本安全需求，5G 安全需继续延续。同时针对未来更强的安全算法攻击方法，5G 可以考虑采用更长的安全密钥或采用更强的安全保护算法。

需考虑服务化架构下的新协议

作为回传网络和核心网数据通信的底层保护方法，网络域安全提供了安全端到端的隧道建立机制，以及信任关系建立机制。5G 核心网需同样支持网元与网元之间，以及安全域与安全域之间的数据传输，因此成熟的网络域安全机制仍旧可延续。另外，5G 安全也需考虑基于服务化架构下网络域的安全机制，以及不同运营商网元之间安全通信的方法。

2.3 面向业务构建可扩展、可编排的智能 5G 安全架构框架

5G 安全架构应该以早期的 eMBB 场景下的核心安全功能为基础，扩展到对 mMTC 和 uRLLC 场景的支持，面向业务构建可扩展、可编排的智能 5G 安全架构，实现差异化安全能力的快速部署和安全能力开放。

5G 安全架构设计原则

在 5G 网络架构之上叠加逻辑安全架构。安全架构应以通信网为基础，针对 5G 整体特征进行安全防护设计。5G 功能相对解耦于其他网络特征或功能，在不影响 5G 整体的情况下具有一定的自我更新和扩展能力。

分域、分面设计安全架构。遵循通信网分域、分面的协议设计原则，将安全特征嵌套其中，这样可以高效调用安全功能；在 5G 架构中，越来越呈现这样一个趋势，逻辑安全功能往往独立于其他网络功能。因此我们可以这样解释 5G 网络安全面，即为一组独立的安全功能，这些安全功能在运营商网络中可以进行单独部署、配置或定制。同时从安全视角考虑风险级别，在设计上应进行安全边界防护设计，并将防护措施部署在靠近潜在攻击点的位置，提高反应速度、缩小影响范围。



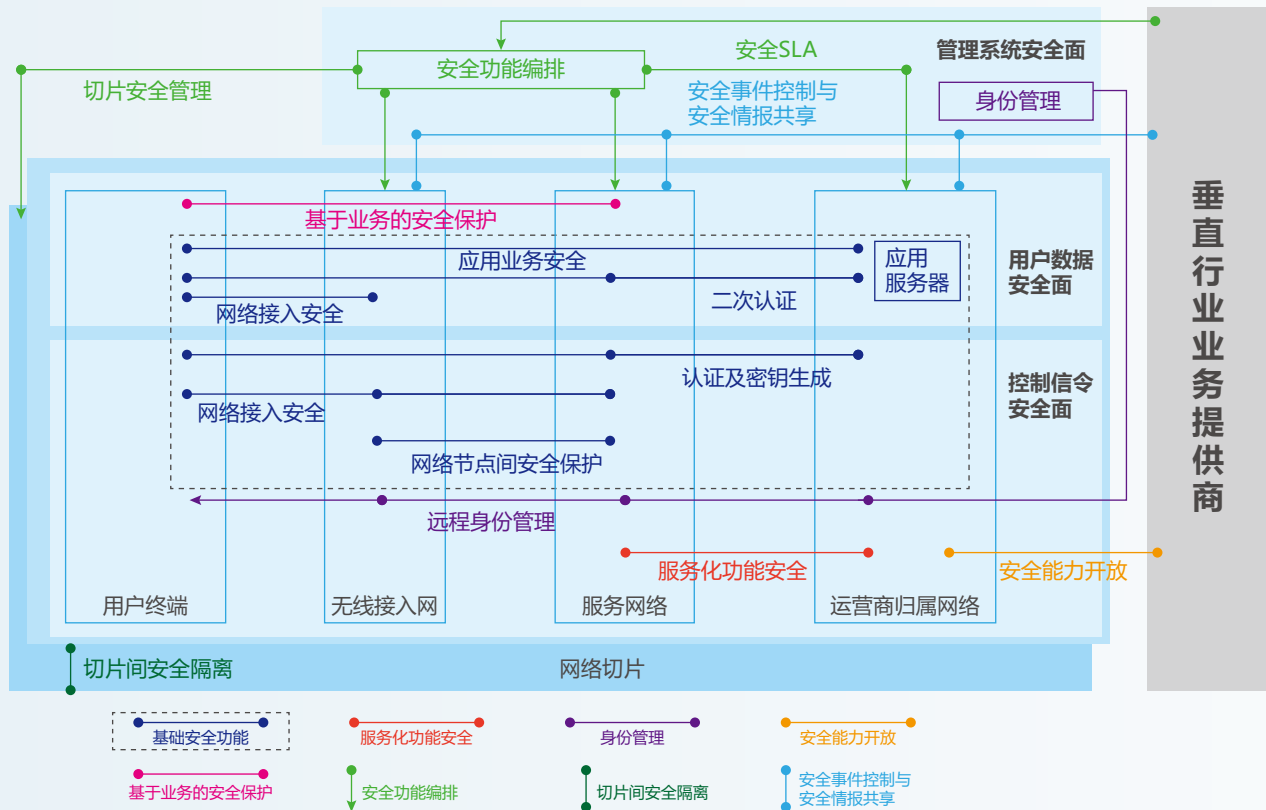
可扩展、可编排的安全架构。不同的业务场景和用户对安全的期望不同，同时不同的时间和事件也可能触发安全功能的提升或降低、安全能力的增多或减少，弹性可伸缩、可编排与可扩展的安全架构才能够支撑业务的灵活和快速部署。

原子化、服务化的安全接口，安全能力对外开放。基于 5G 服务化架构，安全作为 5G 中的逻辑能力，同样需要提供可以被调用的接口，并可以面向垂直行业提供安全能力的开放。

端到端全业务安全管理体系。管理面对单点网络设备的安全和全网安全进行管理，建立一套完善和安全级别高的端到端管理体系是全网安全基础和必要的条件。

5G 安全架构框架图

本文中的 5G 安全架构框架，在 eMBB 场景下的基础安全功能上进行扩充以支持切片安全和安全能力开放，应对 mMTC 场景及 uRLLC 场景的安全需求和挑战，使网络的安全管理更加智能化。蓝色虚线框内的基础安全功能对应 3GPP 5G 安全 TR33.899 version 1.3.0 中的“ Overview of 5G security architecture” 章节。灰色实线框表示垂直行业业务提供商相关的安全功能和接口，其他的功能和接口属于移动运营商的范畴。



三个安全面，两个安全机制：

在 5G 架构中，越来越呈现这样一个趋势，逻辑安全功能往往独立于其他网络功能。因此我们可以这样解释 5G 网络安全面，即为一组独立的安全功能，这些安全功能在运营商网络中可以进行单独部署、配置或定制。

管理系统安全面

在传统的管理面安全基础能力（如账号口令、安全日志等）之上，5G 安全架构中的管理面安全需要具有以下能力。

面向业务的安全功能编排

在生成网络及网络切片的生命周期管理过程中，管理面的“安全功能编排”功能根据业务提供商的安全 SLA，差异化剪裁安全功能和安全保护机制，在相应的业务切片内对网络的安全功能进行编排，高效的部署切片所需的安全功能。

安全功能编排功能从北向接口获取安全 SLA，根据安全 SLA 生成安全策略，进行相应切片的安全功能的组建，并且通过对应的网络安全功能编排接口分别在运营商归属网络、服务网络、接入网络进行安全功能的编排策略下发。网络控制面安全根据安全编排策略配置切片内相应的安全保护机制。

安全 SLA 的获取过程应该依附垂直行业 SLA 的获取过程，同时，安全功能编排和的过程应该依附切片中其他网络功能的编排过程。

可扩展的身份管理

可扩展的身份管理机制继续沿用基于 (U)SIM 卡的身份管理，同时支持基于非对称钥的身份管理机制，对行业、用户、终端的身份进行统一的管理。

eMBB 终端将继续沿用对称钥进行的身份管理，对于行业用户的物联网终端，可以考虑采用非对称身份管理机制，运营商基于全局公钥对行业用户分发身份，再委托行业用户对物联网终端进行远程身份管理。

用户数据安全面

在传统的用户面安全基础能力之上，5G 安全架构中的用户面安全需要具有以下能力。

面向业务的差异化安全保护

根据安全策略剪裁用户面的安全保护机制，以满足不同的业务差异化的数据传输保护需求。运营商网络应根据安全功能编排功能下发的业务安全策略，在控制面配置用户设备和网络之间的用户面数据保护机制，如，密钥长度、密码算法等，并在用户面实施策略对应的安全保护。应由运营商网络负责根据业务安全策略、网络策略、终端策略，来决策、协商、配置适当的用户面安全保护机制。

控制信令安全面

在传统的控制面安全基础能力之上，5G 安全架构中的控制面安全需要具有以下能力。

运营商灵活调用安全功能

根据管理面的安全编排策略，基于服务化架构、虚拟化技术，灵活部署网络安全功能。基于灵活的安全功能部署和调用，高效的提供安全能力开放。

根据业务安全策略、网络策略、终端策略，来决策、协商、用户设备和网络之间的数据保护机制，如，用户面保护的密钥长度、密码算法等。

面向物联网设备，支持可扩展的认证机制和远程身份管理

基于多元化的身份管理机制，进行物联网设备 / 可穿戴设备的远程身份管理，并提供基于对称钥、可扩展支持非对称的认证机制。

切片管理安全机制

切片管理面安全广义上讲主要包含三个方面：1) 切片安全即服务 (Slicing Security as-a-Service or SSaaS) 2) 切片生命周期的安全 3) 切片的智能安全运维。SSaaS 可以使能运营商为垂直行业提供差异化、可定制的安全套餐；监测安全套餐性能；根据需求或监测结果，及时调整增强套餐或删除部分配套、调整资源配置。安全套餐可以包括加密算法、参数、配置黑白名单、认证方法、隔离强度等等。SSaaS 是通过管理面的专门接口为垂直行业提供服务，这个接口必须有充分的安全保证，只有经过认证、授权的签约客户才能使用。

切片生命周期的安全是保障切片在设计、生成、激活、运行、终止等状态的安全并防止潜在的软件漏洞造成的影响、安全存储、安全释放资源。

切片的智能安全运维主要是通过安全感知及监测等技术手段，对切片进行自动化的安全功能编排、安全策略控制、告警。

主动智能安全防御机制

网络智能安全控制中心调度协同安全部件，在运营商网络和垂直行业间，基于安全事件进行信息共享与安全策略控制。通过实现安全部件分布式部署，安全策略自动化配置，使 5G 网络的安全防御由人工被动应对变为智能主动防御，形成统一联动安全防御机制。

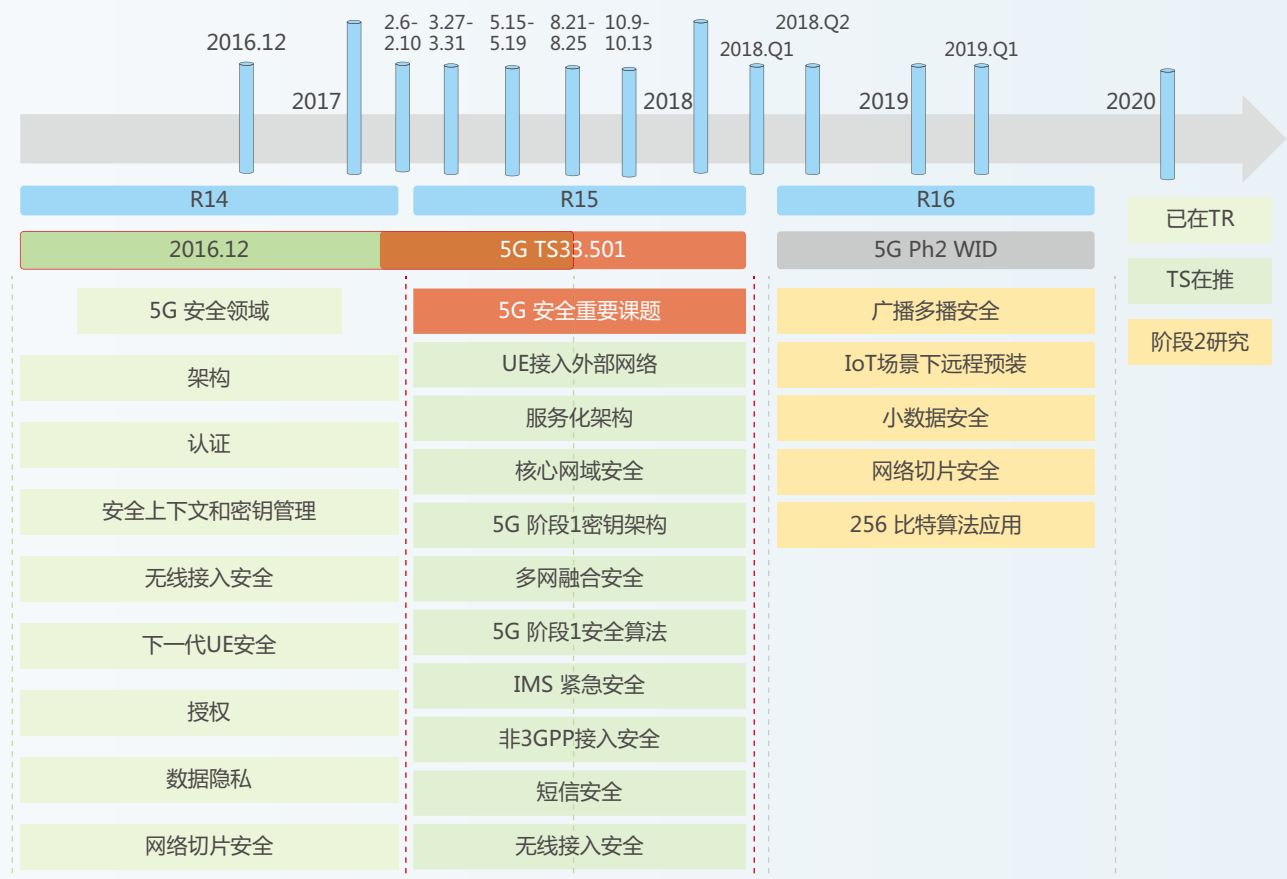


2.4 5G 安全全球标准化进展

5G 安全在 3GPP、IMT-2020、ITU-T 等标准组织中取得了重大进展, 具体来说, 5G phase1 阶段的 5G 安全框架、接入安全、用户数据的机密性和完整性保护、移动性和会话管理安全、用户身份的隐私保护及与 EPS 的互通等相关工作已完成绝大部分。目前, 3GPP SA3 已经启动 256 比特密码算法的研究项目, 且确定在第一阶段标准的 5G 安全信令中需要支持 256 比特密钥。对于 256 比特密码算法, 3GPP 确定在 2018 年 3 月截止的 5G 协议中需要支持算法应用协议标准化, 但不选定具体的算法, 密码算法标准化预计在 5G 标准第二阶段启动。

由于 5G 网络安全特性与方案需要与无线接入网和核心网架构紧密结合, 因此, 除了 SA3 之外, 3GPP SA1, SA2, RAN2, RAN3 中 5G 网络架构以及 5G RAN 的相关研究, 也与 5G 安全标准化工作紧密相关。

与此同时, 在其他标准组织中, NFV/SDN 等新技术将会给 5G 网络安全带来新的影响, ETSI NFV 安全组的研究内容涉及 NFV 安全架构、隐私保护、合法监听、MANO 安全、证书管理、安全管理、安全部署等方面; ONF 以及 ITU-T 的研究内容涉及 SDN 安全的标准化工作。具体 3GPP 5G 安全标准化进展可以参见下图, 其他标准组织的进展可以参考 3GPP 的 5G 安全标准化进展。



03

华为积极推动 5G 安全标准化 共建 5G 安全生态

未来更加多样化的业务场景和新型网络架构将驱动 5G 安全架构变革，也驱动业界共同构建新的安全生态来确保 5G 网络服务各行各业数字化转型的要求。

- 首先希望各国立法机构加强安全法规政策建设，完善网络安全生态基础
- 同时希望传统电信标准组织和各垂直产业组织积极合作，互通有无，构建健康的安全标准生态，共同提升产品和解决方案的安全防护能力
- 最后希望业界推动不同领域技术积极碰撞，共享技术创新成果，加快安全技术升级速度，共同为 5G 提供最佳安全解决方案

3.1 端到端安全评估体系

根据标准进行安全评估是保证 5G 网络安全的有效方法。全球统一的安全评估标准可以整合业界最佳安全实践，进而提升全行业的安全等级。同时，全球统一的安全评估标准也有助于减少单独的认证，从而降低全行业的认证成本。

5G 的安全评估标准应该涵盖“端管云”三部分，以支持构建 5G 端到端的安全评估体系。

“端”和“云”：5G 网络将承载更多的业务，各种类型的终端设备都将接入 5G 网络。同时，5G 网络也开放和第三方应用的接口。不安全的终端设备和第三方应用将对 5G 网络带来风险。终端设备和第三方应用的安全评估标准将有助于解决这些风险。

“管”：虚拟化技术将在 5G 网络设备中广泛应用，5G 网络设备的安全评估标准需要能够评估利用虚拟化云技术实现的 5G 网络设备的安全性。

总结

本文介绍了 5G 安全的新特性，如可扩展身份管理，分布式身份认证，网络切片安全等，5G 安全架构框架也展示了 5G 安全在为多样化服务提供保护方面有巨大潜力。4G 甚至更早期的网络接入安全特性得以继续在 5G 安全框架中得到充分利用。

我们可以得出这样的结论，5G 不仅催生新的数字化行业，还在网络安全方面向前迈进一大步。5G 将为促进现代社会的网络安全、业务安全的进步做出更大贡献。

参考文献



- [1]3GPP TS 23.501: "System Architecture for the 5G System".
- [2]3GPP TS 23.502: "Procedures for the 5G System".
- [3]3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- [4]3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".
- [5]3GPP TS 38.472: "NG-RAN; F1 interface control plane protocol".
- [6]3GPP TS 38.474: "NG-RAN; F1 data transport"

版权所有 © 华为技术有限公司 2017。保留一切权利。

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

商标声明



、HUAWEI、华为、 是华为技术有限公司的商标或者注册商标。

在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司
深圳市龙岗区坂田华为基地
电话: (0755) 28780808
邮编: 518129

www.huawei.com