5G 业务场景与安全设计

2016•11

HUAWEI


5G
4G
4G
3G

目录

引言

5G 网络为移动通信运营商带来了许多新技术和进步。因此，和 3G/4G 相比，运营商能够提供一个新的更好的服务的平台。由于物联网、工业互联网和自动驾驶汽车的发展，移动节点的数量将迅速增加。在移动网络向新方向扩展的同时，移动网络的传统用户将继续享受一系列改进的性能，包括更好质量的视频呼叫，增强现实等。

对新型服务场景和新型设备的扩展意味着与早期的移动网络（例如 GSM，3G 和 4G）相比，安全系列功能也需要显著扩展。来自前几代的安全架构是 5G 安全的良好起点和基础。(U)SIM 卡和 UICC 形式的安全模块已经为移动运营商和他们的客户提供了很好的服务，并且还将继续这样做。基于这些模块，移动网络提供了关键安全功能，诸如用户和网络之间的相互认证以及无线接口上的数据保护。但是这种硬核基础必须得到许多其他安全解决方案的补充，才能全面的满足 5G 网络的安全需求。

整个 5G 服务范围之大，以至于不可能用一刀切的安全解决方案来保护它。相反，在 5G 安全中还需要灵活性，使得在所有服务被充分保护的同时，还可以为需要更高安全性的服务添加额外保护。本白皮书展示了如何在所有主要服务场景中找到创造性解决方案。然而，我们还需继续研究所有这些解决方案如何仍然形成一致的 5G 安全架构。

01

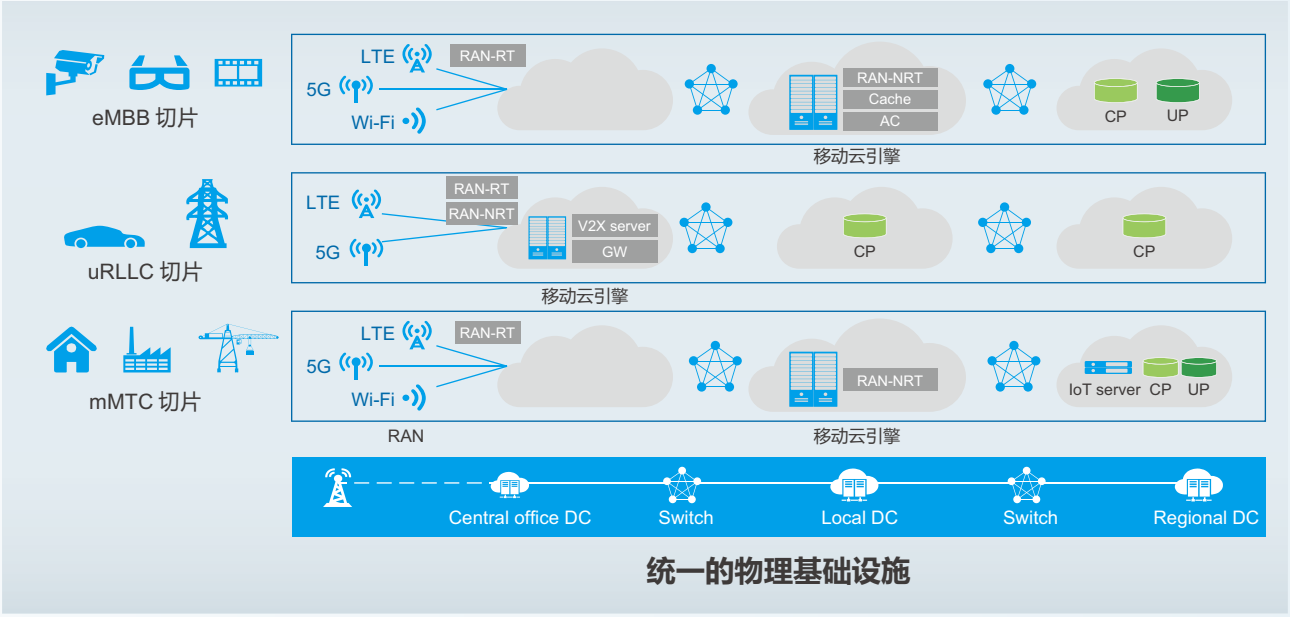
5G 场景和安全设计概要

5G 安全的主要需求和挑战

5G 满足 eMBB/uRLLC/mMTC 场景多样化商业需求

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。

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。



DC：数据中心　　eMBB：增强的移动宽带

mMTC：海量机器通信　　uRLLC：超可靠低时延通信

5G 安全的挑战和机遇

5G 面临 eMBB/uRLLC/mMTC 场景业务多样化、网络架构全面云化、运营商安全能力开放带来的安全挑战和机遇，以及更高的用户隐私保护需求。

业务多样化需要差异化安全保护机制

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。

接入技术和终端的多样化需要统一安全管理

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。不同的 5G 业务需要一些相同的基础安全功能，如接入认证和机密性保护，也需要统一的安全管理。

- **异构接入的安全管理**

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。

- **海量终端的安全管理**

垂直行业采用多样化的 IoT 设备，和传统终端相比存在数量众多、接入集中的特点，需要考虑新的高效接入认证方式。在 5G 中也需考虑如何应对海量终端对网络发起（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。

安全能力开放使能行业客户拓展

业务开放带来安全挑战的同时，也给运营商安全能力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。

安全能力开放使 5G 安全技术发展与业务发展互相带动，安全能力成为 5G 系统中行业应用的催化剂之一。

更高的用户隐私保护需求

5G 网络中业务和场景的多样性，以及网络的开放性要求考虑用户隐私信息线上线下综合防护。用户隐私信息也将随着业务的转移，从封闭的平台转移到开放的平台上，接触状态从线下变成线上，泄露的风险也因此增加。同时，全球对于用户隐私保护的呼声也不断增强。因此，5G 网络需要增强的用户隐私保护设计。

5G 安全设计

5G 系统需要构建通用的安全核心能力，支持多样化的业务，在不同的接入技术、云化网络架构之上建立一个统一的安全管理机制，覆盖安全核心能力。

在通用的安全核心能力基础之上，5G 系统提供差异化的安全功能、策略和解决方案，支持不同的业务场景。

端到端安全保护

端到端数据保护机制提升数据安全性

云化网络架构和异构多接入网络架构中，安全环境更加复杂。端到端数据保护提升云化网络架构中的用户数据安全性。在 5G 网络中采用端到端的方法保护用户数据，减少对云化网络安全环境的依赖，避免接入网复杂的多制式、多连接、多站点协同对数据安全带来的影响。

灵活的差异化安全保护

端到端安全保护可对差异化的业务安全需求提供灵活的数据保护。不同的业务应用有不同的安全需求，通过安全策略协商和基于业务的差异化安全管理，端到端的安全保护可以对不同业务会话提供按需的数据保护。

避免多次加解密的高效安全保护

端到端数据保护避免网络中间节点多次加解密，跟 hop-by-hop 数据保护相比，减少加解密处理次数，降低处理时延，提高效率。

统一认证

支持异构接入统一认证机制

在 5G 网络中，需要高效协同多制式、多接入、多站点的并发接入。因此，5G 网络需要构建一个高效的认证机制，能够在复杂的接入网上建立一个统一的接入安全管理机制。

支持多种认证协议

5G 网络面对不同行业和复杂的业务环境，需要灵活支持多种身份管理机制和认证模式。为了高效的管理多种认证模式，5G 需要一个支持多种认证协议的统一认证框架。

安全能力开放

安全是运营商的优势能力之一，通过安全能力开放，可以为行业客户提供安全服务。在 5G 多业务环境下，运营商可以构建一个以运营商数字身份为中心的业务生态环境，提供一个无缝融合到第三方业务流程的增强安全管理能力与保护机制。

按需安全管理

根据业务场景和安全的差异化需求，5G 安全框架应该具备弹性、灵活处理不同安全需求的能力。安全策略管理框架可以协商和下发特定业务的安全策略到对应的切片和网络节点，满足不同业务差异化的安全需求。

5G 三类业务场景的安全考虑

ITU 将 5G 时代的主要移动网络业务划分为三类：

- **eMBB**

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**

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**

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。

以下章节分三类业务场景分别描述相关的 5G 安全设计方案。

02

eMBB 业务场景安全设计

5G 早期应用 (VR/AR、高清视频) 驱动 5G 网络快速发展

随着移动宽带互联网的快速发展以及智能终端的普及，移动视频业务在运营商的业务比重中已经趋近 50% 并仍将快速增长，与此同时，基于虚拟现实 (Virtual Reality) 、增强现实 （ AugmentReality) 的移动漫游沉浸式的业务正逐渐将成为增强型移动宽带业务发展的方向。可以预见，从 4K/8K 高清视频到随时随地的移动漫游沉浸式体验类业务，对通信管道的连接需求强劲，将成为 5G 的早期杀手应用，并驱动 5G 的快速发展。

因此，5G 核心安全功能需要满足 eMBB 场景下各种业务的安全需求。

5G 安全需支持差异化业务、异构接入、开放的应用环境

VR/AR、高清视频对业务数据保护有不同的安全需求

不同业务的差异化安全需求，在 eMBB 网络切片中要得到相应的满足。eMBB 广泛的应用场景将带来不同的安全需求，对于个人用户，VR/AR 移动漫游沉浸式交互信息将成为下一代社交平台应用；对于行业客户，虚拟现实在行业应用领域和专业领域的产业链已经形成。前者可能要求只对关键信息的传输加密，后者可能要求对所有的环境信息的传输加密，对于个人应用和公共安全监控业务，安全保护强度的要求也可能有所不同。

多制式、多接入、多站点并发高速接入的安全需求

异构接入统一认证和安全管理，对提供高效的高速数据传输非常重要。未来的网络是融合的网络，需要同时支持 5G、Wi-Fi 的并发接入，多种接入制式如果使用不同的认证机制，管理复杂度较高，同时，移动过程中不同接入技术间安全上下文切换效率低、时延高。为简化安全管理，提高异构接入安全上下文切换效率，需要异构接入的统一认证和安全上下文管理。

运营商建立开放业务环境支撑行业客户的安全需求

安全是运营商的优势能力之一 ,可以进一步将安全能力开放给行业客户。行业客户普遍需要对用户进行安全管理 ,对业务内容进行安全保护。运营商已经具备比较完善的安全能力，如数字身份管理能力、认证能力等，并且在长期的运营过程中，与客户已经建立了良好的信任关系，作为运营商的优势能力之一，安全能力可以进一步开放给行业客户，提升行业客户的业务安全强度。

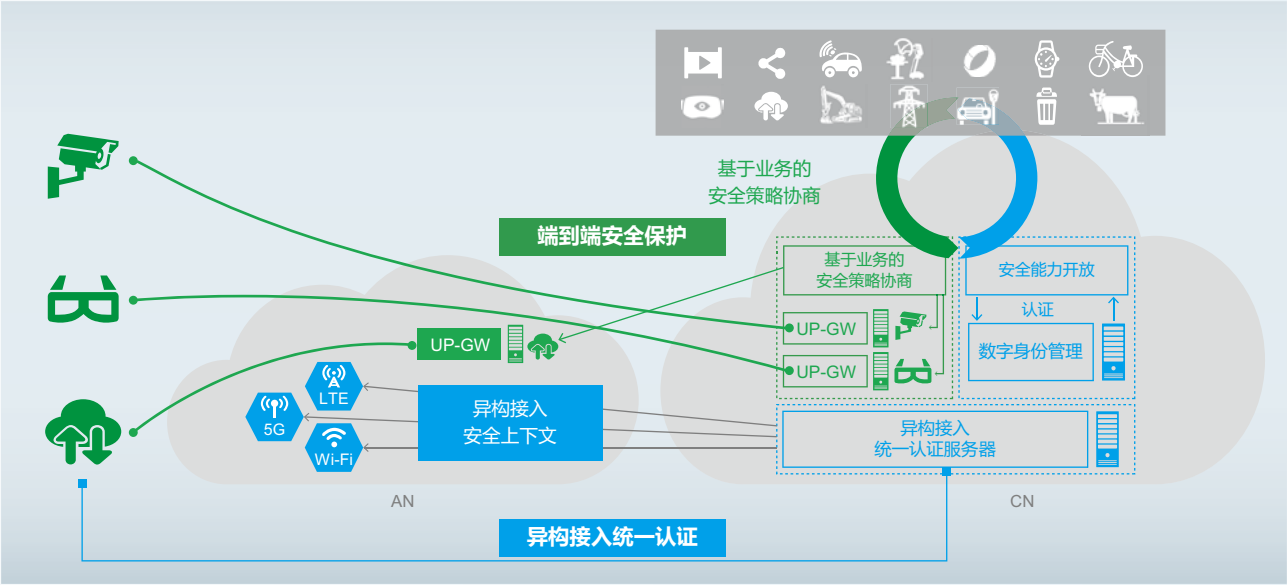
增强的用户隐私保护需求

eMBB 业务需要增强的隐私保护。eMBB 海量的业务（如 VR/AR）包含大量的用户隐私信息，比如个人的业务信息或标识、设备标识，以及地址信息等等，而 5G 网络的开放性使隐私信息的泄露几率增加，例如基于同一基础设施网络不同的业务切片等。另一方面，由于数据挖掘技术的发展，使得隐私信息的提取方式变得更加强大，能够将设备标识与用户标识（如用户的应用或业务标识）相关联，从而挖掘用户的网络行为。因此，在用户接入 eMBB 业务的过程中，隐私信息必须得到更加严密周全的保护。

5G 安全核心功能设计

为满足 eMBB 差异化业务安全需求，支持高速数据传输，支持行业客户的快速发展，5G 安全设计首先应该考虑 eMBB 场景下的核心安全功能，包括：

• 端到端安全保护　　• 统一认证　　• 安全能力开放等



面向业务灵活部署的端到端用户面保护

在 5G 中，我们建议设计更安全、更高效的 UE 到业务锚点端到端的数据安全保护。

端到端用户面保护的终结点

端到端的用户面保护从用户终端开始，终止到运营商网络中的出口网关。出口网关通常部署在核心网，在一些低时延本地业务场景下部署在本地边缘网络。当业务服务器也部署到运营商网络中时，用户面保护也可以终结在网络中的业务服务器。用户面的保护终结点无论在核心网或者是本地边缘网络，都需要位于高安全域，从而保证业务数据处理和存储的安全。

基于会话的端到端用户面保护

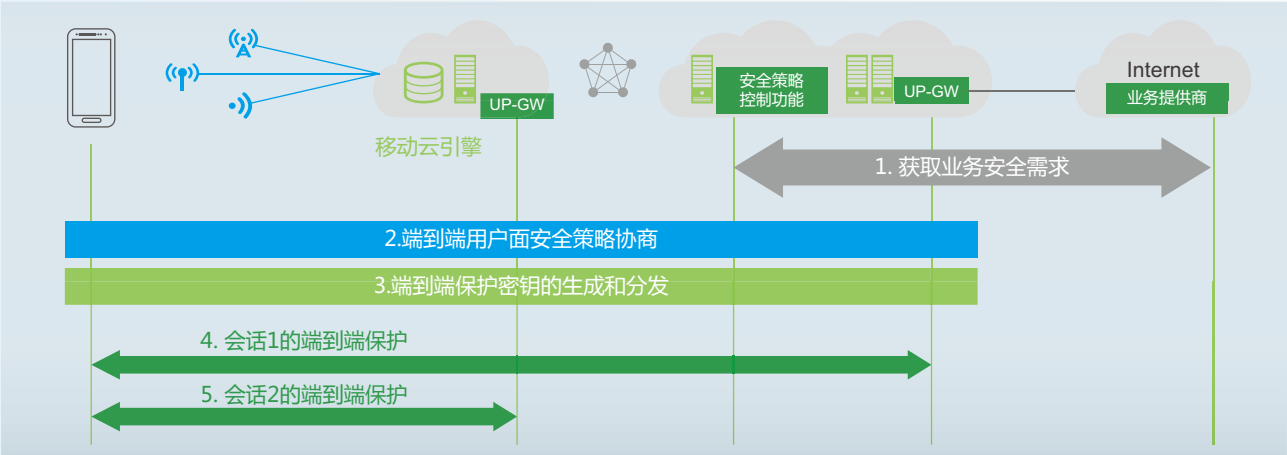
基于不同的会话做端到端数据保护，可以增加安全保护的灵活度。对于同一个用户终端，不同的业务有不同的会话数据传输保护需求，5G 可以对不同的会话数据传输进行差异化的安全保护。

灵活的安全策略协商

5G 端到端保护方案设计能高效的制定灵活的安全策略。通过和业务的交互，5G 系统获取不同业务的安全需求，并根据业务、网络、终端的安全需求和安全能力，运营商网络可以按需制定不同业务的差异化数据保护策略，如，不同的安全保护算法、更长的密钥长度、不同的数据保护终结点。

端到端用户面保护的协议设计

不同的业务承载在基于 PDU 的不同会话中，基于 PDU 传输协议，端到端用户面保护只需要对 PDU 载荷进行端到端数据加密，不对包头进行加密，保证网络节点能解读路由信息。

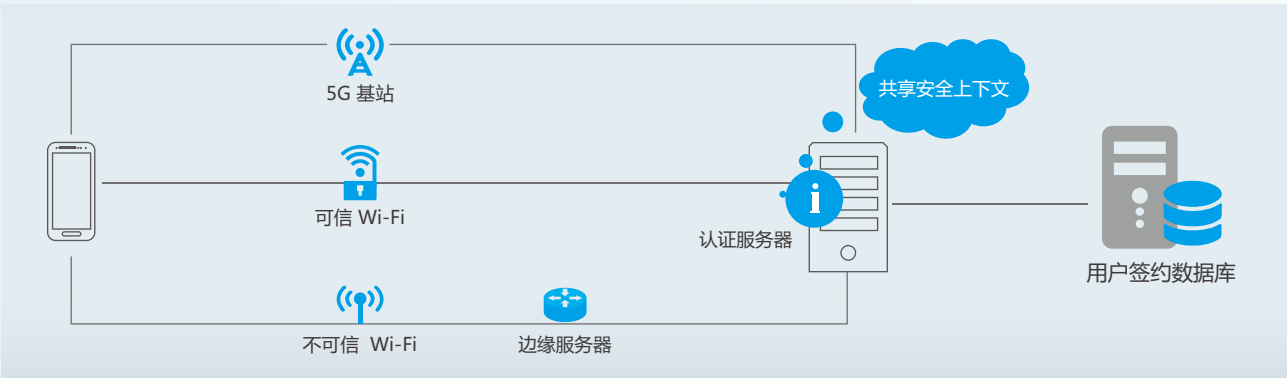


统一开放的认证框架支持多种接入技术和认证协议

未来网络将支持 5G、LTE、Wi-Fi、固定网络等多种接入技术，接入环境可以是可信的或者不可信的。传统上不同的接入技术采用不同的认证框架，在认证和安全上下文管理上需要不同的机制，同一设备在不同的接入技术之间切换时要重新认证。多种认证机制不但在安全管理上较为复杂，而且在不同技术间切换时带来额外的时延。

统一认证框架和安全管理

5G 可以提供一个支持多种接入技术和认证协议的框架，进行统一的认证和安全管理，降低安全管理的复杂度，方便设备在不同的接入技术间切换时可以共享已经建立的认证上下文，减少切换安全时延；同时可以在不同业务认证模式下支持多种认证协议，方便运营商拓展第三方业务。基于 EAP 的认证框架经过多年演进，支持多种认证协议，如基于对称钥的 EAP-AKA，基于非对称钥的 EAP-TLS 等。我们建议基于 EAP 的认证机制设计统一认证框架。



多接入切换安全上下文共享

使用统一的 EAP 认证机制，不同的接入技术可以共享认证产生的安全上下文。例如，当终端使用一种接入技术接入网络后，需要切换到另外一种接入技术时， 可以直接利用已有的安全上下文进行快速认证，不需要重新到用户签约数据库获取新的认证向量，从而降低接入时延。

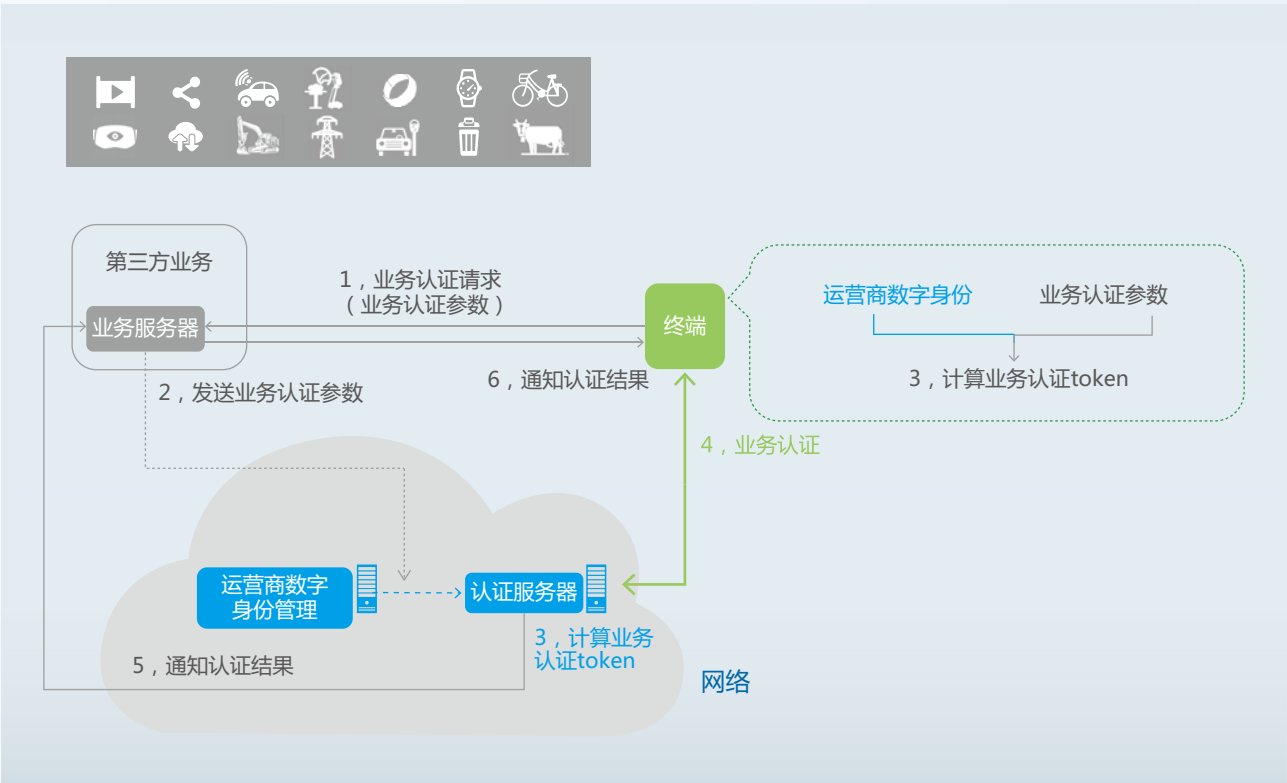
身份管理和认证能力开放促进 5G 业务生态环境的发展

运营商基于 (U)SIM 卡的数字身份系统是覆盖范围最广、用户最多的身份管理系统，运营商的认证机制得到业务和用户广泛的信赖。具有高安全性要求的业务很多基于手机短信验证码做多因子认证，提高业务对用户身份认证的可靠性。

5G 运营商面向业务融合的环境，可以开放基于 (U)SIM 卡的安全能力，增加业务认证维度，进一步增强业务认证安全性。

面向 5G 多样化业务，运营商通过 API 接口开放数字身份管理与认证能力，可以吸纳第三方业务进入运营商平台，有利于构建以运营商为核心的开放业务生态，增强运营商用户粘性，拓展新的业务收入来源。对于第三方业务来说，可以借助被广泛使用的运营商数字身份来推广业务，快速拓展用户。

在业务提供商与运营商建立信任的基础上，运营商将业务信息与运营商数字身份建立关联，终端与业务服务器通过开放 API 使用运营商数字身份与网络认证能力。



加强用户 ID 隐私保护

5G 网络将深入各行各业，越来越多的个人用户和行业用户将使用 5G 网络开展业务，用户隐私保护的重要性也越来越凸显。用户 ID 是用户重要隐私信息，开放的环境下需要加强用户 ID 的保护。

用户 ID 的保护可以采用随机标识替代永久 ID，从而避免永久 ID 在空口的传输。另外，由于 5G 接入网络包括 LTE 基站，因此 IMSI 的保护需要兼容 LTE 的认证信令，可以防御攻击者引导用户至 LTE 接入方式的降维攻击。

另一方面，基于非对称密码技术进行用户 ID 加密也可以有效防止攻击者在空口对用户 ID 的跟踪和窃取。

上述安全核心功能设计除了适用于 eMBB 场景，也适用于 mMTC 场景及 uRLLC 场景。

03

mMTC 业务场景安全设计

5G 网络深度支撑智能交通、智能电网、智能制造等行业应用

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。

由于物联网设备数量庞大，导致垂直行业对网络通信成本十分敏感。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。

mMTC 安全需要支持低成本、高效率的海量连接

面向物联网成百上千亿的连接，基于 (U)SIM 的单用户认证方案成本高昂，而 IOT 场景下终端的 ARPU 较低，因此，传统的认证方式成为制约 IOT 大规模应用及用户数增长的障碍。在 5G 网络中，需要考虑如何降低 IOT 设备在认证和身份管理方面的成本。

采用去中心化模式实现物联网场景下身份管理和接入认证，可以：

- 缩短认证链条
- 实现快速安全接入
- 降低认证开销

同时缓解核心网压力，规避信令风暴以及认证节点高度集中带来的瓶颈风险。

与传统集中式认证机制相比，去中心化认证机制分散了认证节点受到攻击的压力，避免单个网络节点被海量终端同时攻击，从而降低 (D) DoS 攻击的风险。

相当一部分物联网设备将会采用小数据集中发送或分散发送的模式传送业务数据。为提高数据传输效率和网络资源利用效率，在小数据业务中可以采用非对称密码技术实现业务数据和身份认证消息的同时传输。

去中心化模式下的身份管理与认证机制

身份管理与认证机制的去中心化，其实质就是简化在线管理，最大限度降低运营商身份管理的复杂度，消除认证中心节点，减少运营商部署成本。

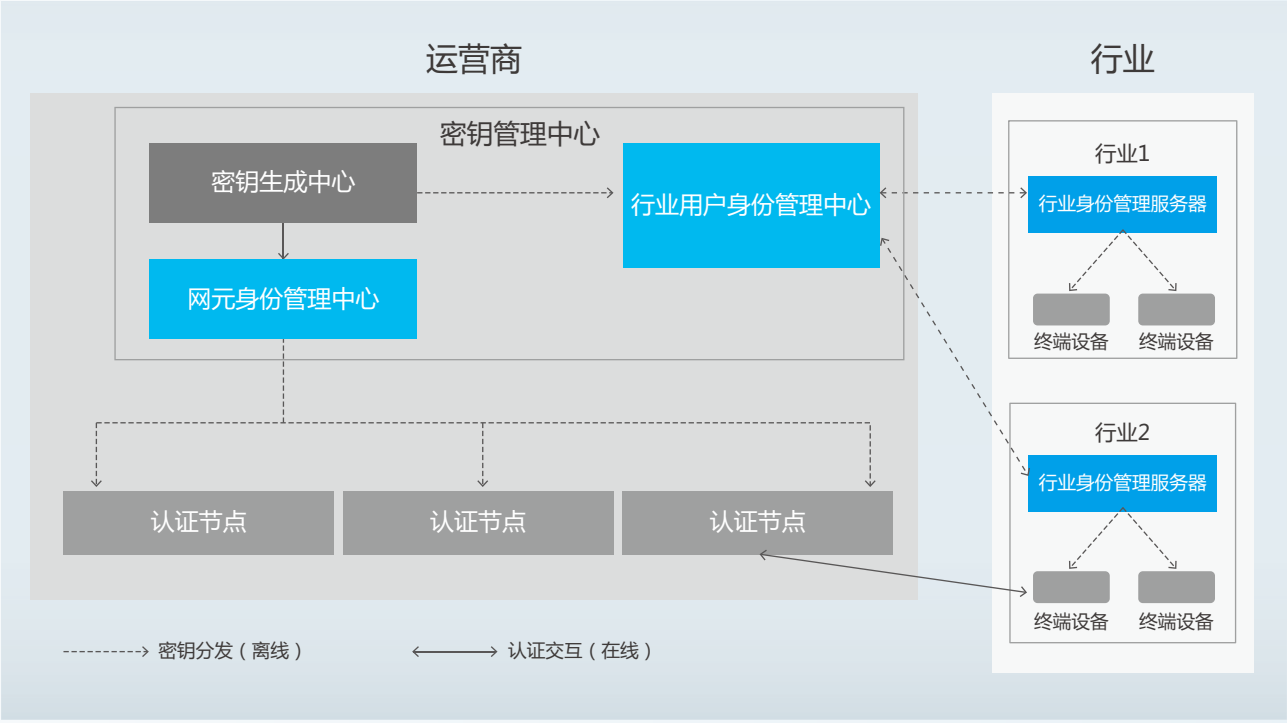
分层身份管理降低管理复杂度

网络与业务融合分层的身份管理设计，有利于运营商与行业客户灵活定义用户身份管理职责，为行业客户提供量身定制的身份管理策略。网络与业务身份的融合分层支持灵活的实现方式，可以由运营商独立生成信任凭证，用于网络接入认证和业务接入认证；也可以由运营商、行业客户联合生成和发放信任凭证，用于网络、业务接入认证。

去中心化认证机制提高安全效率

网络认证节点可以采用去中心化部署方式，如下移至网络边缘，终端和网络的认证无需访问网络中心的用户身份数据库。

非对称密钥体制具有天然的去中心化特点，无需在网络侧保存所有终端设备的密钥，无需部署永久在线的集中式身份管理节点。

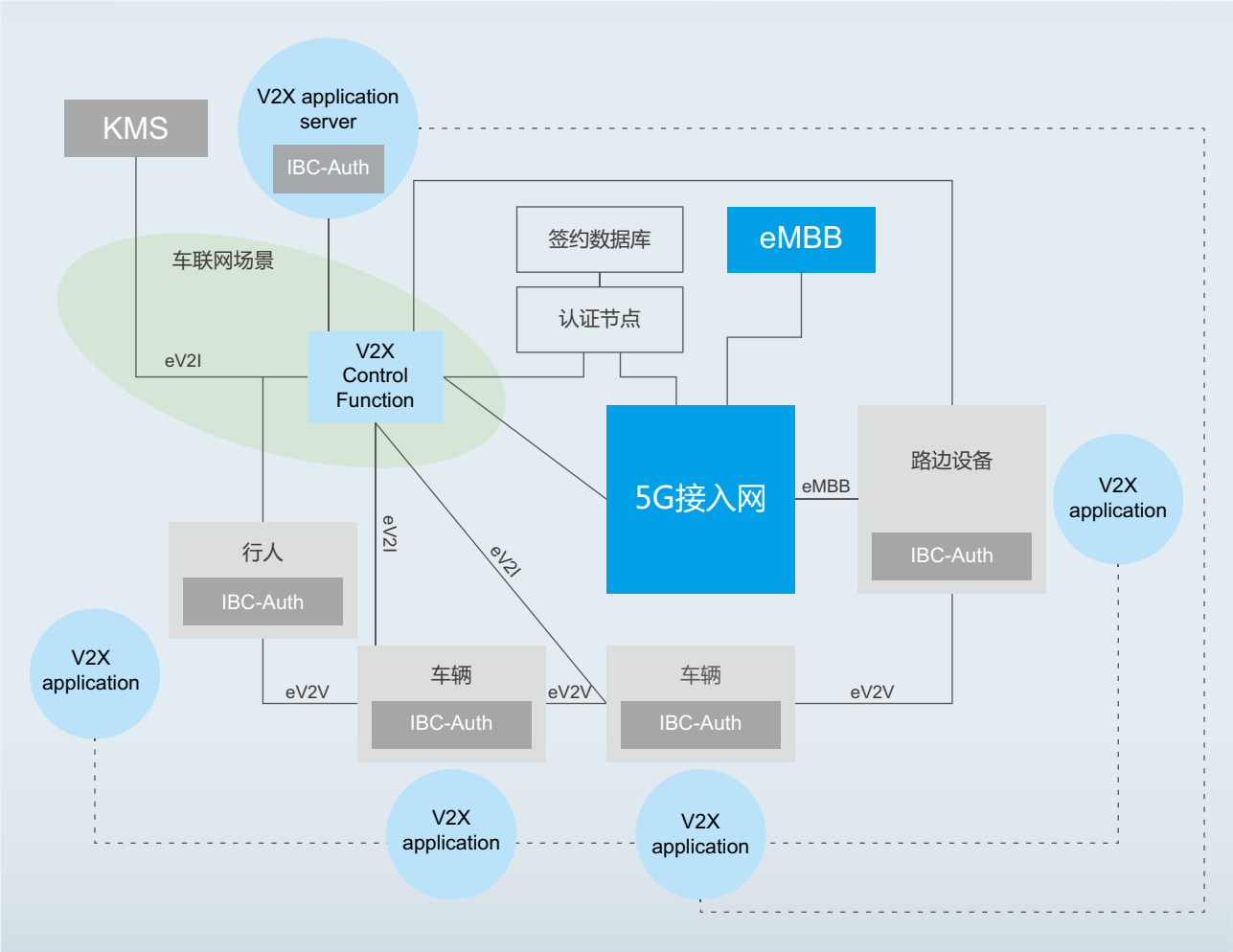


基于 IBC 的去中心化身份管理和认证机制设计

相对于证书管理来讲，基于 IBC 的身份管理，设备 ID 可以作为其公钥，在认证时不需要发送证书，具有传输效率高的优势。IBC 所对应的身份管理与网络 / 应用 ID 易于关联，可以灵活制定或修改身份管理策略。

基于身份的 IBC 认证机制涉及的消息更短、交互轮数更少，符合 5G 场景 mMTC 安全高效率的需求。

在车联网应用中，车联网广播消息的发送是一个高频度应用场景，过滤车辆间的非法信息是重要安全需求，需要在广播消息中携带身份信息进行认证。由于空口广播资源珍贵，车联网对广播消息的长度有限制，如果消息太长，或者认证交互轮数太多，将会导致分包、增加消息时延，影响消息实时性。车联网中的每一辆车的车载设备都可以具有一个基于 IBC 的身份和密钥，在进行广播消息的过程中，直接使用 ID 即可完成消息认证，不需要携带证书，减少消息长度，降低时延。



04

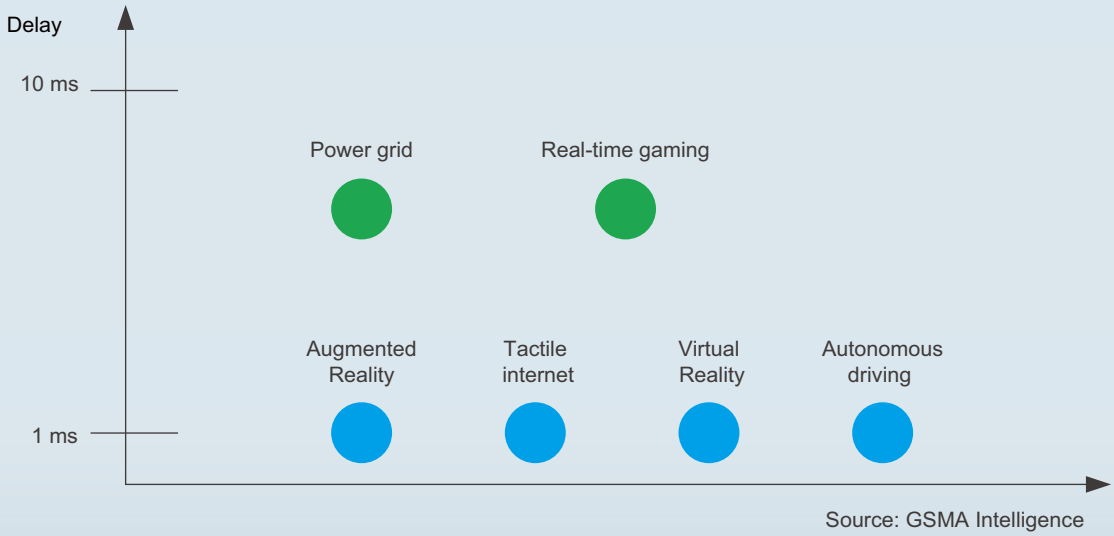
uRLLC 业务场景安全设计

5G 正在使自动驾驶、工业 4.0 等超低时延应用成为现实

超低时延特性是自动驾驶、工业控制广泛应用的前提条件之一。理想情况下 5G 端到端时延要达到 1ms，典型端到端时延为 1-10ms。4G 端到端典型时延是 50-100ms，这意味着 5G 将端到端时延缩短为 4G 的十分之一甚至更多。

uRLLC 指对时延极其敏感的业务，例如自动驾驶 / 辅助驾驶 ,AR,VR,Tactile internet, 工业控制等业务。如果网络时延不能足够低，这些业务将无法让用户得到良好的感受，甚至导致控制失误。

下图描述了未来 5G 将支持多种低于 10 毫秒时延的业务类型。



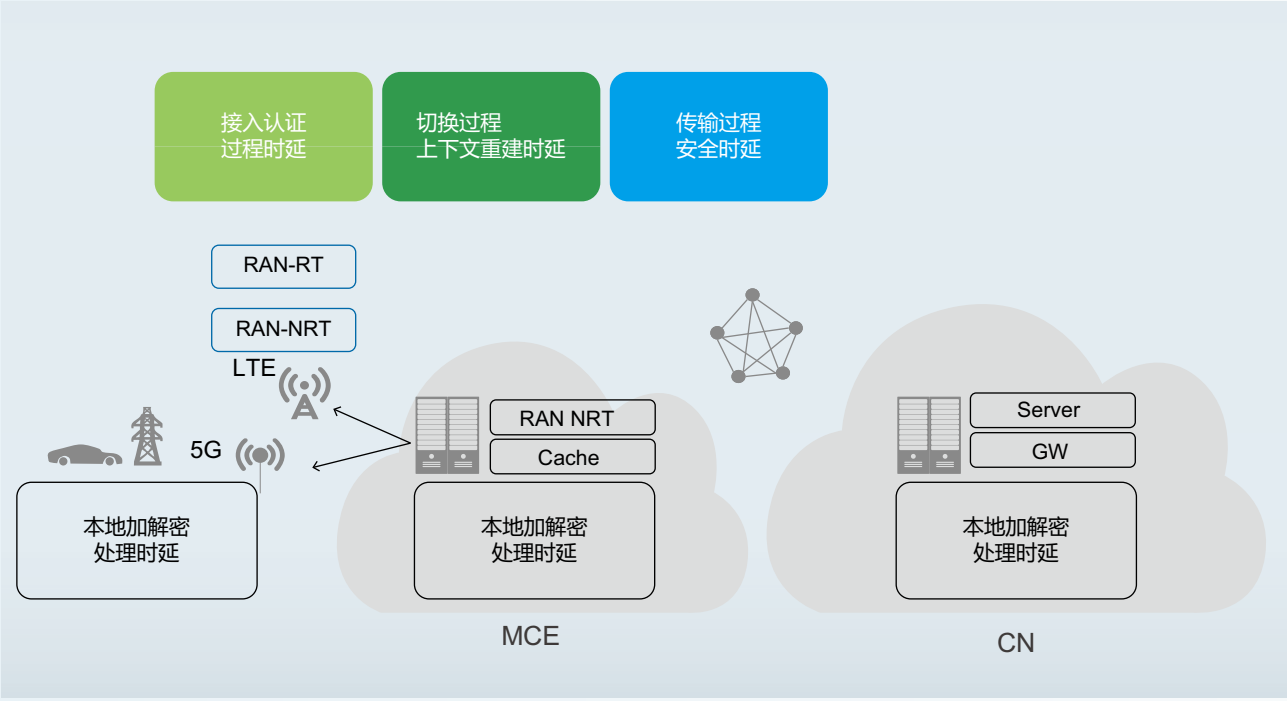
uRLLC 需降低接入认证、传输安全、安全上下文切换的时延

端到端时延是网络多段路径上的时延叠加的结果，仅靠单独优化某一局部的时延都无法满足 1ms 的极致时延要求，因此 5G 超低时延的实现需要在端到端传输的各个环节进行一系列机制优化来降低时延。

5G 低时延的指标达成需要从以下几个维度共同来减少时延：

- 空口传输效率
- 网络架构优化
- 减少传输途经节点并缩短源到目的节点之间的“距离”
- 网络传输协议效率优化
- 业务流编解码效率优化

从安全角度来看，需要优化接入过程身份认证的时延、数据传输安全保护带来的时延，以及数据在网络节点中加解密处理带来的时延。另外，终端移动过程由于安全上下文切换带来的时延也需要进一步优化。



uRLLC 减少整网时延的安全功能设计

为促进达成 5G 网络端到端超低时延的目标，安全方面可从接入认证、数据传输、本地处理和移动切换过程进行优化。

减少认证时延

针对超低时延的业务场景，考虑到安全认证的优化，为了减少设备与网络之间认证时延：

首先可以通过缩短从终端到认证服务器之间的距离，如采用分布式认证，将认证服务器从中心节点下移，从而缩短认证链条来降低认证消息传输时延。

其次可以从认证协议复杂度的角度，设计更高效的认证机制，如减少认证双方传送参数数量或消息长度、降低认证过程中双方消息处理和本地计算的复杂度。

减少数据传输安全保护时延

针对超低时延的业务场景，使用传统的安全机制对传输数据进行安全保护，会在被传输数据基础上增加额外的冗余载荷，这些增加的载荷本身会带来传输负荷的增加，特别是在传输数据很少的应用中安全载荷可能超过数据净荷。

针对降低传输时延，安全方面的优化方向为：减少为保护传输数据而增加的冗余载荷，实现方法可通过设计更优的安全算法来减少加密、完整性保护、防重放机制的附加载荷。另外，提供从终端到业务网关端到端的数据加密保护，也可以节省数据传输时在中间节点多次加解密造成的不必要时延。

减少安全上下文切换时延

高速移动的汽车和高铁列车中的终端，都会在网络中快速切换，4G 的移动性安全机制需要基站在切换的过程中计算、发送、接收密钥，会增加切换过程中的时延。在 5G 网络中，基站的密集部署、多制式、多接入、多站点的协同，需要在快速切换场景下低时延的安全机制。

减少移动切换过程时延，可通过异构统一认证架构、安全上下文高效衍生机制以及减少移动过程中安全上下文在网络节点间转移的等方法。

减少网络节点本地安全处理时延

密码算法的处理逻辑比较复杂，传统通信系统会以专有硬件算法芯片的方式进行等密码运算（如 AES/Snow3G/Zuc），来提高数据吞吐率。

为减少本地加解密处理时延，可引入更高效的密码算法、利用虚拟化 / 云化技术调用充足的计算资源，还可以采用硬件加速、支持并行运算的密码算法达到高速运算的效果，从而降低运算时延。

综上，为支持 5G 所需要的超高可靠低时延能力，需要安全保护机制在不降低安全保护强度的前提下朝以下方向发展：

- 支持端到端加解密保护，减少中间节点加解密时延
- 支持认证节点下移，减少认证传输时延
- 采用新的认证框架与协议，降低认证交互和处理的复杂度
- 采用新的数据传输安全协议，减少密文、完整性保护、防重放的载荷
- 采用更高效的移动性安全上下文迁移和密钥重建机制
- 采用高效密码算法，减少加解密处理时间

05

总结：适应多业务场景进行创新安全设计

5G 安全面临 eMBB/uRLLC/mMTC 场景业务多样化、网络架构全面云化、安全能力开放带来的安全需求、挑战和更高的用户隐私保护需求。5G 系统需要在不同的接入技术、云化网络架构之上建立一个统一的安全管理机制，构建通用的安全核心能力，包括端到端安全保护、统一认证、安全能力开放和按需安全管理，并在安全核心能力之上，提供差异化的安全功能、策略和解决方案，支持不同的业务场景。

5G eMBB 应用（VR/AR、高清视频）驱动 5G 网络快速发展，5G 安全需支持差异化业务、异构接入、开放的应用环境。面向 5G 网络云化架构下多业务环境，安全从基于传输管道的 hop by hop 安全保护发展到基于业务的端到端安全保护。多制式、多接入、多站点的融合网络环境下，一个支持多种接入技术和认证协议的统一开放认证框架，能简化安全管理，提高网络效率。通过身份管理和认证能力开放，可以增强业务认证安全性，促进 5G 业务生态环境发展，提升运营商拓展行业客户的能力。

5G mMTC 为支持多种行业应用场景，如智能交通、智能电网、智能制造等。如何解决运营商在新的 mMTC 场景下所面临的低成本、高效率的海量连接等需求是运营商在 5G 时代面临的主要挑战之一。在 5G 网络中部署去中心化模式下的身份管理与认证机制，降低运营商身份管理成本，提高认证效率，为 5G mMTC 提供高效的安全解决方案。

5G uRLLC 场景下，自动驾驶、工业 4.0 等超低时延应用正在成为现实，uRLLC 需要在保证安全保护强度的前提下，降低安全协议交互和安全处理的时延，支撑 5G 端到端低时延的达成。

商标声明

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