5G信息安全白皮书

White Paper V4.0 L
2017.11

目 录

1 引言

5G 移动通信系统需要支持增强移动宽带、高可靠低时延以及低功耗大连接等应用场景。除了移动互联网应用，5G 还需要为车联网、物联网（IoT）、虚拟现实、高速铁路等新兴行业的发展提供快速响应、无处不在的网络接入，为垂直行业的快速发展、创新提供信息基础平台。5G 新的应用场景、新的技术和新的服务方式给 5G 的安全带来许多新的安全需求与风险。

5G 对不同场景提供的接入方式和网络服务方式存在较大差异，支持的业务交付方式也不同，安全需求的差异性非常明显。特别是物联网应用场景带来的大连接认证、高可用性、低时延、低能耗等安全需求，以及 5G 引入的 SDN/NFV、虚拟化、移动边缘计算和异构无线网络融合等新技术带来的变化和安全风险，对 5G 移动通信系统的接入认证/鉴权、切片安全、数据保护和用户隐私保护等方面提出全新的挑战。

目前对 5G 安全标准进行研究的主要集中在 3GPP SA3、ETSI 和国内的 CCSA TC5 WG5 和 TC8 WG2。3GPP SA3 目前正在研究的技术报告 TR 33.899 是 5G 安全标准化工作的基础，TR33.899（V1.2.0）给出了 17 个安全领域共 109 关键议题（Key Issue）数百个解决方案（Solution），基本上覆盖了 5G 安全的所有安全需求。ETSI 的网络功能虚拟化标准工作组（NFV ISG）将在 5G 网络的基础设施标准化中扮演重要角色，主要目标是研究基于 NFV 的开放、互操作、商业生态链的技术规范。

基于国际国内标准化工作进展和国内相关单位的最新研究成果，本白皮书针对 5G 安全总体架构、认证/鉴别与授权、接入安全、切片安全、密钥体系和终端安全等 10 个 5G 安全领域的安全需求进行了梳理，并针对相应的需求对国内外的解决思路进行了描述，以期对 5G 安全的研究工作有所促进。

2 5G 安全需求

2.1 5G 安全总体架构

“安全总体架构”是对系统安全体系架构的结构化描述，对模型中功能模块与安全模块、安全模块间安全相互关系的定义。科学、合理的安全架构可以有效的指导整个系统具体安全机制设计与技术研发。

5G 安全应打破以往移动通信系统成型后“打补丁式”的升级演进模式，与 5G 移动通信技术同步演进，实现系统安全内生与安全威胁“标本兼治”的目标。为了实现这一目标，5G 安全总体架构（以下简称安全架构）的设计应具备良好的弹性与可扩展性，并能够满足 5G 安全技术的演进发展需求。

具体而言，对应 5G 应用、网络、无线接入、终端、系统等演进带来的新安全需求，可以从以下五个方面概括 5G 安全总体架构的设计需求：

1）5G 将渗透到交通、医疗、工业等多元化的垂直行业和领域，并支持人与人、人与物、物与物间多样化的信息交互。因此，安全架构应面向多样化、海量的应用与终端，支持统一的身份管理和认证功能，支持多元化的信任关系构建；面向多元化安全需求，支持差异化安全策略与模组的灵活适配。

2）随着 SDN、NFV、切片等技术的引入，5G 网络呈现出虚拟化、软件化、开放化等特点。面对这些特点，安全架构应支持高可靠的虚拟化安全技术（如 SDN 安全、切片安全、VNF 安全等）；支持开放接口调用合规性监管，确保服务与能力的安全开放。

3）5G 无线接入网具有多类型接入技术融合、超密集组网等特点，并引入了移动边缘计算（MEC）等新型服务技术。因此，安全架构应支持多类型接入技术融合统一接入安全管理，并具备 MEC 内生服务安全能力。

4）5G 在丰富垂直行业与专用领域的应用，使得 5G 终端类型呈现多元化。因此，安全架构应针对多元化终端的安全需求，支持差异化安全策略与模组的灵活适配，以及高可信终端安全运行环境构建。

5）5G 应用、网络、无线接入、终端等方面的特点，导致 5G 网络的攻击面大幅增加，因此，为了应对潜在未知安全威胁，在安全架构中还需要引入能够对 5G 网络安全态势管理和监测预警的长效手段。

2.2 认证/鉴别与授权

认证/鉴别与授权主要包括以下方面的需求：

（1）广泛网络实体的身份标识支持：在 5G 网络服务背景和物联网应用需求下，用户、机构、网络设备和资源、网络服务等不同种类的网络实体将大量接入，需要 5G 网络对不同类型的实体标识进行广泛的支持。如何定义网络实体的身份标识，以及制定相应的身份标识注册和查询机制，是 5G 网络服务亟待解决的需求之一。

（2）海量网络实体接入的凭证支持：身份凭证是指用于区分网络实体身份标识的可信依据。5G 网络服务需要为物联网提供海量实体身份凭证的支持，如何高效地进行凭证的生成和验证，并针对网络实体不同的安全能力与安全需求等级提供可靠的多级别凭证服务，都将是 5G 网络实体接入凭证的重要研究问题。

（3）统一的网络实体身份鉴别：身份鉴别即对网络实体凭证进行鉴别的过

程。5G 网络中需要接入网络用户、网络设备及网络服务等多类网络实体，网络应用需要对各类实体进行有效身份鉴别。由于网络实体身份凭证的提供方、网络身份凭证类型和鉴别机制都不尽相同，为确保网络应用对于网络实体身份的高效、正确鉴别，5G 网络中需研究并提供统一的身份鉴别机制或服务，使得网络实体可以互通互认，同时在鉴别过程中有效保护网络用户隐私信息。

（4）多元实体间的安全资源授权管理: 5G 网络中，网络实体的广泛接入，将引发网络应用、网络资源的大规模扩张，各类网络应用互通协作也将越来越多，这将带来网络资源跨应用共享的迫切需求。如何通过有效的授权管理来保证网络应用可控、安全地访问特定网络用户网络资源，建立网络身份提供方和网络资源提供方等众多网络实体间的多元信任，是 5G 网络环境下资源共享的重要问题之一。

2.3 接入安全

2.3.1 满足多类型终端、多接入技术、多接入类型

5G 时代要实现万物互联，5G 网络不仅用于人与人的通信，还用于人与物、物与物的通信，为此，5G 网络需要支持多样化的接入终端，多种接入类型和多种接入技术。从终端类型看，分为有卡终端和无卡终端。有卡终端以 SIM/USIM 卡作为用户身份和密钥载体，具备一定的计算和存储能力；无卡终端没有内置专用载体存储身份密钥信息，通常以 IP 地址或者 MAC 作为自己的身份，用数字证书提供安全保障；从接入类型看，5G 网络需要支持 3GPP 接入，非 3GPP 接入，可信接入和非信任接入；从接入技术看，5G 网络除了支持 5G 新无线接入技术之外，还要兼容 3G 接入、LTE 接入、WLAN 和固定接入等技术。因此 5G 网络是融合了多种类型的终端、接入类型和接入技术的异构型网络，而不同的终端，不同的接入类型和接入技术存在不同的安全需求，使用不同的认证协议和密钥协商机制，5G 网络需要研究构建统一的认证框架来融合不同的接入认证机制，满足具有不同安全能力的终端的安全接入需求。

2.3.2 满足典型应用场景

未来 5G 网络需要支持三大类典型应用：增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（uRLLC）。这三类应用场景根据各自的应用特性存在不同的接入安全需求。

eMBB 重点是提供超高带宽，用于满足诸如虚拟现实（VR）、大视频等对带宽有极高要求的业务。3GPP 制定 5G 第一阶段的标准就是为了满足 eMBB 应用。eMBB 应用的接入安全通过继承和扩展 LTE 的接入安全机制实现，主要针

对 LTE 接入下用户首次接入时 IMSI 采用明文传送存在的安全风险，采取了 IMSI 加密传输的机制，另外结合 5G 网络架构，进一步增强了密钥派生机制来满足各接入层次安全传输的需要。

mMTC 应用的主要特点是接入网络的终端数量巨大，终端无卡，安全能力较弱，功耗小，资源受限，小数据传送等。按照传统的接入方式，每个终端和网络之间需要进行多次交互才能完成认证过程，实现网络接入。mMTC 应用下，如果终端仍然延用传统接入方式，海量终端并发接入网络极有可能产生信令风暴，造成网络拥塞；另外，在接入失败情况下终端不断尝试重新接入网络发起认证，这对于低功耗无人值守的 MTC 终端将加速其电池消耗。因此需要研究包括简化认证机制，优化认证协议在内的满足 MTC 设备高效快速接入的轻量化安全接入方式。针对物联网传输的是小数据且是零星传送的数据特征，需要为小数据传送建立通道。如果小数据传送的无线网络缺少安全保护机制，攻击者就有可能通过访问小数据接口入侵网络，因此还需要研究针对小数据的空口传输安全保证机制。

uRLLC 应用对通信可靠性，低时延有极高的要求，例如车联网、远程医疗等应用。网络安全通常与网络性能效率是互为矛盾的，增强网络安全防护机制，必然以牺牲网络性能，降低网络效率为代价，uRLLC 应用也不例外，如果引入安全机制，就必然会影响业务时延。但是安全对于 uRLLC 应用又是不可或缺的，如果车联网业务缺乏安全机制保护，就会存在交通信息被窃取或篡改进而影响到行车安全甚至威胁到生命安全。因此在保证可靠性和低时延等业务性能的同时，需要研究 uRLLC 的接入安全，研究车联网通信时的身份认证、车辆身份信息的保护、数据传输安全等接入安全解决方案。

2.4 移动边缘计算（MEC）安全

2.4.1 移动边缘计算(MEC)内涵与特点

移动边缘计算（Mobile Edge Computing, MEC）作为 5G 网络新型网络架构之一，通过将云计算能力和 IT 服务环境下沉到移动通信网络边缘，就近向用户提供服务，从而构建一个具备高性能、低延迟与高带宽的电信级服务环境。MEC 的特点概括如下：

- 共生融合：MEC 作为移动通信系统的共生系统，与 5G 移动接入网络、回传网络、市省级核心网络融合部署。MEC 系统利用基于服务架构（Service-Based Architecture, SBA）获取 5G 开放服务，并向 5G 网络用户提供边缘服务。

- 按需临近部署：MEC 节点可根据应用服务需求按需、分布式部署于移动网络边缘的多个位置。这种灵活、临近的部署方式在为超低时延要求提供保障的同时也能够降低高带宽业务的数据流对核心网带来的压力。
- 虚拟化构建：在通用硬件平台通过虚拟化技术构建计算环境，承载来自于第三方或运营商的 MEC 应用。为了支持 MEC 快速灵活的部署，MEC 节点可支持与 5G NFV 兼容的虚拟化方式，与 5G NFV 同平台部署。
- 高可协作性：MEC 各节点间的应用与服务具有较高的可协作性。不同的 MEC 节点的应用间能够通过协作的方式向用户提供服务（如移动性导致的服务迁移）。同时，对于具有高可靠性需求的关键应用，可通过在节点间进行服务热备和快恢复，提高系统的应急和容灾能力。此外，通过在多个 MEC 计算节点间使用协作的方式执行安全策略（如分布式加密），在降低单个节点的计算量的同时，还能提升策略的安全性。
- 基于用户信息感知的高质量、个性化服务：MEC 应用能通过与 5G 网络间标准化的协议和接口，感知用户信息，并融合信息技术与通信技术提供更高的用户服务体验。另外，通过对用户信息的进一步挖掘，能够提升 5G 边缘网络数据的商业价值。

2.4.2 MEC 安全需求

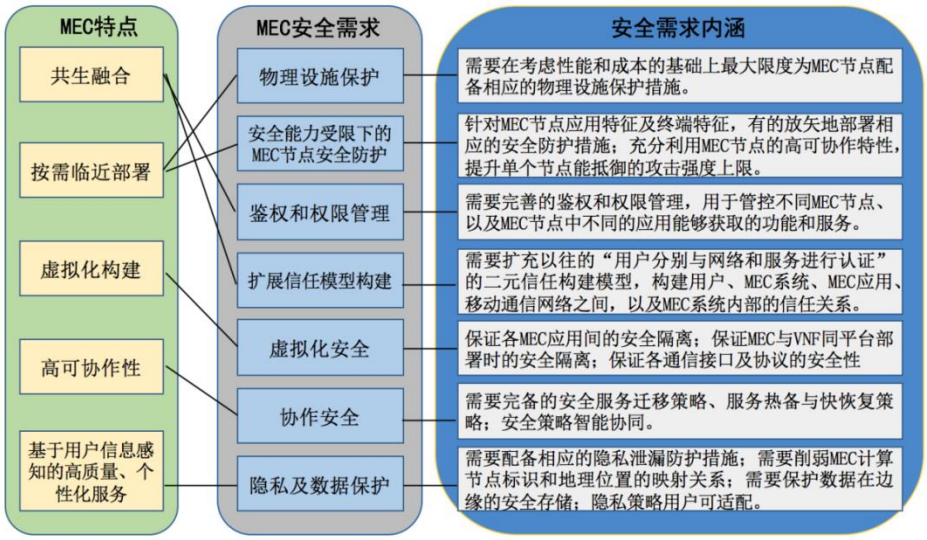

图 1 MEC 安全需求及内涵

MEC 的安全需求总结如图 1 所示，接下来将对其中 MEC 特有的安全需求进行详细描述：

（1）物理设施保护：MEC 按需临近部署的特点在为用户提供高质量服务的同时，也在客观上缩短了攻击者与 MEC 物理设施之间的距离，使得攻击者

更有可能接触 MEC 物理设施，造成 MEC 物理设备毁坏、服务中断、用户隐私和数据泄露等严重后果。另一方面，广泛部署的 MEC 边缘计算节点同样面临着各种自然灾害（如台风、冰雹）和工业灾难的威胁。以上因素都可能直接破坏 MEC 硬件基础设施，造成服务的突然中断以及数据的意外丢失。因此需要在考虑性能和成本的基础上最大限度为 MEC 节点配备相应的物理设施保护措施。

（2）安全能力受限下的 MEC 节点安全防护: 由于性能、成本、部署灵活性要求等多种因素制约，单个 MEC 节点的安全防护能力（如可抵御的攻击种类，抵御单个攻击的强度等）受到限制。因此需要：针对 MEC 节点应用特征及终端特征（IoT 终端/移动智能终端），有的放矢地部署相应的安全防护措施；充分利用 MEC 节点的高可协作特性，通过例如基于智能协同的安全防护等技术，借助周边节点的空闲安全防护资源，提升单个节点能抵御的攻击强度上限。

（3）扩展信任模型构建：MEC 系统与移动通信系统共生融合的部署方式扩充了以往的“用户分别跟网络和服务进行认证”的二元信任关系构建模型。需要构建用户、MEC 系统、MEC 应用、移动通信网络两两之间，以及 MEC 系统内部的信任关系。具体而言：需要构建 MEC 系统与 5G 网络间的信任关系以合法使用 5G 开放网络服务（如本地分流）向用户提供服务；需要构建 MEC 系统与 MEC 应用间的信任关系防止恶意应用接管用户服务；需要构建 MEC 系统与用户间的信任关系以确认 MEC 系统和用户的合法性。在 MEC 系统内部，需要构建 MEC 节点与 MEC 控制器间的信任关系，防止“伪 MEC 节点”恶意接入窃取用户和服务信息；需要构建 MEC 节点间的信任关系以支持节点间协作。

（4）隐私及数据保护：MEC“基于用户信息感知的高质量、个性化服务”的特点在提供便利的同时也让 MEC 应用不可避免的接触到大量移动用户与设备的隐私和数据信息，如用户身份、位置、移动轨迹等。而对这些信息进一步挖掘后，还得到用户的作息规律、生活习惯、健康状况等诸多信息。因此，在 MEC 隐私及数据保护中，需要配备相应的隐私泄漏防护措施，严控第三方 MEC 应用的行为，防止其泄漏、滥用用户的隐私及数据信息；需要通过动态身份标识和匿名等技术削弱 MEC 计算节点标识和地理位置的映射关系，防止第三方根据 MEC 节点位置推断用户的地理位置；需要确保数据在边缘的安全存储；需要向用户提供隐私及数据管理服务，确保隐私策略用户可适配。

2.5 切片安全

虚拟化是 5G 新架构的一个主要特征。NFV 是促使 5G 新架构具备虚拟化特征，从而实现 5G 网络灵活性和弹性等特性的使能技术。NFV 是 2013 年由 13

家运营商发起，由 ETSI 定义，采用虚拟化技术、基于通用硬件实现电信功能节点的软件化，打破传统电信设备的竖井式体系，其核心特征是分层解耦和引入新的 MANO(Management and Orchestration)管理体系。

网络虚拟化后，传统的网络设备功能将以 VNF(Virtualized Network Function，虚拟化网络功能)的方式运行在 NFVI(Network Function Virtualization Infrastructure，NFV 基础设施)上。NFVI 由通用的硬件资源、虚拟化层（即 Hypervisor）以及虚拟资源（虚拟计算、虚拟存储和虚拟网络）组成，为实例化的 VNF 提供计算、存储和网络资源。新增的 MANO 管理体系实现对 NFVI 的管理，包括分配虚拟资源给 VNF，监控和上报虚拟资源以及硬件资源性能以及故障等。

SDN 解耦了设备的控制面和数据面，并且控制面实现集中控制，开放可编程接口供应用层使用，实现了灵活的定义网络。

2.5.1 NFV 安全需求

（1）NFV 的安全需求：

- VNF 安全需求：包括对 VNF 软件包进行安全管理（如上在前以及更新时进行完整性验证）、对 VNF 进行访问控制以及进行敏感数据保护。
- NFV 网络安全需求：包括 VNF 通信安全需求（即 VNF 通信安全需保证通信的双方相互认证，并且通信内容需受到机密性、完整性防重放的保护）及组网安全需求（包含边界防护、安全域划分以及流量隔离）。

（2）MANO 安全需求：

- MANO 实体共有的安全需求：包括需对 MANO 实体进行安全加固，实现安全服务最小化原则，如关闭不必要的服务和端口等；安装防病毒软件，并定期检查、查杀病毒以及升级病毒库；需防止非法访问、敏感信息泄露；需保证 MANO 实体所在的平台可信等。
- MANO 各个实体独有的安全需求：NFVO 遭受 DDoS/DoS 攻击；VNFM 和 VIM 可以运行在虚拟机上，此时会面临虚拟机逃逸、虚拟机隔离失败等虚拟化相关的安全威胁。
- MANO 实体间交互以及 MANO 系统与其他实体间交互的安全需求：通信内容需受到机密性和完整性保护以及防重放；实体间双向认证。
- MANO 管理安全：MANO 系统的需进行账号、权限的合理分配和管理，实行严格的访问控制，并且启用强口令策略等。

2.5.2 SDN 安全需求

SDN 的安全需求主要包括：

- 应用层的安全需求：APP 需对控制器的身份进行认证；APP 和控制器之间的通信要受到完整性和机密性保护；APP 自身要进行安全加固，防止安全攻击。
- 控制器的安全需求：SDN 控制器要具有 DDoS/DoS 防护能力或者限速的能力；SDN 控制器要实现服务器的安全加固、满足安全服务最小化原则、关闭所有不必要的端口和服务，并使用渗透测试相关的工具（包括 nessus, NMAP, Symantec 杀毒工具, wirshack, webscarab 以及 Back Track 等）进行安全检查，修复安全漏洞；SDN 控制器需执行策略冲突检测和防止机制，避免管理策略和安全策略被绕行；SDN 控制器需对接入的 APP 进行身份认证和权限检查。
- 转发层的安全需求：通过设置 ACL，关闭不要的服务和端口，及时修补漏洞等手段加强转发设备自身安全；另外，转发设备具备并开启限速功能。
- 南北向接口的安全需求：需进行双向认证，并且通信内容需进行机密性、完整性和防重放保护；需对协议强壮性进行分析和测试，修复协议漏洞。

2.5.3 网络切片的安全隔离需求

网络切片需要提供不同切片实例之间的隔离机制，防止本切片内的资源被其他类型网络切片中网络节点非法访问。例如医疗切片网络中的病人，只希望被接入到本切片网络中的医生访问，而不希望被其他切片网络中的人访问。

相同业务类型的网络切片之间也存在隔离的需求，例如不同的企业的在使用相同业务类型的切片网络时，并不希望本企业内的服务资源被其他企业的网络切片节点访问。

服务、资源和数据在网络切片中被隔离保护的效果要达到接近于传统私有网一样用户感受，这样才能使得用户能放心的将原本存放在私有网络中的应用数据存放到在云端，用户在享有随时随地可访问私有资源的同时不需要担忧这些资源的安全问题，这样才能促进各种垂直业务的健康快速发展。

当运营商根据业务的不同将网功能分割成不同的网络切片时，需要考虑是否进行切片内的认证和授权，以及如何进行切片内的认证和授权。当切片管理的某些功能开放给第三方时，还需要考虑哪些认证和授权功能可以开放给第三

方，以及由运营商控制的主认证和授权与由第三方控制的二次认证和授权的融合机制。

2.6 数据完整性和机密性

在 5G 网络中无线空中接口仍然存在窃听、篡改等安全威胁。在接入网存在的安全问题主要来自无线的空中接口。空中接口的信息是在无线信道上传输的，入侵者容易捕获手机终端或基站的无线信号，从而非法取得或篡改用户和网络发送的信息。

另外网络域安全是 5G 网络安全的重要环节，用户信息在 5G 网络域内和不同的网络域之间是以明文形式传输的，用户信息可能被窃听，一些用户的机密数据在网络域内可能被窃取，将会对信息安全产生很大影响。由于网络域采用互联网技术进行连接，可能受到病毒的威胁、受到黑客的攻击，传送的数据可能被修改、可能被未授权者获得等。因此，网络域节点间的信息保护、边界保护、病毒防护是保证业务顺利开展的重要安全措施。

2.7 隐私保护

5G 网络需要为不同业务场景提供差异化安全服务，能够适应多种网络接入方式及新型网络架构。这些新场景、新架构和新技术都让 5G 网络有了更高的隐私保护需求。另外，5G 网络针对垂直行业用户会产生大量的敏感信息。迫切需要在 5G 开放网络环境之上，采取措施保证行业用户的隐私安全。

uRLLC 作为 5G 网络典型应用场景广泛应用于车联网自动驾驶及远程工业控制领域。在自动驾驶过程中，车辆的身份信息、位置信息存在被暴露和跟踪的风险，这些隐私信息一旦被泄露，产生的后果是非常严重。mMTC 和 eMBB 场景使得 5G 网络中的业务信息会以几何级别增长。这些信息包含针对某个网络实体的不同测度的描述。通过对这些海量数据的分析，网络用户的隐私信息可能会被泄漏。例如，黑客可能获取某用户的部分移动电话数据、运动手环数据、部分 APP 的消费数据、位置信息数据等等多方面的信息之后，通过对这些数据的分析获取某人特定的隐私信息。在 5G 场景下，如何实现对隐私数据的分级，提高抵抗大数据攻击的隐私保护的能力将会成为一个亟待解决的问题。

5G 网络作为一个复杂的生态系统，存在基础设施提供商、移动通信网络运营商、虚拟运营商等多种类型参与方，用户数据在这个由多种接入技术、多层网络、多种设备和多个参与方交互的复杂网络中存储、传输和处理，面临着诸多隐私泄露的风险。另外，5G 网络中大量引入虚拟化技术，在带来灵活性的同时也使得网络安全边界更加的模糊，在多租户共享计算资源的情况下，用户的隐私数据更容易受到攻击和泄露。相比传统网络而言，这种情况所产生的隐私

泄露影响范围更广、危害更大。因此，对 5G 网络的隐私保护提出了更高的挑战。

当前 4G 网络中，系统已经使用临时签约标识符来增强用户的隐私，降低签约数据通过偷听无线链路的方式被识别和跟踪的可能性。但现有 4G 网络也暴露了一些隐私问题需要解决，比如 IMSI 泄露问题以及位置信息的泄露问题。IMSI 的泄露会直接导致用户身份信息的泄露。因此，在 5G 网络设计之初，需要充分考虑现有 4G 网络中的隐私漏洞，增加适合 5G 网络的安全措施和协议来弥补之前网络的隐私漏洞，保护用户的身份信息和位置信息。

2.8 安全管理

2.8.1 5G 安全管理的必要性

根据 ITU-T 对通信系统 FCAPS 管理模型的定义，安全管理是指对为保护通信系统的工作安全、内容安全而增加的各种安全机制的管理体系总和，目的不仅在于要确保通信网络环境是安全的，也要确保收集的安全相关的信息被适当处理。安全管理包括了管理网络的认证、授权、审计，以及内部/外部用户对网络资源的合法访问控制，也包括了对网络防火墙、入侵检测系统、安全策略的配置和管理。5G 引入 IT 技术的同时也将 IT 面临的安全风险引入，需要安全管理对网络进行统一的管理与监测。

5G 的安全管理需要贴合 5G 网络特有的安全需求，具有独特的解决思路。5G 网络的发展，是在 ICT 融合的大背景下进行的，充分吸收了 ICT 融合的一些基本思想和基础技术，如 SDN、NFV 等。ICT 技术的引入，不可避免的将使 5G 网络面临 IT 网络类似的攻击和威胁，而更广阔的应用场景和虚拟化技术的引入，带来了攻击方式泛在化与安全边界模糊化这两个显著特征：

（1）攻击方式泛在化。5G 网络下攻击源/目标的规模因物物互联的引入得到迅速放大；攻击途径也因异构接入方式的多样化得到了扩展； SDN 控制器受到攻击可能导致整个网络瘫痪或者被劫持；采用 NFV 虚拟化技术的云计算，也会引起数据残留、资源风暴等新的安全问题。

（2）安全边界模糊化。网络的安全边界由于物理分割在 SDN/NFV 架构下已经消失，因此内外网隔离的安全边界需要重新界定；云环境下多租户共用物理资源也导致多个租户的服务可能运行在一个计算节点上，缺乏明确物理边界；接入网络上会承载众多的数据中心和应用程序的网络接口，没有明确的安全边界，造成信任缺失。

考虑到未来 5G 网络的可能演进，因此根本的解决途径是需要通过安全管

理在 5G 网络内实施积极主动的全面监测预警以解决攻击方式泛在化问题；在 5G 架构方面通过引入统一信任框架以信任关系逻辑重构安全边界，解决边界模糊化问题。5G 安全管理应特别对以上解决途径提供支撑。

2.8.2 5G 安全管理需求分析

考虑上述基本要求，5G 安全管理需满足以下需求：

(1)能够管理 5G 安全服务/组件，并提供安全策略调整的统一入口

为了解决 5G 网络存在的攻击方式泛在化的安全问题，5G 网络及网络切片中将会存在各种安全服务或组件，以使 5G 网络及业务抵御来自各种位置的中间人攻击、信息重放攻击、窃听嗅探等安全威胁。例如，网络切片中会存在虚拟防火墙、IDS/IPS 等安全专用设备，同时 VNF 网元在实现时会落实 3GPP 标准规范规定的各种安全措施。5G 安全管理应为运营商/第三方租户提供对这些服务或组件的安全策略调整的统一入口，实现如对虚拟安全专用设备的管理配置、对各种安全措施的参数调整等功能，帮助运营商、租户及时调整网络安全策略以应对网络安全威胁。

(2)能够对 5G 网络安全态势进行监测预警

为了应对攻击方式泛在化的挑战，及时感知到正在进行的、或者潜在的攻击威胁， 5G 网络切片还需要监控切片中各种虚拟安全专用设备的运行状态，对采集到的所有信息加以智能化的整合/分析，定位攻击方式及来源，并将这些信息整合成安全态势及时向管理员告警，以应对 APT、DOS、DDoS 等网络攻击手段。其次，考虑到 5G 网络将新产生大量具有管理功能的网元，如 PCF、AUSF、ARPF、UDM 等，它们都属于敏感网元，一旦被恶意控制，它们自身连同它们所管理的资源本身也会一起被劫持，因此 5G 网络的监测预警也需要将敏感网元状态纳入安全监控审计。

(3)能够为构建 5G 统一的信任管理体系提供安全支撑

5G 网络需要安全管理为统一的信任管理体系提供安全支撑，以应对安全边界模糊问题。按照业界共识，5G 网络会有大量新的参与者、新的设备类型加入价值链，例如运营商、虚拟基础设施提供商、虚拟网络功能供应商、租户、终端用户、终端设备等等类型的角色；以上因素导致了 5G 必定存在多元化的价值链，以及相应的信任关系。信任体系的脆弱，将导致一系列严重安全问题，例如 5G 网络能力开放使得经由控制 API 接口对 5G 网络本身进行恶意功能编排与组合成为可能。因此，5G 安全管理需为价值链中各种角色提供身份凭据及其对应权限的管理服务（包含凭据的颁发、使用、注销、权限关联等方面的内容），并提供认证方面的支撑，解决各个角色/实体之间的多元信任问题，以支

撑安全边界的逻辑重构。

(4)能够为第三方 5G 网络切片/敏感业务提供差异化的安全支撑

5G 网络支持多种类型的切片和业务，以供第三方租户使用；不同的切片/业务除开在性能、QoS 方面的差异之外，还因承载数据的敏感程度差异，具有不同的安全等级要求；安全管理应为这种差异化提供安全支撑。例如，4G 移动通信网络中只对终端接入认证及语音和数据通信等常规服务提供密钥管理的密钥管理体制，已无法满足 5G 多种切片/业务场景下各异的密钥管理新需求，也无法支持基于第三方身份凭据的二次认证；又如，以特殊行业为代表的高安全需求用户在使用 5G 网络的过程中，移动终端之间以及移动终端和后台服务端之间大多数情况下需要进行端到端的认证和加密通信，而普通用户则往往不会存在这种需求；再如，业界至今未对是否在 5G 终端与网络之间使用非对称的密码技术达成一致结论，也未对第三方租户使用非对称密码技术有所提及，未来存在变数。总之，5G 安全管理应对不同的安全要求综合考虑，尽力兼容可能出现的差异化场景，尽力为第三方 5G 网络切片/敏感业务提供匹配的安全支撑。

(5)需要适应 5G 网络特有的网络切片和虚拟化特点

5G 引入网络切片和 SDN/NFV 技术概念之后，安全边界模糊化问题导致了传统的移动通信网络以物理实体为核心的安全防护技术在 5G 网络新环境中已经不再适用。安全性不仅与安全特征的物理部署有关，更重要的是与虚拟资产部署的安全特征有关，需要建立起以虚拟资源和虚拟功能为目标的安全防护体系。因此不仅要在网络切片、NFV 层面研究虚拟化基础设施可信运行及资源隔离与虚拟化网络切片的安全保障机制，更需要在管理架构上进行设计、调整，以适应被管虚拟资源和虚拟功能灵活、多变的组网。

2.9 密钥体系

5G 的密钥层次（key hierarchy）考虑的是如何利用一个根密钥为不同层面，不同类型的消息流提供多个相互独立的密钥的问题。因此，在 5G 的密钥层次中，需要考虑以下问题：

- 不同的接入方式。5G 系统会考虑多种接入方式，因此不同的接入方式可能会需要不同的密钥。
- 移动性管理与会话管理的分离。5G 系统考虑移动性管理与会话管理的分离，因此针对不同的信息流，需要考虑使用不同的密钥进行保护。
- 核心网与接入网的分离。5G 系统承袭 4G LTE 系统设计原理，仍然考虑

核心网与接入网信令的分离，因此仍然需要针对非接入层信令和接入层信令独立考虑安全保护，故而需要独立的密钥

- 加密与完整性。针对信令和用户数据，需要独立的考虑对信息的加密保护和完整性保护，因此针对不同的保护方式，需要不同的密钥。
- 由移动性引入的密钥更新与隔离。5G 系统仍然需要考虑终端在移动状态下的密钥更新与隔离，因此需要考虑密钥的更新问题。
- 密钥之间的相互独立性。为了保证派生的密钥之间具备一定的独立性，因此仍然需要像 4G 那样引入若干中间密钥，借由中间密钥来切断派生密钥之间的关联性。

此外，未来 5G 需要考虑大规模物联网终端接入、超低时延超高可靠性等场景，以及并可能出现用户凭证使用非对称密钥的情况。未来 5G 的密钥体系也可能随着这些场景与用户凭证的变化而发生变化。

2.10 终端安全

从 3G 网络引入移动互联网开始，移动终端日益成为黑客攻击的主要目标。在 3G/4G 阶段，3GPP 一直注重加强对移动网络的安全设计，终端安全则完全交由终端厂家自行开发。由于缺少统一标准的牵引，移动终端安全技术发展缓慢，产业化进展滞后，很快就成为用户隐私泄露的重灾区。近年来，虽然有芯片厂家或终端企业陆续推出了一些安全技术，但总体来说受已有架构的限制，解决不同角度的安全问题，缺乏普适性设计。

5G 网络的安全体系由移动终端侧和网络侧配合共同完成，无论是控制面还是用户面都需要移动终端的安全配合。从信息流向来看，移动终端既是用户信息和隐私数据的源头也是其归宿；从网络切片来看，移动终端是网络安全切片的实现起点也是实现终点；从垂直行业来看，5G 网络的一大特征就是对垂直行业的深度支持，垂直行业存在着多样化的安全要求，其安全能力更是需要移动终端的支持。综上，移动终端安全是 5G 网络安全体系中不可缺少的一环。

移动终端安全涉及到硬件层、操作系统层以及应用层等多个层面的问题，威胁因素主要来自外部网络。解决终端安全问题，首先要从多个层面提升终端自身抵御攻击的免疫能力，同时也要对外部网络如网络接入、应用服务等进行安全增强，引入基于云的安全增强机制来为终端安全提供辅助支撑。5G 网络明确了三种典型应用场景，带来 eMBB、mMTC、uRLLC 三种典型终端，并引入了行业用户作为新的利益相关方，因此 5G 终端安全还需要考虑针对不同应用终端以及不同行业用户群体的双重安全需求。本章节主要围绕终端安全技术需求，结合行业用户和三种典型终端需求进行阐述。

2.10.1 5G移动终端共性安全需求

（1）可信执行环境

伴随着 5G 技术的发展，移动终端正在成为互联网和物联网业务的关键入口，网络攻击面的大幅扩大，敏感信息的指数增加，使得 5G 终端将面临更加艰难的安全环境。为 5G 终端建立可信任执行环境，是 5G 时代的必然要求。

移动终端的运行环境面临来自硬件和软件的威胁，移动终端硬件安全威胁主要来源于终端芯片设计安全漏洞或硬件体系安全防护不足，可导致平台安全权限被获取、存储的隐私数据被窃取等安全风险，需要从硬件角度设计使终端核心器件具有抗物理攻击的能力，为移动终端的安全起到基础作用；移动终端软件系统是移动终端的灵魂，对软件系统的攻击包括：利用操作系统漏洞等获取终端控制权、修改安全策略，利用信息保护缺失、内存监管漏洞、应用程序漏洞等窃取用户信息、篡改信息和信令、植入恶意代码、扰乱系统的正常工作，利用 WIFI、蓝牙等外设配置漏洞吸引终端接入，窃取敏感信息等。利用上述攻击手段，可以轻易地收集用户数据，控制和更改终端软件，甚至在极端情况下，可以遥控瘫痪所有入网的终端，威胁国家网络安全。因此需对移动终端从硬件和软件层面采取有效措施，建立可信执行环境，保证终端平台的安全。

（2）安全体系完备性与可裁剪性

3G/4G时代，终端安全技术的主要驱动力是解决普通民众移动支付等安全问题，终端厂家的安全方案基本是专用和封闭的。但是进入 5G 时代，行业用户成为重要利益相关方以及万物互联成为新生态的趋势，将使行业安全和物联网安全成为 5G 终端安全技术新的强大动力。

终端安全能力包括终端防护、用户认证、入网认证、信息加密、安全存储、应用管理等，涉及平台安全、信息安全、使用安全、安全管理等多方面安全要求。不同行业对终端安全能力有着不同的需求，如果终端业界为不同行业分别设计安全架构，既不经济也不现实。为了高效率地适应差异化安全需求，应该建立统一的终端安全技术体系，该技术体系能够以组件化方式提供完备的的安全能力，同时又能够根据行业需求，方便地进行组件的组合和裁剪，提供高、中、低不同等级的安全能力，满足差异化安全要求。

从国家对信息领域的发展要求来看，在新兴信息领域实施军民战略已上升到国家战略层面。国防行业以及政府、公安等涉及国家安全和社会稳定的特殊行业，对移动通信的需求非常旺盛，安全性有着更高的要求。终端安全体系应该着眼安全能力要求更全面的特殊行业，提供完备的安全功能集。在面向普通垂直行业和普通公众用户时，安全架构能够进行有针对性地功能裁剪，为普通

行业和普通公众用户提供在成本范围内的安全功能。以最小的代价实现通用终端与高安全行业终端安全防护体系的构建，满足国家对信息领域安全建设的要求。

（3）标准化的安全接口

在建立统一的安全体系同时，5G 终端还应该提供开放的安全服务环境，提供标准化的安全接口。通过标准接口，支持第三方安全服务和安全模块的引入，便于行业客户的二次开发，允许行业用户通过标准接口快速地实现行业定制，支持不同行业终端的快速部署与专用化服务，提升终端产品的服务水平和竞争力。

2.10.2 eMBB 终端安全需求

eMBB 终端覆盖了增强移动宽带应用场景，是人与人、人与网、人与物间信息链接的主要载体，也是行业用户开展移动办公等处理行业敏感信息的主要工具。eMBB 终端传输速率高、涉及普通用户隐私/行业用户敏感信息多、支持异构网络连接，因此，它的典型安全需求主要有三个方面，一是要具备与 5G 网络速率相适配的高速率加密能力，同时还具备较低的功耗要求；二是对普通用户具备对个人信息或标识以及地址信息等等隐私信息的保护能力，对行业用户具高等级的认证、端到端加密、信息完整性保护等能力；三是具备异构接入的统一认证和安全上下文管理能力，提高异构接入安全上下文切换效率。

2.10.3 mMTC 终端安全需求

mMTC 覆盖对于联接密度要求较高的物联网应用场景，例如智慧城市、智能电网、智慧家居等，满足人们对于数字化社会的需求。由于物联网设备数量庞大，行业对物联终端的成本比较敏感。但是由于物联终端深入到城市基础设施及民众生活等涉及国计民生的重要部位，其安全性建设也不容忽视。

mMTC 终端的典型安全需求包括：一是轻量级的密码算法和协议，满足 mMTC 终端的低功耗、低带宽要求；二是安全可靠的网络接入模式，如 5G 网络提供为物联终端提供去中心化的身份管理和接入认证模式，包括缩短认证链条、快速安全接入、网络与业务融合分层身份管理等，降低管理复杂度；三是低成本的设备认证和身份管理实现，满足物联终端低成本要求。

2.10.4 uRLLC 终端安全需求

uRLLC 聚焦对时延极其敏感的行业，例如车联网、智慧工业等，满足人们对于数字化工业的需求。因这些行业的信息涉及自动驾驶、路况识别、工业控制等高风险环节，如果被假冒或篡改，将引发很大的安全事件，因此，uRLLC

比普通物联终端有着更高的安全性要求。

uRLLC 终端的典型安全需求包括：一是高安全等级的保护强度，具备高等级的认证、端到端加密、信息完整性保护等能力；二是超高可靠和超低时延的能力，在不降低安全保护强度的前提下，支持认证节点下移，简化认证框架与协议，提高移动性安全上下文迁移和密钥重建机制效率，采用高效密码算法，减少加解密处理时间。

3 主要解决思路

根据前面的需求，各方面主要的解决思路如下。

3.1 5G 安全总体架构

5G 安全总体架构如下图所示。

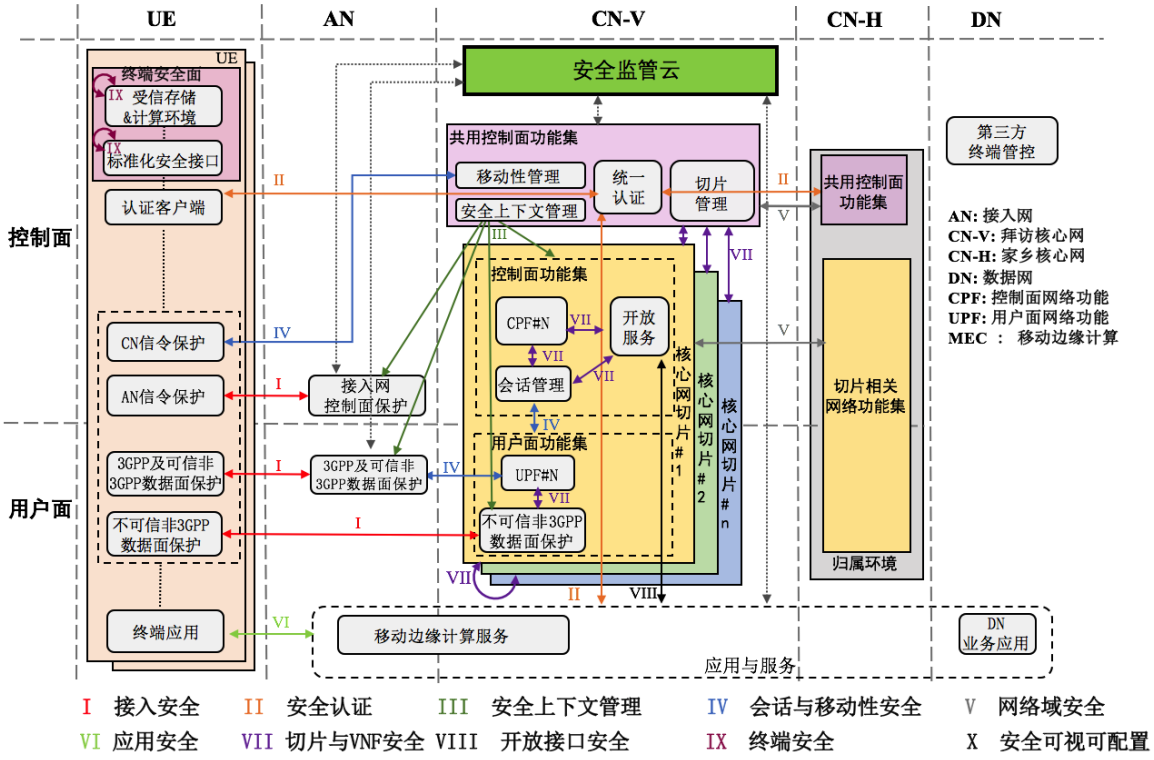

图 2 5G 安全总体架构

如图 2 所示，针对 5G 新型网络架构与典型业务应用场景的安全需求，设计了涵盖认证、接入安全、切片安全、MEC 安全、安全监管、终端安全等核心安全功能的 5G 安全总体架构（以下简称安全架构）。如表 1 所示，该安全架构包含 10 个安全技术集。在 4G LTE 安全技术集的基础上，针对 5G 网络开放性与虚拟化的特点，引入了网络开放接口安全、切片与 VNF 安全的技术集；针对终端的高安全防护能力需求，引入了终端安全技术集；针对移动边缘计算等新型移动服务方式,扩展了应用安全技术集。

表 1 5G 网络安全技术集

编号	名称	含义
1.	接入安全	保证终端接入 5G 网络的数据与信令安全的技术集
2.	安全认证	保证终端、网络与业务相互安全认证的技术集
3.	安全上下文管理	保护终端、接入网、核心网安全上下文的生成、下发等管理过程的安全技术集
4.	会话与移动性安全	保证会话安全性与移动性管理安全性的安全技术集
5.	网络域安全	保证在拜访地的网络功能和家乡的网络功能之间信令和数据交互安全性的技术集
6.	应用安全	保证终端和 MEC、电信网或数据网业务应用之间安全通信的安全技术集
7.	切片与 VNF 安全	保证切片与 VNF 的安全运行，以及保证各切片间、各 NVF 间安全通信的安全技术集
8.	开放接口安全	保证开放服务接口的合理、合法调用的安全技术集
9.	终端安全	提升终端自身安全防护能力以及适配专用领域应用的安全技术集
10.	安全可视可配置	上述安全功能可配置并且用户可获知安全功能的配置

5G 安全总体架构的特点为：

(1) 增强信任关系构建

区别于以往移动通信系统信任关系构建所依赖的用户与网络、用户与业务的二元信任模型，该安全架构通过统一认证的网络功能，支持网络与业务间新的信任关系构建，赋予用户与业务间信任关系新的内涵。

a) 支持网络与业务间新的信任关系构建

首先，在现有二元信任模型基础上，引入网络与业务间的信任构建机制可以提高业务提供商的可信性，降低恶意软件、钓鱼网站等对用户的威胁；其次，对于某些物联网行业应用(如，烟感监控报警)，通过事先建立网络与业务间的信任关系，终端在完成入网认证后不再需要进行业务接入认证，从而简化了用户的业务认证流程。因此，安全架构通过安全认证安全技术集，在统一认证网络功能和应用服务间实现新信任关系的构建。

b) 支持用户与业务间信任关系的新内涵

在业务与网络分别对用户认证机制的基础上，针对多样化应用的安全需求，支持网络统一认证与业务（第三方）统一认证两种机制。

网络统一认证：业务提供方将业务认证委托给电信运营商，通过运营商一次认证达到网络认证和业务认证的双重目的，例如，边缘计算服务等应用场景。

业务（第三方）统一认证：运营商信任业务对用户的认证结果，经一次业务认证，即可为用户提供网络服务，例如，高安全专用领域、工业物联网等应用场景。

(2)异构接入安全

该安全架构支持 3GPP 接入安全，包括：接入层（AS）控制面安全、非接入层（NAS）控制面安全与用户面安全，并支持受信与非受信的非 3GPP 接入安全。对于 3GPP 接入和受信的非 3GPP 接入方式，在接入网实现控制面保护和用户面保护；而对于非受信非 3GPP 接入方式，由于接入方式非受信，将用户面保护功能置于 5G 核心网，采用从用户到核心网端到端的保护方式，防止用户面数据在非受信的非 3GPP 接入网被窃听或篡改。

(3)网络开放能力安全

5G 网络架构将支持部分服务与安全能力通过 API 接口开放给第三方(如业务提供商、垂直行业等)。在安全架构中通过在开放服务网络功能与业务应用间引入开放接口安全技术集，为开放服务被合法、合理的调用提供了保障。

(4)切片与虚拟网络功能（VNF）安全

针对 5G 网络虚拟化的特点，在安全架构中引入了切片与 VNF 安全技术集，实现切片间安全隔离、切片内部不同的 VNF 之间的安全隔离、VNF 访问控制、MANO 安全加固、SDN 控制器安全加固等安全功能。

(5)基于大数据的安全监管

由于 NFV、SDN、网络切片等 IT 技术的引入，以及与诸多垂直行业的深度融合，5G 网络相对于 4G LTE 网络受攻击面大幅增加。因此，要保证 5G 安全的完备设计是一项巨大的难题。

针对这一难题，在安全架构中引入基于大数据技术的“安全监管云”，对 5G 网络进行安全态势管理、监测预警与安全防护。具体而言，在接入网、核心网的网元与各网络功能中部署监测点，各监测点实时采集相应的配置信息与网络运行状态等信息（如信令信息、流量信息、内容信息），所采集的信息将统一汇聚到安全监管云；安全监管云通过智能学习与大数据技术等手段对网络中存在的潜在威胁进行识别和预警；进一步，安全监管云可支持动态安全防护策略的生成、更新和下发；各监测点根据下发的安全防护策略对所在网元和网络功

能重配置以实现系统的主动防御。

（6）终端安全

终端安全是 5G 安全体系中不可缺少的一环。安全架构在终端中引入终端安全面，在终端安全面中通过构建受信存储、计算环境和标准化安全接口，分别从终端自身和外部两方面为终端安全提供保障。终端自身安全保障可以通过构建可信存储和计算环境，提升终端自身的安全防护能力；终端外部安全保障通过引入标准化的安全接口，支持第三方安全服务和安全模块的引入，并支持基于云的安全增强机制，为终端提供安全监测、安全分析、安全管控等辅助安全功能。

3.2 认证/鉴别与授权

根据前面的需求，认证与授权主要从以下方面进行考虑。

3.2.1 广泛网络实体的身份标识支持

当前的网络环境中，存在多种网络实体身份标识方式，包括网络用户的生物特征、法定证件，网络设备的物理标识、MAC 地址，网络应用的注册标识等。上述各种身份标识方案命名标准分散，格式不统一，且扩展性有限，无法有效用于 5G 网络中对海量实体的身份标识。面对用户、设备、数据、服务等网络实体将大量接入，5G 通信网络需要一套标准统一、使用场景灵活的身份标识机制，对各网络实体进行命名支持，OID 对象标识机制可以作为 5G 网络中网络实体的身份标识的技术支撑。

OID（Object Identifier，对象标识符又称为物联网域名）是由 ISO/IEC、ITU-T 国际标准化组织于上世纪 80 年代联合提出的标识机制，采用分层树形结构对任意类型的对象进行全球无歧义、唯一命名。OID 的目标是为了标识通信和信息处理世界中的任何事物，具有可命名并可被注册的性质。OID 是使用无歧义的全局唯一值来标识对象，可保证对象在通信或信息处理中正确地定位和管理。此外 OID 具有分层灵活、扩展性强、跨异构系统等优势，并可兼容现有标识机制，适合作为现有各种应用的元标识机制。如在射频识别（RFID）领域中，ISO/IEC 和 ITU 组织于 2007 年批准将 OID（2.27）作为基于标签 ID 编码机制的元标识。ISO/IEC 15962、ISO/IEC15963 中将 OID 作为各类 RFID 不同标识方案转换的方式，并提供了详细的技术方案，使 OID 成为不同编码机制之间转换桥梁。目前 OID 已经广泛应用于信息安全、医疗卫生、网络管理等领域。

OID 编码结构为树状结构，不同层次之间用“.”分隔，层数无限制，具有很好地扩展性。在标识对象时，标识符为由从树根到叶子全部路径上的结点顺序

组合而成的一个字符串。具体应用场景中，OID 可以使用默认的数字名称，也可以使用自然语言名称，增加对用户的可读性。OID 树形结构的国际根节点下分为 ISO、ISO-ITU 联合、ITU-T 三个分支，其中 ISO、ISO-ITU 联合节点下，由各个国家成员负责国家内部 OID 的管理和注册，其结构如下图所示。

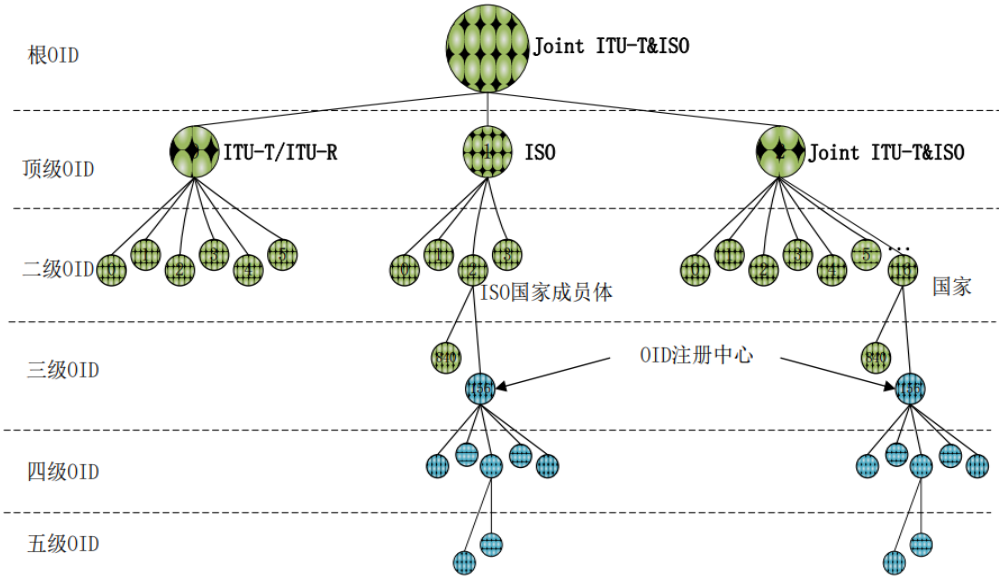

图 3 对象标识符结构示意

在实际应用中，ISO/IEC 国际标准化机构维护顶层 OID 标识，各个国家负责该国家分支下的 OID 分配、注册、解析等工作，实现自我管理和维护。OID 标识机制不存在任何国际专利、知识产权、注册费等方面问题。目前，我国 OID 标识解析系统已研制成功，能够实现和国际根系统对接的同时，保证自主可控性。OID 注册中心自成立以来，已为国内一百多家政府机关、企事业单位和社会团体分配了 170 余项顶级 OID 标识符。OID 在我国各领域有着广泛的应用基础，适宜在 5G 网络中作为广泛网络实体的身份标识支撑技术。

3.2.2 多安全级别的网络实体身份凭证机制

5G 通信网络中，接入的网络实体规模庞大，实体所处环境条件以及各自的安全需求各不相同。网络实体的身份凭证不仅需要认证个体的身份真实性，并将实体的身份标识与凭证进行绑定，还应定义不同的身份凭证安全等级，对网络实体身份凭证的签发和使用场景进行限制和规范。

鉴于网络身份凭证需具备可信性，且易于分发与验证，网络身份凭证的签发应使用非对称密码机制。凭证的可靠性、数据完整性保障由凭证的签发者进行签名实现，凭证的验证者只需要通过公开途径获得相应的验证公钥，即可实现对于凭证的有效验证。使用非对称密码机制进行身份凭证的签发，可确保凭

证签发体系的安全性，同时易于部署与使用。

网络实体身份凭证的签发方在签发过程中应加入安全属性信息，对网络实体的安全级别以及签发环境进行描述。安全属性描述内容包括网络实体身份标识的类型、实体来源、接入的网络环境、签发时提供的身份信息范围等，用以向网络资源提供者申请相应安全等级的服务。身份凭证验证时，凭证的使用方（如网络应用）会根据其凭证的安全属性描述对该实体进行安全等级评估，并根据凭证的身份信息，提供相应安全等级的网络资源或应用服务。

3.2.3 统一的网络实体身份鉴别体系

5G 通信网络中，接入网络实体规模庞大，身份凭证繁多，身份类型各异，为确保各网络实体对网络资源的无缝访问，应定义统一的网络实体身份鉴别机制，提供专业身份服务，实现网络用户、设备、资源、服务的互联互通，并有效保护用户隐私信息。

5G 网络中，网络资源或服务的提供方可以将用户管理托管至独立的网络身份提供方，共享该身份提供方的身份凭证鉴别结果。具体的，网络身份提供方对网络用户、设备等实体进行身份管理，存储并维护其鉴别信息和相关属性信息。网络身份提供方接受网络资源提供方提交的实体凭证鉴别请求，对网络实体进行身份鉴别。鉴别结果及相关网络实体的属性信息经网络身份提供方签名后，返回给网络资源提供方，完成网络实体的身份凭证鉴别过程。

例如，为了降低运营和维护成本，网络应用服务商可将网络用户身份认证权委托给运营商，由运营商统一进行网络和业务认证以达到进行一次认证，各处使用的效果。类似的，对于政府、银行等部分网络应用服务，网络运营商可以信任网络应用服务商，将其作为用户身份鉴别服务的提供者，直接使用其用户身份鉴别结果，为用户提供网络服务,实现跨网络运营商的用户漫游接入计费，方便业务的灵活开展。

统一的网络实体身份鉴别机制应对网络实体提供多安全级别的隐私保护。5G 网络应用场景中，医疗健康、智能家居和智能交通等与用户隐私密切相关的应用会逐渐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，用户的身份、位置、健康等隐私信息将被大量在网络中处理、留存并传输，甚至某些敏感信息（如生物特征）本身作为身份标识信息被各应用公开采集，泄露的风险也因此增加。网络身份提供方在提供身份实体鉴别服务的基础上，还需要考虑不同安全等级的用户隐私保护机制，对各网络资源提供方设置不同的隐私信息访问权限，避免网络资源提供方对用户信息进行关联分析，规范网络身份提供方对的用户隐私信息使用场景。

多个网络身份提供方可以组成身份联盟，在不直接共享身份凭证和隐私信息的前提下，共同对网络资源提供方进行服务。身份联盟内，多个网络身份提供方与众多网络资源提供方进行协商，明确身份服务的提供方和依赖方。用户在网络资源提供方中提交身份鉴别请求时，可以自主选择身份提供者进行身份凭证的鉴别。身份联盟可以在保证网络实体隐私不被泄露的基础上，为用户提供方便的资源和服务访问，进一步扩大网络实体间的互通互认的范围。

3.2.4 多元实体间的安全资源授权管理

5G 通信网络中，网络实体的广泛接入，网络应用与网络资源的大规模扩张，将带来网络资源大范围共享的迫切需求。实现网络资源的共享，需要建立各网络身份提供方、网络资源提供方和资源所有者之间的多元信任，通过有效的授权管理、细粒度的访问控制来保证网络资源的可控、安全共享。

网络资源提供方应对网络用户提供不同安全级别的资源访问权限。网络资源提供方信任网络身份提供方提供的用户身份鉴别结果，根据其凭证的安全属性设置，制定基于属性的访问控制策略，为网络用户提供相应的网络资源访问服务。属性类型包括用户属性、资源属性和环境属性，分别描述了用户实体、网络资源以及用户进行身份鉴别时的环境状况。网络资源提供方维护资源属性，对资源进行型号、所有者、类别等标记；网络身份提供方维护姓名、职级、部门等用户属性，并在用户进行身份鉴别时，获取其凭证安全等级、鉴别时间、鉴别地点等环境属性。在用户请求网络资源时，网络资源提供方根据网络身份提供方提供的属性支持，以及内部设定的访问控制策略，对用户进行具体资源的访问权限判断。

网络应用服务与网络资源提供方之间同样需要建立资源授权访问的渠道。在得到网络资源所有者的许可后，其他网络实体（如其他网络应用服务提供商）可以向网络资源提供方申请访问相应资源。授权管理体制需要明确资源授权访问的协议流程，定义网络资源提供方可授权的资源的范围，以及网络资源提供方、资源所有者、资源请求方等各网络实体的行为边界，实现数据资源、应用服务、接入计费权等网络资源的有效授权管理，建立广泛的网络实体间的多元信任模式。这样，基于统一的网络实体身份鉴别机制，5G 网络可以建立网络资源提供方、网络身份提供方和资源所有者等多方的信任授权体系，构建网络应用间服务资源安全访问的渠道，实现网络服务资源在网络实体间有序、可控的共享。

3.3 接入安全

3.3.1 支持多类型终端、多接入类型、多接入方式

（1） 统一认证框架和层次化密钥

5G 网络支持多种应用场景，不同的应用场景使用不同类型的终端，采用不同的接入技术，5G 网络应提供统一的认证框架，支持多种接入方式和接入凭证，从而保证终端的合法接入，为终端和网络提供接入安全。

（2）支持 3GPP 的接入安全

5G 支持 3GPP 的接入安全基本沿用 LTE 接入的安全机制。通过基于 AKA 机制实现认证和密钥协商，通过 EPS 或者 EAP 方式完成认证过程。在认证完成后，基于根密钥派生出 AS 层、NAS 层以及用户面数据加密和完整性保护所需的密钥。接入网络节点和核心网络节点之间根据安全需求可通过 IPSec 隧道机制提供数据传输安全。

除上述沿用 LTE 安全机制之外，5G 网络增加了用户和核心网络之间用户面数据加密和完整性保护机制。根据具体业务的安全需求，可选择部署相应的安全保护机制，此类安全机制的选择，包括加密终结点的不同，加密算法的不同以及密钥长度的不同。

另外，针对 LTE 网络中，在控制面安全机制尚未建立之前，传递 IMSI 等用户信息带来的隐私泄露的风险，5G 网络考虑采用加密传送机制保护用户隐私，防止泄露。

（3）支持非 3GPP 接入的接入安全

5G 网络支持非 3GPP 接入，其接入模型如下图所示，例如 5G 用户使用 WiFi 接入 5G 核心网络，家庭用户使用固网接入 5G 核心网络，企业用户使用专用网络接入到 5G 核心网络。

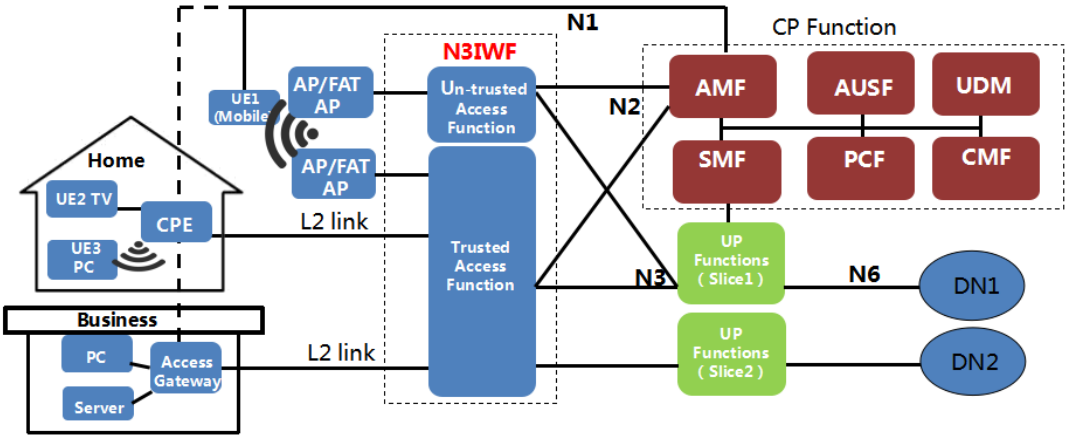

图 4 非 3GPP 接入

3GPP 定义了 N3IWF 提供统一的非 3GPP 接入，包括可信的非 3GPP 接入和非可信的非 3GPP 接入类型。N3IWF 靠近接入网络部署，并提供统一的 N2 和 N3 接口分别和 5G 核心网的控制面和用户面连接。为保证非 3GPP 接入安全，N3IWF 使用 AKA 和 IKEv2 结合的安全保障机制。

N3IWF 的信任接入功能，为用户接入 5G 网络提供的安全功能包括：

- 根据不同的接入技术，提供对应的二层接入机制，例如 PPPoE 接入，IPoE 接入，L2TP 接入等，在建立二层连接之后 N3IWF 支持 5G AKA 认证机制，为用户接入网络提供认证和密钥协商。
- 用户认证成功之后，安全锚点通过 N3IWF 向接入网络和用户提供信令和数据传输加密和完整性保护所使用的安全参数。
- N3IWF 的非信任接入功能，为用户接入 5G 网络提供的安全功能包括：
- 分配专用的物理接口用于连接外部网络
- 配置 VLAN 和 ACL 控制列表阻止非法信令
- 集成防火墙功能用于保护 IKEv2 信令免遭外部网络攻击
- 用户和网络之间的信息（例如接入凭证）交互使用 IKEv2 隧道传送
- 根据应用特征，为不同应用提供差异化 IKEv2 加密和完整性保护算法。

3.3.2 5G 支持典型应用场景的接入安全

（1） eMBB 接入安全

参考 3.3.1 关于支持 3GPP 接入安全 的描述。

（2） mMTC 接入安全

物联网中存在大量的终端需要接入网络，这些终端通常为低功耗资源受限设备，如果采用传统接入认证机制接受海量物联网终端并发接入网络，则极容易产生信令风暴，造成网络拥塞。针对该问题，研究对传统认证机制进行局部优化来满足海量终端接入网络的要求。

- 采用聚合认证方式优化网络信令开销

该方案通过在近用户端部署消息聚合设备，例如信令聚合设备部署于无线接入网络域，配合认证设备（接入认证点、认证服务器）完成对 MTC 终端接入网络的接入认证。聚合认证方式的基本原理框图如下图所示：

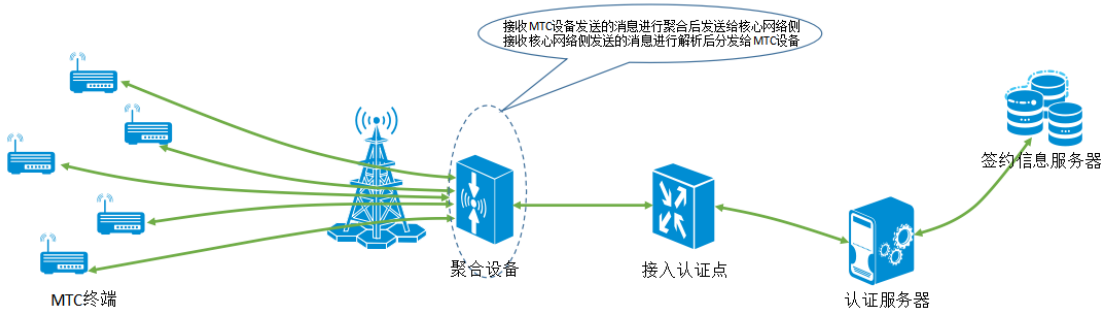

图 5 聚合认证方式

消息聚合设备接收海量 MTC 终端发送的消息，对每个终端的信令消息进行解析，并按照一定的策略进行消息聚合处理，例如将同为接入请求的消息进行解析，提取必要用户信息后，合并为一条接入请求消息。聚合设备将聚合消息发送给接入认证点和认证服务器。认证服务器根据接收的消息，完成对消息中包含的所有用户的认证批处理，例如向签约信息服务器获取对应用户的聚合认证向量。认证服务器将认证结果返回给聚合设备，聚合设备进行消息解析，并将认证结果返回给每个 MTC 终端。

聚合认证方式大大降低了信令开销，从而减轻认证设备的处理负担以及网络中的传输流量。

- 采用群组认证方式优化网络信令开销

该方案对海量 MTC 终端进行分组，为每组用户设立群组网关负责组内 MTC 终端的接入认证。其实现示意框图如下图所示：

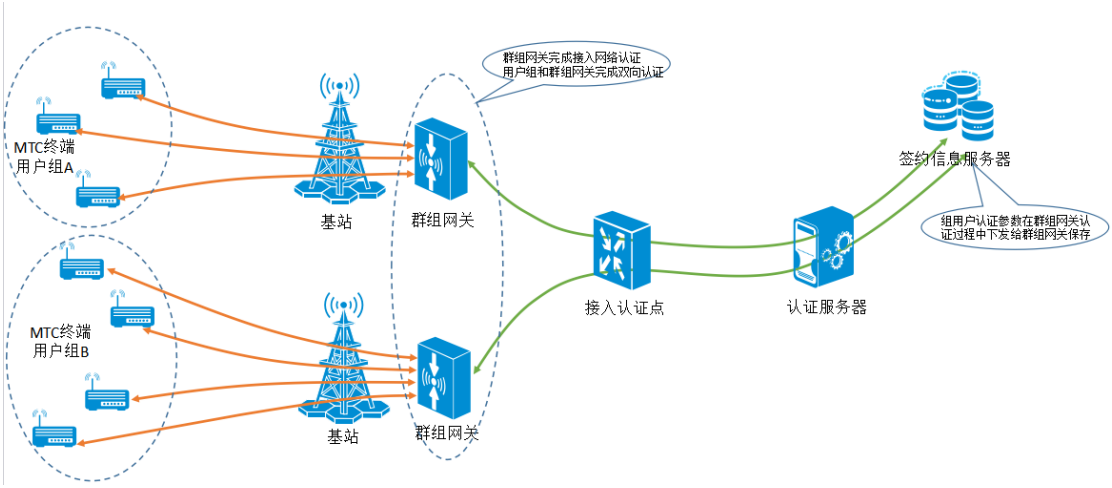

图 6 群组认证

签约信息服务器中存储每组用户的签约信息，包括群组标识，网关标识和组内用户的标识，组内用户的密钥等签约信息。群组用户接入网络的前提是群组网关首先接入网络。群组网关接入网络发起认证时，签约信息服务器接收到群组网关的接入认证参数请求，此时根据组签约信息，签约信息服务器需要为群组网关接入产生认证向量，同时还要为组内所有用户产生认证向量，并将群组认证向量（包含网关认证向量和组用户认证向量）返回给认证服务器。在群组网关接入认证成功之后，认证服务器将对应的组用户认证向量发送给群组网关保存。后续当组内用户接入网络发起认证时，由群组网关作为认证代理，完成对组用户的接入认证。MTC 终端的认证直接和群组网关交互完成，而不需要另外和接入认证点、认证服务器、签约信息服务器等进行信令交互。

群组认证方式要求群组网关首先完成接入网络的认证，认证通过后，网络信任群组网关并将组用户认证向量发送给群组网关，由群组网关完成和组用户的认证。通过这种信任传递的方式完成网络对所有 MTC 设备的认证过程。这种方式减少了 MTC 设备和网络认证设备的认证交互过程，减轻了认证设备的处理负担以及网络中的信令开销。

（3）uRLLC 接入安全

针对超低时延应用，5G 要求控制面从空闲状态切换到连接状态的时长小于 10ms，用户面根据不同的应用时延控制在 1-100ms 之间。

为了实现业务的低时延，其主要技术手段包括：缩短传输距离、简化架构与流程、提升性能、网络轻载等。但是网络中一些安全特性的使用，例如鉴权机制、加密完整性保护，会额外增加信令消息、数据报文处理计算消耗，从而增加时延。

因此，在保证安全的前提下，为降低安全处理带来的额外时延，需要根据终端、网络、应用安全特性进行优化，对 5G 承载网络的安全能力进行取舍、裁剪；另外可以针对不同的应用特征建立对应的网络切片，对安全能力进行统一管理，或者可以由业务层自己定制安全能力，从而不依赖 5G 承载的通用安全能力。具体可以从以下几个方面设计针对超低时延业务的安全。

1）简化安全架构

5G 安全架构是基于互不信任网络考虑的，存在多重安全保护机制，概括起来如下图所示，包括 UE 和 AN 的接入安全，AN 和核心网之间的安全，用户和核心网之间的安全，核心网和业务应用的安全以及用户和应用之间的安全。

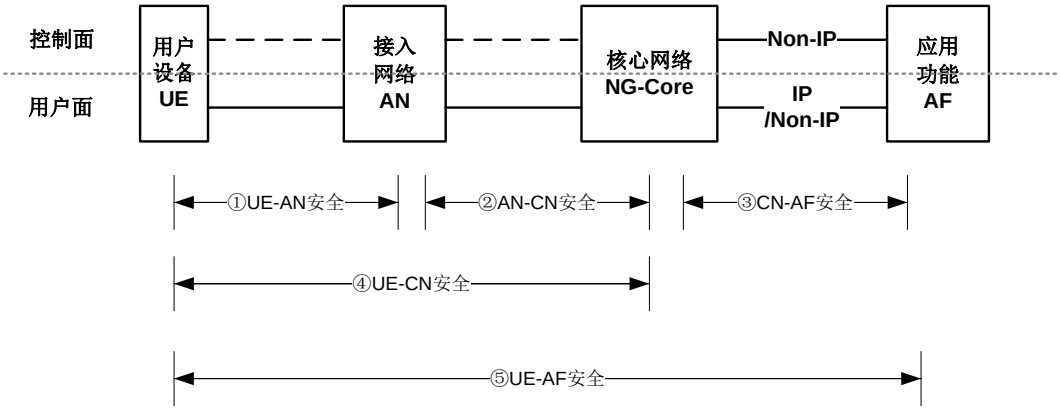

图 7 5G 多重安全保护机制

从上图看出在安全功能实现上存在多个层面的重叠或者多重防护，针对超低时延场景，可以考虑统筹网络规划，尽量减少安全重叠，从原来的五层网络安全压缩到两层甚至一层网络安全。例如将接入网和核心网尽量部署在同一个安全网络域内，避免额外的 AN-CN 安全连接开销；UE 与 AN 之间安全和 UE 与 CN 之间安全只选择其一，减少安全开销；UE 与 AF 之间的安全和 CN 与 AF 之间的安全只选择其一。

2）简化安全流程

为保证控制面状态切换时间在 10ms 以内，对状态切换请求消息（例如业务请求消息）进行简单的本地鉴权，通过完整性保护检查确认合法即可，尽量避免出现完整的 AKA 鉴权流程。

3）简化安全算法

对现有的安全算法进行性能优化。例如将现有 AES 加密算法中基于块加密的 CTR 模式改为基于流加密的 Counter 模式，以提升算法性能。

4）减少不必要的密钥刷新

对于终端设备的移动性切换场景，可以保持 NG 侧 PDCP 层锚定不变，从而不用对密钥进行刷新，降低时延、抖动。

5）区分业务的安全策略

针对机密性要求不高但可靠性要求较高的应用，例如工业控制应用，可以保留完整性保护机制，而选择不加密或者轻量级的加密。通过完整性校验可避免网络篡改数据，预防重放攻击等威胁。

针对机密性和可靠性都有要求的应用，例如智能穿戴应用，考虑尽量选择性能较高的安全算法，例如选择基于流加密的安全算法。

3.4 移动边缘计算（MEC）安全

针对 MEC 系统的特殊安全需求，在传统安全机制的基础上，设计了 MEC 边缘节点硬件设施保护、MEC 系统隐私泄露防护、MEC 三元认证与鉴权方案。其中 MEC 边缘节点硬件设施保护方案针对物理设施防护的安全需求，旨在消除边缘节点暴露的硬件基础设施带来的安全威胁；MEC 系统隐私泄露防护方案针对隐私与数据保护的安全需求，通过管控运行于 MEC 系统中的第三方应用阻止隐私信息流出；而 MEC 三元认证与鉴权方案针对认证、鉴权与权限管理的安全需求，主要解决服务下沉至网络边缘带来的实体间互认证和权限分配问题。

3.4.1 MEC 边缘节点硬件设施保护

MEC 硬件设施保护方案的基本策略为“尽力保护，按需备份”。“尽力保护”指采取一切可行的措施降低 MEC 边缘节点硬件基础设施被破坏的可能。由于 MEC 服务被下沉至网络边缘客观上缩短了其与攻击者之间的物理距离，“尽力保护”的首要目标在于减小攻击者接触到 MEC 边缘节点硬件基础设施的机会。对应的保护措施包括：

- 保护 MEC 边缘节点的支持环境；为 MEC 边缘节点所在基站配备防盗门和门禁监控，加固易被盗取的空调、变压器、蓄电池、电缆，建立动力环境监控系统，加装红外探测器、振动传感器、声光告警设备，实时监测 MEC 边缘节点周围的环境；
- 保护 MEC 边缘节点硬件基础设施：为 MEC 边缘节点硬件基础设施设置单独的隔间，配备独立的门禁系统，为 MEC 边缘节点服务器设备安装加固防护罩和安全锁。

MEC 边缘计算节点可能被置于严酷场景中，面临来自极端气候、自然灾害和工业灾难的威胁。因此，“尽力保护”的另一目标在于降低恶劣环境破坏 MEC

边缘节点硬件基础设施的风险。为此必须强化边缘节点硬件基础设施的防火、防水、防尘、防辐射能力，采用耐高温、防水的线缆、材料和防护外壳制作高尘密水密等级的 MEC 边缘节点服务器设备。

尽管采取了一切可行的措施，“尽力保护”策略无法从根本上解决 MEC 边缘节点硬件基础设施的暴露的问题。一旦 MEC 边缘节点被攻陷或发生故障，MEC 服务能够通过“按需备份”策略得到保持或恢复。“按需备份”指根据 MEC 服务的需求，选择性地进行数据备份。对于可靠性和时延要求极高的服务，如无人驾驶，MEC 系统将其数据分布式地备份到多个领近节点。出现当前节点失效的情况时，距离用户最近、延迟最低的节点直接对用户恢复服务。而对于可靠性和时延要求较为宽松的服务，其数据被备份在 MEC 控制器。当前节点失效时，MEC 控制器将备份数据回传给距离用户最近、延迟最低的节点，之后节点再恢复服务。

3.4.2 MEC 系统隐私泄露防护

为了向用户提供精准服务，MEC 系统将不可避免的接触到大量移动用户与设备的隐私信息，如用户身份、位置、移动轨迹等。因此，MEC 隐私保护的关键在于保证用户隐私信息不通过 MEC 系统任意泄露。

第三方 MEC 应用获得用户隐私信息途径有两种：(1) 直接通过终端客户端获取用户隐私信息；(2) 第三方 MEC 应用通过 MEC 基础平台的 5G 标准开放服务获取用户隐私信息。

为了应对第三方 MEC 应用泄露、滥用用户隐私信息的问题，MEC 节点与 MEC 控制器应协同工作增强 MEC 系统的隐私保护，基本实现框架如图 8 所示，其特点在于：（1）隐私保护策略可适配；（2）MEC 节点监控应用行为；（3）MEC 控制器管控应用与第三方通信。具体而言，首先，用于限制 MEC 应用行为的隐私保护策略可由用户制定或由 MEC 系统适配。隐私保护策略需同时满足隐私信息的安全需求与应用的基本服务要求。隐私保护策略可由以下四部分组成：

- 网络连接限制：规定应用能够使用的通信协议、端口、地址和流量；
- 接口调用限制：限定应用能够使用的接口与服务；
- 数据读取限制：指定应用能够读取的用户数据；
- 虚拟镜像限制：禁止应用使用非法的虚拟镜像。

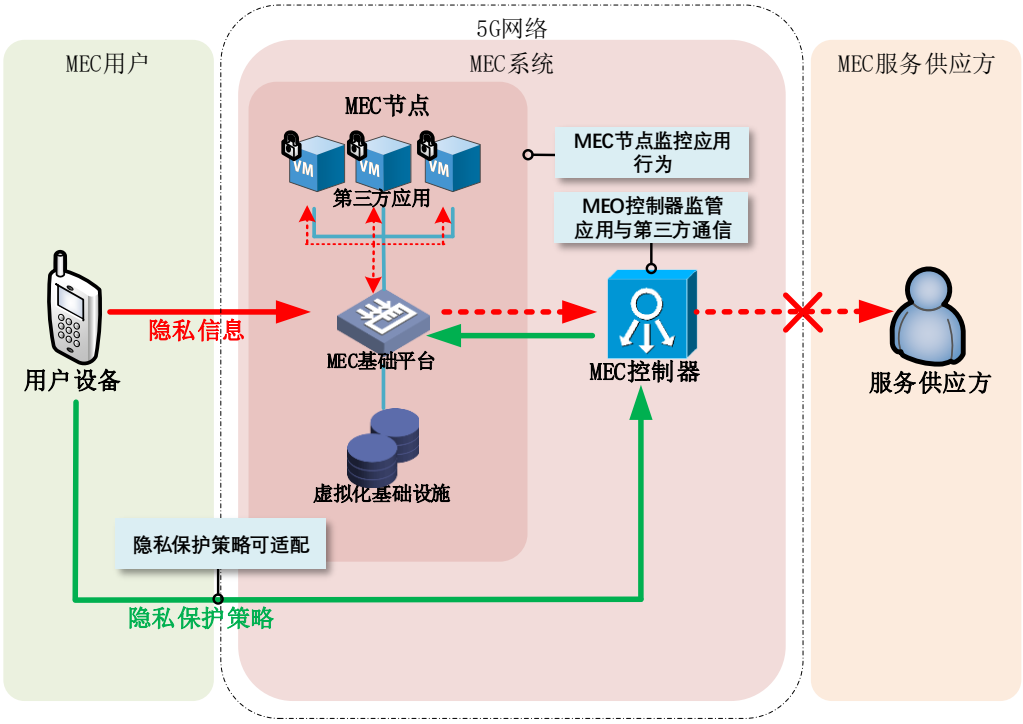

图 8 MEC 系统隐私泄露防护方案框架

考虑到 MEC 低时延的特性，服务提供方提前根据可能的安全策略构造应用并提供给 MEC 系统。接收到用户发布或自主生成的安全策略后，MEC 系统检索与之匹配的应用，同时在 MEC 节点配置相应的虚拟环境。符合安全策略的应用在 MEC 节点的专用虚拟环境中实例化。MEC 节点通过多种措施监控 MEC 应用的行为，相关安全功能包括：

- 输入控制功能：阻止应用非法读取用户隐私信息，严控应用对移动边缘服务的使用；
- 网络控制功能：禁止应用建立任何非法网络连接，阻断第三方对应用的非法访问，控制危险协议以防应用恶意上传数据，限定应用的上行带宽和上传频率；
- 接口控制功能：禁用存在安全隐患的应用编程接口，防范应用利用这些接口操作其他应用、建立 VPN 通道向第三方发送数据、修改 MEC 的安全日志；
- 生命周期管理功能：MEC 节点对隐私信息进行全生命周期的管理，加密存储隐私信息，在隐私信息的发布阶段运用匿名技术，在隐私信息被使用阶段采用访问控制和随机扰动技术；
- 配置不可变功能：维持应用虚拟环境配置的稳定，拒绝来自第三方或应用的修改配置请求；

- 状态断言功能：MEC 节点实时将应用行为记录在日志中，并向用户提供查询日志的接口，或定期向用户推送应用的安全状态。

最后，MEC 应用与外界的通信将由 MEC 控制器进行统一的代理与监管。MEC 控制器代理服务提供方或连接应用的请求，使服务提供方无法直接连接到运行于边缘节点上应用。同时，MEC 控制器负责监管应用发往外界的全部通信，过滤所有数据流中的隐私信息，阻止其流向非法第三方。

3.4.3 MEC 三元认证与鉴权

为保障基本的安全和服务，MEC 系统必须为各实体分配身份，并实现所有实体间的互认证。MEC 通用场景中的相关实体包括隶属于运营商的 MEC 系统（以下称 MEC 系统），第三方提供的 MEC 应用（以下称应用），以及 MEC 用户使用的用户设备（以下称用户），三者构成了 MEC 基本的三元信任模型。其中信任闭环建立的关键在于用户与应用、MEC 系统与应用间的互认证。除此之外，在三元信任模型内部，MEC 系统由 MEC 控制器与 MEC 节点组成，为防止“伪节点”的出现，需由 MEC 控制器对每个新加入的节点进行认证。而在三元模型外部，5G 网络也要对 MEC 系统进行认证。因此，MEC 三元认证方案处理以上 5 种认证关系，如图 9 所示，具体而言：

- MEC 系统与应用互认证：MEC 控制器收到应用提供方的请求，或应用提供方收到来自 MEC 控制器的用户使用应用请求时，MEC 控制器与应用提供方的认证服务器之间进行 MEC 系统与应用的互认证；
- MEC 系统与用户的互认证：用户设备通过 MEC 控制器申请使用应用，或 MEC 控制器协调用户分配应用时，用户设备与 MEC 控制器之间进行 MEC 系统与应用之间的互认证；
- 用户与应用的互认证：在 MEC 系统与应用、MEC 系统与用户之间的互认证完成后，用户设备以 MEC 控制器为代理，连接到应用提供方的认证服务器，进行用户与应用的互认证；
- MEC 控制器认证 MEC 节点：新 MEC 节点加入 MEC 系统时，MEC 控制器代表 MEC 系统认证该 MEC 节点的合法性，对于状态发生改变的 MEC 节点，MEC 控制器对其重新认证；
- 5G 网络认证 MEC 系统：MEC 系统初始化阶段，5G 网络认证 MEC 控制器，确保 MEC 系统安全可靠，图 2 中 5G 网络已进行过对 MEC 系统的认证。

同时，在资源配置的过程中，移动边缘协调器分别对 MEC 节点和用户进

行鉴权，面向不同权限的节点和用户选择性地开放部分服务。MEC 节点进一步对运行于其上的 MEC 应用进行鉴权，开放相应的服务给每个不同的应用。

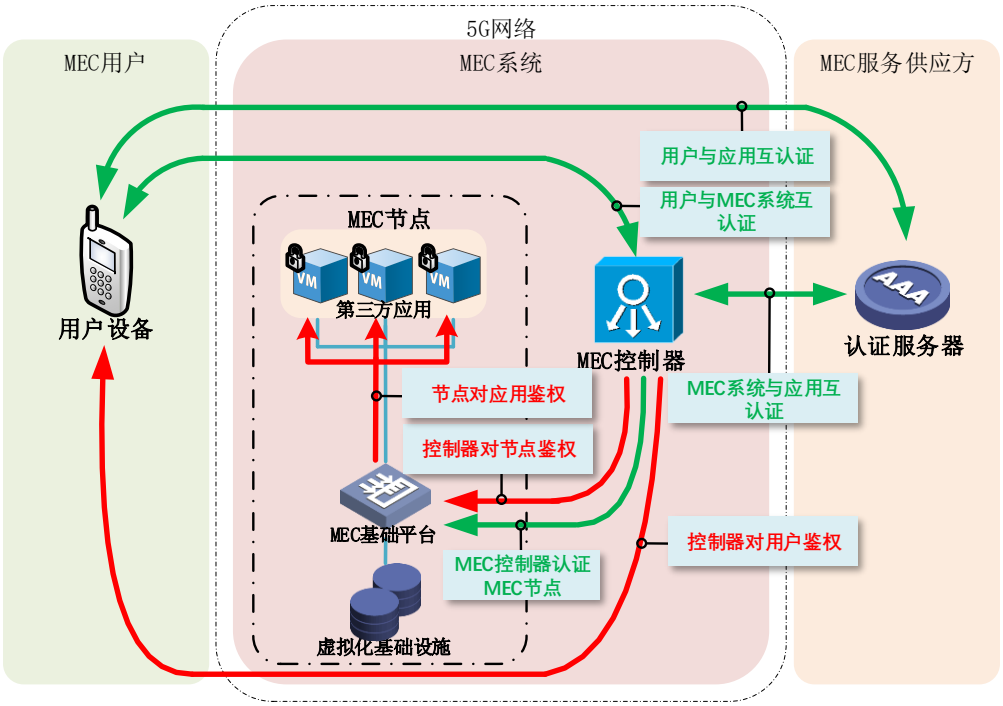

图 9 MEC 认证与鉴权

3.5 切片安全

网络切片将是 5G 网络的重要组成部分，它使运营商能够针对市场的各种需求创建定制网络，以提供优化的解决方案，例如，从功能、性能和隔离等方面。网络切片由支持特定用例的通信服务需求的逻辑网络功能集合组成。

网络切片中的网络功能共享和不同切片之间的隔离可能会带来安全隐患。在某些场景下网络切片允许第三方运行他们自己的功能，甚至可能完全由外部第三方（如企业或者特殊行业）管理，因此与网络切片相关的安全要求中，网络切片的隔离尤其重要。

5G 网络的业务接入模型有多种类型，UE 不仅能够通过不同类型的接入网络如 3GPP 接入系统、非 3GPP 接入系统、可信/不可信的网络接入 5G 网络，而且能够同时接入由不同网络切片提供的服务。因此 5G 网络这些能力组合导致部署场景数量的增加。

同时 5G 网络可以通过网络切片实现不同安全等级的网络，实现按需组网，安全分级，即通过按需组网、安全分级的网络切片安全关键技术，根据业务场景和业务需求实现切片的安全隔离，采用不同的安全机制实现不同的安全

等级，实现终端的接入认证和鉴权和切片间的通信安全，实现 5G 网络的按需组网和安全分级。

3.6 数据完整性和机密性

为了应对网络面临的窃听、篡改等安全威胁，5G 网络在移动终端和网络设备之间提供数据完整性和机密性保护，为用户提供 5G 网络安全保障。

5G 网络数据保护体现为用户面和数据面的数据完整性和机密性保护。目前 5G 网络用户面数据保护终结点为基站，即提供移动终端到基站之间的用户面数据完整性和机密性保护。5G 网络信令面数据保护终结点为基站和核心网，即同时提供移动终端到基站之间的信令面数据完整性和机密性保护、移动终端到核心网之间的信令面数据完整性和机密性保护。

为了应对 5G 网络域内和不同网络域之间的信息安全问题，5G 网络域内和不同网络域之间一般采用 IPSec 对传输的数据进行完整性和机密性保护。对于边界保护采用划分安全域的方式，在安全域的边界进行保护。

为了进一步保证行业的业务应用安全性，也可在终端的应用层增加端到端的数据保护，对传输的数据进行完整性和机密性保护。

3.7 隐私保护

5G 网络提供差异化的隐私保护能力，不同用户、不同业务场景对隐私保护的需求不尽相同，因此需要针对不同的用户和业务场景采用不同技术措施解决 5G 网络的隐私保护问题。另外，根据隐私数据在 5G 网络中的实际使用情况，从数据采集传输、数据脱敏、数据加密、安全基线建立、数据发布保护等方面采用不同技术措施保证数据的隐私安全。5G 网络中隐私保护所采用的主要技术措施有：

（1）数据加密技术

数据加密是 5G 网络中保证数据隐私安全的最有效手段之一，也是隐私保护过程中采用的最常见技术手段之一。按照实现思路，可以将其划分为静态加密技术和动态加密技术。从实现的层次上，可以分为存储加密、链路层加密、网络层加密、传输层加密等。采用加密技术可以有效保证 5G 网络隐私数据的机密性、完整性和可用性。

针对 5G 网络虚拟化和云化的新特点，可以引入一些新的加密技术来保证数据的隐私安全。比如同态加密技术，该技术提供了一种对加密数据进行处理的功能。同态加密技术对加密的数据处理得到输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的结果相同。

（2）基于限制发布的隐私保护技术

在 5G 网络数据发布过程中，限制发布技术即是有选择地发布原始数据、不发布或者发布精度较低的敏感数据, 以实现隐私保护。当前此类技术的研究集中于数据匿名化: 即在隐私披露风险和数据精度间进行折中, 有选择地发布敏感数据及可能披露敏感数据的信息, 但保证对敏感数据及隐私的披露风险在可容忍范围内。目前，比较成熟的匿名化技术有 k-anonymity（k-匿名化）,l-diversity（l-多样化）,t-closeness（t-贴近性）技术等。下一步的研究重点，将是针对 5G 网络中需要发布的结构化隐私数据，制定更好的匿名化原则、设计更高效的匿名化算法，使得 5G 网络发布的数据既能很好的保护隐私，又能具有较大的利用价值。

（3）访问控制技术

访问控制技术也是 5G 网络隐私保护采用的最常用技术手段之一。访问控制可以通过策略和技术手段保证隐私数据不被非法使用和窃取。传统的访问控制技术包括用户口令、数字证书、USB KEY、生物识别技术等。这些技术同样可以应用到 5G 网络之中。另外，针对 5G 网络功能实体的协议交互流程处理中的隐私安全，可采用基于规则、流程的访问控制技术，使得攻击者无法通过假冒合法用户访问用户数据库的方式窃取用户隐私信息。

（4）虚拟存储和传输保护技术

为保证隐私信息在 5G 虚拟化网络存储过程中的隐私安全，可采用用户数据库的动态迁移和随机化存储技术。动态迁移技术可以在保证虚拟机上服务正常运行的同时，将一个虚拟机的数据从一个物理主机迁移到另一个物理主机的过程。这使得攻击者即使成功入侵用户数据库也无法锁定要窃取的用户数据。

隐私信息在 5G 网络传递过程中的隐私安全，可以根据 5G 网络传输协议交互流程，采用相关信息的动态关联和协同重组技术，使得攻击者无法通过数据挖掘技术从散布的用户数据中分析出有价值的用户隐私信息。

（5）5G 网络隐私增强技术

目前，很多组织都在研究 5G 网络的隐私增强技术。当前研究的重点主要集中在使用非对称密钥加密的方法来加密 5G 网络的永久标识符（IMSI），或是使用伪 IMSI 的方法来隐藏用户的永久标识符。加密永久标识符的方法是在终端侧通过公钥对永久标识符进行加密，网络侧通过私钥对永久标识符进行解密，该技术方案可以有效保证 IMSI 传输过程中的隐私安全，但需要增加一套公钥基础设施（PKI），对使用的非对称密钥进行分发和管理。伪 IMSI 的方法是将原本系统中需要传送 IMSI 的地方，使用伪 IMSI 进行替代。该技术方案需要

增加额外的信令开销来保证伪 IMSI 的不断更新。这两种方法都可以有效的防止用户签约身份信息的泄露。同时，由于有效保护了用户的身份隐私，所以即便攻击者得到了用户的位置信息，也不知道对应于这个位置的身份是谁，通过这样保护用户身份的方法间接地也保护了用户的位置隐私。

3.8 安全管理

5G 安全管理需要为认证/鉴别与授权、接入安全和切片安全等提供基础的管理平台，为 5G 网络引入 5G 统一身份和授权管理，构建统一的信任管理体系。这部分内容在前面已有较多描述。除此之外，5G 还需要对网络进行安全监测预警与管控，以解决攻击方式泛在化问题，对 IT 技术引入的安全风险进行防范与管控。

5G 网络安全监测预警与管控是以切片为分割单位组织工作的，可以通过在 5G 网络切片中关键拓扑位置上部署虚拟化探针、虚拟化防火墙等安全功能，以及以实体形态部署探针、防火墙等物理安全设备，跟踪网元实时运行状态，同时通过统一的标准接口收集来自切片中安全敏感的虚拟化设备(如 PCF、AUSF 等)的上报事件等等手段，多渠道实现安全态势感知信息的收集，然后采用基于大数据的关联归并、融合分析和深度挖掘等多种技术手段，结合协议还原识别、静态特征匹配、动态行为分析、异常行为挖掘等层次化检测方法，从离散的、孤立的数据中探测发现潜在的安全威胁，多维度、多视角的将安全态势数据推送至安全态势管理与监测预警管理中心进行可视化展示。然后结合预警知识库、预案知识库给予辅助决策；管理员角色根据决策适时调整网络节点的安全策略（含虚拟化网元之间的安全策略或者安全用途虚拟化网元的配置/设置策略，等等），从而提升集中式运维管理效率和能力，实现 5G 网络的安全态势管理与监测预警。总体实现思路如下图所示：

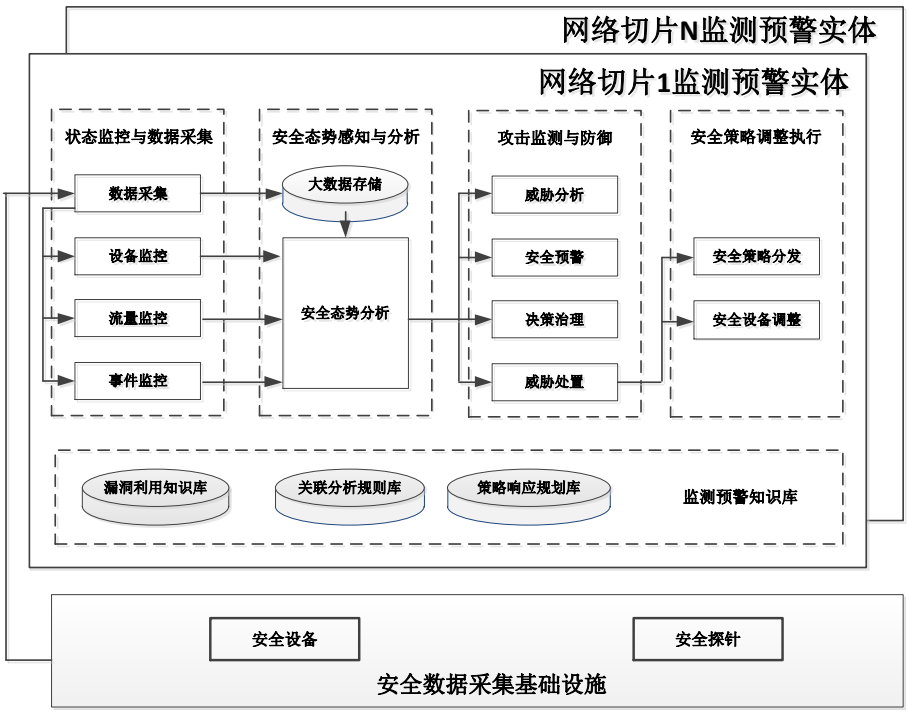

图 10 5G 网络安全监测预警与管控实现思路

5G 网络安全监测预警与管控包含以下几个部分：

1）监测预警知识库

可以通过 5G 网络中不同位置的安全感知工具，管理网络系统设施如服务器、网络设备或软件等，根据地址信息，通过数据聚合分析大量数据，根据分析结果捕捉整个系统状态，建立捕捉系统状态模型，进行可视化、共享、查询和分析，识别以前或正在进行的攻击和威胁，并在某些情况下，自动对安全事件进行相应的反应。

2）状态监控与数据采集

状态监控依靠设备状态监控实现，通过定义切片内部网络设备、安全设备、服务器、终端等设备的状态管理、故障管理和安全通告管理接口，实现基于策略的应急响应处置和业务跟踪功能，包括预警信息库、漏洞库、处理预案库等。

3）安全态势感知与分析

安全态势感知与分析是指通过对虚拟化安全设备及物理环境基础设施安全设备进行广泛采集，将各类告警数据和运行状态数据进行统计分析、关联分析、预测分析和影响性分析等处理，用以有效识别 APT 攻击、DDoS 攻击等安全威胁。安全态势分析包括静态特征检测、动态行为分析、异常行为挖掘、事

件关联分析和综合态势分析五个方面。

4）攻击监测与防御

复合攻击包括若干个攻击步骤，每一个攻击步骤依赖于前一个攻击步骤的输出结果，而复合攻击中的每一个攻击步骤由该步骤所对应的告警信息折射出来。基于威胁分析与决策治理技术，分析攻击步骤之间及攻击步骤与告警信息间的关系，进行安全预警，并通过提取各个攻击步骤阶段相应的攻击意图后，计算预测未来持续的攻击步骤和有效修复建议，实现对网络防御能力的动态调整，同时结合大数据技术，研究安全风险特征，实现安全预警和防御。最后通过与网络切片内虚拟网元、防火墙之类安全设备的安全策略联动，实现威胁处置。

5）安全策略调整执行

当管理员通过安全态势感知和分析对当前 5G 网络的安全态势形成一定了解并认为有必要进行安全策略调整的时候，可以将调整目标进行分解，拆分/形成一系列的对应到不同虚拟化设备中的安全策略，通过统一的接口将这些策略下发到各个虚拟化设备中予以执行，同时收集这些策略的执行结果，跟踪网络的安全态势更新，验证安全策略调整的有效性。

3.9 密钥体系

通过密钥体系，5G 系统可以提供核心网控制面（即非接入层）的机密性、完整性密钥，还可以提供无线网（即接入层）控制面的机密性、完整性密钥，用户面的机密性和可选的完整性密钥，以及用来支持网络分片、新空口、非 3GPP 无线接入网（non-3GPP RAT）、后向兼容 SAE/LTE 等的密钥。

目前，5G 将空口安全的终结点放在接入网内，而针对切片的安全留待将来解决，因此目前的核心网与接入网的密钥主要考虑面向 MM 移动性管理的安全密钥衍生。

考虑到其他接入方式，还引入了 3GPP 之外的其他接入网的密钥：因此，密钥层次中针对现有 3GPP 无线网络和 non-3GPP 无线网络均产生独立的密钥。

每个切片中必须有一个 SMF 会话管理服务尚未成为共识，因为一直以来核心网都被认为是可信的，而核心网切片之间通过虚拟化技术实现了资源的隔离；到各个切片的信令，由可信的 AMF 来进行转发，且 AMF 和 SMF 之间是安全链路，所以可认为是 AMF 与各个切片的 SMF 之间是安全的，所以在虚拟化技术做好切片间隔离的前提下，并不需要单独的 SM 密钥来保护 NAS SM。

目前 5G 密钥衍生是基于有共享 K 的前提，以 LTE 的密钥层次作为基础。

考虑了 5G 会引入多种认证机制，考虑所有密钥是否需要以及密钥如何衍生。接入层密钥可以直接由 SEAF 进行推衍而非接入层机密性与完整性保护密钥不能像 4G 那样直接由 SEAF 进行推衍。

此外，针对攻击者通过核心网攻击获取接入层的密钥参数的情况，有一些隔离接入层与非接入层的密钥体系被提出。其设计思想是：通过与无线链路相关的、不需要分发的物理层密钥，使得终端和接入点能够不依赖核心网，独立产生并更新与无线链路、节点强相关性的加密和完整性保护密钥作为接入层密钥；而终端和核心网协商使用与身份信息强相关的加密和完整性保护密钥作为非接入层密钥；接入层密钥的更新过程与非接入层密钥的更新过程完全独立；接入层密钥根据无线通信信道特征的变化随时更新。

3.10 终端安全

在终端安全体系中，密码是其核心支撑技术。密码技术与终端的不同结合方式，带来两种不同的安全体系结构，这两种体系结构各有其鲜明的特点。

1、物理门卫式体系结构

红黑隔离的物理门卫式安全体系架构，是在终端内部的信息通路上物理地串接密码处理部件，形成物理流过式的密码安全处理，实现安全数据所在的“红区”与非安全数据所在的“黑区”隔离的安全架构。该架构具有以下三个特点：一是可确保在“红区”没有任何来自“黑区”的非安全数据；二是可为“红区”阻拦来自“黑区”的所有已知和未知网络攻击，包括零日漏洞攻击等；三是该架构的安全性易于证明，能够适用民用安全、商用安全、特殊安全等多种使用场景。

考虑到当前 4G 技术状态向 5G 演进过程中的不同发展阶段，结合 5G 网络安全特性以及终端产业特点，提出两种技术路线：

（1）“可配置高速接口的终端 SoC 芯片+外置安全芯片”技术路线

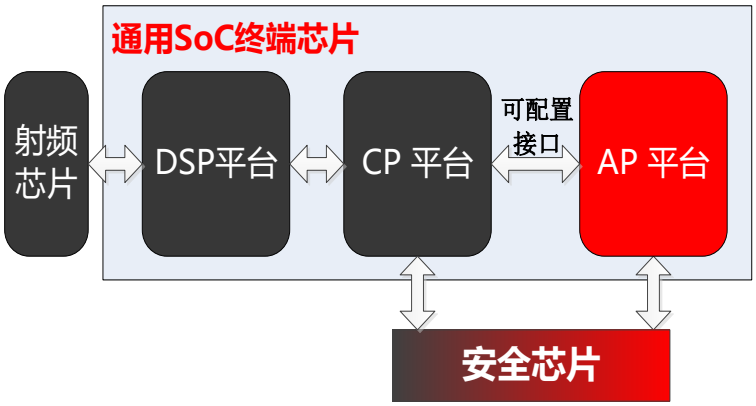

图 11 外置安全芯片路线

在通用 SoC 终端芯片的设计过程中，分别创建 AP 模块、CP 模块的外部高速接口，该高速接口可外接密码处理模块（又称安全芯片），如图 11 所示。AP 和 CP 之间没有物理接口连接，两者之间信息交互的桥梁是安全芯片，必须经过安全芯片的处理后，红区和黑区之间的信息才能够交互。

该高速接口应采用标准化设计。行业用户可按照标准接口，选配行业安全芯片，实现终端安全能力的行业定制。对没有安全需求的终端，可直接短接该接口。

（2）“AP+密码模块+CP”的三合一终端芯片技术路线

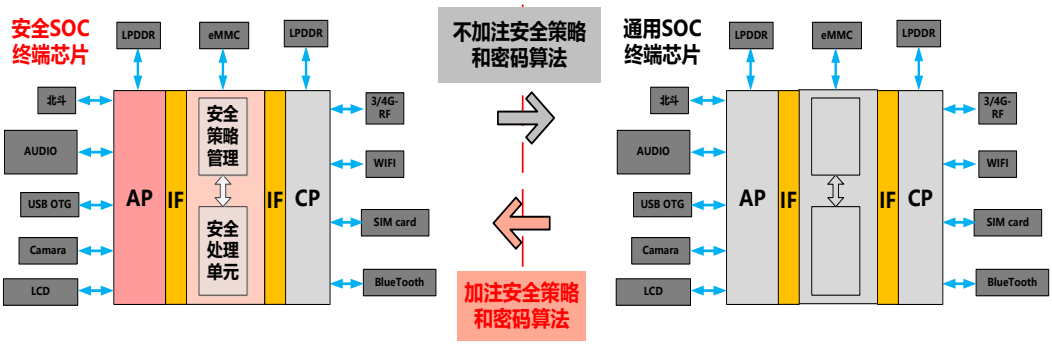

图 12 三合一技术路线

5G 终端将实现 1Gpbs 传输速率，为了同时满足终端的高速信息保护要求和低电量消耗要求，可以将 AP、CP 以及安全部件等硬件模块进行芯片集成化设计，在芯片内实现不可旁路的物理流过式安全处理，如图 12 所示。

开放芯片的安全服务接口。为了支持第三方安全服务植入，实现行业定制，需要开放芯片内安全模块的安全接口，开放芯片的运算资源和存储资源，通过行业认可的安全策略注入和密码注入，满足不同行业的定制要求。

2、逻辑门卫式体系结构

“逻辑门卫式体系结构”是指在终端内部的信息处理通路上，通过系统软件调用安全模块的方式，实现对信息的保护和执行环境的保护。从执行环境的安全启动、操作系统加固、运行时动态度量到信息的传输加密、存储加密、应用安全、输入/输出控制等功能，采用分层、组合的方式调用安全模块，达到逻辑门卫式的安全防护效果。按其技术路线可分为 TEE 和虚拟化技术两种。

逻辑门卫式体系结构可根据行业安全需求或业务类型安全需求，按需部署相应的安全保护机制，为不同行业或业务提供差异化安全服务。

（1）TEE

基于 TrustZone 技术实现的可信执行环境（TEE）的核心理念是将可信资源

与非可信资源在硬件上实现隔离。TrustZone 从硬件安全扩展来提供资源隔离，软件提供基本的安全服务和接口，将软硬件资源隔离成两个环境（分别为安全世界和普通世界），仅通过 Monitor 模式实现两个世界之间切换时的上下文备份和恢复，最终实现构建可编程环境，以防止资产的机密性和完整性受到特定攻击。基于 TrustZone 技术可信执行环境的软件框架如下图。

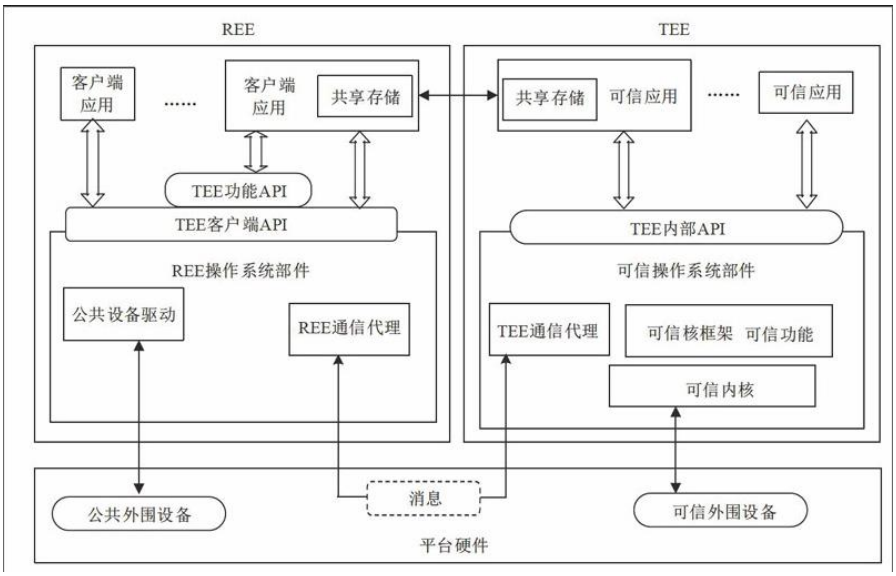

图 13 可信执行环境的软件框架

可信执行环境通过安全启动，构建终端信任链体系，实现普通世界和安全世界运行环境可信。可信执行环境在安全世界里采用独立的安全操作系统、独立的安全应用、独立的设备驱动，安全操作系统可通过系统调用方式为普通世界提供安全服务。同时可在普通世界通过系统内核安全增强、框架层安全加固、应用安全机制和云端管控实现系统安全增强。

面对 5 G 多种应用场景和业务需求，基于 TEE 的终端安全体系架构，应可根据业务类型不同或根据具体业务安全需求，从安全启动、系统加固、运行时度量、安全存储、应用安全和云连接等角度，采用定制、裁剪和组合的方式，按需部署安全保护措施（如轻量级安全算法、简单安全协议、群组认证、设备管理和远程升级等），最大限度地发挥硬件的安全能力，为系统提供硬件级的安全保障。

标准安全接口。基于 TrustZone 技术的可信执行环境，是一个能力开放的平台，应可以向第三方或者垂直行业开放安全能力接口如：认证授权接口，可信接口（可信认证、可信应用、可信存储、可信数据管理、可信发布、可信状态显示），安全服务接口（密钥管理、密码算法、安全存储、安全时钟资源和服务、网络加密接口、安全策略配置），可扩展应用接口（金融应用、移动支付、数字版权等应用接口）。

（2）虚拟化技术

逻辑门卫式体系结构还可基于虚拟化技术实现。该解决方案主要包括硬件层、引导层、运行空间隔离层、操作系统层和应用层几部分，从硬件底层起，通过有序部署虚拟机、安全增强操作系统和具有安全功能的安全模块，综合运用软件完整性保护、运行空间隔离、操作系统加固、应用安全保护等技术，构建移动终端的安全架构。在运行空间隔离层采用虚拟化技术为上层操作系统和应用提供安全的空间隔离和时间隔离，提供安全的运行环境，满足垂直行业安全服务对信息处理的差异化需求。基于虚拟化技术的软件框架如下图。

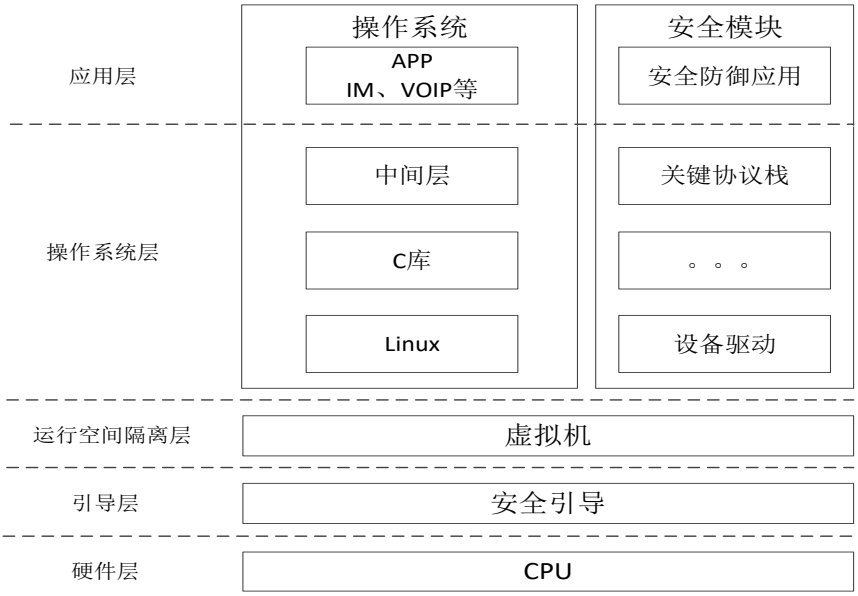

图 14 基于虚拟化技术的软件框架

终端硬件较为复杂，产品定制周期长，产业链支持难度大，采用虚拟机技术可在不改变移动终端硬件的基础上，在底层为上层系统提供安全可靠的分区防护，通过分区使得不同的上层组件可单独部署、评估，使得上层组件易于安全实现；结合移动终端硬件处理器特性，采用虚拟化技术实现分区隔离、信息流控、最小特权管理、安全监视及检查等安全机制。对于所采用的虚拟化技术方案，应具备代码量小、安全性易验证和可形式化证明等特性，确保上层操作系统和应用所需的信息保护不被破坏、安全相关功能不被旁路。

标准安全接口。虚拟机厂家在终端及操作系统厂家配合下，完成运行空间隔离层的适配工作，在运行空间隔离层为上层操作系统提供安全模块（包括密码模块等关键设备驱动、分组等关键协议栈、管控等安全防御应用子功能集）服务的同时，通过空间隔离安全机制支持现有操作系统层及应用层提供的各种安全策略、安全认证、存储、网络加密等安全功能。

4 5G 安全标准化

5G 信息安全的国际标准化工作主要涉及 3GPP SA3、ETSI NFV 和 ITU-T SG17、NGMN 等多个国际标准化组织。

3GPP SA3 在 2016 年 2 月召开的第 82 次会议上，SA3 开始了 5G 安全立项 Study on the Security Aspects of the Next Generation System 的研究工作，此研究项目承接 SA2 的 5G 研究，收集、分析和研究下一代网络中潜在的安全威胁和需求，同时与 SA2、RAN2 和 RAN3 合作开展下一代网络的安全架构和接入网安全研究。

在研究基础上，3GPP SA3 在 2017 年 3 月召开的第 86 次会议上，SA3 开始了 5G 安全标准立项 5G System and Security Architecture-Phase 1 的标准工作，主要侧重安全框架、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以及与 EPS（演进的分组系统）的互通等相关的工作，计划在 2018 年 3 月完成第一阶段的标准制定工作，后续 3GPP 将开展 5G 安全的第二阶段的研究和标准制定工作，如切片安全、能力开放安全、256 比特密码算法等相关标准工作。

ETSI 主要针对 NFV 的安全进行了研究，在 NFV 下专门成立了安全子组对 NFV 安全进行深入研究，主要聚焦 NFV 安全架构、隐私保护、合法监听、MANO 安全、证书管理、安全管理、安全部署等方面的研究和标准化制定。ONF 和 ITU-T 在 SDN 安全方面也进行了相关的标准化工作。

NGMN 在 2015 年 2 月发布了《5G 白皮书》，表达了其在 5G 愿景、需求、技术与架构、频谱、IPR 生态、以及路线图等方面的观点。该白皮书得到了大量全球知名运营商的参与和支持。随后，NGMN 的安全团队先后发布了 3 个安全技术报告，内容涵盖接入网、DoS 攻击、切片、边缘计算、低时延以及用户体验一致性等方面的安全考虑。进入 2017 年，NGMN 成立了正式的 SCT 安全工作组，全面开展 5G 端到端架构、5G 能力开放，以及车联网等方面的安全技术工作。在 10 月初正式发布的《5G 端到端架构框架》白皮书中，分别从网络层、业务使能层、业务应用层、管理与编排、终端设备几个方面阐述了 5G 安全的技术需求，同时也提出了 5G 身份管理需进行系统化设计的倡议。

5 总结

未来 5G 通信网络将面临多样化的业务场景，应用多种虚拟化安全技术和接入技术，在终端接入、服务接口、业务认证等多方面具有新的安全需求。本文在认证授权、接入安全、切片安全、安全监管、终端安全等核心安全功能方

面进行阐述，明确 5G 网络安全需求和架构，为 5G 网络整体架构设计、业务流程、算法机制及标准化工作方面给出了解决思路。

随着 5G 网络安全标准化的全面展开和研究的不断深入，本工作组愿与全球 5G 相关组织、企业、科研机构和高效加强合作，共同推动 5G 网络安全需求与架构相关研究，促进安全可信的 5G 新型网络产业的蓬勃发展。

参考文献

[1] 3GPP TR 33.899: “Study on the security aspects of the next generation system”

[2] 3GPP TR 23.799: “Study on Architecture for Next Generation System”

[3] 3GPP TS 23.501: “System Architecture for the 5G System”

[4] 白皮书“5G 网络安全需求与架构”，IMT-2020(5G)推进组，2017 年 6 月

[5] 对象标识符(OID)白皮书)2015, 中国电子技术标准化研究院, 2015.7

[6] 信息安全技术 鉴别与授权 安全断言标记语言, GBT 29242-2012

[7] OpenID Connect Core 1.0, https://openid.net

[8] OAuth 2.0 Framework, RFC 6749, https://oauth.net/2/

[9] 李宏佳、王利明、徐震，等，5G 安全: 通信与计算融合演进中的需求分析与架构设计，信息安全学报. 2018(1): 1-14.

鸣谢

诚挚的感谢如下单位和人员对本白皮书做出的贡献：（排名不分先后）

卫士通信息安全公司：	曾浩洋、田永春、张力、范子君、吴坤、王俊
中国移动研究研究：	彭晋、庄小君、齐旻鹏、左敏
中国科学院信息工程研究所	荆继武、王利明、李宏佳、王琼霄、徐震、赵宇航
北京数字认证股份有限公司	詹榜华、李亚得、李向锋

大唐电信	徐晖、周巍
中国信息通信研究院	袁琦
中兴通讯	毛玉欣、闫新成、 李岩、周延潮
信息保障技术重点实验室	付宁、穆继会、李婷
华为公司	刘斐、康鑫、李铁岩
西安电子科技大学	李晖、李兴华、曹进、付玉龙
信息工程大学	赵华、游伟
清华大学	赵明、田志刚
兴唐通信科技有限公司	朱晖、周迪、吕晓晨
深圳市中兴物联科技有限公司	薛智军、郑显举
北京元心科技有限公司	李涛、姜哲
未来移动通信论坛	栗洁、刘娴婧

未来移动通信论坛

FUTURE MOBILE COMMUNICATION FORUM