白皮书
2017-06

IMT-2020

IMT-2020(5G)推进组

5G网络安全需求与架构

目　录

引言 1
5G 网络安全挑战和需求 1
5G 安全总体目标 6
5G 网络安全架构 6
5G 网络新的安全能力 8
5G 安全标准化建议 16
总结和展望 17

IMF-2060（5G）推进组于 2013 年 2 月由中国工业和信息化部、国家发展和改革委员会、科学技术部联合推动成立，组织架构基于原 IMT-Advanced 推进组，成员包括中国主要的运营商、制造商、高校和研究机构。推进组是聚合中国产学研用力量、推动中国第五代移动通信技术研究和开展国际交流与合作的主要平台。

5G 网络安全需求与架构

1 引言

经过三十多年的飞速发展，移动通信已成为应用最为普及的信息通信技术。当前，全球新一轮科技革命和产业变革正孕育兴起，跨行业、跨领域的融合创新不断深入，对移动通信技术也提出了更高的要求。随着移动互联网、物联网及行业应用的爆发式增长，未来移动通信将面临千倍数据流量增长和千亿设备联网需求。5G 作为新一代移动通信技术发展的方向，将在提升移动互联网用户业务体验的基础上，进一步满足未来物联网应用的海量需求，与工业、医疗、交通等行业深度融合，实现真正的“万物互联”。

5G 网络新的发展趋势，尤其是 5G 新业务、新架构、新技术，对安全和用户隐私保护都提出了新的挑战。5G 安全机制除了要满足基本通信安全要求之外，还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，保护用户隐私，并支持提供开放的安全能力。当前，5G 国际标准化工作已全面展开，5G 安全也成为业界关注的焦点。本白皮书基于 5G 需求与愿景研究进展，分析 5G 网络面临的安全问题和发展趋势，提出 5G 网络安全需求和架构，为后续 5G 网络安全技术的研究和设计奠定基础。当前业界需要尽快形成 5G 网络安全框架并推动达成产业共识，从而指导 5G 安全国际标准及后续产业发展。

2 5G 网络安全挑战和需求

2.1 新的业务场景

5G 网络将来不仅用于人与人之间的通信，还会用于人与物以及物与物之间的通信。目前，5G 业务大致可以分为 3 种场景： eMBB（增强移动宽带）、mMTC（海量机器类通信）、和 uRLLC（超可靠低时延通信），5G 网络需要针对这三种业务场景的不同安全需求提供差异化安全保护机制。

eMBB 聚焦对带宽有极高需求的业务，例如高清视频，VR（虚拟现实）/ AR（增强

现实）等，满足人们对于数字化生活的需求。eMBB 广泛的应用场景将带来不同的安全需求，同一个应用场景中的不同业务其安全需求也有所不同，例如，VR/AR 等个人业务可能只要求对关键信息的传输进行加密，而对于行业应用可能要求对所有环境信息的传输进行加密。5G 网络可以通过扩展 LTE 安全机制来满足 eMBB 场景所需的安全需求。

mMTC 覆盖对于连接密度要求较高的场景，例如智慧城市，智能农业等，能满足人们对于数字化社会的需求。mMTC 场景中存在多种多样的物联网设备，如处于恶劣环境之中的物联网设备，以及技术能力低且电池寿命长（如超过 10 年）的物联网设备等。面向物联网繁杂的应用种类和成百上千亿的连接，5G 网络需要考虑其安全需求的多样性。如果采用单用户认证方案则成本高昂，而且容易造成信令风暴问题，因此在 5G 网络中，需降低物联网设备在认证和身份管理方面的成本，支撑物联网设备的低成本和高效率海量部署（如采用群组认证等）。针对计算能力低且电池寿命需求高的物联网设备，5G 网络应该通过一些安全保护措施（如轻量级的安全算法、简单高效的安全协议等）来保证能源高效性。

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。低时延和高可靠性是 uRLLC 业务的基本要求，如车联网业务在通信中如果受到安全威胁则可能会涉及到生命安全，因此要求高级别的安全保护措施且不能额外增加通信时延。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。从安全角度来看，降低时延需要优化业务接入过程身份认证的时延、数据传输安全保护带来的时延，终端移动过程由于安全上下文切换带来的时延、以及数据在网络节点中加解密处理带来的时延。

因此，面对多种应用场景和业务需求，5G 网络需要一个统一的、灵活的、可伸缩的 5G 网络安全架构来满足不同应用的不同安全级别的安全需求，即 5G 网络需要一个统一的认证框架，用以支持多种应用场景的网络接入认证（即支持终端设备的认证、支持签约用户的认证、支持多种接入方式的认证、支持多种认证机制等）；同时 5G 网络应支持伸缩性需求，如网络横向扩展时需要及时启动安全功能实例来满足增加的安全需求、网络收敛时需要及时终止部分安全功能实例来达到节能的目的。另外，5G 网络应支持按需

的用户面数据保护，如根据三大业务类型的不同，或根据具体业务的安全需求，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，或者加密算法的不同，或者密钥长度的不同等。

2.2 新技术和新特征

为提高系统的灵活性和效率，并降低成本，5G 网络架构将引入新的 IT 技术，如软件定义网络 SDN（软件定义网络）和 NFV（网络功能虚拟化）。新技术的引入，也为 5G 网络安全带来了新的挑战。

5G 网络通过引入虚拟化技术实现了软件与硬件的解耦，通过 NFV 技术的部署，使得部分功能网元以虚拟功能网元的形式部署在云化的基础设施上，网络功能由软件实现，不再依赖于专有通信硬件平台。由于 5G 网络的这种虚拟化特点，改变了传统网络中功能网元的保护很大程度上依赖于对物理设备的安全隔离的现状，原先认为安全的物理环境已经变得不安全，实现虚拟化平台的可管可控的安全性要求成为 5G 安全的一个重要组成部分，例如安全认证的功能也可能放到物理环境安全当中，因此，5G 安全需要考虑 5G 基础设施的安全，从而保障 5G 业务在 NFV 环境下能够安全运行。另外，5G 网络中通过引入 SDN 技术提高了 5G 网络中的数据传输效率，实现了更好的资源配置，但同时也带来了新的安全需求，即需要考虑在 5G 环境下，虚拟 SDN 控制网元和转发节点的安全隔离和管理，以及 SDN 流表的安全部署和正确执行。

为了更好地支持上述 3 个业务场景，5G 网络将建立网络切片，为不同业务提供差异化的安全服务，根据业务需求针对切片定制其安全保护机制，实现客户化的安全分级服务，同时网络切片也对安全提出了新的挑战，如切片之间的安全隔离，以及虚拟网络的安全部署和安全管理。

面向低时延业务场景，5G 核心网控制功能需要部署在接入网边缘或者与基站融合部署。数据网关和业务使能设备可以根据业务需要在全网中灵活部署，以减少对回传网络的压力，降低时延和提高用户体验速率，随着核心网功能下沉到接入网，5G 网络提供的安全保障能力也将随之下沉。

5G 网络的能力开放功能可以部署于网络控制功能之上，以便网络服务和管理功能向第三方开放。在 5G 网络中，能力开放不仅体现在整个网络能力的开放上，还体现在网络

内部网元之间的能力开放，与 4G 网络的点对点流程定义不同，5G 网络的各个网元都提供了服务的开放，不同网元之间通过 API（应用程序接口）调用其开放的能力。因此 5G 网络安全需要核心网与外部第三方网元以及核心网内部网元之间支持更高更灵活的安全能力，实现业务签约、发布，及每用户每服务都有安全通道。

2.3 多种接入方式和多种设备形态

由于未来应用场景的多元化，5G 网络需要支持多种接入技术，如 WLAN（无线局域网络）、LTE（长期演进）、固定网络、5G 新无线接入技术，而不同的接入技术有不同的安全需求和接入认证机制；再者，一个用户可能持有多个终端，而一个终端可能同时支持多种接入方式，同一个终端在不同接入方式之间进行切换时或用户在使用不同终端进行同一个业务时，要求能进行快速认证以保持业务的延续性从而获得更好的用户体验。因此，5G 网络需要构建一个统一的认证框架来融合不同的接入认证方式，并优化现有的安全认证协议（如安全上下文的传输、密钥更新管理等），以提高终端在异构网络间进行切换时的安全认证效率，同时还能确保同一业务在更换终端或更换接入方式时连续的业务安全保护。

在 5G 应用场景中，有些终端设备能力强，可能配有 SIM（用户身份识别模块）/USIM（通用用户身份识别模块）卡，并具有一定的计算和存储能力，有些终端设备没有 SIM/USIM 卡，其身份标识可能是 IP 地址、MAC（介质访问控制）地址、数字证书等；而有些能力低的终端设备，甚至没有特定的硬件来安全存储身份标识及认证凭证，因此，5G 网络需要构建一个融合的统一的身份管理系统，并能支持不同的认证方式、不同的身份标识及认证凭证。

2.4 新的商业模式

5G 网络不仅要满足人们超高流量密度、超高连接数密度、超高移动性的需求，还要为垂直行业提供通信服务。在 5G 时代将会出现全新的网络模式与通信服务模式。同样地，终端和网络设备的概念也将会发生改变，各类新型终端设备的出现将会产生多种具有不同态势的安全需求，在大连接物联网场景中，大量的无人管理的机器与无线传感器

将会接入到 5G 网络之中，由成千上万个独立终端组成的诸多小的网络将会同时连接至 5G 网络中，在这种情况下，现有的移动通信系统的简单的可信模式（即一个用户及其通信终端和运营商）可能不能满足 5G 支撑的各类新兴的商业模式，需要对可信模式进行变革，以应对相关领域的扩展型需求。为了确保 5G 网络能够支撑各类新兴商业模式的需求，并确保足够的安全性，需要对安全架构进行全新的设计。

同时 5G 网络是能力开放的网络，可以向第三方或者垂直行业开放网络安全能力，如认证和授权能力，第三方或者垂直行业与运营商建立了信任关系，当用户允许接入 5G 网络时，也同时允许接入第三方业务。5G 网络的能力开放有利于构建以运营商为核心的开放业务生态，增强用户黏性，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。

2.5 更高的隐私保护需求

5G 网络中业务和场景的多样性，以及网络的开放性，使用户隐私信息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。例如在智能医疗系统中，病人病历、处方和治疗方案等隐私性信息在采集、存储和传输过程中存在被泄漏、篡改的风险，而在智能交通中，车辆的位置和行驶轨迹等隐私信息也存在暴露和被非法跟踪使用的风险，因此 5G 网络有了更高的用户隐私保护需求。

5G 网络是一个异构的网络，使用多种接入技术，各种接入技术对隐私信息的保护程度不同。同时，5G 网络中的用户数据可能会穿越各种接入网络及不同厂商提供的网络功能实体，从而导致用户隐私数据散布在网络的各个角落，而数据挖掘技术还能够让第三方从散布的隐私数据中分析出更多的用户隐私信息。因此，在 5G 网络中，必须全面考虑数据在各种接入技术以及不同运营网络中穿越时所面临的隐私暴露风险，并制定周全的隐私保护策略，包括用户的各种身份，位置，接入的服务等。

4G 网络已经暴露出泄露用户身份标识（如 IMSI（国际移动用户标识）暴露问题）的漏洞，因此在 5G 网络中需要对 4G 网络的机制进行优化和补充，通过加强的安全机制对用户身份标识进行隐私保护，杜绝出现泄露用户身份标识的情况，解决已有的 4G 网络的漏洞。另外，由于 5G 接入网络包括 LTE 接入网络，因此用户身份标识的保护需要兼容 LTE 的认证信令，防御攻击者引导用户至 LTE 接入方式，从而执行针对隐私性的降维攻

击。同时，攻击者也可能会利用 UE 位置信息或者空口数据包的连续性等特点进行 UE 追踪的攻击，因此 5G 隐私保护也需要应对此类位置隐私的安全威胁。

3 5G 安全总体目标

5G 时代，一方面，垂直行业与移动网络的深度融合，带来了多种应用场景，包括海量资源受限的物联网设备同时接入、无人值守的物联网终端、车联网与自动驾驶、云端机器人、多种接入技术并存等；另一方面，IT 技术与通信技术的深度融合，带来了网络架构的变革，使得网络能够灵活地支撑多种应用场景。5G 安全应保护多种应用场景下的通信安全以及 5G 网络架构的安全。

5G 网络的多种应用场景中涉及不同类型的终端设备、多种接入方式和接入凭证、多种时延要求、隐私保护要求等，所以 5G 网络安全应保证：

- 提供统一的认证框架，支持多种接入方式和接入凭证，从而保证所有终端设备安全地接入网络。
- 提供按需的安全保护，满足多种应用场景中的终端设备的生命周期要求、业务的时延要求。
- 提供隐私保护，满足用户隐私保护以及相关法规的要求。

5G 网络架构中的重要特征包括 NFV/SDN、切片以及能力开放，所以 5G 安全应保证：

- NFV/SDN 引入移动网络的安全，包括虚拟机相关的安全、软件安全、数据安全、SDN 控制器安全等。
- 切片的安全，包括切片安全隔离、切片的安全管理、UE 接入切片的安全、切片之间通信的安全等。
- 能力开放的安全，既能保证开放的网络能力安全地提供给第三方，也能够保证网络的安全能力（如加密、认证等）能够开放给第三方使用。

4 5G 网络安全架构

5G 网络安全架构的设计需满足上述新的安全需求和挑战，包括新业务、新技术新特

征、接入方式和设备形态等。5G 网络安全架构的设计原则包括，支持数据安全保护，体现统一认证框架和业务认证，满足能力开放，以及支持切片安全和应用安全保护机制。

5G 网络安全架构如图 1 所示。

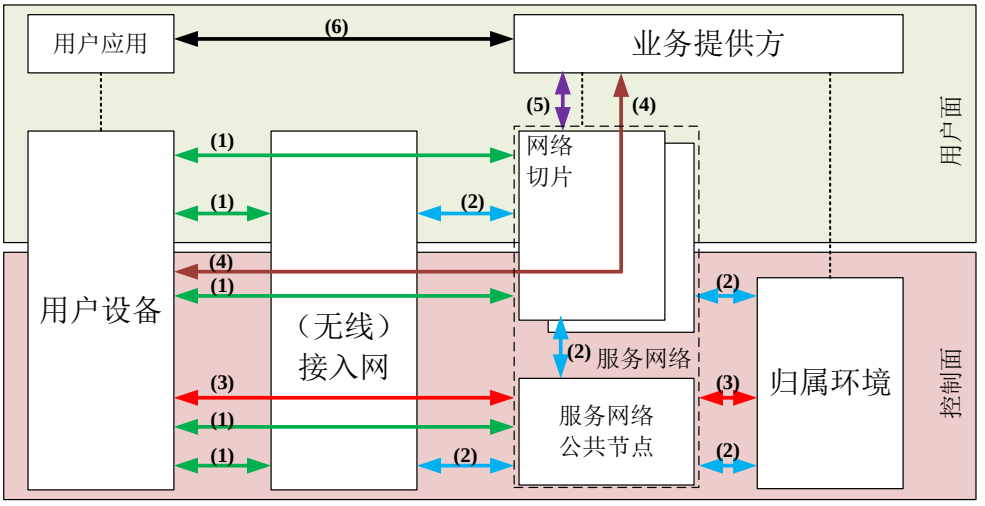

图 1　5G 网络安全架构示意图

根据 5G 安全设计原则，将 5G 网络安全架构分为以下八个安全域：

1）网络接入安全：保障用户接入网络的数据安全。

✧ 控制面：用户设备（UE）与网络之间信令的机密性和完整性安全保护，包括无线和核心网信令保护。其中核心网信令包括 UE 到服务网络公共节点的信令保护，以及根据切片安全需求部署的 UE 到网络切片（NS）内实体的信令保护。

✧ 用户面： UE 和网络之间用户数据的机密性和/或完整性安全保护，包括 UE 与（无线）接入网之间的空口数据保护，以及 UE 与核心网中用户安全终结点之间的数据保护。

2）网络域安全：保障网元之间信令和用户数据的安全交换，包括（无线）接入网与服务网络共同节点之间，服务网络共同节点与归属环境（HE）之间，服务网络共同节点与 NS 之间，HE 与 NS 之间的交互。

3）首次认证和密钥管理：包括认证和密钥管理的各种机制，体现统一的认证框架。具体为：UE 与 3GPP 网络之间基于运营商安全凭证的认证，以及认证成功后用户数据保护的密钥管理。根据不同场景中设备形式的不同，UE 中认证安全凭证可以存储在 UE 上

基于硬件的防篡改的安全环境中，如 UICC（通用集成电路卡）。

4）二次认证和密钥管理：UE 与外部数据网络（如，业务提供方）之间的业务认证以及相关密钥管理。体现部分业务接入 5G 网络时，5G 网络对于业务的授权。

5）安全能力开放：体现 5G 网元与外部业务提供方的安全能力开放，包括开放数字身份管理与认证能力。另外通过安全开放能力，也可以实现 5G 网络获取业务对于数据保护的安全需求，完成按需的用户面保护。

6）应用安全：此安全域保证用户和业务提供方之间的安全通信。

7）切片安全：体现切片的安全保护，例如 UE 接入切片的授权安全，切片隔离安全等。

8）安全可视化和可配置：体现用户可以感知安全特性是否被执行，这些安全特性是否可以保障业务的安全使用和提供。

5 5G 网络新的安全能力

5.1 统一的认证框架

5G 支持多种接入技术（如 4G 接入、WLAN 接入以及 5G 接入），由于目前不同的接入网络使用不同的接入认证技术，并且，为了更好地支持物联网设备接入 5G 网络，3GPP 还将允许垂直行业的设备和网络使用其特有的接入技术。为了使用户可以在不同接入网间实现无缝切换，5G 网络将采用一种统一的认证框架，实现灵活并且高效地支持各种应用场景下的双向身份鉴权，进而建立统一的密钥体系。

EAP（可扩展认证协议）认证框架是能满足 5G 统一认证需求的备选方案之一。它是一个能封装各种认证协议的统一框架，框架本身并不提供安全功能，认证期望取得的安全目标，由所封装的认证协议来实现，它支持多种认证协议，如 EAP-PSK（预共享密钥），EAP-TLS（传输层安全），EAP-AKA（鉴权和密钥协商）等。

在 3GPP 目前所定义的 5G 网络架构中，认证服务器功能/认证凭证库和处理功能（AUSF/ARPF）网元可完成传统 EAP 框架下的认证服务器功能，接入管理功能（AMF）网元可完成接入控制和移动性管理功能，5G 统一认证框架示意如图 2 所示：

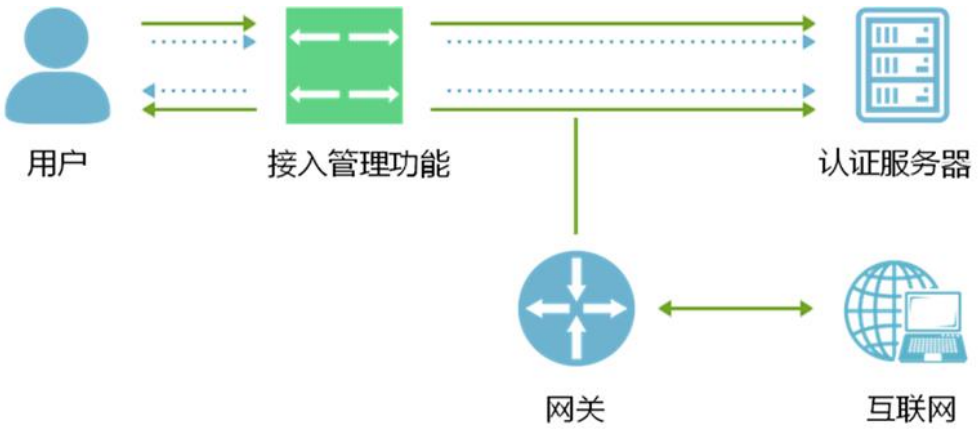

图 2　5G 统一认证框架示意

在 5G 统一认证框架里，各种接入方式均可在 EAP 框架下接入 5G 核心网：用户通过 WLAN 接入时可使用 EAP-AKA'认证，有线接入时可采用 IEEE 802.1x 认证，5G 新空口接入时可使用 EAP-AKA 认证。不同的接入网使用在逻辑功能上统一的 AMF 和 AUSF/ARPF 提供认证服务，基于此，用户在不同接入网间进行无缝切换成为可能。

5G 网络的安全架构明显有别于以前移动网络的安全架构。统一认证框架的引入不仅能降低运营商的投资和运营成本，也为将来 5G 网络提供新业务时对用户的认证打下坚实的基础。

5.2　多层次的切片安全

切片安全机制主要包含三个方面：UE 和切片间安全、切片内 NF（网络功能）与切片外 NF 间安全、切片内 NF 间安全。

切片安全机制如图 3 所示。

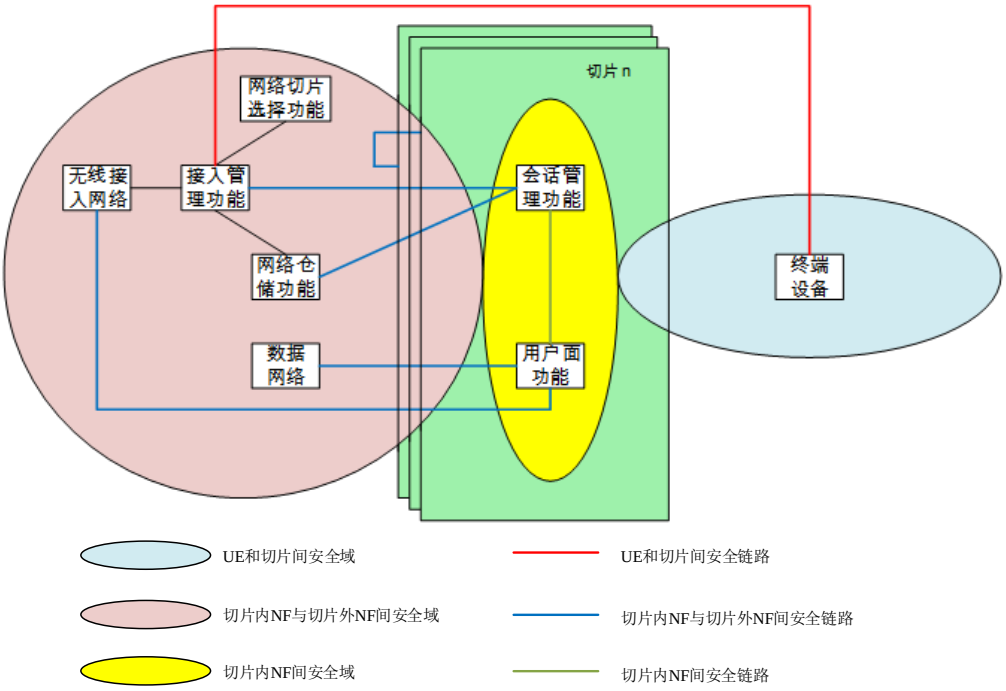

图 3　切片安全机制

5.2.1　UE 和切片间安全

UE 和切片间安全通过接入策略控制来应对访问类的风险，由 AMF 对 UE 进行鉴权，从而保证接入网络的 UE 是合法的。另外，可以通过 PDU（分组数据单元）会话机制来防止 UE 的未授权访问，具体方式是： AMF 通过 UE 的 NSSAI（网络切片选择辅助信息）为 UE 选择正确的切片，当 UE 访问不同切片内的业务时，会建立不同的 PDU 会话，不同的网络切片不能共享 PDU 会话，同时，建立 PDU 会话的信令流程可以增加鉴权和加密过程。UE 的每一个切片的 PDU 会话都可以根据切片策略采用不同的安全机制。

当外部数据网络需要对 UE 进行第三方认证时，可以由切片内的会话管理功能（SMF）作为 EAP 认证器，为 UE 进行第三方认证。

5.2.2 切片内 NF 与切片外 NF 间安全

由于安全风险等级不同，切片内 NF 与切片外 NF 间通信安全可以分为三种情况：

A、　切片内 NF 与切片公用 NF 间的安全

公用 NF 可以访问多个切片内的 NF，因此切片内的 NF 需要安全的机制控制来自公

用 NF 的访问，防止公用 NF 非法访问某个切片内的 NF，以及防止非法的外部 NF 访问某个切片内的 NF。

网管平台通过白名单机制对各个 NF 进行授权，包括每个 NF 可以被哪些 NF 访问，每个 NF 可以访问哪些 NF。

切片内的 SMF 需要向网络仓储功能（NRF）注册，当 AMF 为 UE 选择切片时，询问 NRF，发现各个切片的 SMF，在 AMF 和 SMF 通信前，可以先进行相互认证，实现切片内 NF（如 SMF）与切片外公共 NF（如 AMF）之间的相互可信。

同时，可以在 AMF 或 NRF 做频率监控或者部署防火墙防止 Dos/DDos 攻击，防止恶意用户将切片公有 NF 的资源耗尽，而影响切片的正常运作。比如，在 AMF 做防御，进行频率监控，当检测到同一 UE 向同一 NRF 发消息的频率过高，则将强制该 UE 下线，并限制其再次上线，进行接入控制，防止 UE 的 Dos 攻击；或者在 NRF 做频率监控，当发现大量 UE 同时上线，向同一 NRF 发送消息的频率过高，则将强制这些 UE 下线，并限制其再次上线，进行接入控制，防止大范围的 DDos 攻击。

B、切片内 NF 与外网设备间安全

在切片内 NF 与外网设备间，部署虚拟防火墙或物理防火墙，保护切片内网与外网的安全。如果在切片内部署防火墙则可以使用虚拟防火墙，不同的切片按需编排；如果在切片外部署防火墙则可以使用物理防火墙，一个防火墙可以保障多个切片的安全。

C、不同切片间 NF 的隔离

不同的切片要尽可能保证隔离，各个切片内的 NF 之间也需要进行安全隔离，比如，部署时可以通过 VLAN（虚拟局域网）/VxLAN（虚拟扩展局域网）划分切片，基于 NFV 的隔离来实现切片的物理隔离和控制，保证每个切片都能获得相对独立的物理资源，保证一个切片异常后不会影响到其他切片。

5.2.3 切片内 NF 间安全

切片内的 NF 之间通信前，可以先进行认证，保证对方 NF 是可信 NF，然后可以通过建立安全隧道保证通讯安全，如 IPSec。

5.3 差异化安全保护

不同的业务会有不同的安全需求，例如，远程医疗需要高可靠性安全保护，而部分物

联网业务需要轻量级的安全解决方案（算法或安全协议）来进行安全保护。5G 网络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可以满足这样的多样性需求。同样的，5G 安全设计也需支持业务多样性的差异化安全需求，即用户面的按需保护需求。

用户面的按需保护本质上是根据不同的业务对于安全保护的不同需求，部署不同的用户面保护机制。按需的保护主要有以下两类策略：

1）用户面数据保护的终结点。终结点可以为（无线）接入网或者核心网，即 UE 到（无线）接入网之间的用户面数据保护，或者 UE 至核心网的用户面数据保护。

2）业务数据的加密和/或完整性保护方式。如，不同的安全保护算法、密钥长度、密钥更新周期等。

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。

基于业务的差异化用户面安全保护机制如图 4 所示。

图 4　基于业务的差异化用户面安全保护机制示例

图 4 中，根据应用与服务侧的业务安全需求，确定相应切片的安全保护机制，并部署相关切片的用户面安全防护。例如考虑 mMTC 中设备的轻量级特征，此切片内数据可以根据 mMTC 业务需求部署轻量级的用户面安全保护机制。另外，切片内还包含 UE 至核心网的会话传输模式，因此基于不同的会话做用户面数据保护，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，5G 网络也可以对不

同的会话数据传输进行差异化的安全保护。

5.4 开放的安全能力

5G 网络安全能力可以通过 API 接口开放给第三方业务（如业务提供商、企业、垂直行业等），让第三方业务能便捷地使用移动网络的安全能力，从而让第三方业务提供商有更多的时间和精力专注于具体应用业务逻辑的开发，进而快速、灵活地部署各种新业务，以满足用户不断变化的需求；同时运营商通过 API 接口开放 5G 网络安全能力，让运营商的网络安全能力深入地渗透到第三方业务生态环境中，进而增强用户黏性，拓展运营商的业务收入来源。

开放的 5G 网络安全能力主要包括（但不限于）：基于网络接入认证向第三方提供业务层的访问认证，即如果业务层与网络层互信时用户在通过网络接入认证后可以直接访问第三方业务，简化用户访问业务认证的同时也提高了业务访问效率；基于终端智能卡（如 UICC/eUICC/ iUICC）的安全能力，拓展业务层的认证维度，增强业务认证的安全性。

5.5 灵活多样的安全凭证管理

由于 5G 网络需要支持多种接入技术（如 WLAN、LTE、固定网络、5G 新无线接入技术），以及支持多样的终端设备，如部分设备能力强，支持(U)SIM 卡安全机制；部分设备能力较弱，仅支持轻量级的安全功能，于是，存在多种安全凭证，如对称安全凭证和非对称安全凭证。因此，5G 网络安全需要支持多种安全凭证的管理，包括对称安全凭证管理和非对称安全凭证管理。

- 对称安全凭证管理

对称安全凭证管理机制，便于运营商对于用户的集中化管理。如，基于(U)SIM 卡的数字身份管理，是一种典型的对称安全凭证管理，其认证机制已得到业务提供者和用户广泛的信赖。

- 非对称安全凭证管理

采用非对称安全凭证管理可以实现物联网场景下的身份管理和接入认证，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。

面向物联网成百上千亿的连接，基于(U)SIM 卡的单用户认证方案成本高昂，为了降低物联网设备在认证和身份管理方面的成本，可采用非对称安全凭证管理机制。

非对称安全凭证管理主要包括以下两类分支：

证书机制和基于身份安全 IBC（基于身份密码学）机制。其中证书机制是应用较为成熟的非对称安全凭证管理机制，已广泛应用于金融和 CA（证书中心）等业务，不过证书复杂度较高；而基于 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。

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。

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。去中心化部署方式示意如图 5 所示。

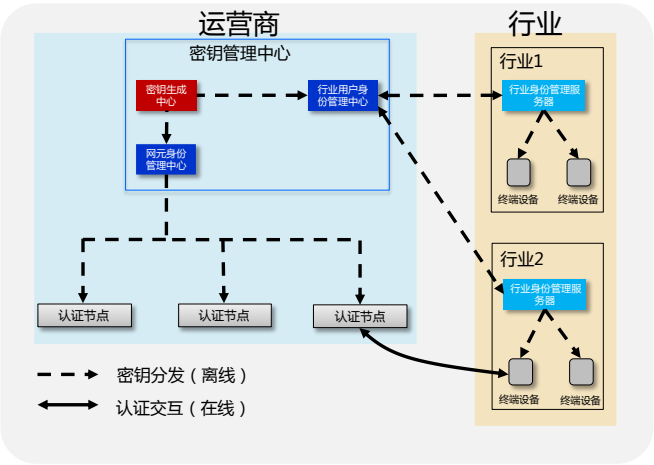

图 5　去中心化安全管理部署示意图

5.6　按需的用户隐私保护

5G 网络涉及多种网络接入类型并兼容垂直行业应用，用户隐私信息在多种网络、服务、应用及网络设备中存储使用，因此，5G 网络需要支持安全、灵活、按需的隐私保护机制。

- 隐私保护类型

5G 网络对用户隐私的保护可以分为以下几类：

✧ 身份标识保护

用户身份是用户隐私的重要组成部分，5G 网络使用加密技术、匿名化技术等为临时身份标识、永久身份标识、设备身份标识、网络切片标识等身份标识提供保护。

✧ 位置信息保护

5G 网络中海量的用户设备及其应用，产生大量用户位置相关的信息，如定位信息、轨迹信息等，5G 网络使用加密等技术提供对位置信息的保护，并可防止通过位置信息分析和预测用户轨迹。

✧ 服务信息保护

相比 4G 网络，5G 网络中的服务将更加多样化，用户对使用服务产生的信息保护需求增强，用户服务信息主要包括用户使用的服务类型、服务内容等，5G 网络使用机密性、完整性保护等技术对服务信息提供保护。

- 隐私保护能力

在服务和网络应用中，不同的用户隐私类型保护需求不尽相同，存在差异性，因此需要网络提供灵活、按需的隐私保护能力。

✧ 提供差异化隐私保护能力

5G 网络能够针对不同的应用、不同的服务，灵活设定隐私保护范围和保护强度（如提供机密性保护、提供机密性和完整性保护等），提供差异化隐私保护能力。

✧ 提供用户偏好保护能力

5G 网络能够根据用户需求，为用户提供设置隐私保护偏好的能力，同时具备隐私保护的可配置、可视化能力。

✧ 提供用户行为保护能力

5G 网络中业务和场景的多样性，以及网络的开放性，使得用户隐私信息可能从封闭的平台转移到开放的平台上，因此需要对用户行为相关的数据分析提供保护，防止从公开信息中挖掘和分析出用户隐私信息。

- 隐私保护技术

5G 网络可提供多样化的技术手段对用户隐私进行保护，使用基于密码学的机密性保护、完整性保护、 匿名化技术等对用户身份进行保护，使用基于密码学的机密性保护、完整性保护对位置信息、服务信息进行保护。

为提供差异化隐私保护能力，网络通过安全策略可配置和可视化技术，以及可配置的隐私保护偏好技术，实现对隐私信息保护范围和保护强度的灵活选择；采用大数据分析相关的保护技术，实现对用户行为相关数据的安全保护。

6 5G 安全标准化建议

6.1 总体目标

IMT-2020(5G)推进组全力支持在 ITU 和 3GPP 框架下研制全球统一的 5G 安全技术标准，积极采用创新技术满足 5G 网络安全需求，推动 5G 安全统一认证架构、按需的安全保护、切片安全以及 256 比特密钥长度密码算法等技术的国际国内相关标准化工作。

未来将分如下两阶段积极推动 3GPP 开展 5G 安全标准化工作：

第一阶段，在 2018 年 3 月之前，完成安全框架、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）的互通等相关研究工作；

第二阶段，在 2019 年 12 月之前，重点推进切片安全、能力开放安全、256 比特密钥长度密码算法等相关工作。

6.2 重点工作

IMT-2020(5G)推进组 5G 安全方面接下来的重点工作包括两方面：

1）5G 网络安全架构设计

设计灵活可扩展的安全架构，分析安全机制和协议，研究切片安全、安全能力开放、安全凭证管理及按需的用户隐私保护等的具体技术实现方法。

2）256 比特密钥长度对称密码算法的国际标准化

目前 3GPP SA3 已经启动在 5G 网络中采用 128 比特密钥长度和 256 比特密钥长度对称密码算法的讨论，推进组将尽快推动 ZUC-256（密钥长度为 256 比特）等密码算法的

评估相关工作，积极推动 ZUC-256 等密码算法成为国际标准。

6.3 其他标准化组织相关工作

目前 3GPP SA3 已经在开展 5G 安全相关标准化工作，包括研究项目（如，下一代系统安全技术研究）和标准项目（如，5G 系统安全架构和流程），计划在 2018 年 3 月完成 REL-15 的标准化工作。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。

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（管理和编排）安全、证书管理、安全管理、安全部署等方面；ONF（开放网络基金会）以及 ITU-T 的研究内容涉及 SDN 安全的标准化工作。

7 总结和展望

面向未来更加多样化的业务场景、多种接入方式、多种设备形态、新的商业模式、更高的隐私保护需求以及新型网络架构的安全需求，5G 网络安全架构将支持数据安全保护，统一的认证框架和业务认证，多层次的切片安全、差异化安全保护、开放的安全能力、多种安全凭证管理以及按需的用户隐私保护等。尽早明确 5G 网络安全需求和架构，在 5G 网络的整体架构设计、业务流程、算法和后续标准化工作中综合考虑 5G 安全要求，有助于最终实现构建更加安全可信的 5G 新型网络的目标。

随着 5G 网络安全标准化工作的全面展开和研究的不断深入，IMT-2020(5G)推进组愿意与全球 5G 相关组织、企业、科研机构和高校加强合作，共同推动 5G 网络安全需求与架构相关研究，促进 5G 安全标准以及产业的蓬勃发展。

主要贡献单位

CAICT 中国信息通信研究院 China Academy of Information and Communications Technology

中国移动 China Mobile

China unicom 中国联通 创新·改变世界

中国电信 CHINA TELECOM 世界触手可及

HUAWEI

大唐电信 大唐电信科技产业集团 DATANG TELECOM TECHNOLOGY & INDUSTRY GROUP

NOKIA 上海贝尔

ZTE 中兴

信威通信

INFORMATION ENGINEERING UNIVERSITY 信息工程大学

联系方式
电话：+86-10-62300182
邮箱：imt2020@catr.cn
版权所有©IMT-202(5G)推进组