# 5G网络的认证体系

# Authentication Framework of 5G Network

齐旻鹏/QI Minpeng，彭晋/PENG Jin

（中国移动通信研究院，北京 100053）
(China Mobile Research Institute, Beijing 100053, China)

**摘要**：接入认证是保障网络安全的基础。随着网络变得越来越复杂，认证机制逐步地将不同的参数分发、密钥产生、网络和接入场景等各方面纳入统一考虑，最终在5G中呈现出统一的认证框架。这使得5G网络可以为各种不同类型的终端提供安全的认证机制和流程。

**关键词**：5G；安全；认证

**Abstract**: Access authentication is the basis of network security. While network grows more and more complex, consideration for authentication is also wider to involve different aspects like parameter distribution, key generation, network type and access scenarios. As a result, a unified authentication framework is proposed for 5G, which enables the 5G network to provide secure authentication mechanisms and process networks for different types of terminals.

**Key words**: 5G; security; authentication

DOI：10.12142/ZTETJ.201904003
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.tn.20190709.1528.002.html

网络出版日期：2019-07-09
收稿日期：2019-05-20

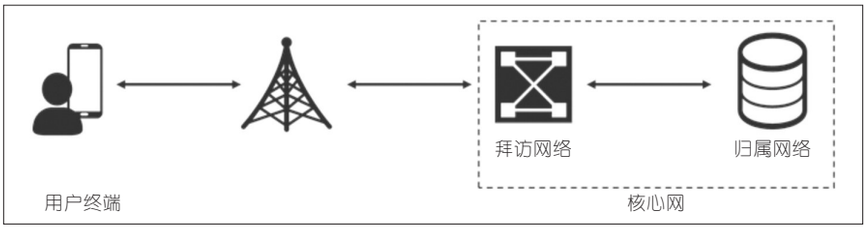
## 1 概述

移动通信网络作为国家重要基础设施，承载着网络通信任务，为用户提供语音、网络浏览，乃至多媒体业务等多种服务，已经深刻地融入至人们日常的生产生活过程中。随着5G的到来，移动通信网络不仅影响个人生活的方方面面，同时也进一步地对社会生活产生重大影响。同时，移动通信网络也成为攻击者的目标。攻击者会针对用户和网络发起假冒、伪造、篡改、重放等主动攻击，也会通过窃听、跟踪等方式发起被动攻击。因此，为了保证移动通信网的安全和运营商、用户的权益，鉴权认证机制成为保护移动通信网的第一道防线[1]。

移动通信网通常由3部分组成，即核心网（CN）、无线接入网（RAN）和用户设备（UE）。其中，移动用户设备通常属于用户个人[1]，由用户直接控制；而接入网与核心网属于运营商，由运营商直接控制。考虑到用户漫游的需求，运营商被进一步分为保存用户信息的归属网络运营商，以及直接为用户提供接入服务的拜访网络运营商，具体如图1所示。

当用户尝试接入网络时，用户与网络需要确认真实身份，以避免攻击者冒充真实用户或者提供虚假网络服务，造成非法网络接入或者骗取用户的个人信息。因此，用户接入网络时首先需要进行认证。

移动通信网络的认证采用经典的“挑战-响应”机制进行，即用户与网络之间共享一个秘密信息，然后网络侧根据该信息产生一个挑战信息并发送给用户，用户根据挑战基于同样的秘密信息产生一个响应发回网络，网络再判断响应是否符




▲图1 用户与网络的连接示意图

合要求，从而判定用户是否为合法用户。该认证的流程如图2所示。

## 2 移动通信网络中的认证技术演进

移动通信网络从2G的全球移动通信系统（GSM）时代引入认证技术，发展到今天的第5G，经历了一系列的技术进步和换代。

### 2.1 2G认证

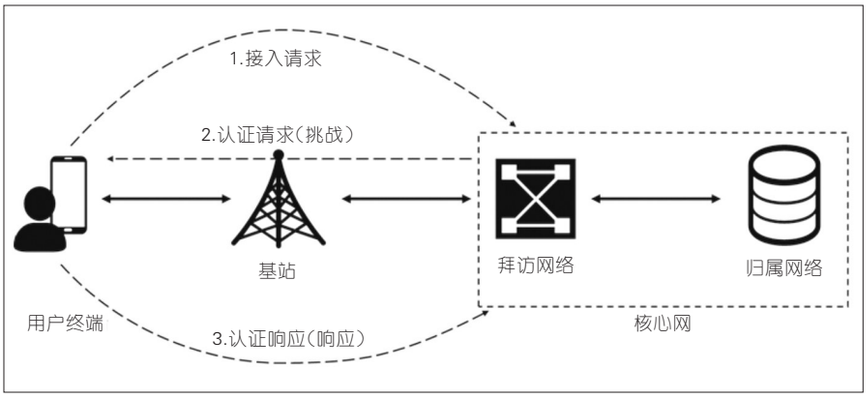
在GSM时代，人们对安全的期望是能够跟有线电话一样安全。GSM在设计时，仅考虑对用户身份的识别，防止非法的用户接入，而未考虑用户对网络的身份校验。因此，GSM中的认证，只是一种单向的认证方式。出于对移动性的考虑，GSM的认证被设计成由直接为用户提供接入服务、拜访地运营商的拜访位置寄存器（VLR），对用户进行相关的认证；而负责维护用户签约信息、归属地的归属位置寄存器（HLR）只负责提供用户认证的安全参数。GSM认证如图3所示。

随着技术的发展，分组传送方式也被引入至移动通信网络中，形成通用分组无线服务技术（GPRS）网络，并引入了数据服务节点（SGSN）。SGSN既然负责对用户进行移动性管理，也就负责对终端的接入认证。用户认证信息同样来自于负责维护用户数据签约信息的归属地HLR；因此，为了便于在GPRS中对用户进行管理，由拜访地SGSN为用户进行认证，由归属地HLR提供认证参数，从而实现了GSM/GPRS在认证参数分发上的统一。GSM/GPRS的技术的认证，具体如图4所示。

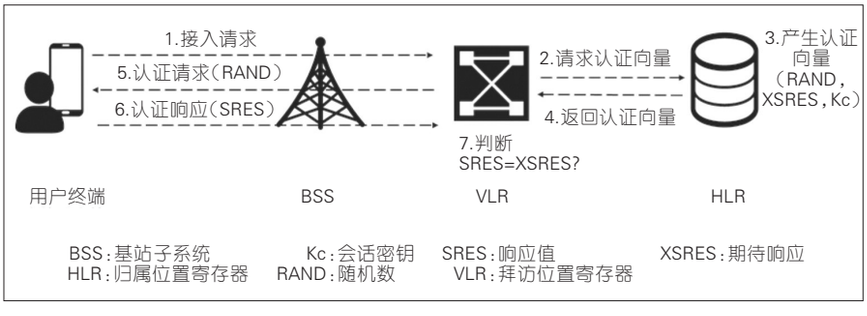
### 2.2 3G认证

到了3G时代，人们意识到在GSM/GPRS认证过程中可能存在伪装网络和重放等风险，如攻击者通过伪装网络的方式，诱骗用户接入虚假网络，进而可以通过构造虚假号码向用户推送垃圾信息甚至诈骗信息，使得用户遭受侵害。因此，3G引入双向认证机制，增加了用户对网络的认证能力，如图5所示[2]。

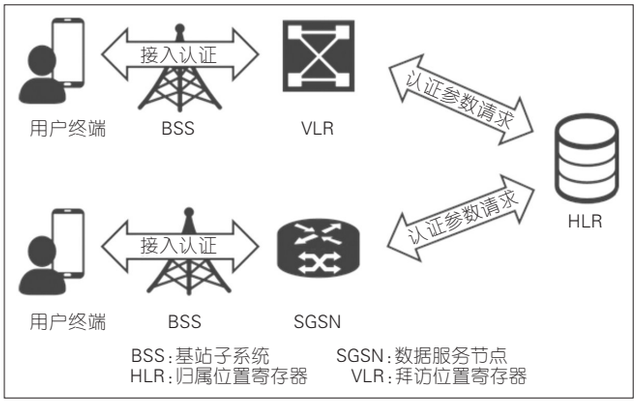
更为重要的是，GSM/GPRS认证所对应的响应值（RES）和会话密钥Kc之间是相互独立的。当时仅是为了方便计算和传送，便在推荐实施方案中将相关参数同时产生并由HLR一并传递给VLR。但从3G认证开始，认证机制在设计时就将认证与后续通信所需要使用的会话密钥绑定在了一起，认证参数的产生与会话密钥的产生过程不可分割。这就使得攻击者无法通过分割



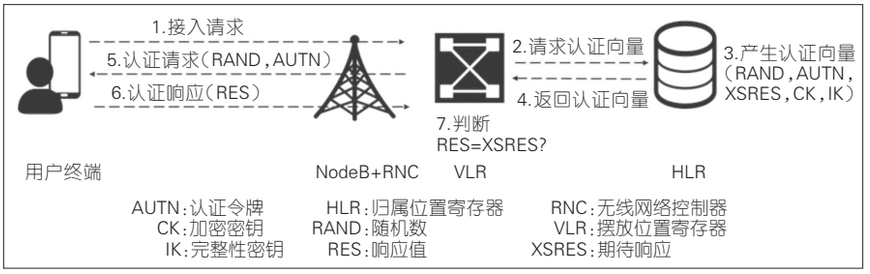

▲图2 认证示意图




▲图3 全球移动通信系统认证




◀图4
全球移动通信系统/分组无线服务技术认证




▲图5 3G认证

认证参数和会话密钥参数的方式实现对用户或网络身份的替代。所以，3G认证机制被叫做认证与密钥协商机制（AKA），该机制实现了认证参数与会话密钥参数之间的统一考虑。认证与密钥的产生具体如图6所示[2]。

### 2.3 4G认证

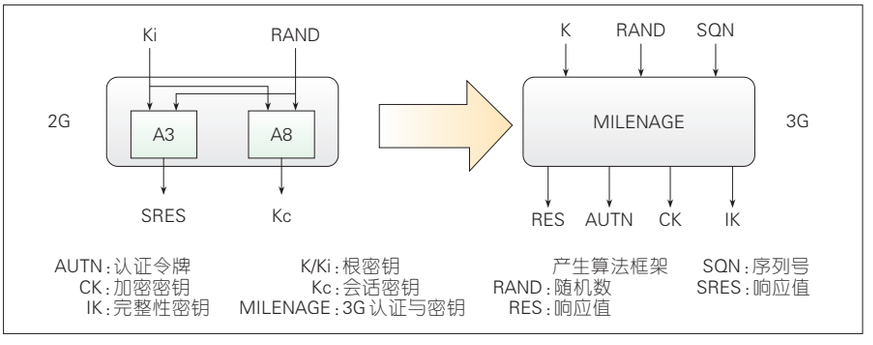
到了4G时代，认证机制又得到了进一步扩展。一方面，2G/3G时代的认证参数由归属网络产生，所以用户认证的实际上是归属网络。但与用户直接进行双向认证的是拜访网络的网元，这就导致用户无法对拜访网络进行认证，而只能间接地依赖于归属网络对拜访网络的完全信任对拜访网络进行认证。例如，中国用户漫游至其他国家时，认证参数仍由中国运营商提供，用户认证的仍是中国运营商网络；但此时双向认证发生在中国用户和其他国家的网络运营商之间，中国用户无法认证接入的其他国家网络的身份。这种做法在4G时得到了一定程度的纠正。在4G的认证过程中，拜访网络需要将其网络标识（ID）发送给归属网络，归属网络在产生认证所需参数时将拜访网络的ID作为生成参数之一引入，从而使得用户也可以在认证时对拜访网络的身份进行验证。

另一方面，随着蜂窝接入和无线局域网（WLAN）技术的长期并行，4G开始考虑用户通过WLAN等非蜂窝方式接入4G核心网的场景。对应地，在认证方面，4G也设计了面向非蜂窝接入的认证体系，第一次引入了基于EAP的认证框架，具体如图7所示。

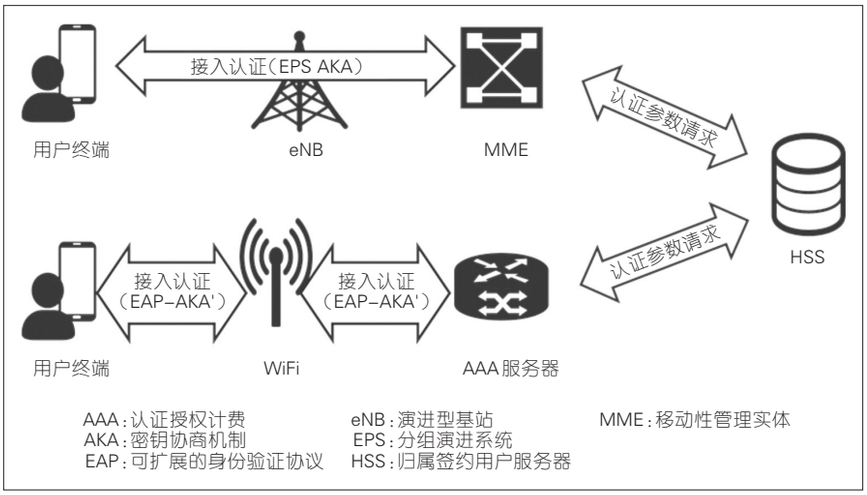
## 3 5G网络中的认证机制

随着通信网络技术的发展，第5代移动通信网络被提上日程。5G通信网络的设计目标面向3大场景：增强型移动宽带（eMBB）、高可靠低时延（uRLLC）以及海量机器类通信（mMTC）。因此，5G通信不仅考虑人与人之间的通信，还将考虑人与物、物与物之间的通信，进入万物互联的状态。

这种情况下，5G认证面临着新的安全需求。一方面，为了适应多种类型的通信终端，并使得它们能够接入通信网络，5G系统将进一步地扩展非蜂窝技术的接入场景。例如，电表、水表、摄像头等物联网设备通常采用蓝牙、WLAN等技术与网络相连，这类设备采用5G系统通信时仍倾向于使用原有的连接方




▲图6 认证与密钥产生




▲图7 4G不同接入方式下的认证统一

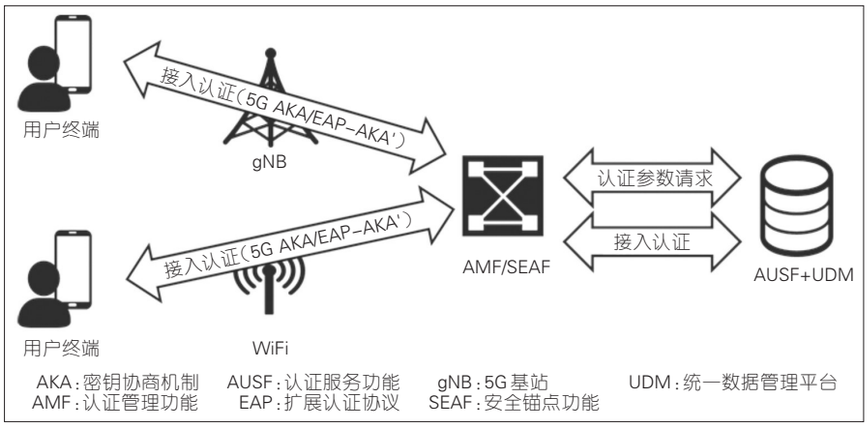
式。这就导致传统面向蜂窝接入的认证机制需要进一步地向非蜂窝接入的方式扩展。另一方面，传统认证机制下，拜访地/归属地的两级移动网络架构下的认证机制要求归属网络无条件信任拜访网络的认证结果。但随着网络的发展，出现了越来越多的安全隐患，拜访网络和归属网络之间的信任程度在不断降低。例如，拜访地运营商可以声称为某运营商的用户提供了接入服务而实际未提供，导致计费纠纷。对于5G的通信来说，相比于人与人之间的语音通信和数据交互，万物互联下的移动通信将会承载更多的设备测控类信息，因此对接入安全的要求更高。例如，当5G系统被垂直行业用于传递远程操控的控制消息。这使得5G认证还需要加强归属网络对用户终端的认证能力，使其摆脱对拜访网络的依赖，实现用户在归属地和拜访地等不同地点间的认证机制统一。5G还引入了对用户身份的进一步增强保护，使得用户的永久身份不在空中接口上进行传输，拜访网络还需要从归属网络获得用户的身份信息。这就导致拜访网络和用户终端之间无法直接对身份信息进行确认。因此，为了简化设计，5G认证过程中对用户的认证信息也需要进行确认。

基于上述需求，5G提供了2种认证框架，分别被称为5G-AKA和EAP-AKA′，如图8所示。

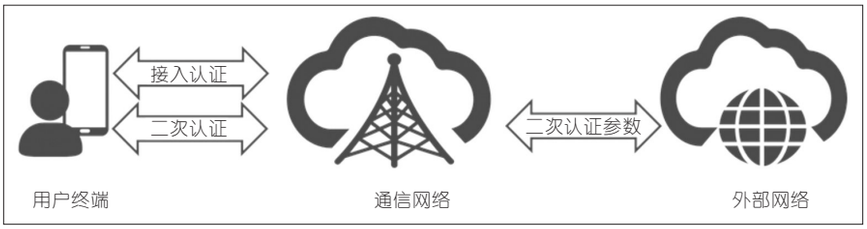
此外，5G网络将更多地为垂直行业提供服务，而垂直行业对5G网络提出了更多的需求。例如，需要通过5G新增的网络切片特性来为垂直行业提供定制化的服务，包括为特定的业务提供数据通道建立前的认证机制[3]。因此，5G系统引入了二次认证的概念，即在用户接入网络时所做认证之后为接入特定业务建立数据通道而进行的认证。在该认证过程中，第一次使用了非运营商控制的信任状要求。例如，当5G网络用于为高保障业务系统提供通信时，用户通过接入认证后并不能直接与业务系统建立连接，而是利用业务相关的信任状与用户终端进行认证，并在认证通过的情况下才允许5G网络为用户建立与业务系统间的通信链路，从而提升对业务系统的保护，具体如图9所示。

## 4 结束语

随着移动通信技术的不断发展，移动通信系统对于人们的生产生活影响越来越大，所需要面对的需求也越来越多，故而网络变得越来越复杂，这使得对应的认证机制也需要考虑越来越多的因素和场景。在认证机制的演进过程中，逐步实现了对认证参数分发形式的统一、对认证参数和密钥参数产生的统一、对拜访网络和归属网络的统




▲图8 5G的认证示意图




▲图 9 二次认证的示意图

一、对不同接入场景的统一，以及对认证框架的统一。正是有了这些不同角度和层面的统一，使得 5G 网络可以为各种不同类型的终端提供安全的认证机制和流程，并为后续安全保护打下了坚实的基础。

但同时我们也要看到，5G 的认证仍然面临着诸多挑战，例如学术界通过形式化分析方法对 5G 认证机制进行评估[4-5]，发现了一些潜在的风险点并促使网络协议改进。在通信网络的演进过程中，考虑网络的后向兼容性，无线通信系统始终坚持以对称密钥作为认证的基础，并因此衍生出一系列的安全参数。因此，基于对称密钥的信任状是整个网络认证和后续安全保障的基础。但对于 5G 及后续的网络，需要考虑更多的应用场景，并需要与垂直行业做更深入的结合。这些条件下，可能产生新形态的信任状需求。因此，如何做到不同形态的信任状的统一，将会是后续认证演进的考虑方向。此外，对于轻量级的物联网应用，如何充分发挥无线通信网络已有的安全优势，实现通信网络和业务之间认证的统一，降低物联网终端的能耗，提升安全保障效率，也是目前 5G 标准正在研究制定的内容之一。

**参考文献**
[1] 胡鑫鑫,刘彩霞,刘树新,等. 移动通信网鉴权认证综述[J]. 网络与信息安全学报, 2018, 4(12): 1–15
[2] 3GPP. 3G Security; Security Architecture: 3GPP TS33.102[S]. 2013
[3] 栗栗,彭晋,齐晏鹏,等.移动通信网中的密码算法演进之三——认证篇[EB/OL].[2019–05–20]. https://mp.weixin.qq.com/s/SoA1bY4AZtbGbUKmU_X17Q
[4] BASIN D, DREIER J, HIRSCHI L, et al. A Formal Analysis of 5G Authentication[J].2018, (2):22–25.DOI:10.1145/3243734.3243846
[5] BASIN D, DREIER, HIRSCHI J, RADOMIROVIC L, S, et al. A Formal Analysis of 5G Authentication[C] //25th ACM Conference on Computer and Communications Security. USA: ACM, 2018: 1383–1396. DOI: 10.1145/3243734.3243846

**作 者 简 介**

**齐晏鹏**，中国移动通信研究院安全所项目经理、中国移动 3GPP 安全与隐私小组代表等；长期从事 LTE、5G 等基础网络通信安全研究，并参与物联网、车联网等系统安全设计工作，目前主要负责 5G 系统安全架构与协议研究；申请并获得授权专利 10 余项，发表 10 余篇论文。

**彭晋**，中国移动通信研究院安全所所长，曾担任 ITU–T SG13 报告人、3GPP SA1 UDC 子组主席等；研究方向为电信核心网、电信网安全、云计算安全、大数据安全等；曾负责多项国家科研项目，并参与 ITU–T、3GPP、GSMA 等国际标准工作。

⬅上接第 5 页

发展，实现 5G 技术发展与技术安全相统一。

**参考文献**
[1] 3GPP. Security architecture and Procedures for 5G System (Release 15): 3GPP TS 33.501 [S]. 2019
[2] 3GPP. 3GPP System Architecture Evolution (SAE); Security Architecture: 3GPP TS 33.401 [S]. 2012
[3] 3GPP. Catalogue of General Security Assurance Requirements: 3GPP TS 33.117[S]. 2017
[4] 3GPP. 5G Security Assurance Specification (SCAS); NR Node B (gNB): 3GPP TS 33.511[S]. 2019
[5] 3GPP. 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF): 3GPP TS 33.512[S]. 2018
[6] 3GPP. 5G Security Assurance Specification (SCAS); User Plane Function (UPF): 3GPP TS 33.513[S]. 2018
[7] 3GPP. 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) Network Product Class: 3GPP TS 33.514[S]. 2018
[8] 3GPP. 5G Security Assurance Specification (SCAS); Session Management Function (SMF): 3GPP TS 33.515[S]. 2018
[9] 3GPP. 5G Security Assurance Specification (SCAS); Authentication Server Function (AUSF): 3GPP TS 33.516[S]. 2017
[10] 3GPP. 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) Network Product Class: 3GPP TS 33.517[S]. 2018
[11] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class: 3GPP TS 33.518 [S]. 2018
[12] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) Network Product Class: 3GPP TS 33.519[S]. 2018

**作 者 简 介**

**杨红梅**，中国信息通信研究院主任工程师、CCSA TC5 WG12 副组长；主要研究领域为移动通信 3G、4G、5G 核心网及安全；负责并完成 4 项国家重大专项课题，牵头制定了移动通信核心网和安全领域多项行业标准，多次获得 CCSA 科学技术奖；发表文章 30 余篇，主编专著《演进分组系统（EPS）业务应用技术》。

**赵勇**，中国电信股份有限公司北京分公司高级工程师；研究领域为移动通信核心网及业务；牵头负责并完成了多个业务平台的云化工作；发表文章 10 余篇。