5G网络安全认证体系研究

Research on 5G Network Security Certification System

谢泽铖，徐　雷，张曼君，郭新海，苏俐竹（中国联通研究院，北京 100048）
Xie Zecheng，Xu Lei，Zhang Manjun，Guo Xinhai，Su Lizhu（China Unicom Research Institute，Beijing 100048，China）

摘　要：
针对5G网络“一网赋能万业”的开放性特点以及多终端、多行业的接入趋势，5G网络安全认证体系在以运营商USIM卡为基础的主认证上，增加了垂直行业客户可控的二次认证和切片认证，丰富和拓展了5G网络的安全认证体系。在运营商安全认证的基础上，最大程度满足垂直行业客户的不同安全需求。详细介绍了5G网络的安全认证体系，涵盖主认证、二次认证和切片认证。

关键词：
5G网络；主认证；二次认证；切片认证
doi：10.12045/j.issn.1007-3043.2022.09.008
文章编号：1007-3043（2022）09-0032-07
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In view of the open characteristics of 5G network "one network enables all industries" and the access trend of multi terminals and multi industries，the 5G network security certification system has added secondary authentication and slice authentication controlled by vertical industry customers except to the primary authentication based on USIM card，which enriches and expands the security certification system of 5G network. It can meet the different security needs of vertical industry customers to the greatest extent on the basis of security certification of operators. The security authentication system of 5G network is introduced in detail，including the primary certification，secondary certification and slice certification.

Keywords：
5G network；Primary certification；Secondary certification；Slice certification

引用格式：谢泽铖，徐雷，张曼君，等. 5G网络安全认证体系研究[J]. 邮电设计技术，2022（9）：32-38.

1 概述

5G网络作为下一代移动通信技术的发展方向，是新一轮科技革命和产业变革的载体，将助力传统产业的转型升级。5G网络不再局限于人与人之间的通信，还考虑了人与物、物与物之间的通信，进入万物互联的状态，进一步扩展了在不同场景下向垂直行业提供服务的能力。考虑到5G网络“一网赋能万业”的开放性特点以及多终端、多行业的接入趋势，5G网络安全认证体系在以运营商USIM卡为基础的主认证上，增加了垂直行业客户可控的二次认证和切片认证，丰富和拓展了5G网络的安全认证体系。在运营商安全认证的基础上，最大程度满足垂直行业客户的不同安全需求。本文将对5G网络的安全认证体系做详细的介绍，涵盖主认证、二次认证和切片认证。

图1给出了5G网络的安全认证体系示意。UE入网时向核心网发起注册请求，由5G主认证控制5G用户终端是否可接入运营商5G网络，由核心网网元

收稿日期：2022-07-28

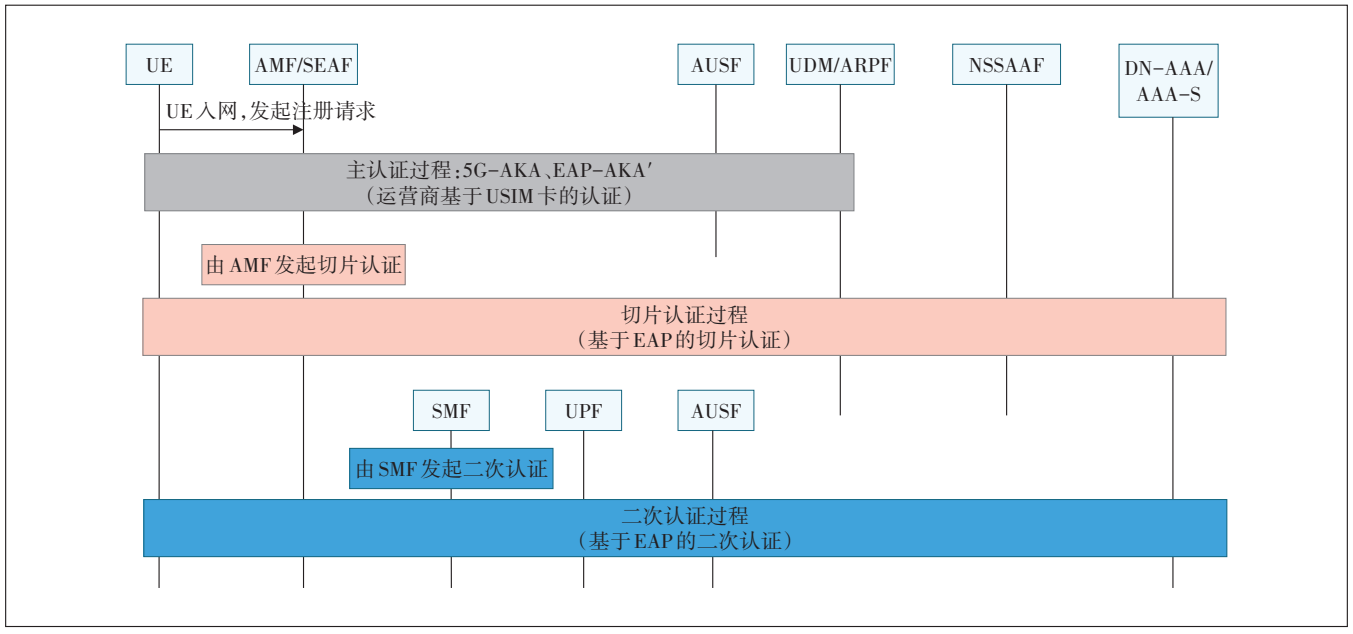

图1　5G网络中的安全认证

AMF、AUSF、UDM共同完成5G用户终端与5G网络之间的双向鉴权认证；切片认证用来控制用户终端能否接入垂直行业切片，由AMF对用户终端发起切片接入认证流程，确保接入切片的用户终端合法；二次认证用来控制用户终端是否可接入垂直行业的企业网络，在用户发起PDU会话建立请求时，由SMF触发二次认证，由垂直行业客户侧的DN-AAA对UE进行认证授权。

2 主认证

2.1 主认证应用场景

在移动通信网络从2G到5G的发展过程中，主认证的流程也在不断完善。主认证主要应用场景是验证用户身份的合法性，避免非法用户接入移动网络或者避免攻击者通过伪基站向用户提供虚假网络服务，因此主认证是用户接入移动网络必不可少的一环。

移动网络中一般采用基于“挑战-响应”的AKA（Authentication and Key Agreement）认证协议。用户接入网络需要通过长期密钥K实现UE和网络之间的相互认证，并推导出会话密钥，密钥分别存放在运营商网络的核心网和用户的SIM（2G）/USIM（3G、4G、5G）卡中，后续通信时需要使用的其他密钥基于长期密钥通过不可逆的函数衍生。5G网络的主认证包括5G-AKA和EAP-AKA′ 2种方式，涉及的网元如图2所示，包括AMF/SEAF、AUSF、UDM/ARPF等网元。

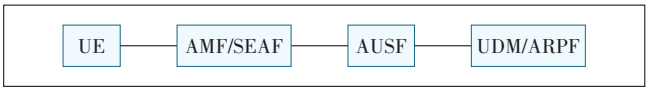

图2　主认证相关网元

2.2 5G AKA认证流程

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。但若拜访网络和归属网络之间的信任程度较低，仍然存在一些安全风险，例如拜访地运营商可以声称为某归属运营商的用户提供了接入服务而实际未提供服务，导致计费纠纷等。相比4G网络中的AKA认证，5G-AKA认证加强了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认证机制的统一。

3GPP TS 33.501规范中详细描述了5G-AKA的认证过程，如图3所示。具体认证流程如下。

a）归属网络的UDM使用长期密钥和RAND随机数，生成一个预期响应XRES*，XRES* = KDF（K,RAND）；UDM/ARPF应创建一个包含RAND、AUTN、XRES*和KAUSF的5G HE AV。

b）UDM向AUSF发送生成的5G HE AV。

c）AUSF存储XRES*。

d）AUSF根据安全的单向函数计算HXRES*。其中HXRES*由XRES*和RAND做SHA256运算得到，

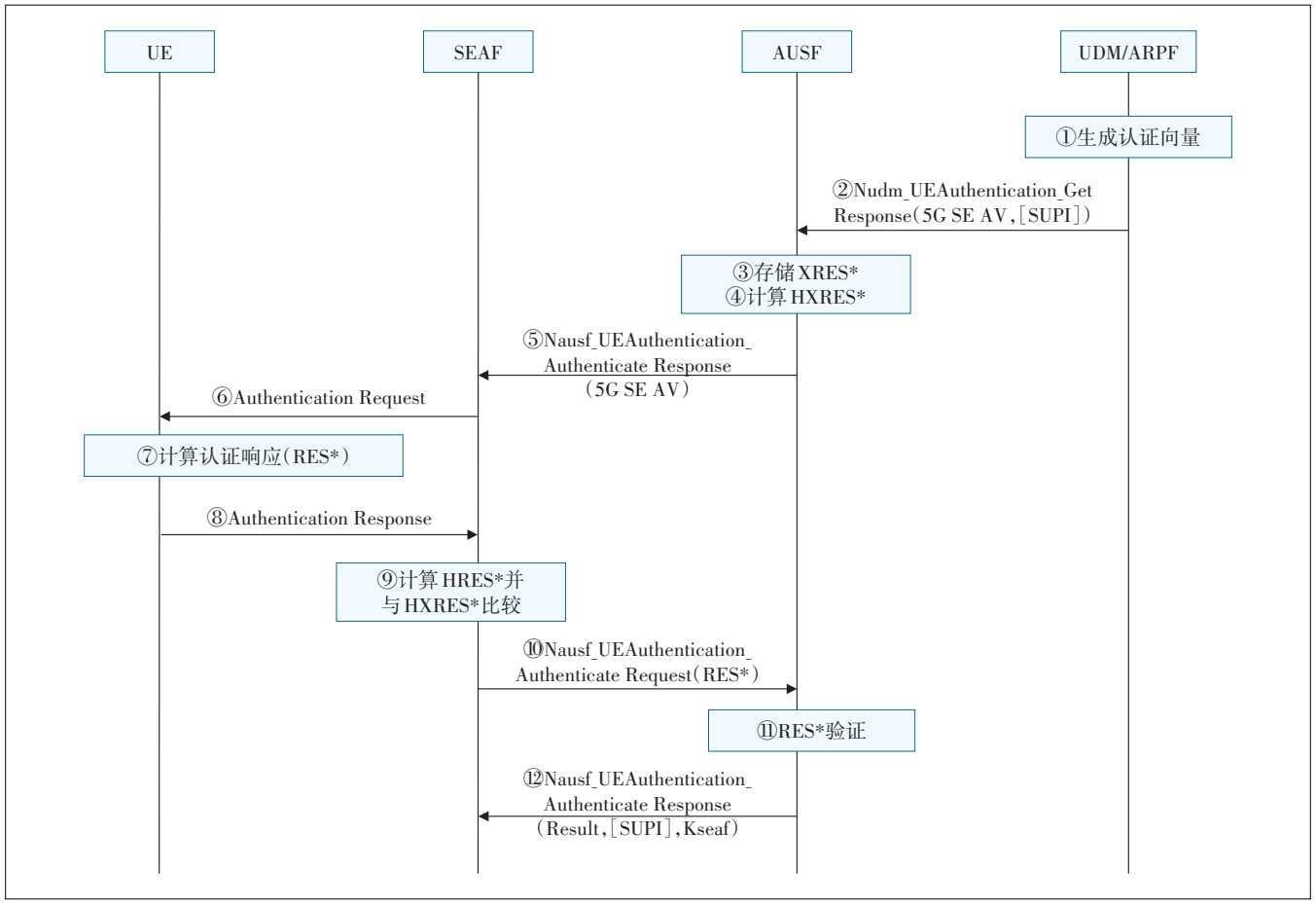

图3　5G AKA认证

HXRES* = SHA256(XRES*,RAND)。由于通过安全的单向函数生成HXRES*，所以不能由HXRES*推出XRES*。归属网络将RAND和HXRES*分享给拜访网络。从XRES*计算出HXRES*，从K_{AUSF}推衍出K_{SEAF}，然后用HXRES*和K_{SEAF}分别替换5G HE AV中XRES*和K_{AUSF}，生成5G SE AV。

e）AUSF将5G SE AV发送给AMF/SEAF。

f）SEAF通过NAS消息向UE发送RAND和AUTN。

g）终端用USIM卡里预置的K和RAND计算出RES*，正常情况下，这个参数与XRES*是相同的。

h）UE在NAS消息认证响应中将RES*返回给SEAF。

i）SEAF根据同样的单向算法通过RES*计算HRES*，并比较HRES*和HXRES*。若两值一致，SEAF从服务网的角度认为认证成功；否则，SEAF认为认证失败，并向AUSF指示失败。

j）AMF/SEAF将RES*进一步发送给归属网络的AUSF进行验证。

k）AUSF将RES*和存储的XRES*比较，从而知道拜访网络确认通过认证并从终端处获得了RES*，因为从归属网络发送给拜访网络的HXRES*是推导不出XRES*的，拜访网络必须从终端处获得，也就是必须完成一次认证，从而无法欺骗归属网络。

l）AUSF向SEAF指示认证是否成功。

2.3 EAP-AKA′认证流程

5G网络将EAP-AKA′认证方式提升到了和5G-AKA并列的位置。EAP认证框架实现了5G网络与其他异构网络的统一接入认证需求，即在使用5G无线网接入的时候，也可以采用EAP-AKA′认证方式。EAP框架非常灵活，既可运行在数据链路层上，不必依赖于IP协议；也可运行于TCP或UDP协议之上。由于这个特点，EAP具有很普遍的适用性，支持多种认证协议，如EAP-PSK、EAP-TLS、EAP-AKA、EAP-AKA′等。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。

3GPP TS 33.501中详细描述了EAP-AKA′的认证过程，如图4所示。具体认证流程如下。

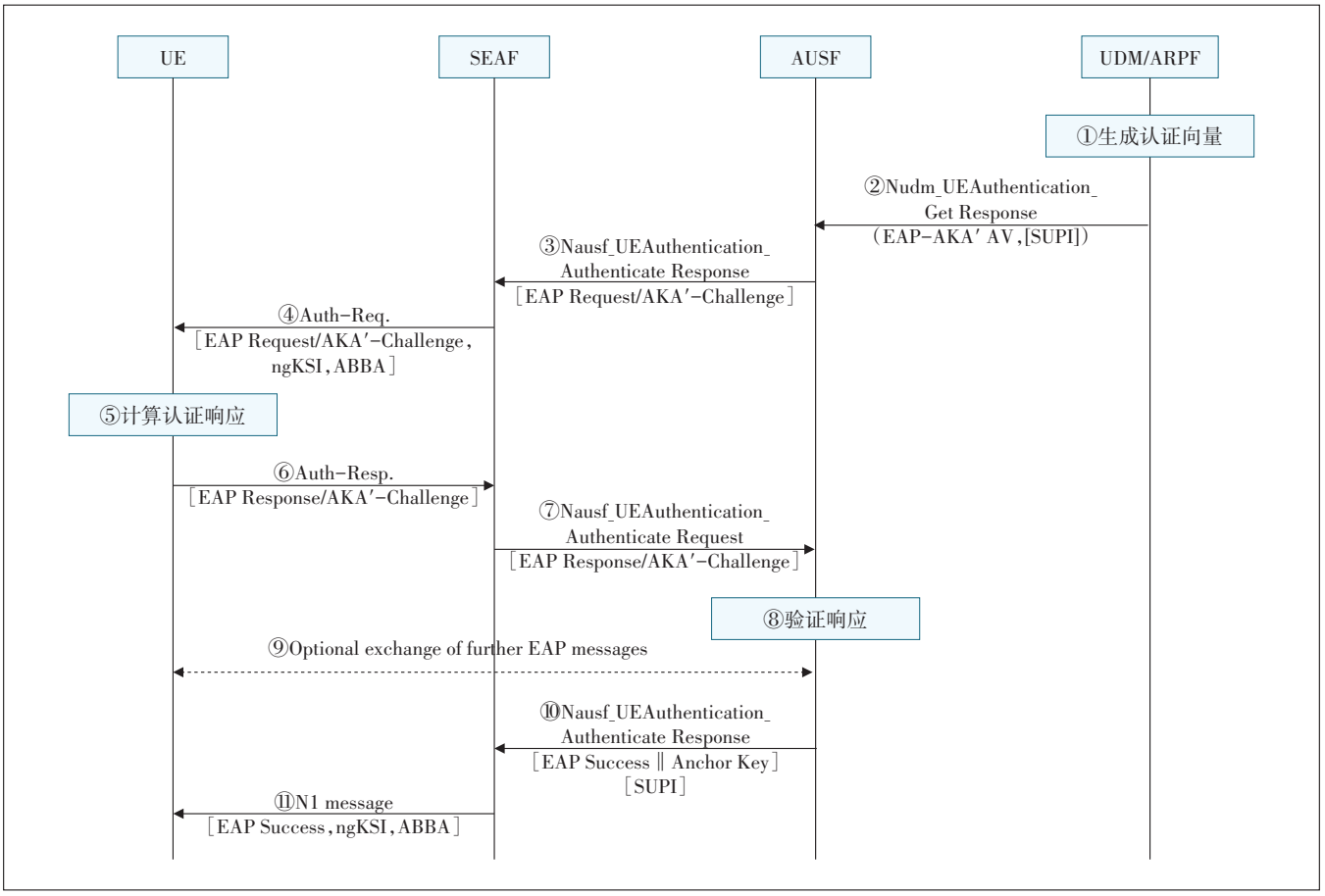

图4　EAP-AKA′认证

a）归属网络的DM/ARPF首先生成认证向量EAP-AKA′ AV（RAND、AUTN、XRES、CK′、IK′）。

b）UDM向AUSF发送生成的EAP-AKA′ AV。

c）AUSF将EAP-Request/AKA′-Challenge消息发送至AMF/SEAF。

d）SEAF在NAS消息认证请求中将EAP-Request/AKA′-Challenge消息透明转发给UE。

e）UE根据USIM卡里预置的K和收到的RAND计算出RES*。

f）UE在NAS消息Auth-Response消息中将EAP-Response/AKA′-Challenge消息发送至SEAF。

g）SEAF将EAP-Response/AKA′-Challenge消息透明转发给AUSF。

h）AUSF验证该消息。若AUSF不能成功验证该消息，返回错误消息。

i）（可选）AUSF和UE可通过SEAF交换EAP-Request/AKA′-Notification和EAP-Response/AKA′-Notification消息；SEAF透明地转发这些信息。

j）AUSF向SEAF发送EAP Success消息，该消息应被透明地转发给UE。

k）SEAF在N1消息中将EAP Success消息发送到UE。

3　二次认证

3.1　二次认证应用场景

5G开启了万物互联的新时代，电信运营商将完成以面向普通公众用户为主到面向公众和垂直行业并重的转变。垂直行业用户所访问的数据业务关系到国计民生或商业机密，相较于普通公众用户有着更高的安全需求。面向对终端有多重接入控制需求的工业互联网等垂直行业客户，5G网络可以为其提供底层认证通道，由垂直行业客户自己选择或定制具体的认证算法和协议，实现自主可控的二次认证。二次认证通过，则为用户建立PDU会话并提供网络服务，否则

不能为用户建立PDU会话。5G用户和核心网的主认证完成之后，在用户建立PDU会话时，由SMF发起二次认证。二次认证涉及的网元包括AMF、SMF、UPF、AUSF、DN-AAA等，如图5所示。

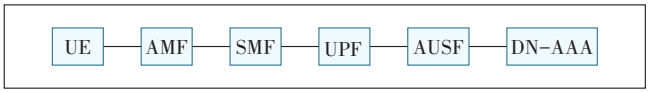

图5　二次认证相关网元

3.2 二次认证流程

二次认证由外部数据网络的DN-AAA服务器对用户进行认证授权，UE和DN-AAA之间的认证使用EAP认证框架，由SMF执行EAP认证的角色。3GPP对二次认证所采用的具体认证协议没有规定，符合EAP框架的认证协议都可以使用，如口令验证协议（Password Authentication Protocol，PAP）、询问握手认证协议（Challenge Handshake Authentication Protocol，CHAP）和安全传输层协议（Transport Layer Security，TLS）等。

3GPP TS 33.501中详细描述了二次认证的认证过程，如图6所示。具体认证流程如下。

a）NG-UE通过使用其网络接入凭证执行和AUSF/ARPF之间的基本认证过程注册到网络，并且和AMF建立NAS安全上下文。

b）当UE有业务时，UE通过发送包含PDU会话建立请求消息的会话管理NAS消息发起建立新的PDU会话。

c）AMF选择合适的V-SMF/H-SMF请求为用户建立PDU会话，当PDU会话建立过程中只包括单个SMF的情况，例如非漫游或者本地疏导场景中，单个的SMF扮演V-SMF和H-SMF的角色。

d）H-SMF从UDM获取用户签约数据，SMF检查UE请求是否符合用户签约数据和本地策略，触发二次认证。

e）二次认证基于EAP认证过程从外部DN-AAA服务器得到授权。

f）完成认证过程后，DN-AAA服务器发送EAP成功消息给H-SMF。

g）若认证成功，则SMF等网元继续为用户建立PDU会话；否则不能建立PDU会话，返回失败消息。

4 切片认证

4.1 切片认证应用场景

为满足垂直行业客户对于移动网络的不同需求，5G网络引入了网络切片技术，为不同行业客户提供多个端到端的虚拟网络。为保证合法切片用户接入网络切片，在用户初始接入时，通过切片选择辅助信息（Single Network Slice Selection Assistance Information，NSSAI）选择AMF。切片认证的主要应用场景为高安全需求的行业客户根据自己的业务特点自主可控用户终端是否可以接入切片，显然由运营商控制的主认证和网络切片选择不能满足其需求，因此5G网络中引入了切片认证。切片认证时，首先用户通过NSSAI选择合适的切片接入，再由AMF根据UE的签约信息发起切片认证流程。切片认证能够在运营商主认证的基础上，更多考虑垂直行业等第三方客户的需求，由第三方客户根据自己的需求对用户进行是否可以使用切片资源的额外认证。例如垂直行业客户限制仅仅在客户认可的IMSI清单内的行业终端才可以接入到客户专属切片，从而确保将网络切片分配给正确的签约用户，保证切片的接入认证安全。

切片认证涉及的网元包括AMF、NSSAAF、AAA-P（可选网元）和AAA-S（Authentication Authorization Accounting-Server），具体如图7所示。其中SEAF/AMF承担EAP认证者的角色，并通过NSSAAF与AAA-S进行通信。如果AAA-S属于第三方，则NSSAAF通过AAA-P与AAA-S联系，NSSAAF和AAA-P可以合设。

4.2 切片认证流程

在主认证结束后，基于UE的签约信息或UE欲接入切片的安全策略，AMF向执行二次认证的AAA-S服务器发送切片内认证请求，从而触发一个切片认证过程。基于AAA-S返回的认证结果，AMF决定是否允许UE使用切片资源。

3GPP TS 33.501中详细描述了切片认证的基本流程，如图8所示。UE成功完成主认证后，归属/服务PLMN向AMF和UE授予允许接入的S-NSSAI列表，具体认证流程如下。

a）UE发送携带S-NSSAI列表的注册请求。

b）UE与AMF/SEAF、ARPF/UDM、AUSF交互，完成主认证流程。对于后续的注册请求，如果UE已经通过认证并且AMF具有有效的安全上下文，则可以跳过主认证。

c）AMF应根据本地存储的信息或来自UDM的签约信息，确定每个S-NSSAI是否需要网络切片认证和

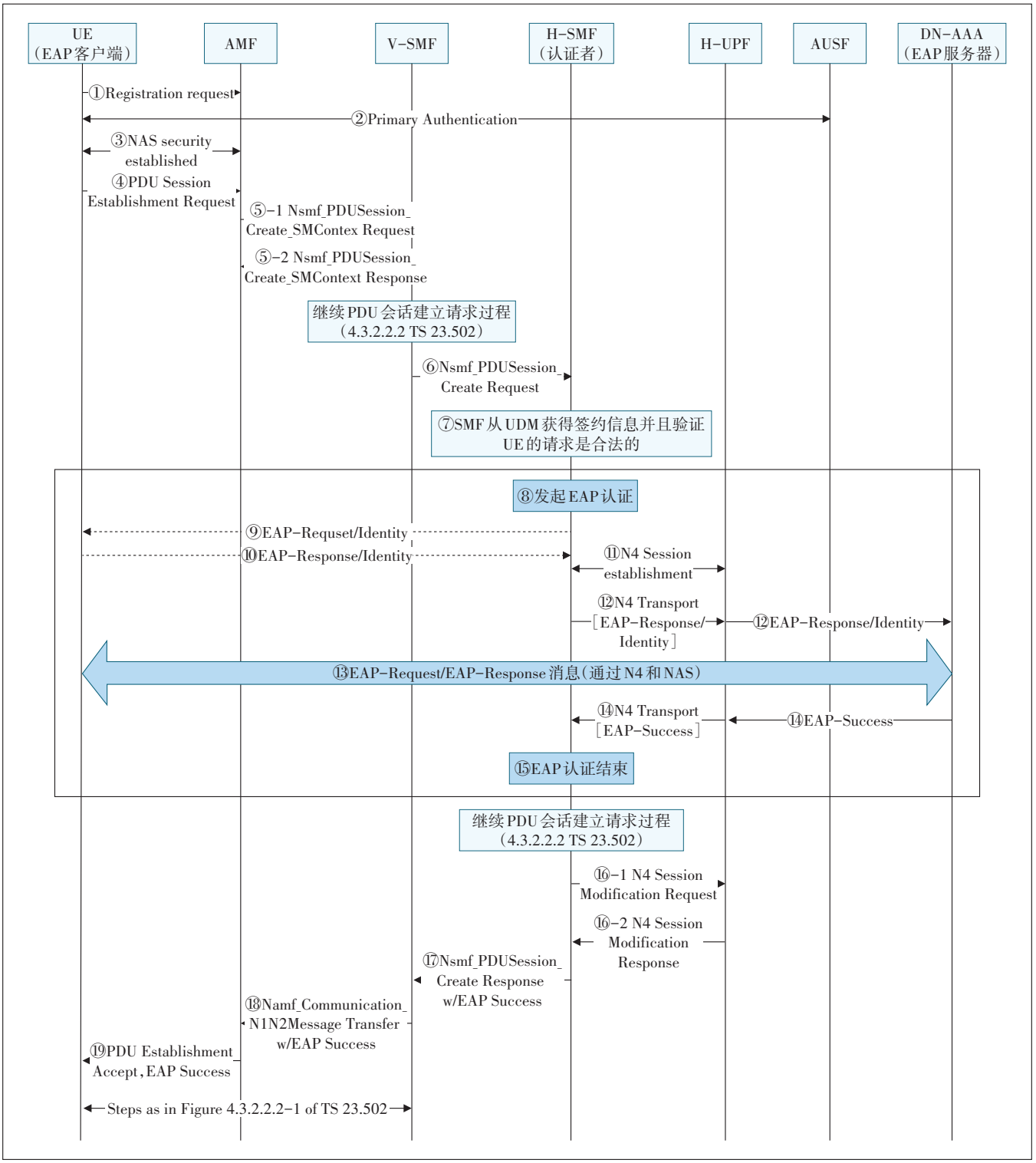

图6　5G网络中的二次认证

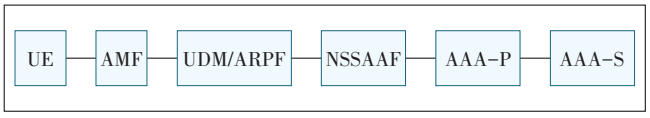

图7　切片认证相关网元

授权。

d）AMF向UE发送注册接受消息。

e）对于需要进行网络切片认证和授权的用户，执行基于EAP的网络切片认证流程。UE和AAA服务器

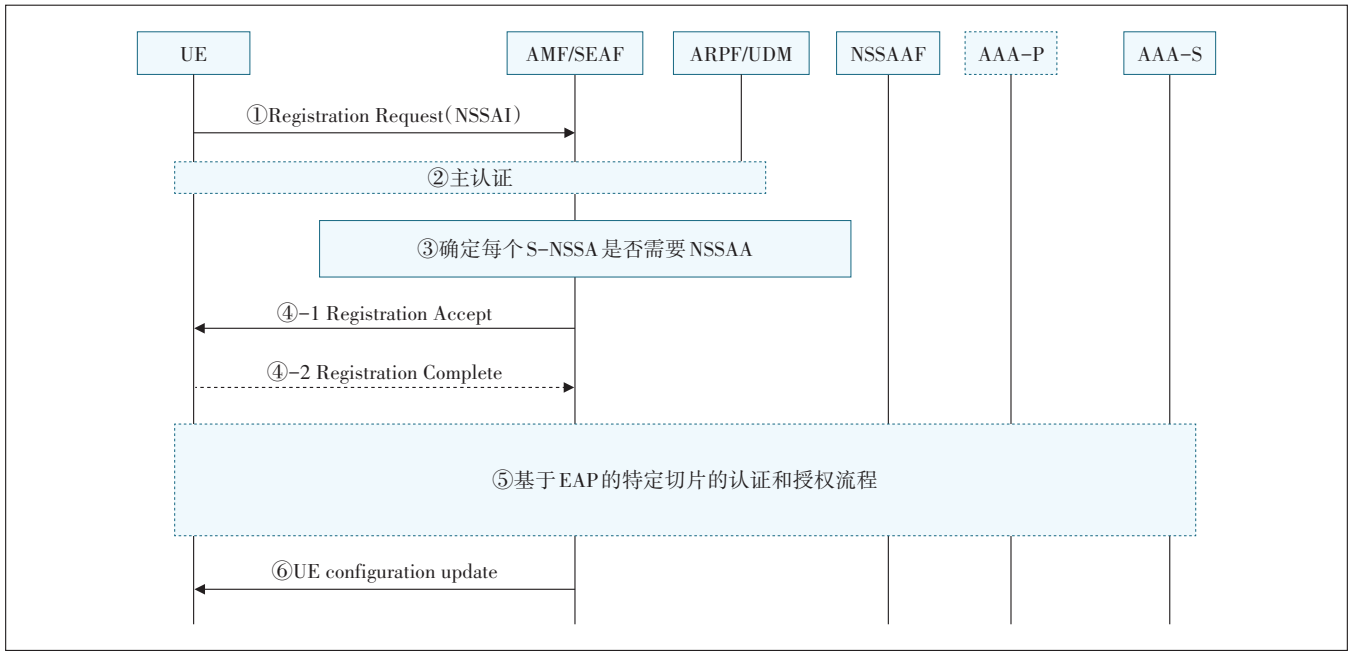

图8　切片认证流程

之间的网络切片认证使用IETF RFC 3748中定义的EAP框架，可以使用多种EAP方法，如PAP、CHAP、PPP、TLS、MD5等认证协议。

f）AMF根据e）的结果，向UE发送UE配置更新消息从而更新请求的S-NSSAI状态。

5 结束语

5G网络拉通了从工厂级到设备级的无线连接，助力工业互联网、电力能源等垂直行业的数字化转型。5G网络与各垂直行业深度融合的新业态是推动社会经济数字化转型的重要动力，未来将会有越来越多的行业借助5G网络实现产业升级。面对垂直行业对5G网络提出的更高安全需求，5G网络对其安全认证体系做了丰富和拓展，在运营商主认证的基础上，引入了切片认证和二次认证，使用了非运营商控制的信任状。后续需要加强与垂直行业客户的合作，不断优化主认证、二次认证、切片认证的融合机制，促进垂直行业的安全、可靠、高质量发展，助力全行业安全数字化转型。

参考文献：

[1] 3GPP. System architecture for the 5G System（5GS）：3GPP TS 23.501 [S/OL]. [2022-04-25]. ftp://ftp.3gpp.org/Specs/.
[2] 3GPP. Security architecture and procedures for 5G system（Release 16）：3GPP TS 33.501 [S/OL]. [2022-04-25]. ftp://ftp.3gpp.org/Specs/.
[3] 张应辉，李一鸣，李怡飞，等. 5G异构网络中基于群组的切换认证方案[J/OL]. 计算机工程与应用：1-11[2022-05-24]. http://kns.cnki.net/kcms/detail/11.2127.TP.20210730.0902.002.html.
[4] 王建英，吕俟林，许建明. 可应用于5G网络的垂直行业二次认证方法浅析[J]. 通信技术，2020，53（10）：2538-2542.
[5] 齐旻鹏，彭晋. 5G网络的认证体系[J]. 中兴通讯技术，2019，25（4）：14-18.
[6] 李长隆，古毅，王俊. 5G二次认证协议的分析与设计[J]. 通信技术，2019，52（7）：1733-1739.
[7] 周艳，何承东. 5G安全的全球统一认证体系和标准演进[J]. 移动通信，2021，45（1）：21-29.
[8] 陈福莉，王俊，杜鑫. 企业/行业用户5G二次身份认证方案初探[J]. 通信技术，2019，52（7）：1740-1743.
[9] 周巍. 5G网络切片安全技术研究[J]. 移动通信，2019，43（10）：38-42.
[10] 游伟，李英乐，柏溢，等. 5G核心网内生安全技术研究[J]. 无线电通信技术，2020，46（4）：385-390.
[11] 徐子钧，刘建伟，李耕. 面向5G mMTC的网络切片安全研究[J]. 网络与信息安全学报，2022，8（1）：95-105.

作者简介：
谢泽铖，毕业于北京交通大学，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，毕业于北京理工大学，教授级高级工程师，博士，主要从事网络与信息安全研究工作；张曼君，毕业于西安电子科技大学，高级工程师，博士，主要从事网络与信息安全研究工作；郭新海，毕业于北京交通大学，工程师，硕士，主要从事网络与信息安全研究工作；苏俐竹，毕业于怀卡托大学，工程师，硕士，主要从事网络与信息安全研究工作。