5G消息安全认证体系研究

Research on 5G Messaging Security Authentication System

李雨汝[1]，宋玉磊[2]，蒋　璇[3]（1. 国家无线电监测中心检测中心，北京 100043；2. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007；3. 中讯邮电咨询设计院有限公司，北京 100048）

Li Yuru[1], Song Yulei[2], Jiang Xuan[3]（1. The State Radio_monitoring_center Testing Center, Beijing 100043, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd. Zhengzhou Branch, Zhengzhou 450007, China; 3. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China）

摘　要：

介绍了5G消息安全认证需求，分析了5G消息对于SIP及HTTP 2种请求的认证实现方式。对5G消息终端、IMS网络、业务系统在认证体系中的角色及相互衔接进行了阐述，结合5G消息行业聊天机器人应用，对聊天机器人认证关键流程进行了研究；对引入第三方认证机构对企业实现客观的认证给出建议，最后展望了5G消息相对于OTT厂商小程序应用的安全优势，会在公共安全领域带来全新的交互式服务。

关键词：

5G消息；安全认证；聊天机器人；小程序

doi：10.12045/j.issn.1007-3043.2021.05.009

文章编号：1007-3043（2021）05-0033-05

中图分类号：TN915

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

It introduces the security authentication requirements of 5G messaging, and analyzes the authentication implementation of 5G messaging for SIP and HTTP requests. It describes the roles of UE, IMS network and business system in the authentication system and their mutual connection. Combined with the application of chatbot in 5G messaging business, it studies the key process of chatbot authentication, and also gives suggestions on introducing a third-party certification authority to realize the objective certification of enterprises. Finally, the security advantages of 5G messaging compared with the small program application of OTT are prospected, which will bring new interactive experience.

Keywords：

5G messaging; Security authentication; Chatbot; Mini program

引用格式：李雨汝，宋玉磊，蒋璇. 5G消息安全认证体系研究[J]. 邮电设计技术，2021(5)：33-37.

0 引言

5G消息是RCS业务在5G时代的落地应用。终端的普及、创新应用的丰富、用户体验的提升将会驱动5G消息渗透至千行百业。终端原生、以手机号码作为用户体系唯一标识的特点让即时通信回归到了可信联系的本质；A2P通知由于其消息即服务的特点，前向赋能企业和其用户之间连接服务的智能化再升级，后向构建了认证、支付、大数据、ASR、NLP、搜索、卡片合成、视频客服、应用制作等能力及内容服务生态。

5G消息相比OTT厂商公众号能提供更安全、更便捷、更高效、更高触达率的交互式应用，安全是5G消息的基础能力底座，也是政府政务、金融保险等对安全等级要求比较高的行业应用的关键业务诉求。认证是5G消息安全体系中的重要环节，包括用户认证和Chatbot应用认证两大环节。

1 用户认证安全分析

1.1 5G消息体系结构

5G消息属于RCS业务，基于IMS网络来承载，通

收稿日期：2021-04-09

过4G/5G及Wi-Fi网络来接入，RCS AS处理消息业务逻辑，MaaP平台实现消息即平台功能，对接行业应用（见图1）。

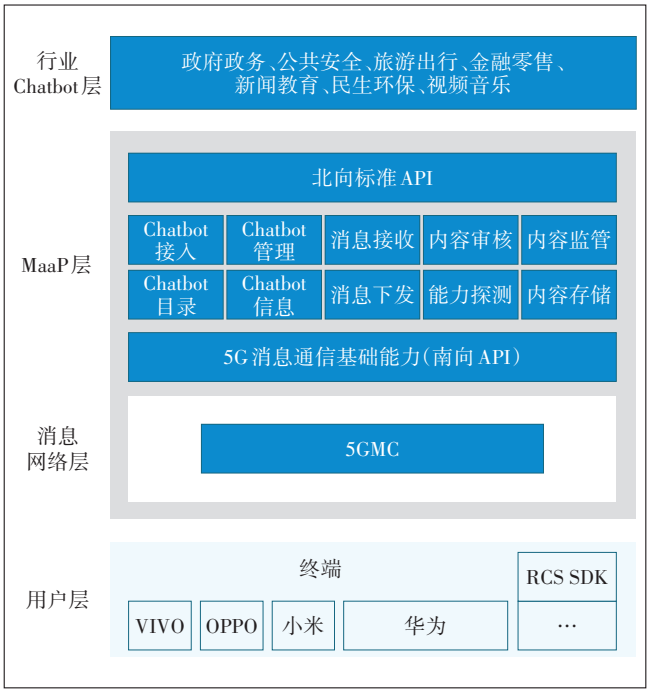

图1　5G消息体系结构图

1.2 注册认证安全分析

5G消息业务属于IMS业务范畴，业务注册时采用SIP协议进行交互，使用AKA方式进行认证。IMS-AKA鉴权的主要流程如下。

a）P-CSCF的地址通过P-CSCF发现过程获得。需要注册的归属域名从ISIM中获得，携带IMPI和IMPU进行注册尝试。

b）此时，P-CSCF收到的消息没有一致性安全保护。P-CSCF根据Request-URI将注册消息路由到用户归属域的接口I-CSCF。I-CSCF从用户归属的HSS中获取能够为用户服务的S-CSCF信息，并将注册消息转发给该S-CSCF。

c）由于用户当前没有在S-CSCF中注册，所以需要向HSS设置Registration Flag（pending），指示正在注册。S-CSCF以用户的IMPI为关键字，向HSS索取鉴权向量5元组，包括RAND、AUTH、XRES、CK和IK。

d）S-CSCF保存全部鉴权向量5元组。将RAND、AUTH、XRES、CK和IK在SIP 4XX应答中发给I-CSCF，由其转发给P-CSCF。

e）P-CSCF收到该SIP 4XX应答之后，保存CK和IK，将其余部分转发给UE。CK和IK的扩展将用做IPsec ESP传输模式下安全联盟需要的保密密钥和一致性密钥。

f）UE获得AUTH后，提取MAC和SQN，并自行利用共享密钥IK计算XMAC，判断XMAC是否和MAC一致，SQN是否在合理数值范围，以辨别IMS网络是否合法。UE利用共享密钥和RAND计算鉴权响应RES，并重新发起注册过程。

新的注册过程使用的IP地址不变，但端口号须与SA中协商的一致。选择的P-CSCF和S-CSCF必须与初始注册过程一样。

g）S-CSCF比较从UE获得的RES和曾从HSS获得的XRES，如果一致，则UE认证鉴权通过，可以享受服务。S-CSCF向HSS设置Registration Flag（registered），并从HSS中获取用户属性和业务信息。最后向UE发送SIP 2XX注册完成响应。

5G消息采用五元组进行认证，使用手机号码构建IMPU以及IMPI进行注册，相比于APP、小程序等OTT应用采用用户名、密码、短信验证码的方式进行验证无论从流程还是对外信息暴露方面均具有较高的安全性。

1.3 HTTP业务认证安全分析

在5G消息中，使用HTTP协议进行交互的网元有DM服务器、AS中的HTTP内容服务器、MaaP平台的Chatbot目录服务器、Chatbot信息服务器以及HTTP内容服务器。

1.3.1 DM交互

5G消息业务中，终端根据用户SIM卡归属的运营商构建出DM设备标准域名（如http://config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org），并向该域名发起HTTP（HTTPS）请求，该请求不涉及到用户操作，采用Token或者Session的方式进行认证。

1.3.2 GBA认证

当用户通过HTTP方式上传下载多媒体信息以及通过HTTP方式去获取Chatbot列表以及Chatbot详细信息时，采用GBA方式对用户进行认证。GBA认证的详细流程如图2所示。

GBA认证有效利用AKA鉴权的特性对非SIP请求进行认证，对于GBA鉴权中涉及到的主要关键点分析如下。

a）NAF地址：NAF地址通过DM配置文件获取，格式为域名或者IP地址形式，由于IP地址易变更，基本采用域名方式。

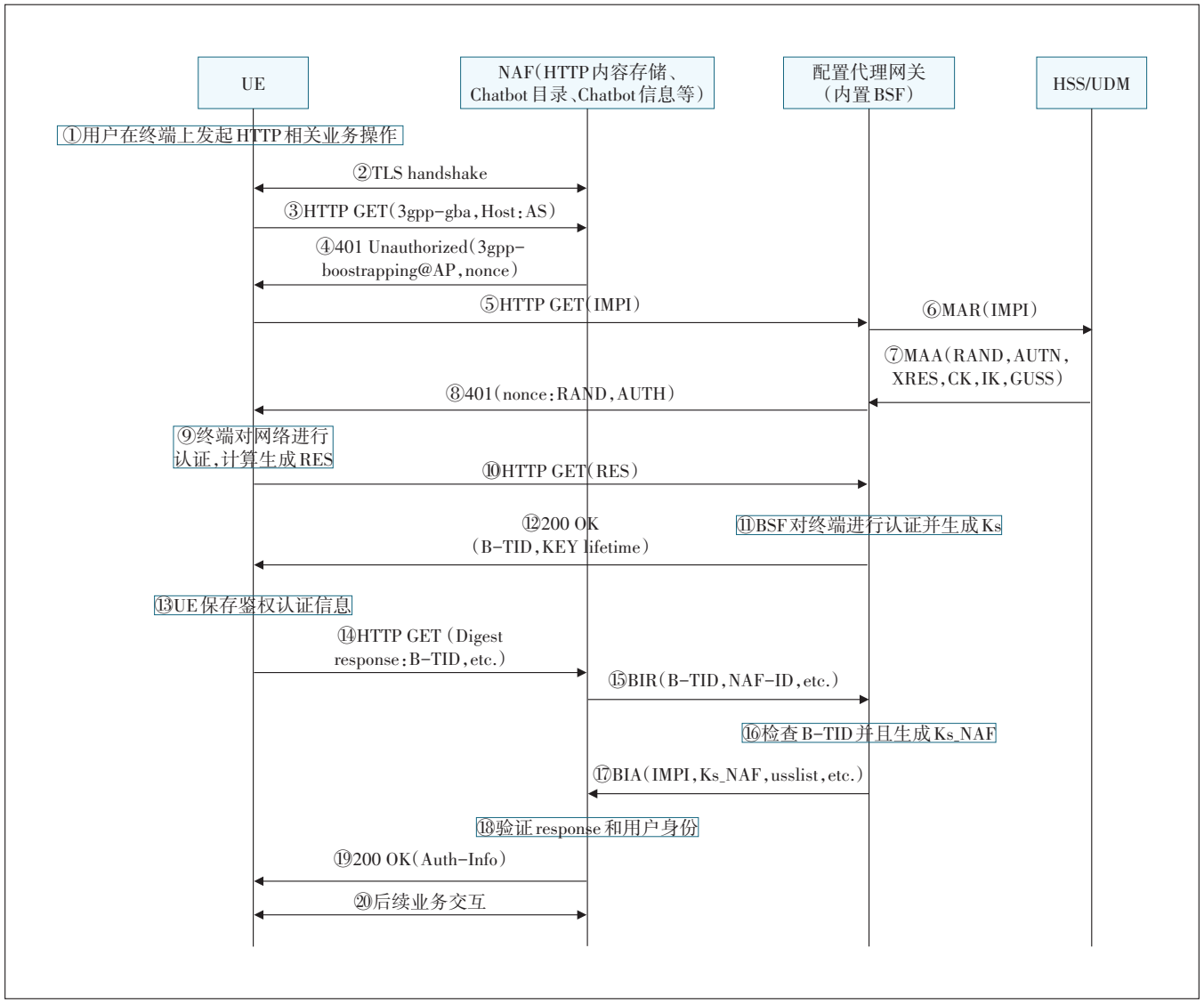

图2　GBA认证流程图

b）HTTP或者HTTPS：UE请求使用HTTP还是HTTPS方式不但决定了传输层协议是否安全，而且决定了NAF_ID的取值方式，根据3GPP定义，NAF_ID=FQDN of the NAF‖Ua security protocol identifier。若为HTTP方式，Ua security protocol identifier为（0x01，0x00，0x00，0x00，0x00）；若为HTTPS方式，则Ua security protocol identifier为（0x01，0x00，0x01，yy，zz），其中"yy，zz"为HTTPS中CipherSuite Code值。在GBA鉴权具体实施的过程中采用HTTPS方式保障了传输层面的安全性。

c）BSF网元：BSF网元的域名需要终端根据SIM卡信息导出，其标准格式为：bsf. mnc<MNC>. mcc<MCC>. pub. 3gppnetwork. org。目前VoLTE网络中终端也根据上述域名去查找Ut服务器，因此建议BSF网元和Ut服务器合设。

d）BIA消息的验证方式：

（a）检验BSF返回的USS信息中的认证方式（GBA-ME、GBA-U等）是否与UE携带的认证方式（基于请求消息中的realm）一致，如果一致，则进行后续操作；如果不一致，则给UE返回401认证失败消息。

（b）NAF根据用户的USS信息，验证UE传送过来的身份信息IMPU，如果一致，则进行后续操作；如果不一致，则给UE返回401认证失败消息。

（c）利用B-TID（用户名）和Ks_NAF（口令）进行HTTP Digest计算response，并与请求消息头域Authorization中的response值比对，如果一致，则通过认证，继

续后续操作；如果不一致，则给UE返回401认证失败消息。

对于OTT应用，其在通过HTTP访问应用时，无法对用户的身份进行认证。在5G消息里，当用户通过HTTP访问应用服务器时，采用GBA方式则保障了应用访问的安全合规性。

1.4 系统认证角色分析

终端：5G消息是一款要求原生终端支持的应用，终端是认证系统的发起点，对于SIP应用，要求支持AKA鉴权方式；对于HTTP应用，则要求支持GBA认证，并要求该功能和应用服务器侧保持一致，终端开启了GBA认证，若应用侧不支持，对于HTTP Get请求，终端侧可以忽略GBA鉴认证要求，但是对于Post请求，若应用侧不支持GBA鉴权方式，则会导致业务交互失败。

HTTP服务器：HTTP服务器是应用的鉴权点，需要支持并开启GBA认证方式，并和BSF进行BIR以及BIA消息交互，根据交互结果和终端侧信息进行比较达到认证鉴权目的。

BSF网元：BSF网元是GBA认证流程中重要的一环，它通过Ub接口和终端进行交互，通过Zn接口和NAF（HTTP应用服务器）交互，通过Dz以及Zh接口和HSS进行交互，并可以作为GBA鉴权的网络能力开放网元，在物联网等领域将认证能力对外开放（见图3）。

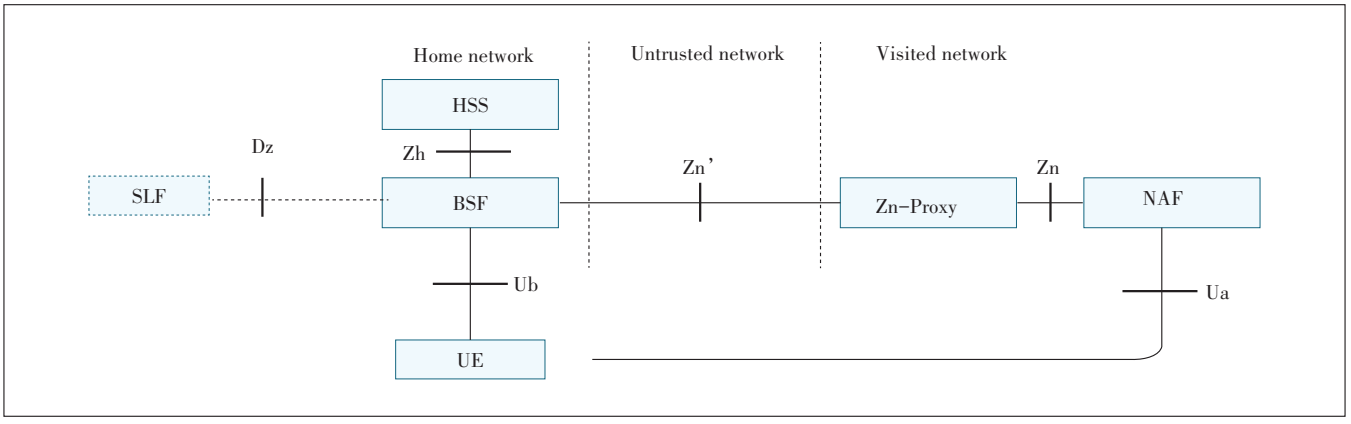

图3　BSF网元接口系统图

IMS核心网：对于SIP认证，IMS核心网P-CSCF、S-CSCF、HSS需要参与并支持AKA认证方式，对于HTTP认证，HSS需要通过Zh接口和BSF交互返回鉴权认证向量。

2 Chatbot认证安全分析

2.1 MaaP平台

消息即平台（MaaP——Message as a Platform），是5G消息网络中将消息能力开放给企业的核心网元，企业侧应用（Chatbot）通过MaaP平台以SIP或者HTTP方式进行交互，南向对接RCS AS及终端，主要功能包括Chatbot接入、Chatbot目录、Chatbot信息、HTTP内容存储，消息收发、消息审核、能力探测等。

2.2 Chatbot认证

2.2.1 Chatbot签名

认证机构通过JWS（JSON Web Signature）的方式对Chatbot进行签名，JWS主要包括如下信息。

a）Payload：包括Chatbot Service ID、Chatbot Name以及Iconfingerpirnt信息，并以Base64编码呈现。

b）Protected：至少包括加密算法Alg以及Crit Header，其中Crit包含botvfexpires值表明签名的到期日期，以Base64编码呈现。

c）Header（Unprotected）：包括Kid属性，用来指示加密算法的公钥值，以Base64编码呈现。

d）Signature：对Payload、Portected、Header等3个部分内容使用私钥进行加密，并以Base64编码进行呈现。

认证机构签名后将签名信息以及Chatbot信息发送至MaaP平台。

2.2.2 Chatbot签名核查流程

MaaP平台对签名核查流程如下。

a）如果Chatbot详情信息不包含verification-signatures签名信息，则Chatbot将被视为未认证。

b）如果验证签名属性与JSON序列化中的JWS不对应，则Chabot将被视为未验证。

c）解码Base64后，验证签名的有效荷载不包含

Chatbot ID以及Chabot名称，则Chatbot将被视为未验证。

d）如果JWS中Protected的Alg算法不属于[RFC7518]的推荐算法，则Chatbot将被视为未验证。

e）如果JWS中Protected的Crit对象不包括botvf-expires属性，则Chatbot将被视为未验证。

f）如果Header中未包括公钥Kid值，则Chatbot将被视为未验证。

g）如果Payload中的Iconfingerpirnt信息与Chatbot详情信息中的图标指纹信息不匹配，则Chatbot将被视为未验证。

h）若以上步骤顺利验证完成，则JWS签名信息验证完毕，若Chatbot详情信息不包含图标的信息，则Chatbot认证成功，若Chatbot详情信息中图标包含指纹信息，当“指纹”属性的值与Chatbot信息中图标的URL所指文件的SHA-256散列相匹配时，Chatbot验证应被视为成功。

当MaaP平台对Chatbot认证成功后，verification-info中的bot-verification字段将设置为True；终端得到该信息后将向客户展示认证机构以及认证到期时间；至此，Chatbot认证流程完整结束。

3 第三方认证机构引入建议及展望

5G消息的普及必将会带来千万级别的Chatbot应用，对Chatbot应用的管理和认证将是一项新的任务，哪些Chatbot值得信任需要公平公正客观的评价体系，建议引入第三方权威认证机构进行认证，运营商按照Chatbot认证规则对认证进行校验，为行业应用创造良好的生态，让有价值的应用能够快速地得到认可和普及，让用户也更方便地找到可信任的应用。

5G消息的建设及发展需要终端、运营商网络、业务平台及行业应用的相互协同和共同发展。相信借助5G消息完善的安全认证体系以及原生、互联互通等OTT应用不具备的特征，一定会给政府政务、公共安全、旅游出行、金融零售、新闻教育、民生环保等领域带来全新的交互体验，创造更多的价值。

参考文献：

[1] GSMA. RCS Universal Profile Service Definition Document Version 2.4 [EB/OL]. [2021-03-16]. https://www.gsma.com/futurenetworks/wp-content/uploads/2019/10/RCC.71-v2.4.pdf.

[2] GSMA. Rich Communication Suite -Advanced Communications Services and Client Specification Version 12.0 [EB/OL]. [2021-03-16]. https://www.gsma.com/newsroom/wp-content/uploads//RCC.07-v12.0-5.pdf.

[3] GSMA. P2A Discovery for RCS [EB/OL]. [2021-03-16]. https://www.gsma.com/futurenetworks/wp-content/uploads/2020/02/RCS-P2A-Discovery-Whitepaper.pdf.

[4] GSMA. IMS Device Configuration and Supporting Services Version 7.0 [EB/OL]. [2021-03-16]. https://www.gsma.com/newsroom/wp-content/uploads//RCC.15-v7.0.pdf.

[5] GSMA. RCS and Payments [EB/OL]. [2021-03-16]. https://www.gsma.com/futurenetworks/wp-content/uploads/2020/02/RCS-and-Payments-Whitepaper-1.pdf.

[6] GSMA. RCS Business Messaging in Japan [EB/OL]. [2021-03-16]. https://www.gsma.com/futurenetworks/wp-content/uploads/2019/12/1-RCS-Business-Messaging-in-Japan-single-combined-low-res-ENGLISH.pdf.

[7] GSMA. Enabling your Network for RCS Business Messaging [EB/OL]. [2021-03-16]. https://www.gsma.com/futurenetworks/wp-content/uploads/2019/08/GSMA-MAAP-Launch-Options-V1.pdf.

[8] IP Multimedia (IM) session handling IM call model Stage 2: 3GPP TS 23.218 [S/OL]. [2021-03-16]. https://www.3gpp.org/specifications/specifications.

[9] IP Multimedia Subsystem (IMS) Stage 2: 3GPP TS 23.228 [S/OL]. [2021-03-16]. https://www.3gpp.org/specifications/specifications.

[10] IETF. JSON Web Algorithms (JWA) [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/rfc/rfc7518.html.

[11] IETF. Hypertext Transfer Protocol - HTTP/1.1 [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/info/rfc2616.html.

[12] IETF. HTTP Authentication: Basic and Digest Access Authentication [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/info/rfc2617.html.

[13] IETF. Session Initiation Protocol (SIP) Extension for Instant Messaging [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/info/rfc3428.html.

[14] IETF. Instant Message Disposition Notification (IMDN) [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/info/rfc5438.html.

[15] IETF. Alternative Connection Model for the Message Session Relay Protocol (MSRP) [EB/OL]. [2021-03-16]. https://www.rfc-editor.org/info/rfc6135.html.

[16] CHEN Z, CHEN S, XU H, et al. A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain [J]. IEEE Access, 2018(6): 55372-55379.

作者简介：

李雨汝，研究员，硕士，主要从事无线电频谱研究相关工作；宋玉磊，毕业于华中科技大学，硕士，主要从事5G消息研究及平台开发工作；蒋璇，毕业于北京信息科技大学，学士，主要从事5G消息研究及产品运营工作；刘茜溪，毕业于北京交通大学，硕士，主要从事5G消息研究及平台开发工作。