 DOI: https://doi.org/10.12349/iser.v3i2.604

Introduction of 5G USIM Consistency Test Based on CTP3500

Guoqing Li Xinlei Gao

The State Radio-monitoring-center Testing Center, Beijing, 100041, China

Abstract

User cards carry the important functions of mobile user identity identification and network access authentication.In terms of access authentication. 5G SA network adds new features such as user privacy protection, EAP-AKA' authentication / 5G AKA authentication, 5G key system and 5G security context, which put forward new requirements for 5G user cards.

Keywords

USIM; 5G SA; network access and authentication encryption

基于 CTP3500 的 5G USIM 一致性测试简介

李国庆 高鑫磊

国家无线电监测中心检测中心 中国·北京 100041

摘 要

用户卡承载移动用户身份标识和网络接入认证的重要功能。5G SA网络在接入认证方面新增不同于4G网络的用户隐私保护、EAP-AKA'认证/5G AKA认证、5G密钥体系及5G安全环境等特性，这些特性对5G用户卡提出新的要求。

关键词

USIM；5G SA；网络接入与认证加密

1 引言

为了针对支持 5G 通信的设备检测，论文主要介绍基于 CTP3500 平台，对 5G 卡机接口中的 USIM 进行测试与分析，以此来判断支持 5G 通讯的终端是否符合 GCF 认证标准。

2 研究背景与意义

随着人们对高效网络服务的需求，中国的移动通信技术发展迅猛，从最初的 2G、3G、4G，到 5G 移动通信技术，中国的移动通信技术发展步伐较快，5G 技术的发展已位居世界前列 [1]。在 5G 这一新型基础设施之上，云计算、大数据、物联网、人工智能、区块链等新一代信息技术集成汇聚，将孕育出诸多新模式、新业态，催生多个万亿元规模的新兴产业，成为数字经济发展的强劲动能。海量数据的便利存储与高速传输，人工智能的精准识别与分析判断，区块链共识技术的数据安全保障等，这些都将促进社会优质资源的共享与使用，提升社会管理水平，带动社会服务方式的变革。与 LTE 网络相比，5G 在业务场景、接入网、核心网等多个方面将发生显著变化，对承载网提出了“更大带宽、超低时延、高可靠性”的要求以及网络切片、灵活组网等新需求 [2]。5G 网络部署有基于 EPC 的非独立组网（NSA）和基于 5GC 的独立组网（SA）方案。运营商目前主流采用 NSA Option 3a/3x 和 SA Option 2 模式。NSA Option 3 只引入 5G 新空口（NR），控制面锚定在 4G 基站（LTE）侧，5G 终端使用现网已发行 4G 卡可以实现基本的接入认证、使用 5G 无线网络的基本通信业务。由此带来的 5G 检测业务也呈发展趋势，越来越多的终端在支持 5G 技术的同时，也要符合 3GPP 所规定的技术规范。

3 USIM 与 5G SA 网络安全模型

全球用户身份模块（USIM），也叫做升级 SIM，是在 UMTS（通用无线通信系统）网络的一个构件。除能够支持多应用之外，USIM 卡还在安全性方面对算法进行了升级，并增加了卡对网络的认证功能，这种双向认证可以有效防止黑客对卡片的攻击。该技术可以作为 GSM 网络的另一种高速数据业务载体，它将成为第二代到第三代移动通信 SIM 卡良好过渡的技术依托，该技术早在 1991 年就被提出来作为研究方向，UMTS 除支持现有的一些固定和移动业务外，

【作者简介】李国庆（1999–），男，中国河北衡水人，本科，通信工程师，从事5GNR无线通信技术研究与5G移动终端协议测试研究。

还提供全新的交互式多媒体业务。UMTS 使用 ITU 分配的、用于陆地和卫星无线通信的频带。它可通过移动或固定、公用或专用网络接入，与 GSM 和 IP 兼容。以非漫游这种最基本的业务情景为例，5G SA 网络安全模型由 UE 和网络组成，包括：USIM（Universal Subscriber Identity Module）、ME、RAN、核心网，如图 1 所示。

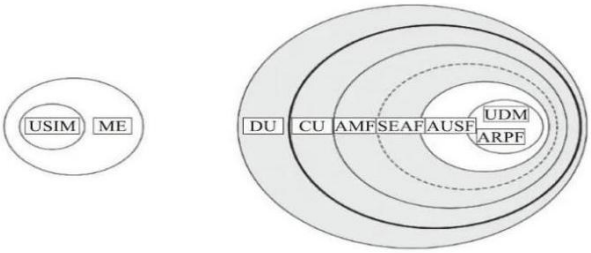

图 1 非漫游情景的 5G 安全模型

UE由USIM和移动设备（ME）组成，USIM驻留在5G用户卡上实现安全认证功能（下文所指的5G用户卡功能均在USIM模块实现）。无线接入网（RAN）分为分布式单元（DU）和中央单元（CU），DU和CU共同构成5G基站gNB。核心网中，AMF（Access and Mobility Management Function）是非接入层（NAS）安全的终止点；SEAF（Security Anchor Function）持有UE与网络主认证之后派生的访问网络的根密钥（称为锚定密钥）KSEAF；AUSF（Authentication Server Function）保留一个可重用的密钥KAUSF（同样在主认证后派生），以便在不同接入网技术（即3GPP接入网和非3GPP接入网，如IEEE 802.11无线局域网WLAN）同时注册UE时重用；ARPF（Authentication credential Repository and Processing Function）保存认证信息；UDM（Unified Data Management）使用存储在UDR（Unified Data Repository）中的用户签约数据，来执行各种功能，如认证凭据生成等。

3GPP 在 3GPP TS 31.121 标准中对机卡测试 USIM 部分进行了明确规定。下面以其中的最基础的 CASE 5.3.1 具体测试内容进行分析。

4 CASE5.3.1 测试内容介绍

4.1 测试目的

如果运营商决定由 ME 计算 SUCI，则归属网络运营商应该在运营商允许的 USIM 中提供保护方案标识符的列表。USIM 中的保护方案标识符列表可以按照优先级的顺序包含一个或多个保护方案标识符。ME 将从 USIM 读取 SUCI 计算信息，并从其支持的方案中选择在 USIM 获得的列表中具有最高优先级的保护方案。本测试的目的是验证 ME 是否正确执行了读取 $EF_{SUCI\_Calc\_Info}$、$EF_{Routing\_Indicator}$ 和 EF_{IMSI} 命令以及验证 ME 使用零方案执行 SUCI 计算过程。

4.2 测试流程

①在仪表提供 244083 的网络情况下，打开待测终端 UE。

② UE 向 NG-SS 发送注册请求，指示 5GS 注册类型 IE 为“初始注册”并且 5GS 移动身份信息元素类型为“SUCI”。

③在接收到具有 5G GUTI 的注册接受消息时，UE 向 NG-SS 发送注册完成消息。

4.3 预期结果

第一，在步骤①之后，ME 应读取 EF_{IMSI}、$EF_{Routing\_Indicator}$ 和 $EF_{SUCI\_Calc\_Info}$。

第二，在步骤②中，UE 将在注册请求中的 5GS 移动身份 IE 中包括如下编码的 SUCI。

4.4 测试操作

使用 CTP3500 平台模拟实际工作环境。将终端的 APN 设置为 1，“ip”，“test”，” 0.0.0.0”,0,0,0,0,,,,,,,,, “” ,,,,0 并删除其他 APN。校准功率补偿值使得待测终端可以顺利搜索并自动注册仪表提供的 244083 网络。然后开始测试例并重启终端。确保终端处于自动搜网状态然后自动注册网络并关机，流程结束。

4.5 测试结果

第五代移动通信技术（Fifth-Generation Mobile Communication System，5G）与长期演进技术（Long Term Evolution，LTE）建立通信的过程相似，都是以小区搜索作为用户设备接入无线网络与基站建立通信的第一步 [3]。5G 通信系统在帧结构、同步信号以及信道编码等方面与 LTE 系统不同。分析图 2 的测试信令流程图可以发现，注册过程主要由以信令：Registration_request，authentication_request，RRC_SETUP 以及他们的返回信令和 UE 能力获取信令组成。先是系统消息广播。gNodeB 将系统消息广播给小区中的所有 UE。系统消息中承载着小区的关键参数以及配置信息。当 UE 处于以下场景时，会主动读取系统消息：开机选择小区驻留，重选小区，切换完成，从其他 RAT 系统进入 NG-RAN，从非覆盖区返回覆盖区。次之进行的是寻呼（可选）。5GC 发现有下行数据需要到达处于空闲态的 UE 时，如 UE 被呼叫，会触发寻呼 UE。然后进行随机接入，当 UE 作为被叫收到寻呼消息时，或者作为主叫需要和网络建立链接时，UE 向 gNodeB 请求随机接入。接着进行信令链接建立 建立 UE 到 5GC 的信令链接，包括 RRC 信令连接，专用 NG-C 连接。最后 PDU Session 建立 5GC 出发 gNodeB 建立 PDU session。

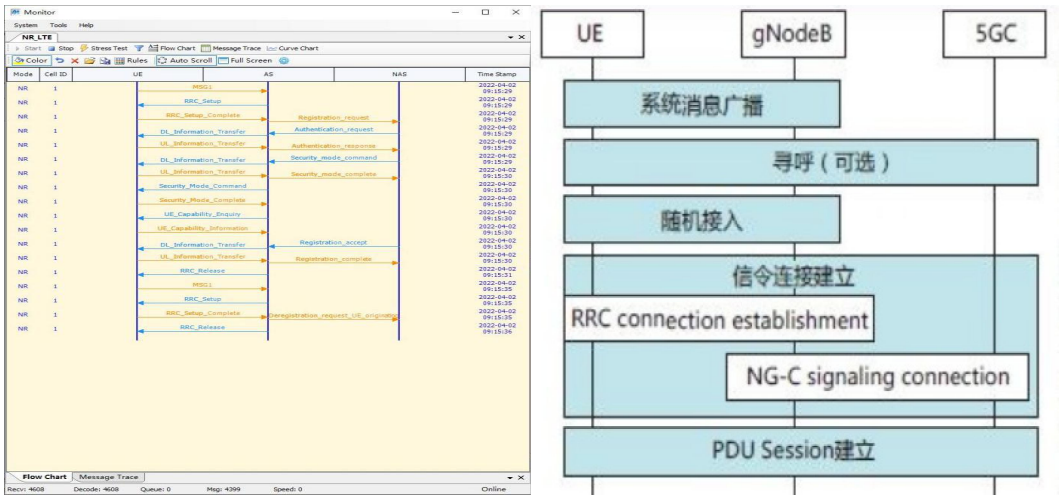

图 2 测试信令流程图

4.6 测试过程中可能遇到的问题

①无法收到 RRC_SETUP 信令。可能的原因是终端所收到的仪表提供的网络信号差，可以尝试增大上下行功率直到接入成功。

② UE 能力获取错误。在系统配置中的终端信息与实际值不匹配，修改系统内的终端信息包含 PICS 内的参数，使之匹配。

③ PDU Session 建立不成功。可能与终端设置的 APN 有关，建议查询手机移动网络内的 APN 设置，一般情况下建议删除全部默认 APN，并根据 case 建立一个期望的 APN。但是也存在多 PDU 并存的终端，需要根据实际情况进行分析。

5 前景与展望

5G SA 在中国已开启商用大幕，相比 4G 相对稳定的网络架构，5G 混合的 LTE/NSA/SA 网络环境，对 4G 卡的后向兼容需求及 5G 卡新增的安全隐私功能等，都带来了更复杂的 5G 终端机卡兼容要求。物联网时代的到来，使得 5G 将会面临海量连接的场景 [4]。随着 5G 技术的逐步发展与普及，越来越多的 5G 终端将涌现在市场中，如何根据行业技术标准严格把控终端质量，如何根据技术规范合理评价终端性能，已经成为当下的重要议题。5G USIM 一致性测试也将伴随 5G 技术发展而更加重要。

参考文献

[1] 张雪飞.浅谈通信工程中5G移动通信技术的运用[J].中国设备工程,2022(5):41-42.

[2] 马培勇,吴伟,张文强,等.5G承载网关键技术及发展[J].电信科学,2020,36(9):122-130.

[3] 郭秋阳.5G下行信号的同步与检测技术研究[D].成都:电子科技大学,2019.

[4] 郭永娜.5G多用户非正交共享接入中干扰消除技术研究[D].哈尔滨:哈尔滨工业大学,2016.