

面向消费领域的 eSIM 安全威胁及应对措施研究

Research on Consumer-Oriented eSIM Security Threats and Countermeasures

刘 觅, 李佳俊, 衣莉莉, 王海涛(联通华盛通信有限公司, 北京 100032)

Liu Mi, Li Jiajun, Yi Lili, Wang Haitao(Unicom Vsens Communications Co., Ltd., Beijing 100032, China)

摘 要:

eSIM 技术凭借远程配置和多 Profile 管理这 2 个特点, 已逐步应用于移动通信消费电子领域, 增加了用户使用通信设备的便利体验, 也推动了消费电子智能化进程。该技术在场景应用落地的同时也面临着诸多安全方面的挑战。对 eSIM 的安全机制及相应安全风险进行了系统分析, 分别从终端、系统、业务和数据 4 个层面提出安全提升措施, 涵盖 APP 签名检查、一单一码机制、机卡绑定、传输加密及业务规则规范化等可执行方法, 提升了 eSIM 业务的整体安全性, 也抑制了 eSIM 相关的电信诈骗事件发生。

关键词:

eSIM; 安全风险; 反电信诈骗; 机卡绑定; 安全提升

doi:10.12045/j.issn.1007-3043.2026.09.005

文章编号: 1007-3043(2026)09-0026-06

中图分类号: TN918

文献标识码: A

开放科学(资源服务)标识码(OSID):



Abstract:

Relying on remote provisioning and multi-Profile management, eSIM technology has been gradually applied in the consumer electronics of mobile communications. It not only improves users' experience of using communication devices, but also drives the intelligent evolution of consumer electronics. Meanwhile, as eSIM technology is put into practice across various scenarios, it also faces numerous security challenges. A systematic analysis of the security mechanisms and corresponding security risks of eSIM is conducted, and security enhancement measures are proposed from four dimensions: terminal, system, service and data. These measures include executable methods such as APP signature verification, one-order-one-code mechanism, device-eSIM binding, transmission encryption and service rule standardization, which not only improve the overall security of eSIM services, but also curb telecom fraud related to eSIM.

Keywords:

eSIM; Security risk; Anti-telecom fraud; Device-eSIM binding; Security enhancement

引用格式: 刘觅, 李佳俊, 衣莉莉, 等. 面向消费领域的 eSIM 安全威胁及应对措施研究[J]. 邮电设计技术, 2026(9): 26-31.

0 引言

eSIM 技术应用正进入快速发展阶段, 目前全球超过 400 家电信运营商已正式支持 eSIM 相关服务^[1]。在消费类电子范畴中, eSIM 技术已逐渐渗透各类消费类电子产品, 路由器、智能手表、平板电脑等终端都已陆续采用 eSIM 技术作为通信功能的基础^[2]。采用 eSIM 技术的智能手机已规模化应用, 为国内 eSIM 的发展提供了强有力的参考与指引^[3]。

eSIM 技术在落地应用时, 逐步显现出诸多安全问题, 遇到了众多安全困扰。不法分子借助 eSIM 技术和场景的特性实施了多种违法行径, 凭借将 eSIM 转化为实体 SIM 卡、盗用 eSIM 通信套餐资源、远程开户、截取 Profile 等做法实施电信诈骗活动^[4], 造成用户的财产损失, 不利于社会的稳定。

因此, 在推进 eSIM 技术的运用、挖掘 eSIM 应用场景的同时, 必须构建与 eSIM 技术应用场景、业务流程契合度高的安全防护能力。本文聚焦面向消费领域的 eSIM 应用, 全面剖析当前 eSIM 技术应用所面临的主要安全风险, 重点分析 eSIM 安全技术、业务流程、数

收稿日期: 2026-07-16

据管理等方面的内容,给出具备实操性与落地可行性的安全提升方案,采用技术、业务跟管理相结合的举措,缓解 eSIM 所面临的安全风险,为 eSIM 技术的有序发展提供可靠的安全后盾。

1 eSIM 业务概述

eSIM 是将传统 SIM 卡功能嵌入到终端设备的嵌入式通用集成电路卡(eUICC)中的通信服务模式。该技术支持将用户通信鉴权等关键电信卡数据(称为 Profile)远程下载到终端 eSIM 中^[5],进而实现语音、短信以及数据等基础通信功能。凭借单张 eSIM 卡支持多 Profile 这一特性,用户可在不同网络中灵活切换,极大改善了网络选择的便利性和使用的体验^[6]。

eSIM 业务生态主要由 GSMA、运营商、终端厂商以及芯片制造厂商与卡商等组成。其中,GSMA 承担制定 eSIM 相关技术标准的工作,实现安全机制与身份认证流程的统一;运营商承担 Profile 生成、用户开户、网络鉴权以及业务运营等工作,完成对 eSIM 全生命周期的统筹管理;终端厂商从事设备研发生产、eSIM 卡集成相关工作,完成终端设备管理及移动通信网络接入;芯片厂商与卡商供应安全的 eSIM 卡,保证电信卡数据的安全存储与运用。eSIM 业务涉及核心通信鉴权数据的生成、传递、下载、留存,以及用户开通、启用等各个阶段,各个环节都可能遭到安全上的威胁,面临安全隐患。

2 面向消费领域的 eSIM 技术框架

如图 1 所示,eSIM 总体技术框架由 eSIM 设备、eSIM 卡、eSIM 管理平台、ES 授权服务器、WS 签约服务器以及 cBSS 组成。

a) eSIM 卡:嵌入式 SIM 卡,以 JavaCard、GP 技术为

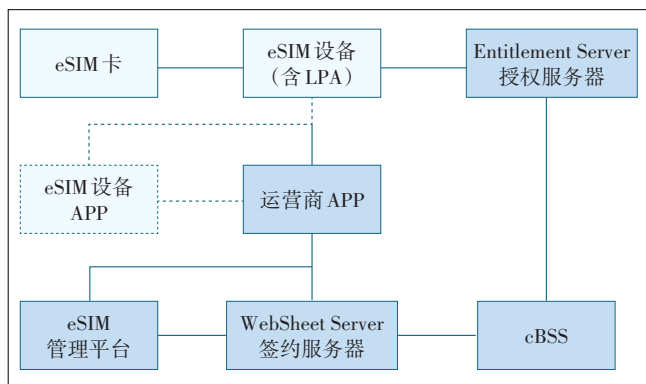


图 1 eSIM 技术框架

基础,安全存储卡数据,提供用户通信网络鉴权能力。

b) eSIM 设备:安装有 eSIM 卡的设备终端,在开户成功后,从 eSIM 管理平台下载卡数据至 eSIM 卡,下载后具备语音及短信等电信功能。

c) eSIM 设备 APP:部分 eSIM 消费电子设备,如可穿戴设备,使用 eSIM 设备 APP 获取 IMEI、EID 等关键信息。

d) eSIM 管理平台:负责 eSIM 电子卡数据的生成,并为 eSIM 终端提供下载服务。

e) Entitlement Server(ES 系统):负责向 eSIM 设备终端提供鉴权和授权服务,接收来自 eSIM 设备终端的用户套餐余量、套餐计划等业务查询、套餐订购请求和特定业务开通请求。

f) cBSS:负责接收 ES 的业务查询及业务开通请求,并将签约信息返回给 ES;负责接收 ES 发送的特定业务开通请求。

g) WebSheet Server:负责具体的用户业务签约开通。

3 eSIM 安全机制

3.1 总体开通流程

eSIM 总体开通流程如图 2 所示。

a) 用户触发操作,并进行用户认证,选择卡号与资费。

b) 用户在 LUI 中触发添加电子卡的操作。

c) LPA 获取下载所需参数,LUI 获取激活码(如手动输入、自动填充或扫描 QR 码)^[7]。

d) 执行电子卡下载流程,下载电子卡。

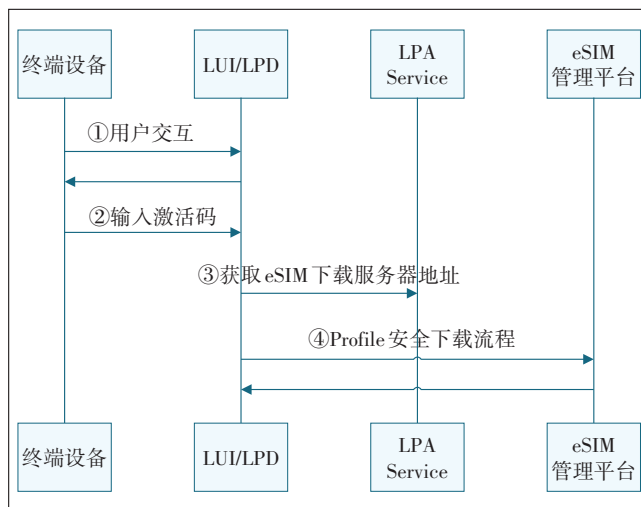


图 2 eSIM 总体开通流程

3.2 安全机制

eSIM 由于采用公众网络进行数据传输, 面临 Profile 数据泄漏、窃取、篡改等安全风险。GSMA 从多种技术层面制定了安全标准, 以保障 eSIM 数据在下载、存储等环节的安全性^[8]。

3.2.1 加密技术

在通信协议层面, eSIM 管理平台服务器采用 TLS 加密协议和证书认证与设备进行通信。在 Profile 传输层面, 采用国际标准的加密算法对数据进行加密, 并采用哈希算法对 Profile 数据进行摘要计算和完整性保护。在存储保护层面, 使用 eSIM 卡芯片硬件级安全模块, 对电信卡关键数据进行加密存储。

3.2.2 认证机制

RSP 标准要求体系里的各实体必须通过 GSMA 所定义的安全认证, 保障参与 eSIM 生产、管理、安装、使用等阶段的所有实体都是可信的。

采用挑战—响应机制, 设备跟运营商依靠共享密钥完成身份验证, 防止未被批准的设备访问 eSIM 相关管理系统, 保障只有合法设备才可以下载、安装 Profile。

在 eSIM 开户过程中, 采用双因素或多因素认证方式对用户身份进行认证, 如身份证件与人脸比对等相结合的方式。

通过本地 Profile 下载 (LPD) 和本地用户接口 (LUI) 等组件, 对 eSIM 配置文件下载和安装进行管控。

3.2.3 eSIM 卡

如图 3 所示, eSIM 卡采用标准的 Javacard+GP 架构, 包含平台层、GP 框架层和应用层^[9]。其中, 平台层

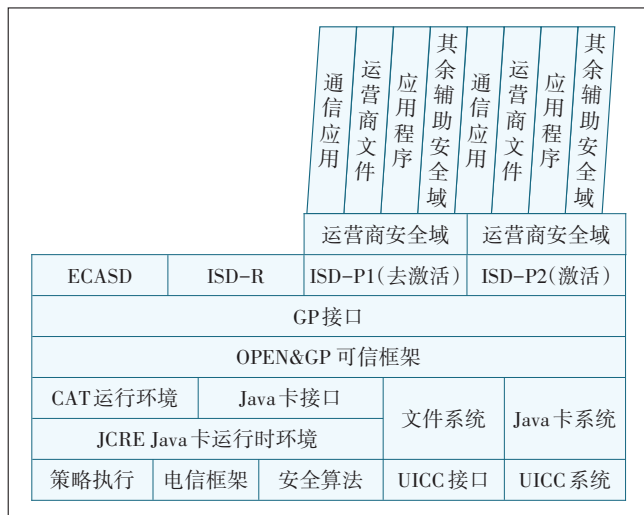


图 3 eSIM 卡技术架构

包含 CAT 运行环境、Java 卡接口、JCRE Java 卡运行时环境等模块; GP 框架层包含 OPEN&GP 框架、GP 相关 API 接口等; 应用层包含 ECASD、ISD-R、运营商安全域等, 以及装载于运营商安全域内的行业应用、扩展应用等模块。

eSIM 卡通过上述技术架构实现 GP 安全域配置、生命周期管理、权限管控、安全通道等能力, 以及上层 JavaCard 应用的安全管理。

3.2.4 证书链

消费领域 eSIM 业务体系中的 PKI 证书系统分为根证书、卡商证书和 eUICC 证书 3 个级别^[10] (见图 4)。其中, 根证书为自签名证书, 是整个 eSIM 信任链的起点。卡商证书又称 EUM 证书, 由根证书签发, eUICC 证书由卡商证书签发。其他如 TLS 等证书也由根证书签发, 所有证书均为 X.509 格式。

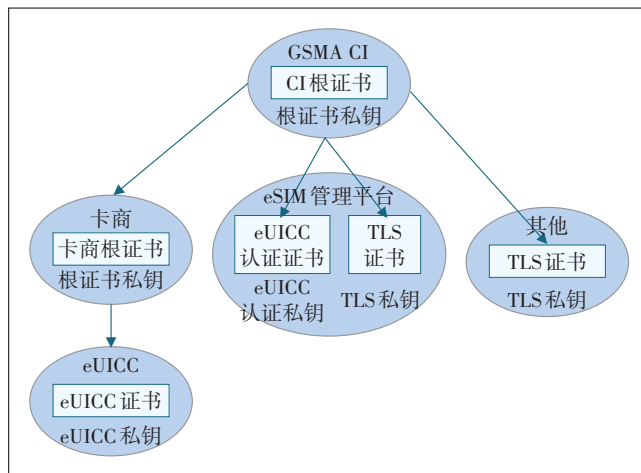


图 4 eSIM 证书链

在进行证书验证时, 对签发者进行逐级认证, 直到根证书。根证书验证通过自身公钥对其签名信息进行验证, CA 证书验证通过根证书的公钥对证书签名进行验证, 用户证书验证通过对应 CA 证书的公钥对证书签名进行验证。

4 eSIM 安全风险与安全提升措施

4.1 eSIM 安全风险

虽然 GSMA 针对 eSIM 安全定义了一整套安全架构, 运营商也针对 eSIM 安全制定了相应的安全业务规则以及技术方案, 但随着技术的发展, eSIM 安全仍然面临新的安全风险, 重点安全风险如下。

4.1.1 终端设备风险

4.1.1.1 芯片拆解涉诈风险

在运营商 APP 等线上自有渠道办理 eSIM 业务时,一般没有实体卡片核验环节。不法分子可通过购买廉价 eSIM 设备,拆解终端设备和 eSIM 卡芯片,再封装成实体 SIM 卡并插到 GOIP、猫池等诈骗终端,来批量获取诈骗通信基础设备,形成诈骗号码池实施诈骗,影响用户财产安全。

4.1.1.2 机卡分离模型风险

大多运营商会建立机卡分离模型,即通过运营商的后台判断用户使用的设备与卡是否为开户时在后台绑定的对应设备和卡,并通过模型分析用户的使用特性,判断是否为风险场景,从而决定是否实施通信控制。

此种方式仅在开户时校验 eSIM 与终端的绑定关系(EID/IMEI 匹配),机卡分离模型的判断具有一定滞后性,即用户通话话单形成后才触发机卡分离模型判断。用户使用时,传统机卡分离监测模型难以实时获取终端信息,无法及时判断终端与 eSIM 卡是否分离,如果 eSIM 卡芯片被移植至其他设备进行诈骗,将错过制止涉诈事件发生的黄金时间。

4.1.1.3 数据篡改绕过风险

运营商 APP 与 eSIM 终端在交互数据等信息时,会传输 EID、IMEI、激活码等关键信息,部分设备可能会被 Root,从而导致传输数据被篡改使用。例如,将黑名单终端的 EID、IMEI 伪装成合法终端的 EID、IMEI,或者拦截激活码转发至其他设备实现“一码多机使用”。并且单个 Root 设备可批量生成虚假终端信息,溯源追踪时难以定位真实终端。

4.1.2 APP&EID 伪造风险

在部分 eSIM 消费电子业务场景中,用户通过运营商 APP 开通 eSIM 通信业务时,运营商 APP 需依赖终端厂商提供的 APP 相关功能接口,以获取设备的 EID、IMEI 等关键信息^[11]。

攻击者可通过开发伪造终端的厂商 APP,模拟合法终端 APP 的通信行为,向运营商 APP 传输虚假的设备信息。

在 eSIM 业务全生命周期中,从 Profile 数据生成、用户下载 Profile 到网络鉴权,EID 都是核心关联数据。若 EID 被伪造,攻击者可骗取运营商向伪造 EID 对应的设备下发本属于其他用户的 Profile,导致合法用户的 eSIM 业务无法正常使用,而伪造设备则可冒用他人身份接入网络,造成流量套餐、号码权限被盗用。

若多台设备使用相同的伪造 EID,当其中一台设备出现违规行为时,运营商无法通过 EID 定位真实设备,导致责任追溯失效,或误判合法用户为违规者。

4.1.3 传输入侵风险

eSIM 电子卡数据的下载地址是与用户业务订单绑定的固定值,用户在营业厅办理 eSIM 业务时,该地址会生成对应的二维码,用户通过运营商 APP 扫描二维码即可触发 Profile 下载。

用户在办理业务时,若二维码被他人拍照、截屏,或营业厅工作人员违规泄露,不法分子可在远程异地扫描该二维码,实现远程开户实施诈骗^[12]。

4.1.4 信息篡改风险

在 eSIM 业务办理的操作阶段,各系统之间需要传递 EID、IMEI、用户信息、设备参数等关键数据,部分运营商采用明文方式传输这个数据,造成数据在公众网络的环境里暴露,即使用 TLS 等传输协议实施数据传输,攻击者也可凭借中间人攻击等手段截取所传输的数据,获取并篡改用户的 EID、设备信息等敏感数据,进而实施非法活动。

4.2 eSIM 安全提升措施

在 eSIM 业务应用落地过程中,采用技术防护措施是抵御上述风险的核心防线,需从终端、系统、卡方面建立一体化的安全措施,以下是 3 类重点安全技能提升措施。

4.2.1 终端安全提升

APP 安全校验是针对终端 APP 伪造、信息明文传输风险的专项安全提升措施,确保运营商 APP 与终端厂商 APP 之间通信的真实、可信。

APP 签名是由开发者使用专属的数字证书对 APP 进行签名生成的唯一标识,相当于 APP 的“数字身份证”。运营商 APP 在与终端 APP 通信前,先校验其签名的合法性,仅通过校验的 APP 才能建立通信,从源头杜绝伪造 APP 接入。其具体实现步骤如下。

a) APP 签名值备案。终端厂商将其官方 APP 的签名值提交给运营商,存入运营商的可信 APP 签名库。

b) 通信前签名校验。运营商 APP 发起通信请求时,先向终端 APP 发送自身的签名信息,含签名证书和 APP 包名。

c) 终端 APP 校验运营商 APP 签名。对比内置的运营商官方签名公钥,确认对方为合法运营商 APP,防止伪运营商 APP 骗取设备信息。

d) 终端 APP 响应时,向运营商 APP 发送自身的签

名信息,含签名值和APP包名。

e) 运营商的应用程序校验终端厂商应用的签名。运营商系统后台查询可信APP签名库,认定终端厂家APP签名为可信的APP签名,而且终端厂家APP的版本是正确的版本,若终端厂家APP签名值与版本不匹配,直接拒绝后续的交互。

f) 防御签名信息被篡改。当双方开展校验的时候,APP签名信息需采用散列、加密等途径进行加固,防止攻击者将签名信息篡改后绕过校验。

4.2.2 系统安全提升

4.2.2.1 一单一码

如前述,激活码(Activation Code)是由运营商提供给用户的数据,用来请求卡数据的下载安装^[13],按照GSMA规范要求,其定义如表1所示。

表1 eSIM Profile 下载激活码格式

名称	是否必须	描述
AC_Format	是	激活码格式
分隔符	是	设为“\$”
eSIM下载服务器地址	是	eSIM下载服务器的英文域名
分隔符	是	设为“\$”
AC_Token	是	-
分隔符	否	下列字段存在时出现并设为“\$”
eSIM下载服务器编号	否	CERT.DPauth.ECDSA中的编号
分隔符	否	下列字段存在时出现并设为“\$”
确认码标识符	否	存在确认码并需要用户输入时出现并设为“1”

在用户业务办理过程中,生成激活码时,针对确认码标识符这一数据项,不再为默认的缺省值,而是由eSIM管理平台动态生成。其设计原则为一次业务订单对应一个唯一、临时、不可复用的下载凭证,将Profile下载地址与用户的具体业务订单号深度绑定,从而实现下载激活码的时效性、唯一性、关联性三大特性,确保仅合法用户的指定设备能完成下载。

原有激活码示例为:1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815(不存在确认码标识符),升级后激活码格式为:1\$SMDP.GSMA.COM\$04386-AGYFT-A74Y8-3F815\$1.3.6.1.4.1.31746\$1(存在确认码标识符)。

安全设计原则如下。

a) 订单关联性。动态激活码与订单强绑定,一个订单仅存在一个有效激活码,且无法被用于其他订单的Profile下载。

b) 时效性。激活码有效期设为短时效(如3~5 min),超时后自动失效,需用户重新申请生成,避免二维码被长期留存盗用。

c) 设备关联性。仅允许与提交订单时关联的设备扫描,其他设备扫描后,运营商APP会校验EID不匹配,直接拒绝下载请求。

d) 有效性。当设备成功完成Profile下载后,系统立即标记该动态下载码“已使用”,避免重复下载导致的Profile滥用。

4.2.2.2 传输数据加密

针对APP间数据明文传输的风险,对EID、固件版本、设备序列号等终端关键信息和激活码等关键数据进行加密传输,具体安全设计如下。

a) 协议选择。采用TLS1.3协议建立通信通道传输数据。

b) 提高数据加密强度,在使用TLS传输加密的基础上,运用运营商与终端厂商预先商量好的非对称密钥对EID等关键数据进行二次加密,形成双层加密模式,进一步增进安全性。

c) 实施数据完整性校验,开始传输数据时同步生成消息认证码,接收方借助MAC验证数据有无被篡改,若校验结果失败,则拒绝后续交互。

4.2.2.3 端卡协同安全提升

机卡绑定是阻止电信涉诈分子利用eSIM设备进行异地电信诈骗的最有效手段。通过将eSIM的唯一标识(EID)与设备的硬件唯一标识(IMEI/MEID)深度绑定,实现“一机一卡一身份”,彻底杜绝EID伪造,拆除移用等风险。其实现原则为终端设备和eSIM卡物理上不可分离,即终端设备与eSIM卡双重绑定。

eSIM终端与卡状态转换示意如图5所示,具体安全设计如下。

a) 未做机卡绑定的eSIM处于eSIM初始状态,可以接收合法终端的机卡绑定指令。

b) 终端和eSIM开始机卡绑定流程,绑定成功的

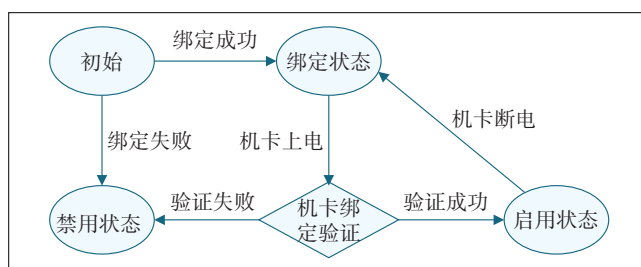


图5 eSIM终端与卡状态转换示意

卡进入 eSIM 绑定状态,如果绑定失败,达到最大重试次数的 eSIM 将进入禁用状态且不允许重试。

c) 绑定成功的卡并不能直接使用,在每次重新上电时,主动通知终端或等待终端查询当前状态,然后由终端发起机卡校验操作。达到最大重试次数后,eSIM 进入禁用状态。如校验成功,eSIM 进入启用状态,开放所有功能。

d) 处于启用状态的 eSIM 在断电重启后,重新进入绑定状态,等待机卡校验。

4.2.3 业务安全提升

业务安全是构建整体安全防护体系的重要防线。eSIM 的安全保障不仅依赖技术手段,还需通过严格的业务安全管理措施予以支撑和约束^[14]。

4.2.3.1 终端合法性管控

仅允许已在运营商 eSIM 终端库中完成备案的合法终端办理业务。终端设备须通过工信部进网认证,eSIM 卡须符合 EAL4+ 安全认证等级及 GSMA 相关标准。

4.2.3.2 虚拟位置与异常网络拦截

运营商 APP 实时检测并禁止在网络代理或 VPN 等非可信网络环境下进行业务办理。同时,通过地理定位限制 eSIM 卡数据仅可在中国大陆地区下载,防范伪装位置非法开户。

4.2.3.3 增强活体检测安全机制

采用“灵动炫彩活体识别”技术,结合前端“动态炫彩光效与多模态动作检测”与后端基于 CADDMM 的深度伪造防御算法,有效识别并预警外接摄像头、视频流篡改等攻击行为。

4.2.3.4 开户历史与跨省操作管控

首次开户仅限线下自有营业厅办理,非首次开户需校验历史订单信息。依托高危跨省风险模型,对存在“他省办理记录异常”或“EID 多地频繁绑定”等行为的终端实施管控^[15],限制异常设备办理业务。

4.2.3.5 完善特殊客户身份核验流程

特殊客户群体如政企客户批量开户后,实际使用人须至归属地自有营业厅,凭有效身份证件完成真实性核验及人证一致性比对,通过后方可激活号码,全面防范“虚假企业+冒名使用”风险。

5 结语

在移动通信消费电子领域,eSIM 技术应用已成为产业发展不可逆转的趋势,但其全面推广始终受安全

威胁这一关键因素的制约。本文聚焦 eSIM 终端安全、系统安全以及业务安全三大核心风险维度,针对性提出了安全能力提升措施。为稳步推进 eSIM 技术规模化应用,需持续完善 eSIM 安全体系建设,可分阶段推广 eSIM 应用,前期聚焦满足机卡绑定的特定终端,在运营商线下营业厅风险可控的情况下办理 eSIM 业务,后期随着推广范围的逐步扩大,同步优化安全认证流程与风险防控机制,强化跨部门、跨产业链的安全协同联动,实现全面线上办理 eSIM 业务,最终推动移动通信消费电子产业智能、安全、便捷发展。

参考文献:

- [1] 中国信通院泰尔终端实验室. eSIM 产业热点问题研究报告(2025 年)[R]. 北京:中国信通院,2025.
- [2] 周迅,李敏. 基于 eSIM 卡上送交通卡交易数据的稳定性和安全性的应用研究[J]. 江苏通信,2025,41(1):38-42,64.
- [3] 杨旸,臧楠棋. eSIM 技术的现状与发展前景[J]. 数字通信世界,2019(2):126.
- [4] 罗晓哲. eSIM 卡空中写号技术发展与安全问题分析[J]. 数字通信世界,2019(8):60,37.
- [5] 黄海昆. eSIM 及其远程配置技术与应用[J]. 电信科学,2016,32(9):162-167.
- [6] 云铸. eSIM 优势与瓶颈分析研究[J]. 数字通信世界,2021(1):49-50.
- [7] 贾丰庸,桂烜,杨剑. 面向消费电子 eSIM 的 LPA 技术研究[J]. 广东通信技术,2018,38(6):49-52.
- [8] 仇剑书,康建雄,严斌峰. eSIM 安全性分析及实现方案研究[J]. 互联网天地,2016(11):5-9.
- [9] 黄健,黄健文,李俊磊,等. eSIM 卡安全架构研究[J]. 信息技术与网络安全,2018,37(3):53-56,60.
- [10] 李宏平,孟玉明,张立星,等. PKI 数字证书在 eSIM 安全上的应用研究[J]. 信息通信技术,2018,12(6):34-39,55.
- [11] 王光旭. 手机号码绑定 APP 的安全问题研究[J]. 网络空间安全,2018,9(10):83-86.
- [12] 卢丹,吴宏建. eSIM 卡空中写号技术发展与安全问题分析[J]. 电信网技术,2016(2):1-6.
- [13] 胡博,严斌峰,仇剑书,等. 面向产业互联网 eSIM 终端的激活方案研究[J]. 信息技术与网络安全,2019,38(2):26-28,45.
- [14] 张珊,曾俊华.《反电信网络诈骗法》下电信运营商的合规风险及应对策略[J]. 法制博览,2024(30):46-48.
- [15] 张柳凤,李凡,吴晓姝. 信息化背景下电信运营商的反诈骗系统设计研究[J]. IT 经理世界,2024(8):109-111,127.

作者简介:

刘觅,高级工程师,硕士,主要从事电信卡技术及安全管理工作;李佳俊,正高级工程师,博士,主要从事移动通信终端技术及管理;衣莉莉,高级工程师,硕士,主要从事智能卡技术管理工作;王海涛,高级工程师,硕士,主要从事智能卡技术相关工作。