基于超级 SIM 卡内生安全的标识在线分发系统设计

綦振禄 [1]
QI Zhenlu

摘 要 针对传统在线证书分发系统中存在的终端身份认证强度不足、证书传输易被窃篡改、私钥存储安全风险高等问题，文章设计实现了一种基于超级 SIM 卡内生安全的标识在线分发系统，以超级 SIM 卡的硬件安全模块为可信根，构建标识在线分发中“终端 - 传输 - 云端”的三级安全防护体系，实现标识文件的安全分发与存储，有效抵御传输篡改、存储泄露、非法认证等攻击，可满足高并发与低延时的安全认证要求，为解决在线证书分发的“最后一公里”安全问题提供有效技术路径。

关键词 超级 SIM 卡；在线发证；SM9 标识分发；VPN 身份认证；数据安全传输

doi：10.3969/j.issn.1672-9528.2026.05.033

0 引言

随着数字化在工作、生活中的普及，在数字化网络空间上，在线证书作为重要的信任基石，已经广泛应用于金融交易、公共安全等关键领域。通过调研发现传统的在线证书分发机制，通常是采用用户名 + 密码组合或软证书进行身份认证，这种简单的验证方法当前极易遭受暴力破解、钓鱼攻击、恶意软件窃取等威胁。并且证书若采用明文传输或简单的加密策略，在传输过程中，被其他人非法截获，被破解后，对方就可以伪装成合法用户，进入系统，以合法身份窃取用户数据，用户数据安全面临严峻挑战 [1]。

超级 SIM 卡是在通用的 SIM 卡基础上，内置符合国密标准支持硬件加速密码运算的硬件安全模块，内部增加了加密存储空间用来存储密钥等重要信息，存储空间采用物理防护策略，并且具有访问控制、安全审计等软件保护措施。

近年来，超级 SIM 卡在身份认证、加密通信领域应用不断拓展，各大运营商都基于超级 SIM 卡进行大规模的研发投入，建设基于超级 SIM 卡的可信认证平台，实现手机号、实体卡、证书文件三者绑定认证。其中中国移动通过自己的高可信平台为超过 5 000 万的企业用户提供身份验证服务 [2]；中国联通也在物联网场景中，利用超级 SIM 卡的内生安全机制，为用户的终端设备提供有效身份验证与数据传输安全 [3]。当前，针对超级 SIM 卡的研究主要侧重于身份认证机制优化、通信加密算法适配，而基于超级 SIM 卡的在线证书分发应用的系统性研究却极为少见 [4-5]。

另一方面，随着物联网设备的规模化普及，其异构化部署特性与轻量化安全需求之间的矛盾日益凸显。传统公钥基础设施（PKI）依赖的数字证书体系，需通过证书权威机构（CA）、注册机构（RA）等多节点协同完成证书签发与验证，存在密钥管理链路长、终端存储开销大、跨域认证兼容性差等问题，难以适配海量低功耗物联网设备的安全需求 [6]。为此，本研究引入标识密钥体系（IBC）替代传统数字证书体系，以用户唯一标识作为核心索引，在标识注册系统中基于 SM9 国密标识密码算法，直接生成与该标识绑定的非对称公私钥对。这种“标识即公钥”的认证模式，不仅省去了证书申请、吊销、更新等管理环节，降低了密钥资源的运维成本与部署复杂度，还能通过标识与设备 / 用户身份的强绑定，实现“一次注册、多域通行”的跨场景认证能力。

本文通过深入研究超级 SIM 卡内生安全能力，结合 SM9 密钥管理方案，设计了一套基于超级 SIM 卡的标识在线分发的专用系统，文中作者结合自身的专业基础，对系统架构、关键技术实现进行了详细阐述，通过实验方法验证系统性能与安全性，提出了一种解决在线证书分发安全性难题的新路径。

1 超级 SIM 卡空中发证技术

本文设计的超级 SIM 卡安全认证系统，核心依托 3GPP 5G 通用引导架构（GBA）技术，构建 PKI 数字证书空中分发机制。系统以集成嵌入式安全元件的超级 SIM 卡为可信硬件载体，凭借 eSE 的物理隔离与加密能力实现密钥、证书等敏感信息安全存储，同时借助 5G 网络电信级安全认证体系，将证书通过可信通道分发至 SIM 卡，最终通过标准化接口为移动终端提供传输加密、身份认证、免密登录等安全服务，解决传统软证书“存储不安全、传输易劫持”的核心问题。

超级 SIM 卡之所以能实现安全空中发证，关键在于其集成多维度核心能力，具体如下：

1. 公安部第一研究所 北京 100048

（1）GBA 认证支撑：作为 3GPP 标准网络安全技术，GBA 可依托超级 SIM 卡内置用户签约数据，与运营商认证中心完成双向认证并生成会话密钥，为“终端 - 云端”建立端到端安全信道，保障证书分发等业务的认证安全性。

（2）BIP 协议适配：BIP 是一种由 3GPP 定义的面向连接传输协议，该协议不受传输载体的限制，实现远程服务器与终端上的 SIM 卡进行直接数据交互，解决了采用传统短消息承载证书时“符号量受限、安全性差”的问题。

（3）多 API 接口兼容： SIM 卡遵循 GP 与 3GPP 规范，提供多种 API 调用接口，用户应用可通过 API 接口与 SIM 卡进行数据交互，降低跨系统适配成本，极大提升系统灵活度。

（4）硬件级加密覆盖：eSE 安全芯片内置加密引擎，既支持国密算法，也兼容国际通用加密算法，通过硬件级加密避免密钥暴露，保障证书相关操作安全，满足不同场景加密需求。

此外，超级 SIM 卡还集成存储隔离、访问权限管控、防克隆等辅助安全机制，形成全链路防护体系，进一步保障安全应用可用性。

图 1 所示系统的基本工作流程：

（1）安全信道建立：用户终端加电后，超级 SIM 卡通过 4G/5G 网络触发 GBA 认证，完成双向认证并生成会话密钥，建立“SIM 卡 - 证书分发系统” 加密信道；第三方应用通过标准 API 将证书申请请求经该信道发送。

（2）证书请求与生成：证书分发系统验证请求合法性后，向证书管理系统发起证书申请；证书管理系统按策略生成数字证书，通过安全通道传输至证书分发系统。

（3）证书下发与存储：证书分发系统用 GBA 会话密钥加密证书，通过 BIP 协议下发至终端；终端将数据转发至超级 SIM 卡，由 eSE 解密并存储于安全分区，最终 SIM 卡向应用返回“证书就绪”通知，流程结束。

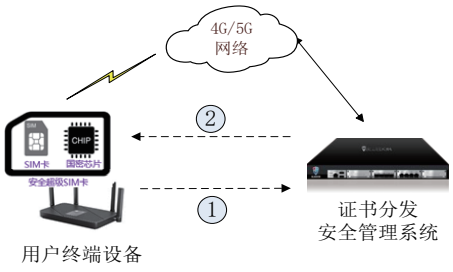

图 1 超级 SIM 卡证书分发系统

2 SM9 密钥管理技术体系

基于 SM9 密码体系的密钥管理系统包含标识注册机构（RA）、私钥生成系统（PKG）、公开参数服务器（PPS），以及用户的终端设备（TE）。基于 SM9 的 KMS 系统框图如图 2 所示。

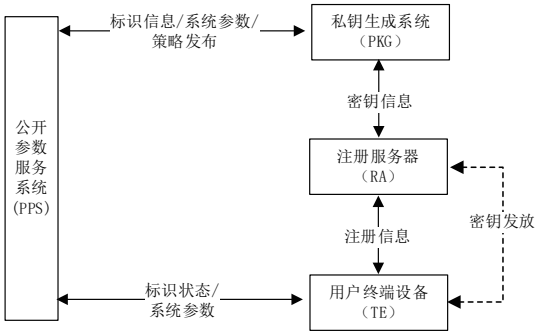

图 2 密钥管理系统框图

图 2 中各功能模块实现的任务：

（1）RA 功能模块，接收并审核用户注册信息，审核通过后向 PKG 提交申请，生成密钥，并将密钥导出给用户。

（2）PKG 功能模块，接收 RA 的信息，生成密钥标识文件。

（3）PPS 功能模块，用于用户信息查询，包含用户标识状态、密码参数等。

（4）用户终端实体，提供注册信息，接收密钥。

从图 2 可以看出，SM9 密钥系统中关键任务是密钥分发步骤。以往的离线式密码管理系统流程，用户通过 RA 导出私钥文件到存储载体，再通过存储载体将私钥文件导入用户终端设备。当对于海量的终端用户时，必然耗费大量的人力时间成本，而且当用户终端与密码系统比较分散时，存在存储载体移交过程中数据泄露问题。并且这种离线方式的密钥导入机制，不利于后续密钥到期更新操作。因此需要设计一种安全有效的在线私钥分发机制，以应对具有海量终端用户安全接入的需求。

3 系统方案设计

在第三方 VPN 的实际应用场景中，身份认证强度不足与数据传输安全性低是两大核心痛点——前者常表现为传统账号密码认证易被暴力破解、动态令牌存在中间人攻击风险，后者则因部分 VPN 采用的对称加密算法密钥协商环节薄弱，导致数据在传输过程中面临被窃取、篡改的威胁。为此，本设计方案针对性引入基于 SM9 国密标识密码算法的密码认证体系，通过算法的标识特性与加密能力，同时实现第三方 VPN 的双向身份认证与端到端数据加密传输，从根本上解决上述安全隐患。

通过以上论述可知，公钥生成机制是基于 SM9 算法的标识密码体系与传统 PKI（公钥基础设施）体系的主要差异。传统 PKI 体系由证书授权中心（CA）为用户公钥签发数字证书，在身份认证阶段，用户需通过证书验证公钥归属与有效性；而基于 SM9 算法的密码体系以用户 ID 作为生成公钥的依据，用户 ID 通常可以是终端设备的硬件序列号、板载

通信模块的 IMEI 码、硬件网卡的 MAC 地址等，但必须保证在本系统中是唯一的标识 ID。SM9 密钥系统可通过这个唯一标识 ID 直接计算出用户公钥，没有额外的证书授权环节。这在第三方 VPN 系统中具有极高的应用价值：一方面，在 VPN 接入时省去了复杂的证书管理流程，无需搭建证书授权中心，也无需用户接收证书、保存证书；另一方面，无需担心传统 PKI 体系中因证书过期未更新、证书吊销同步延迟、证书损坏等问题导致的 VPN 认证失败，保障了 VPN 接入的稳定性与连续性。

在 SM9 密钥管理体系中，标识管理系统在整个安全架构中承担极其重要的角色，它负责核心密钥产生与结构化标识文件打包的关键步骤，其运作机制严格执行国家密码技术标准，确保密钥与凭证的安全性：第一步，标识管理系统预先生成 SM9 全局主公钥参数；第二步，用户终端向标识管理系统提交注册申请，标识管理系统利用用户 ID，通过 SM9 密钥派生算法生成该终端的用户私钥；最后，系统将系统公钥、用户私钥、标识属性元等数据封装为标识文件。该标识文件并非简单的信息组合，而是具备多重功能的安全凭证：其中包含的用户私钥与用户 ID 可用于验证终端身份合法性；并且在后续 VPN 会话的加密运算中，系统公钥与用户私钥可直接作为密钥载体使用；标识属性元数据可作为权限管控依据在 VPN 接入流程中的多个环节进行验证操作。

其中分发系统的核心任务是依托超级 SIM 卡的内生安全能力，将该标识文件安全可信地分发至目标用户终端，确保整个分发过程中私钥不暴露、文件不被篡改。具体设计框架如图 3 所示。其中用户 VPN 标识管理系统负责验证标识密钥请求的合法性，并按策略生成密钥，存储在本地。证书分发安全管理系统负责用 GBA 会话密钥加密证书，通过 BIP 协议下发至终端。终端设备负责将密钥数据转发至超级 SIM 卡，由 eSE 解密并存储于安全分区。用户业务 VPN 网关负责在用户终端设备和业务服务器间建立一条 SSL 隧道，保证业务数据安全。

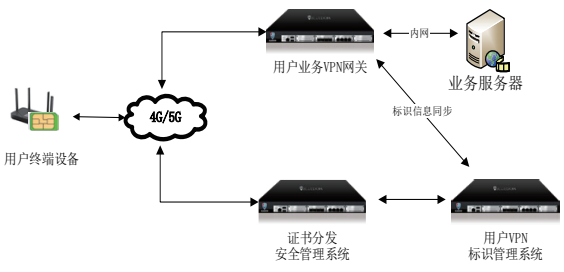

图 3 基于超级 SIM 卡内生安全的标识在线分发系统架构

4 流程设计

4.1 标识注册设计

标识注册是确保 SM9 标识合法性的前置环节。用户登录至标识管理系统进行标识注册，提交申请人信息、设备信息、标识信息、使用范围等信息，申请签发 SM9 标识密钥。标识管理系统核验通过后，标识管理系统基于 SM9 算法的主公钥参数与用户标识，调用硬件加密模块生成用户私钥；同时将用户标识、私钥指纹、权限信息录入数据库备案，形成唯一的标识注册记录，供后续分发与审计查询。

4.2 标识分发流程设计

基于超级 SIM 卡安全通道的标识分发流程，需围绕“传输安全、存储安全、身份绑定”三大核心目标设计，覆盖从请求到应用的全链路，具体流程如下：

（1）标识请求

用户在终端设备上启动 SM9 标识申请客户端，客户端通过超级 SIM 卡的 API 接口触发标识请求流程：首先，超级 SIM 卡生成 16 字节随机数作为会话种子，结合卡内预置的根密钥，通过 SM4 算法生成临时会话密钥；随后，客户端通过 BIP 协议，将‘标识申请指令 + 用户终端 IMSI 号 + 随机数’封装为请求数据包，其中数据包头部采用 TLS PSK 协议握手，确保传输链路的双向认证与数据加密。该过程可有效抵御中间人攻击与重放攻击，保障申请指令的安全性。

（2）分发系统标识请求处理

SM9 标识分发系统接收到请求数据包后，首先通过 BIP 协议解析出核心数据，再启动双重验证机制：①身份验证：分发系统向运营商 AuC 发送超级 SIM 卡 IMSI 号与验证请求，AuC 返回基于 GBA 认证的身份验证结果，确认用户终端的合法性；②权限验证：分发系统查询标识管理系统的注册备案信息，验证该用户是否已完成标识注册、当前请求是否在权限有效期内。双重验证通过后，分发系统向标识管理系统发起标识文件获取请求，请求数据携带经 SM2 算法签名的分发系统身份证书，确保请求来源可信。

（3）标识管理系统标识检索与封装

标识管理系统接收到请求后，首先通过 SM2 公钥验证分发系统的签名合法性，验证通过后基于请求中的用户 IMSI 号与标识 ID，在数据库中检索对应的标识文件；为进一步提升传输安全性，系统采用“二次加密”策略：先用 SM4 算法对标识文件进行加密，再用 SM9 算法的系统公钥对 SM4 密钥进行加密，形成“加密标识文件 + 加密密钥”的双层加密数据包，避免单一加密算法被破解导致的文件泄露风险。随后将该数据包发送至分发系统。

（4）分发系统标识文件分发

在标识文件向用户终端的分发环节，流程核心围绕 “安全解密 - 格式适配 - 可靠传输”展开。

分发系统接收到从标识管理系统传来的双层加密数据包后，首先启动解密流程，该双层加密设计是为实现“密钥与文件分离保护”，外层通过 SM9 用户私钥解密，解密后获取

用于内层加密的 SM4 对称密钥；随后用该 SM4 密钥解密内层数据，最终还原出原始的 SM9 标识文件，确保文件在分发前始终处于加密保护状态，防止传输源头的数据泄露。

为确保标识文件能被超级 SIM 卡的 eSE 安全存储并调用，分发系统需对原始标识文件进行格式适配，按照 GlobalPlatform（GP）规范，将标识文件封装为 eSE 可识别的安全文件格式，该格式会明确文件的存储权限、数据结构，同时添加文件完整性校验字段，避免后续导入时因格式不兼容导致存储失败或文件损坏。

格式适配完成后，分发系统通过 BIP 安全通道将封装后的文件下发至用户终端：BIP 通道是超级 SIM 卡与网络侧交互的专用安全链路，其核心优势在于内置帧校验机制，每传输一帧数据，都会附加帧校验序列（FCS），终端接收后会重新计算帧校验值并与 FCS 比对；若比对不一致，终端会立即请求重传，有效避免因网络丢包、信号干扰导致的文件片段缺失或数据篡改，确保标识文件完整、无误地传输至用户终端，为后续 VPN 认证奠定基础。

（5）标识文件存储

用户终端接收到分发系统通过 BIP 通道下发的标识文件后，会立即启动安全导入流程，依托超级 SIM 卡的专用 API 接口，将文件完整转发至卡内的 eSE 模块，这一步跳过终端操作系统的开放存储区域，直接在硬件安全通道内传输，防止文件在终端本地被窃取或篡改。

eSE 接收到文件后，首要操作是验证文件签名，通过内置的 SM9 系统公钥，对文件附带的签名信息进行校验，确认文件确实来自合法的分发系统、未被非法篡改后，才进入后续存储环节；若签名验证失败，eSE 会直接丢弃文件并记录异常日志，从源头阻断非法文件注入。验证通过后，eSE 将标识文件存储于自身的专用安全分区，该分区采用物理隔离设计，且仅开放 SM9 算法的私钥调用接口，只有通过 eSE 预设的安全指令，才能触发标识文件的密钥调用，从硬件层面杜绝密钥泄露风险。同时，eSE 会自动记录文件存储日志，日志内容包括“文件接收时间、文件版本号、签名验证结果、存储分区编号”等关键信息，且日志采用只读模式存储，后续可通过企业管理平台调取日志进行审计查询，便于追溯文件存储过程中的异常行为，进一步保障标识文件的全生命周期安全。

（6）标识文件应用

当用户终端接入第三方 VPN 时，标识文件的应用流程如下：①客户端发起认证，携带服务器挑战值：用户触发 VPN 接入后，客户端与服务器建立临时链路，服务器生成 32 字节随机挑战值，附带服务器 ID、加密算法版本发送给客户端。客户端将挑战值、终端 IMEI、SIM 卡号转发给超级 SIM 卡，校验卡片与终端绑定关系。② SIM 卡调用标识文件，生成 SM9 签名：超级 SIM 卡校验终端绑定关系通过后，调用 eSE 内加密存储的标识文件，提取用户私钥，按 SM9 规范对挑战值签名，并加入卡片唯一硬件序列号，生成签名响应反馈给客户端。③客户端封装材料，发送至服务器：客户端封装“标识文件公钥 + 签名响应”，计算 SM3 哈希值防篡改，形成认证请求包，通过临时链路发送给服务器。④服务器验证签名，建立 VPN 隧道：服务器校验哈希值通过后，用 SM9 系统公钥验证签名，确认身份合法后生成 SM4 会话密钥，加密后发送给客户端。客户端用 SIM 卡私钥解密密钥，建立 VPN 加密隧道。⑤隧道通信，端到端加密：传输敏感数据时，客户端调用 SIM 卡私钥按 SM9 加密数据，服务器用户公钥解密，实现端到端安全传输，无需用户手动管理密钥。

5 结论

本文对超级 SIM 卡内生安全技术进行了深入研究，并提出了一套基于超级 SIM 卡内生安全的标识在线分发系统，利用其安全芯片级的密码防护和硬件存储能力，为标识密钥远程在线分发和存储提供了安全方案。通过安全性与性能实验验证，基于超级 SIM 卡的 SM9 标识在线分发系统可实现标识文件的安全分发与存储，有效抵御传输篡改、存储泄露、非法认证等攻击；同时在分发时延、VPN 接入效率、并发处理能力上表现优异，可满足第三方 VPN 等对安全性与实时性要求较高的业务场景需求。

参考文献：

[1] 中国网络空间安全协会 . 2023 年网络安全态势研判分析年度综合报告 [R]. 北京 : 中国网络空间安全协会 ,2024.

[2] 中国移动研究院 . 中国移动超级 SIM 卡技术白皮书 [Z]. 北京 : 中国移动研究院 ,2020.

[3] 中国联合网络通信集团有限公司 , 中讯邮电咨询设计院有限公司 . 安全超级 SIM 卡物联网应用技术规范 [Z]. 北京 : 中国联通集团 ,2022.

[4] 许锡明 , 庄严 , 杨汉坤 , 等 . 基于超级 SIM 卡的可信身份认证技术应用与探讨 [J]. 网络安全和信息化 ,2024(10):132-134.

[5] 庄仁峰 , 庄严 , 蒋周良 , 等 . 国密算法技术与超级 SIM 卡融合技术的研究与应用 [J]. 电信工程技术与标准化 , 2022, 35(12): 12-15.

[6] 李佩源 , 刘建伟 . 基于超级 SIM 的 5G 端云安全体系架构与关键技术 [J]. 中兴通讯技术 ,2023,29(1):13-19.

【作者简介】

蔡振禄（1976—），男，山东青岛人，硕士，副研究员，研究方向：音视频信号采集、数据加密、网络数据安全传输等。

（收稿日期：2025-09-22 修回日期：2026-05-09）