中国移动新一代超级 SIM 芯片技术要求白皮书

（2022 年）

中国移动研究院

北京中电华大电子设计有限责任公司

紫光同芯微电子有限公司

紫光展锐（上海）科技有限公司

银行卡检测中心

目　次

前　言

SIM 卡是运营商认证用户身份的硬件载体，具有高等级的安全特性，是运营商与用户间的重要硬件触点。

自移动网络诞生以来，起初手机终端的业务仅有打电话、发短信， SIM 卡仅仅实现了电信功能，承担终端侧的入网认证职责，起到业务安全保障作用。随着通信网络、终端技术的不断演进，手机终端的业务也演变为支持丰富多样的第三方业务，继而对 SIM 卡软硬件的需求也发生了变化，期望除电信功能外发挥更大的作用。随着 GP 多应用、NFC 以及 5G 技术的普及，数字身份、数字人民币、安全认证、金融、社保等各种应用涌现，中国移动已成功推出了超级 SIM 卡,有效承载了行业伙伴各类业务，成为国家数字经济的安全基础载体。

为了进一步满足更多行业的合作需求，进一步提升用户的用卡体验，中国移动联合产业链提前规划新一代超级 SIM 安全芯片的能力，涉及处理速度、通信速率、存储空间、多元化接口和安全特性。

本白皮书旨在基于中国移动超级 SIM 卡的发展方向，以承载新一代中国移动超级 SIM 业务为目标，为规划设计可支撑新一代超级 SIM 卡的安全芯片相关技术提供参考和指引。

中国移动希望联合各行业合作伙伴探索高质量的 SIM 卡业务，提升 SIM 卡价值，推动 SIM 卡发展成为承载各类业务的高安全性优质容器，构建 SIM 卡业务生态体系，服务用户生活，为产业各方带来更为广阔的市场契机。

1 概述

随着近年来智能手机不断普及和网络技术的逐步提升,手机安全问题逐渐凸显。同时移动互联网对各行业的渗透越来越高，已经涉及金融、水利、电力、政务等领域，移动互联网安全引起了政府部门的高度重视，消费者也越来越关注手机安全。SIM 卡可作为手机上的安全锚点，实现集安全启动、数据加密、安全存储于一体的终端安全保障体系，为个人用户日益增多的数字资产提供全方位的保护。

随着中国移动对 5G 通信网络进行全面升级，夯实经济数字化转型基础，不断丰富 5G 应用场景，拓展信息消费的新业态、新模式。中国移动成功推出了超级 SIM 业务，基于超级 SIM 卡的多应用及 NFC 技术实现了在数字身份认证、金融支付、数字证书、公交支付、车联网、门禁等领域的应用，对各行各业的数字化转型提供了更多的机会和选择，同时也对超级 SIM 卡芯片的容量和性能提出了更高要求。

《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》明确提出稳妥推进数字人民币研发。目前，人民银行研发的数字人民币已进入研发试点阶段。其中数字人民币硬件钱包基于安全芯片等技术实现数字人民币相关功能，其载体形式多种多样：IC 卡、可视卡、手环、手表等，但是凭借手机的庞大用户群体，SIM 卡无疑将成为非常重要的载体。数字人民币特色的“双离线”支付要想 100%覆盖各个应用场景，并实现快速稳定交易，为消费者带来更好的刷卡支付体验，也必须确保 SIM 芯片的接口传输速率更快、处理性能更高。

综上，根据习总书记提出的“推进产业数字化、数字产业化”的发展要求，中国移动超级 SIM 卡作为数字经济时代国家关键信息基础安全载体，为各行业的信息安全提供基础支撑和保障。超级 SIM 卡的高安全芯片为了承接越来越多的安全应用，将实现全方面的升级换代，新一代超级 SIM 芯片，容量更大、性能更快、安全性更高：

- 容量更大。为了满足传统及新兴应用的更高要求，新一代超级 SIM 芯片对内部存储空间（ROM/FLASH）及 RAM 空间进行了全面提升，而且支持外挂存储器进行扩展。
- 性能更快。为了满足各行各业用户的应用使用体验，新一代超级 SIM 芯片对 CPU 架构、主频、Cache 容量等方面进行了全面升级，性能达到国际先进水平。此外，为加快数据传输速度，进一步提升了 ISO7816 接口的传输速率，并支持高速 SPI 接口。
- 安全性更高。为了保证用户数据安全，满足不同行业的安全管理要求，新一代超

级 SIM 芯片通过 EAL5+、国密二级等高安全级别要求的安全认证，增加支持 RSA4096、SM9 等更多安全算法。

2 典型应用场景

2.1 大容量场景

- 装载更多应用

当前超级 SIM 卡产品用户可用空间 500KB，按一个应用 50KB 计算可以装载 10 个应用，搭载新一代芯片的超级 SIM 卡用户空间将至少提升 100% ，达到 1MB 以上容量，用户平均可以下载 20 个应用。

面向 2C 市场，用户可以同时下载并使用数字身份、数字人民币、公交一卡通、校园一卡通、门禁等各类应用。面向 2B 市场，超级 SIM 可提供移动安全增值服务，内置国密数字证书应用，为政企用户增加身份认证、数字签名、数据加解密、安全存储、动态口令等功能，实现业务系统的整体安全性提升。

- 支持 COS 升级

随着超级 SIM 生态的不断壮大，承载业务灵活多变，对 COS 提出更多的功能要求，当前超级 SIM COS 版本的迭代更新仅能通过更换新卡实现，用户体验差，并在一定程度为超级 SIM 发展带来不良影响，为解决上述问题，需要 SIM 卡 COS 支持在线静默升级。为保证升级过程不影响用户的正常使用及升级过程的稳定性，需要新版本 COS 下载完成后再进行切换，但当前 SIM 卡芯片容量不足以安装新旧两套 COS。新一代超级 SIM 卡芯片存储空间大幅提升能够支撑双 OS 备份，可以实现用户不换卡即可完成在线升级。

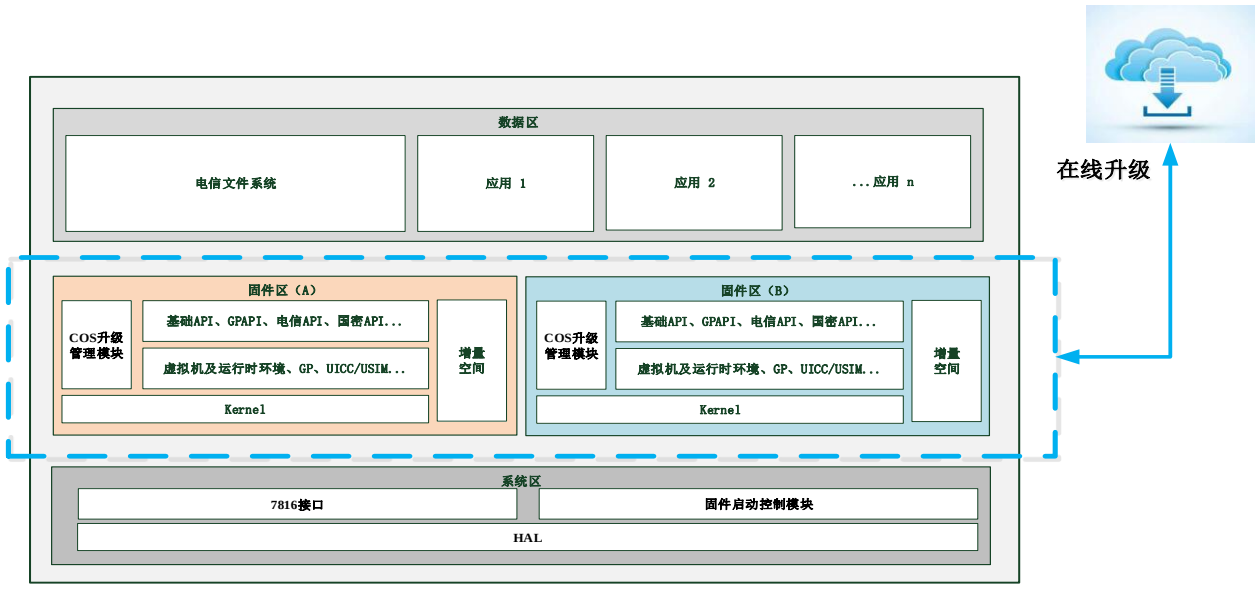

图 1：COS 在线升级

2.2 高性能场景

新一代超级 SIM 芯片从指令处理、算法运算、接口通信等方面进行全方位的性能提升，对一个事务或一个交易中的全流程进行了性能优化，解决了某一环节的低性能影响整个应用性能的难题，在交通、认证等低时延的场景需求中有效地提升了用户业务体验。尤其，交易流程复杂，涉及各种存储器、算法操作的数字人民币应用，其双离线模式的交易时间可缩短至 500ms 以内，使超级 SIM 卡可以成为用户高频数字支付的“硬钱包”。

同时，由于存储空间增加，应用下载和 COS 在线升级所涉及的通信和处理的数据量也将增大数倍，超级 SIM 芯片的性能提升也将对此有显著的正向作用，给用户提供更快捷、简单的应用服务。

2.3 可扩展场景

- 支持外接 Flash

超级 SIM 卡嵌入式存储空间的提升，可以满足片内操作系统与应用安装运行的需求，但随着更复杂、空间要求更高的应用不断推出，为了能快速实现产品的扩容迭代，新一代芯片支持通过 SPI 接口外接 Flash 来扩展存储容量，应用可根据数据的类型及其安全存储需求，将数据存储至内部存储区或扩展存储区。外接 Flash 的扩展存储区可以根据业务需求增加至 64MB，可用于存储应用数据文件、量子通话密钥等。

- 支持蓝牙接口

新一代超级 SIM 芯片通过 SPI 接口可扩展支持蓝牙协议，可打通手机 APP 与 SIM 卡之间的接口，实现蓝牙车钥匙、蓝牙数字人民币交易等场景。

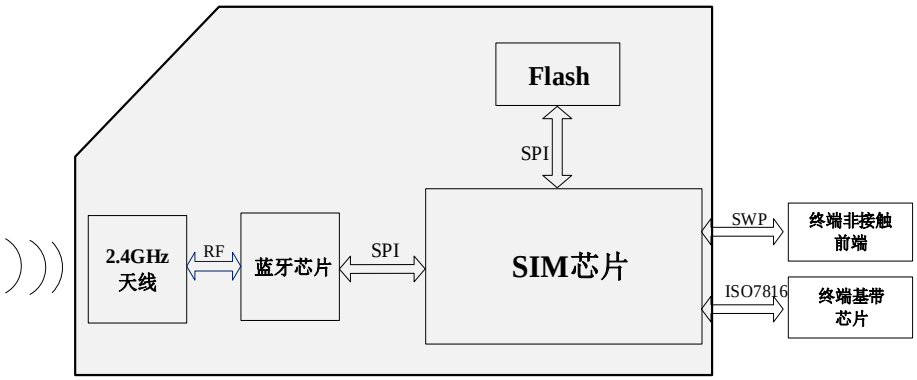

图 2：超级 SIM 可扩展硬件架构

3 芯片典型性能指标

3.1 芯片架构

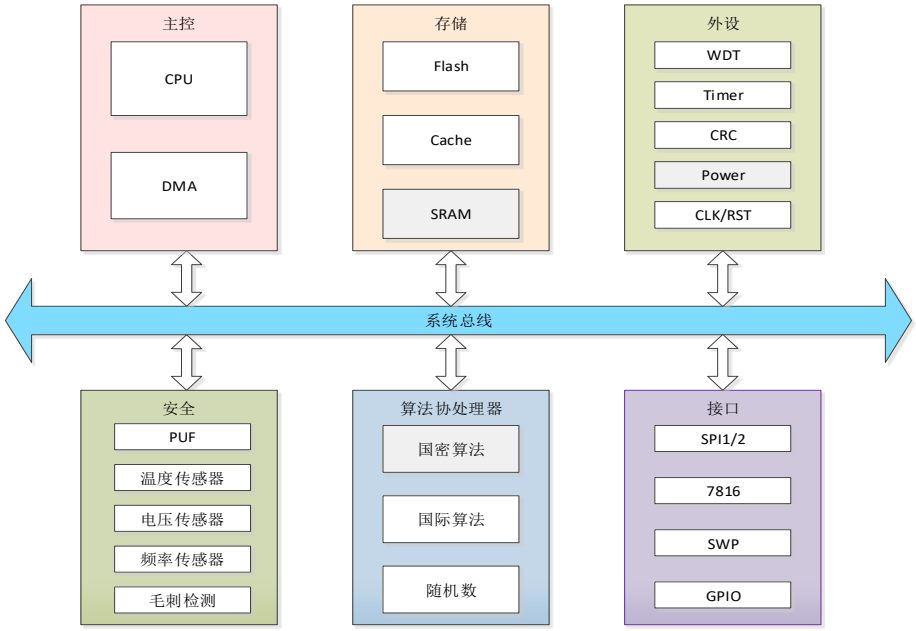

图 3：超级 SIM 芯片架构

3.2 微处理器

采用 32 位高性能 CPU 核，主频达到 120MHz 以上（含）、支持三级流水、Cache 空间达到 16KB 以上（含）。

3.3 存储器

RAM 容量为 64KB 以上（含）。

片内存储空间（Flash）容量为 2.5MB 以上（含），支持 10 万次擦写，数据保持至少 10 年，支持对擦除后的空间进行字写或多字写，Flash 擦写性能不低于表 3-1：

表 3-1 FLASH 擦写特性

	典型性能
页擦除时间	不超过 3ms
字编程时间	不超过 55us

3.4 算法协处理器

支持主流国家商用密码算法及国际算法，国家商用密码算法至少支持：SM2、SM3、

SM4、SM9，国际算法至少支持 RSA（2048/4096）、ECC_Secp256r1、X25519、ED25519、DES/TDES、AES(128/192/256)、SHA256，安全算法性能数据参见附录 A。

3.5 物理电气特性

芯片的物理特性、电气特性应遵循《中国移动用户卡硬件技术规范》 、《中国移动用户卡 COS 技术规范》的要求。

3.6 通信接口

为了适应多接口协同工作，芯片在各接口上均提供了 DMA 机制，且支持各接口同时工作。

3.6.1 ISO 7816

芯片支持 ISO7816 接口，遵循《中国移动用户卡硬件技术规范》、《中国移动用户卡 COS 技术规范》的要求。

为提高 7816 接口传输速度，扩展支持最高外部时钟 20MHz 8 分频，即 2.5Mbps 传输速率。

3.6.2 SWP

芯片支持 SWP 协议，支持卡模拟及读卡器模式，可选支持点对点模式，遵循《中国移动用户卡硬件技术规范》的要求。

3.6.3 SPI

至少支持两路 SPI 接口：

- 支持主\从模式，主从模式支持最高时钟频率至少 20MHz（VCC 1.8V）；
- 支持 SPI 时钟的极性及相位的四种配置；
- 主模式支持 Normal、Dual、Quad 端口三种连接模式，从模式支持 Normal 连接模式。

4 芯片安全要求

4.1 安全认证

新一代超级 SIM 芯片需通过以下安全认证：

- EAL5+以上（含）安全认证；
- 银联卡芯片安全认证或 EMVCo 安全认证；

- 国密二级以上（含）安全认证。

4.2 物理防克隆功能（PUF）

芯片支持物理防克隆功能（PUF），PUF 数据可认为是由制造差异产生独特“指纹”信息，通过提取芯片在制造过程中所产生的差异，就能够生成芯片独特的“指纹”信息。 该“指纹”具有不可复制、不可预测、上电产生和掉电消失等特性。PUF 技术一方面可提高芯片安全防护能力，一方面还可应用于身份识别、密钥存储和生成等领域。芯片可通过 PUF 生成安全硬件根密钥（至少 48bit），安全硬件根密钥掉电后消失，不保存在 NVM 中。

4.3 扩展存储器的安全存储

芯片针对外接扩展存储器进行读写数据时支持硬件级实时加解密，有效保证外接存储器中的数据安全。

5 结束语

数字经济时代带来新的发展契机，新一代超级 SIM 芯片在处理能力、安全能力和机卡接口上全面升级，丰富了国内、国际密码算法种类，同时对算法性能进行了全面提升，作为国家关键信息基础安全载体，助力各行各业的数字化转型，产品将于 2023 年完成研发及验证、2024 年具备商用条件。

中国移动希望携手产业链不断完善超级 SIM 卡的关键技术与功能，进一步提升机卡接口速率突破现有瓶颈，扩大容量承载更多应用，希望以超级 SIM 卡为载体，为产业各方提供更加广阔的市场契机。联合各行各业加快 SIM 应用产品创新，丰富应用场景，逐步将身份证、数字人民币、银行卡、公交卡、一卡通（政府、企业、社区、校园等）、门禁、U 盾、车钥匙等功能与 SIM 卡结合，构建 SIM 卡业务生态体系，利用 SIM 卡渗透到用户生活的方方面面，提供便捷、全方位的服务，将 SIM 卡打造为服务社会的安全基础设施，不断满足人民日益增长的美好生活需要。

缩略语列表

缩略语	英文全名	中文解释
AES	Advanced Encryption Standard	高级加密标准
API	Application Programming Interface	应用程序接口
ECC	Elliptic curve cryptography	椭圆曲线加密
EAL	Evaluation Assurance Level	安全评估保证级别
PUF	Physically Unclonable Functions	物理防克隆功能
RSA	Rivest / Shamir / Adleman asymmetric algorithm	Rivest / Shamir / Adleman 非对称算法
SIM	Subscriber Identifier Module	移动网络用户身份模块
SPI	Serial Peripheral Interface	串行外设接口
SWP	Single Wire Protocol	单线通信协议
TDES	Triple Data Encryption Algorithm	三重数据加密算法

参考文献

[1]《中国移动用户卡硬件技术规范》，中国移动

[2]《中国移动用户卡 COS 技术规范》，中国移动

附录 A：安全算法性能

表 A-1 安全算法性能要求

算法类别	算法函数	输入长度（字节）	典型性能（ms）	说明
SM2	SM2 密钥对生成	—	3.8	
	SM2 签名	32	4.5	不含密码杂凑处理过程
	SM2 验签	32	5.5	不含密码杂凑处理过程
	SM2 加密	256	10.2	
	SM2 解密	352	7.5	
RSA2048	RSA2048 密钥对生成（非 CRT 模式）	—	2790	
	RSA2048 密钥对生成（CRT 模式）	—	2520	
	RSA2048 加密	256	1.5	
	RSA2048 解密（非 CRT 模式）	256	182	
	RSA2048 解密（CRT 模式）	256	56	
SM3	SM3 算法		0.5	
SHA256	SHA 256 算法		0.2	
TDES	TDES CBC 加密	256	1.6	TDES 2KEY 模式
	TDES CBC 解密	256	1.6	
	TDES ECB 加密	256	1.6	
	TDES ECB 解密	256	1.6	
AES	AES 256 CBC 加密	256	0.85	
	AES 256 CBC 解密	256	0.85	
	AES 256 ECB 加密	256	0.85	
	AES 256 ECB 解密	256	0.85	
SM	SM4 CBC 加密	256	1.1	
	SM4 CBC 解密	256	1.1	
	SM4 ECB 加密	256	1.1	
	SM4 ECB 解密	256	1.1	

ECC（Secp256r1）	ECC 密钥对生成	—	5.8	
	ECC 签名	32	6.5	不含杂凑处理过程
	ECC 验签	32	9.3	不含杂凑处理过程
	ECC 加密	256	12.7	
	ECC 解密	336	8.8	
X25519	25519	—	5.0	
ED25519	密钥生成		6.0	
	签名	32	9.0	不含杂凑处理过程
	验证	32	10.3	不含杂凑处理过程
SM9	SM9 签名	512	39.5	
	SM9 验证	512	68.5	
	SM9 序列加密	512	47.3	
	SM9 序列解密	608	39.5	
	SM9 分组加密	512	40.2	
	SM9 分组解密	608	29.9	
	SM9 密钥封装	32	35.3	
	SM9 密钥解封	128	27.6	
	SM9 密钥交换	32	85.9	