中国电信5G SA安全增强SIM卡

白皮书

（2020 V1）

中国电信集团有限公司 发布

目　次

中国电信 5G SA 安全增强 SIM 卡白皮书

1 前言

5G 是国家工业和信息化产业发展的一个重要战略，是各行各业数字化转型的催化剂，《中国制造 2025》要求突破第五代移动通信(5G)技术，《国家信息化发展战略纲要》指出 5G 要在 2020 取得突破性进展。5G 支持增强移动宽带、超高可靠低时延通信和海量机器类通信三大类应用场景，从人与人通信连接拓展延伸到人与物、物与物通信连接，5G 将开启一个万物互联的新时代。

根据国家 5G 战略部署，2020 年是 5G 大规模商用年，中国将大力开展 5G 网络建设，全面升级通信服务，不断满足日益丰富的通信和业务应用的发展需求。随着通信网络技术的高速发展，通信智能卡作为用户数据安全存储和网络接入身份认证的载体，从最开始的只能支持网络接入鉴权认证功能发展到支持存储用户信息、STK 增值服务、远程文件管理、移动支付应用以及数据加解密等功能，但信息安全始终是通信智能卡的首要核心。现阶段用户通过使用运营商已发行的 4G 卡接入 5G 网络，现有的 4G 卡缺少 5G 标准中定义的新功能和新增的卡文件与服务，用户身份数据在通信过程中使用明文传输，位置信息不够精准，已经不能满足 5G 网络的信息与安全要求；单一认证鉴权模式无法适应运营商发展第三方业务应用需要；NATIVE 的卡片架构，随着 5G 行业应用的深入拓展，不能很好地去应对各种业务发展的要求，用户享受不到 5G 网络带来的全新体验与业务服务。根据 5G 发展策略及 5G 网络特点，需要一种全新的 5G SA 安全增强 SIM 卡（下文统一简称为“5G 卡”）作为接入 5G 网络的身份识别模块、加载各种 5G 行业应用的支撑载体，5G 卡实现包括用户身份隐私保护、GBA 第三方的应用鉴权等功能新特性，为用户数据和业务应用提供安全保障，将助力运营商发展第三方移动应用业务。

中国电信 5G SA 安全增强 SIM 卡白皮书，旨在明确用户卡的发展方向，引导通信智能卡产业合作伙伴进行 5G 卡的相关产品研发，以及为 5G 终端、5G 网络以及相关行业应用开发等产业链的合作伙伴提供 5G 卡的技术要求与参考指导，共同促进 5G 业务 2020 大规模的商用部署应用与发展。

本白皮书根据 5G 业务发展要求，提出 5G 卡的基本功能要求、架构要求、技术要求。根据本白皮书，产业合作伙伴可开展相关产品的规划与研发、进行必要的技术储备等工作，一起助力推动 5G 业务的发展，为用户提供更好的服务与体验。

2　5G 卡的特征及应用场景

ITU 定义了 3 个 5G 应用场景：eMBB（增强移动宽带）、URLLC（高可靠低时延通信）和 mMTC（海量机器类通信）。eMBB 提供极高的数据速率和广域的覆盖能力，典型应用包括超高清视频、虚拟现实、增强现实等；URLLC 对时延和可靠性要求非常严格，典型应用包括工业控制、无人机控制、智能驾驶控制等；mMTC 满足大量机器的通信需求，典型应用包括智慧城市、智能家居等。5G 与不同行业深度融合，应用于各种新业务和应用场景，从人与人通信连接拓展延伸到人与物、物与物的连接，开启“万物互联”。连接到 5G 网络的所有设备都需要 5G 卡进行身份认证，产业链对 5G 卡的安全性和可靠性提出了更高的要求,电信运营商在 5G 卡安全性和可靠性方面将面临比 4G 时代更大的挑战。

随着 5G 的加速发展，5G 国际标准组织也在推进 5G 标准的制定，现阶段 R15 已基本冻结， R16、R17、R18 版本仍在制定和完善过程中。为满足不同行业的安全可靠接入要求，R15 和 R16 规范新增了用户隐私保护、5G 移动性管理、GBA 认证等 5G 关键技术，以实现电信运营商和行业合作伙伴要求的安全性接入和可靠性连接等关键要求。

5G 卡新增用户隐私保护技术，利用高安全等级算法对 5G 空口传递的 SUPI 进行加密计算为 SUCI，在 5G 接入网络接入鉴权前将 SUPI 的密文 SUCI 传递到 5G 网络后台进行身份认证，避免 SUPI 明文在 5G 空口被非法跟踪截获，保护用户的身份隐私。为保证连接的可靠性，提升二次驻网的连接速度，新增 5G 移动性管理功能，利用 5G 卡内置的位置信息文件、安全上下文的文件，记录 5G 连接设备的位置信息和驻网信息，实现 5G 连接设备的二次快速入网，提升实际应用过程的连接可靠性。

4G 网络中用户身份信息在通信过程中明文传递问题，5G 网络利用 5G 卡内的 SUCI 加密计算功能进行了修正，用户的身份在 5G 网络中只能以 SUCI 方式加密传递。在 5G 网络中的各种连接设备，如工业物联网设备，个人终端，冰箱、电视、空调等家用设备，每个设备都有一个身份标识，5G 通过 SUCI 计算方案可保护接入用户的身份隐私，避免被跟踪攻击。在智能医疗系统和智能交通中，病人病历、处方和治疗方案、车辆位置和行驶轨迹等业务信息是涉及人生安全的高安全等级数据，在 4G 网络中黑客可能会通过跟踪锁定用

户身份后攻击这部分用户隐私数据，5G 网络 SUCI 方案避免了用户身份的跟踪，减少了从用户身份信息攻击关键数据的可能性。在 4G 时代用户手机终端上的各种移动互联网应用利用获取到的用户身份信息，对用户行为进行大数据分析，通过用户数据进行非法的利益获取，通过 SUCI 隐私保护方案可避免用户身份的泄露，进一步保障用户的行为数据安全。

5G 卡新增的 GBA 功能具备为行业合作伙伴应用提供统一的业务接入认证能力，运营商在 5G 网络中部署的 BSF 网元和 NAF 应用接入服务功能实现第三方的业务接入认证功能。

在 mMTC 场景下有海量智能设备和监测设备需要连接到 5G 网络，例如智慧城市需要对交通设施、空气、水、电等监测设备进行连接，智慧农业需要对环境温湿度、土壤水分、二氧化碳等监测设备进行连接。在 mMTC 场景中需要连接的设备种类、行业类型较多，各行业对安全认证能力的建设差异性较大，低安全等级的接入设备容易成为被攻击的目标。电信运营商利用其行业地位和自身信誉作为担保，为各行业合作伙伴提供统一的 5G 接入认证与服务。行业合作伙伴可利用 5G 卡的 GBA 认证能力为接入设备进行安全接入认证、创建安全数据通道。5G 卡新增 GBA 功能提升了 5G 业务接入认证的一致性和可拓展性，避免了行业认证能力重复建设，节约了建设和运营成本，使得行业合作伙伴可将更多的资源投入到自身的业务建设。

3　5G 卡架构与功能

3.1 5G 卡架构

5G卡采用Javacard与GP架构，同时支持电信运营商的5G基本通信功能和针对行业合作伙伴的应用管理功能。5G卡的通信功能为上层应用提供5G数据短信、OTA BIP管道服务，通过ECC与RSA等运算能力为上层应用提供认证服务；通过Javacard层实现Java虚拟机为上层应用提供应用运行环境，同时提供JavaAPI接口供上层应用调用底层的基本通信接入能力与运算能力。GP层利用安全域、安全通道、权限、生命周期等安全模块为上层应用提供安全管理环境，防止应用之间相互访问，为外部构建管理应用的安全通道，通过权限的配置限制应用的使用范围。

5G卡通过Javacard与GP架构体系实现对行业应用的动态管理，对卡片的存储、内存空间以及运算性能要求较高，不仅需要承载运营商通信功能、Javacard与GP安全架构外，还应能装载运营商的自有应用和部分行业应用，如数字身份识别、电子现金、市民卡、公交

等。为实现对应用和高安全等级数据的安全防护，5G卡还应具备支持ECC、RSA、AES等高安全等级的算法能力。

3.2 5G 卡功能

通信功能是5G卡的一项基本功能，提供接入电信运营商5G网络能力，以便为用户提供5G语音、短信、数据等服务。5G卡根据3GPP规范为满足中国电信发展5G用户及多样化的5G移动业务要求，增加了5G移动性管理、用户身份隐私保护、安全认证加强、GBA认证、5G接入控制、5G USAT事件等功能。

3.2.1 5G 移动性管理功能

终端开机或重新进入网络覆盖区时，先尝试选择终端内存中保存的RPLMN（ Registered PLMN，即终端上次关机或脱网前登记的PLMN）接入，如果RPLMN为空或选择失败，则读取卡的相关PLMN选网文件(HPLMN、EHPLMN、UPLMN、OPLMN)并按照指定顺序（HPLMN/ EHPLMN→UPLMN→OPLMN→按信号质量或信号强度）尝试接入网络。5G卡的PLMN选网文件中的RAT编码需要新增5G网络的NG-RAN编码以利于终端优先、快速接入5G网络。

终端通过3GPP或Non-3GPP方式接入5G网络，分别产生3GPP、Non-3GPP的安全上下文和位置信息。安全上下文保存服务网络派生密钥、上下行NAS计数器、完整性算法参数、加密算法参数、安全能力等，位置信息保存5GS-GUTI、上次访问注册的TAI。终端读取安全上下文信息和位置信息用于网络快速接入和网络认证。5G卡可以通过设置服务和新增文件的方式保存5G安全上下文和位置信息。

3.2.2 用户身份隐私保护功能

在5G网络中，5G卡存储用户永久标识SUPI，是移动网络中用户(人/物)的唯一标识，用于协助5G连接设备在网络接入时向5G网络提供用户身份标识、以完成接入认证后使用5G业务。用户身份标识为SUPI（有IMSI和NAI两种），用户卡连接到5G核心网时，SUPI不使用明文在网络中传输，5G卡将使用ECC椭圆曲线的PKI加密机制产生接入5G网络的临时会话密钥，用于本次传递SUCI的计算，5G网络利用ECC的PKI的加密机制产生会话密钥，解密SUCI获取到SUPI完成对用户的身份认证。在SUPI传递过程中，5G卡利用用户身份隐私保护技术，将SUPI加密为SUCI进行传递，避免了5G用户身份明文SUPI在空口被明文截获，保护了用户身份隐私。

3.2.3 安全认证功能

5G卡存储3GPP访问时由终端使用AKA流程产生的KAUSF和KSEAF，KSEAF可防止一个服务网络冒充其它服务网络，目的是为了终端可能接入3GPP和非3GPP两种网络时使用，KAUSF用于基于本地的运营商政策认证和密钥协商使用。

3.2.4 GBA 认证功能

GBA提供一种三方的鉴权模式，运营商通过在5G网络内新增BSF网元和NAF服务功能，利用5G AKA鉴权流程为应用和应用服务器之间建立安全通道密钥，再利用安全通道密钥为应用和应用服务器之间建立起安全通道，进行身份认证与安全通信。

3.2.5 5G 接入控制功能

5G中引入了MPS（Multimedia priority service）/MCS（Mission critical service）服务的优先级控制，5G卡内设置高优先级服务的接入特性，接入特性使用时结合接入种类，实现特殊服务的接入控制。

3.2.6 USAT 事件功能

3.2.6.1 呼叫控制

在LTE的Call Control上增加PDU会话的控制部分，终端在建立呼叫前需先将会话信息和服务小区信息发送给卡，5G卡有权利对所有的PDU连接过滤处理（允许、修改、拒绝），增强了卡片对应用过程的控制能力。

3.2.6.2 网络拒绝事件

5G卡引入5GMM REGISTRATION REJECT消息，当终端收到该消息时应通知5G卡该事件的发生，且会携带被网络拒绝的原因，如非法终端、5GS服务不可用、PLMN被禁用，同步失败等信息，卡片对返回信息做处理，可根据具体业务场景对该事件进行管理。

3.2.6.3 5G 数据连接状态改变事件

终端探测到5G数据连接发生改变，通知卡片，卡片对返回信息解析处理，可根据具体业务场景对事件进行管理。

3.2.6.4 OPEN CHANNEL 命令

5G卡将OPEN CHANNEL指令扩展到5G PDU会话，支持在WLAN和IMS环境下完成Receive Data/Send Data数据交互。

3.2.7 漫游优选控制功能

当5G卡漫游优选控制服务开启时，用户在访问网络的初始注册期间，归属地网络会下发一些控制信息到漫游地网络，控制终端的行为，包括首选网络和接入技术组合的列表。

4 5G 卡关键技术要求

4.1 5G 移动性管理技术

5G通过在卡内新增选网文件记录5G网络NG-RAN编码、支持存储3GPP访问及Non-3GPP访问网络时的5G位置信息及NAS安全上下文信息，为5G终端提供了一种快速二次驻网的能力。终端首次登网成功后会将5G-GUTI、上次访问TAI以及5G状态更新、终端安全能力、密钥KAMF、上下行的NAS count值等信息更新至5G卡内，以实现终端的快速二次登网。

4.2 用户身份隐私保护技术

5G卡通过SUCI加密计算功能实现用户身份隐私保护、防止用户信息被监听、用户位置信息泄露、防止伪基站跟踪。5G卡SUIC计算通过3GPP规范定义的ProfileA与ProfileB两种流程计算实现，两种流程中使用ECC高安全等级算法生成会话密钥，对IMSI和NAI两种类型SUPI进行加密传递。5G卡根据3GPP规范定义了GET IDENTITY指令，供终端向卡获取SUCI传递给网络进行用户身份认证。

4.3 5G 安全认证技术

5G卡与网络之间采用双向认证机制防止鉴权过程中的卡和网络仿冒，5G卡采用了EAP-AKA’和5G AKA两种双向认证和密钥协商机制，卡内存储3GPP访问时由终端使用AKA鉴权过程中产生的KAUSF和KSEAF，5G卡与ARPF保存相同的用户密钥K、各自维护卡存储的同步序列号SQNMS和网络存储的同步序列号SQNHE。

4.4 GBA 认证技术

5G卡为了利用运营商鉴权网络优势和认证权威性，在卡内开发了GBA业务接入认证功能，为产业链提供统一的业务接入认证能力。5G卡内支持GBA鉴权初始化、BSF引导服务、

NAF服务服务流程，并在网络端配置BSF网元、NAF服务器，利用AKA鉴权机制、密钥分散机制产生临时会话密钥KS、业务接入认证密钥NAF KEY，实现业务安全接入。

4.5 5G USAT 事件

5G卡为了更好的提供安全可靠的连接能力，5G卡根据3GPP规范增加了USAT能力：

1） 5G卡新增5G网络拒绝事件(Network Rejection Event)、5G数据状态连接状态改变事件(Data Connection Status Change Event for 5GS)，5G卡可根据具体业务场景对该事件进行相应的策略管理。

2） 5G卡新增5GS OPEN CHANNEL COMMAND，以便在(I-)WLAN和IMS环境下能够完成Receive Data/Send Data数据交互。

3） 5G卡新增支持NG-RAN信息扩展(Provide Local information extended to support NG-RAN information)，通过此扩展指令可向终端获取5G网络信息。

4） 5G卡可根据预设参数对所有的PDU连接过滤处理（允许、修改、拒绝），实现PDU呼叫控制。

4.6 5GS 文件和 5GS 服务要求

5G卡为支持5G新增的SUCI计算、移动性管理等功能，根据3GPP规范在USIM文件架构下增加了DF5GS文件目录，包括EF位置文件EF5GS3GPPLOCI、EF5GSN3GPPLOCI，及安全上下文文件EF5GS3GPPNSC、EF5GSN3GPPNSC，鉴权文件EF5GAUTHKEYS、EFUAC_AI，SUCI计算信息文件EFSUCI_Calc_Inf。同时5G卡内服务列表UST新增了n° 122- Service n° 130服务，以向终端指示5G卡内支持的服务能力。

通过对3GPP R15、R16规范的跟踪研究与试验，中国电信同时制定了《中国电信用户卡需求白皮书-5G卡通信功能分册》规范，对移动性管理、用户身份隐私保护、新增文件与服务等5G关键功能与技术进行了具体的要求描述，可供中国电信产业合作伙伴进行5G卡、5G终端、5G网络以及相关行业进行应用与产品的研发做参考。

5 结束语

5G基于第四代移动通信系统演进而来，对终端、无线、业务、网络进行了融合与创新，在信息感知与信息获取控制方面带来革命性影响，5G通信以物为基础，广泛应用于车联网、

物联网、智慧城市等场景。5G卡在5G产业链中承载了选网接入、身份验证、应用承载功能，5G卡的关键技术为将为5G用户提供安全、可靠的5G连接能力。

5G网络建设已上升至国家战略层面，将在2020年大力推进5G基础设施的部署工作，电信运营商已开始在国内主要城市进行5G服务测试。随着5G商用部署的逐步开展与深入，3GPP标准组织、产业链也在不断完善和开发制定新的5G技术。本白皮书根据3GPP R15和R16进行制定，在5G商用部署初期阶段向产业链发布，旨在向产业链展示5G卡的用户身份隐私保护、移动性管理、GBA业务认证等核心功能，希望携手产业链进一步完善、开发5G卡的关键技术与功能，共同提升广大用户的5G体验。

6 名词解释

术语	全称	定义
SUPI	Subscription Permanent Identifier	5G系统中的用户标识
SUCI	Subscription Concealed Identifier	5G系统中隐藏的用户标识，加密后的SUPI
IMSI	International Mobile Subscriber Identity	2/3/4G系统中的用户身份标识
NAI	Network Access Identifier	网络访问标识符
AKA	Authentication and Key Agreement	认证与密钥协商协议
KAUSF	Key of Authentication Server Function	认证服务器密钥
KSEAF	Key of SEcurity Anchor Function	安全定位功能密钥
5GMM	5GS mobility management	5GS移动性管理
GUTI	Globally Unique Temporary Identifier	5G用户临时标识，相当于终端在网络中的临时身份证号
TAI	Tracking Area Identity	位置区域标识符
PLMN	Public Land Mobile Network	公共陆地移动网

PDU	Ptotocol data unit	协议数据单元
GBA	General Bootstrapping Architecture	一种通用认证机制，可以为应用层业务提供统一的安全认证服务
UST	USIM Service Table	USIM应用下的服务列表