2020·广州
世界5G大会
WORLD 5G CONVENTION

以终端为中心的5G安全体系

WHITE PAPER V7.0 K
2020.11

未来移动通信论坛
FUTURE MOBILE COMMUNICATION FORUM

以终端为中心的 5G 安全体系

2.0 版

UE Centric Security in 5G

V2.0

摘　要

5G 的业务能力提升、业务多样性扩展、终端形态多样、能力多样、部署环境多元化，以及网络的虚拟化、边缘计算、网络开放等新的特征和技术的引入，特别是在智能网联车和各种垂直行业中的应用，使得 5G 安全遇到前所未有的威胁和风险，5G 终端安全的重要性也日益凸显。本白皮书分析了 5G 中的终端和系统的安全威胁，以及传统和新兴的安全解决方案，在 V1.0 版本的基础上，增加了基于 EAT 协议和硬件安全令牌的 5G 终端状态证言、面向用户和终端的 5G 应用认证和密钥管理、更安全的基础可信根等内容，进一步丰富了“以终端为中心的 5G 安全体系”概念。

在“以终端为中心的 5G 安全体系”中，介绍了实施可信技术打造可信终端，并以此为信任根建立以用户所信任和授权的终端为中心的 5G 安全体系，并将可信概念扩展、开放给用户的周边设备和其它应用，可以解决 5G 中处于最末端的终端安全以及高层应用安全，其核心是对用户和用户使用的各种业务提供安全保障，实现“用户域安全联盟”。作为使用者个人的扩展，终端可能代表多个角色。本白皮书讨论了角色分配、隔离、切换相关的安全性和隐私保护。

Abstract

5G system is designed with new features, like high capability network, diverse service, diverse terminal/equipment, and their diverse capability, diverse deployment environment. 5G network also introduces network-function-virtualization, network slicing, edge computing, and network openness. New and high-security threats come along with all those features, especially for ICV and various 5G vertical applications. The importance of 5G terminal security is becoming increasingly prominent. In this whitepaper, we analyzed the threats, then traditional and emerging security solutions. Beyond V1.0, we added new solutions on EAT protocol and hardware security token based 5G terminal security status attestation, user and terminal oriented 5G Authentication and Key Management for

Applications, more secured essential Root of Trust. Those contents further enrich the concept of *UE centric security framework in 5G*.

In the *UE centric security framework*, the trusted UE is built, by implementing the trusted computing and remote attestation technologies. Based on the trusted root, i.e. the user trusted and authorized UE, a security chain is enabled. Through hardware-token solution and secure key derivation functions, the trust opens to peripherals of the user and other authentication ends. The goal is to realize “Security Federation of User Domain”. One UE may represent multiple roles or multiple users, therefore we discussed the separation of the contexts and the protection of privacy.

修订列表

本版白皮书在 1.0 版基础上主要进行了如下增补和修订：

- 更新了“摘要”和“Abstract”；
- 将原“4.2.3 5G ME 认证过程”合并入 4.2.2 节；
- 修改 5.1 节标题和概述部分；
- 新增“5.2 终端中的基础可信根”节；
- 新增“5.5 基于 EAT 协议和硬件安全令牌的安全状态证言”节；
- 新增“5.6 5G 应用级密钥推衍”节；
- 新增“5.7 终端作为用户对外操作的新型可信根”节；
- 更新了“6 总结和建议”章节；
- 增补“参考文献”和“缩略语”；
- 其它编辑性修正和更新；

目　录

摘　要 1

ABSTRACT 1

修订列表 3

目　录 4

1　前言 7

2　5G 应用与终端 7

2.1　5G 网络特征与场景 7
2.2　消费娱乐类 8
2.3　金融支付类 8
2.4　政企办公类 9
2.5　工业互联网类 10
2.6　基础设施联网类 10
2.7　行业定制专用类 11
2.8　数字钥匙 12
2.9　终端为中心的 5G 应用 12

3　安全威胁 12

3.1　终端安全威胁 12
3.1.1　病毒、蠕虫和木马 *12*
3.1.2　克隆终端 *13*
3.1.3　带病终端 *13*
3.1.4　终端劫持 *13*
3.1.5　DDos 攻击 *14*
3.1.6　芯片攻击 *14*
3.1.7　数据窃取 *14*
3.2　终端应用系统级安全威胁 14
3.2.1　敏感数据泄露 *14*
3.2.2　用户隐私泄露和财产损失 *15*
3.2.3　非法接入和越权使用 *16*
3.3　通信安全威胁 16
3.3.1　位置追踪 *16*
3.3.2　伪基站与降阶攻击 *16*
3.4　终端作为信任根开放后的安全威胁 17

3.5 5G 系统安全威胁 18
4 安全解决方案 18
4.1 传统方案 19
4.1.1 用户认证和授权 19
4.1.2 通信加密和完整性保护 20
4.1.3 终端侧安装杀毒软件 21
4.1.4 网络和服务器侧部署防火墙 21
4.2 新兴和附加方案 22
4.2.1 5G SUCI 22
4.2.2 对 5G 终端的认证 23
4.2.3 5G 网络安全 28
4.2.4 伪基站防护 29
4.2.5 基于终端底层调用监控的病毒和恶意行为检测 29
4.2.6 可信环境和可信终端 30
4.2.7 虚拟机隔离 32
5 终端为中心的安全 33
5.1 终端可信技术 33
5.1.1 可信终端 34
5.1.2 可信存储 36
5.1.3 可信执行环境 36
5.1.4 可信启动 37
5.1.5 可信硬件密码运算 38
5.1.6 可信调试 39
5.1.7 可信用户界面 39
5.1.8 可信传感器 40
5.1.9 隐私保护 41
5.2 终端中的基础可信根 41
5.3 远程证明 42
5.4 终端安全令牌 43
5.4.1 基本流程 43
5.4.2 基于本地生物识别的用户认证 44
5.4.3 安全保护 44
5.5 基于 EAT 协议和硬件安全令牌的安全状态证言 45
5.6 5G 应用级密钥推衍 47
5.7 终端作为用户对外操作的新型可信根 50
5.8 可信能力开放 50
5.8.1 终端/用户授权的可信外设 50
5.8.2 网络与服务互信 51
5.9 多角色隔离与转换 52
6 总结和建议 53

参考文献 **53**
缩略词表 **54**
关键词 **55**
致谢 **56**

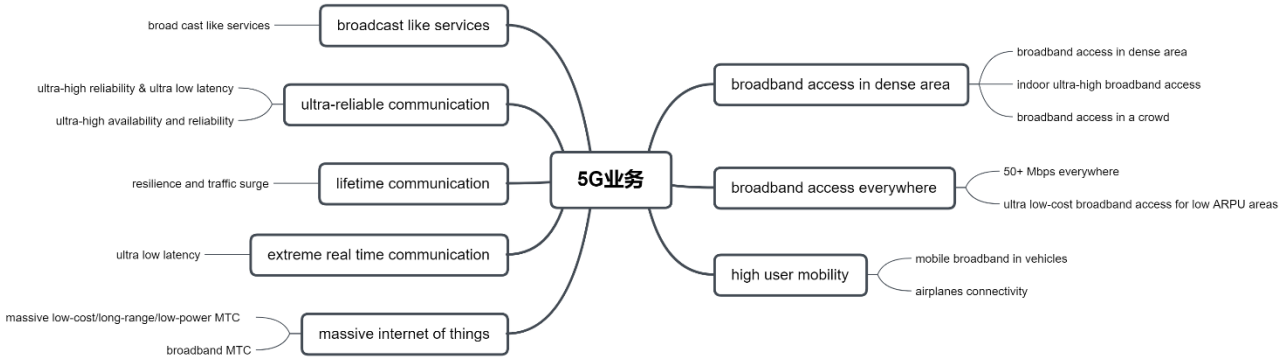
1　前言

随着移动互联网和工业互联网的发展，移动终端（UE）在个人生活中越来越占据了重要位置。5G 网络的部署，将进一步促进人和终端的结合，提高终端为个人生活服务和行业应用的便利性。部署和应用 5G 的新的安全机制设计，应用最新的终端安全技术，可以在提高便利性的同时，提升数据安全性和个人信息安全性。

2　5G 应用与终端

2.1　5G 网络特征与场景

NGMN 在[4]中，总结了 5G 的业务特征。根据这些业务特征，本章讨论了 5G 对传统业务的影响以及可能带来的新业务场景，并给出了 5G 时代的安全风险和需求。



5G 业务特征

随着移动互联网的发展，终端（UE）在个人生活中越来越占据了重要位置。5G 移动蜂窝网络除在覆盖性（例如飞机覆盖）、移动性（例如高速移动）、连接性、使用性能（速率/时延）、可靠性等方面有极大的提高外，还带来新的特性，例如 D2D 直接通信、大量物联网终端接入、广播通信等。5G 网络能力和应用开放系统又为 5G 开辟新的应用提供了支撑平台。因此，5G 将对已有的移动业务进一步提升，创造新的业务和新的商业模式，从方方面面影响用户的工作、出行、娱乐、生活。5G 也将开辟工业、商业、服务、政务等方面的新时代。

2.2　消费娱乐类

Ovum 发布的《5G 娱乐经济报告》中对未来十年进行预测，5G 用户的月平均流量将从 2019 年的 11.7GB 增长 7 倍，其中 90%将被视频消耗。报告预计，5G 在未来十年将为传媒和娱乐产业带来 1.3 万亿美元的新营收。到 2028 年，5G 将会为传媒产业带来 3350 亿美元的营收，在无线所带来营收中的比重会提升到 79.9%。

5G 的高速率和高容量会带来多媒体业务和 VR/AR 业务的大规模爆发。超高分辨率刷新率的视频音频会提升人们对多媒体业务的体验。结合 5G 低时延特性，交互性的娱乐将称为主流，例如 AR 游戏、体育、娱乐节目 VR 直播等。近年来新兴起的个人直播也走出户外，多以移动的形式为主。社交将以多媒体和 VR/AR 为主要交互形式。VR/AR 购物也为电子商务提供更贴近用户的平台能力。从 LTE 系统商用对业界的影响可以预期，5G 将会带来更多的娱乐形式和商业模式创新，更好地服务于人的休闲娱乐。

除了强大的通信能力以外，5G 终端将会给用户带来更好体验的录制、播放能力，以及用户交互能力。为了提高用户体验，相应的环境感知能力也得到提升，例如更准确的定位、速度、运动识别，甚至可能会引入新的传感模式。

为支撑用户的消费娱乐，5G 终端需要有更强的处理器、图形/声音/音乐处理能力，更大更快的存储，以及多模式的、强大的通信能力。

娱乐系统中的安全风险主要是个人信息保护相关的，以及某些 AR/VR 系统被攻击后产生的财产或心理损害。

2.3　金融支付类

移动互联网带来了移动支付的发展。在中国，移动支付已经成为零售业的主要支付方式，替代了传统的现金交易方式。由于基础设施的差异，中国的移动支付发展道路与国外的信用卡为中心的道路差异明显。欧美移动支付以信用卡为中心，以卡号和 APP 为主要支付方式，而中国则以 APP 内支付平台支付和零售扫码支付为主。

5G 网络提供了高速率、高可靠性、高效海量 MTC 接入、D2D 直接通信等能力。移动支付除提高可靠性、提高性能、提高体验外，会出现新的支付形式。例如，

- 移动钱包。移动终端设备作为基本支付凭证。

- 非接触、无需手动操作的自动支付。物联网的发展，D2D 直接通信，借助 WLAN、蓝牙、NFC 等与 5G 网络无缝配合，将当前的扫码支付转变到非接触无操作的自动支付。例如停车费、高速费自动缴付。
- 移动 PoS 机，即将商家的 PoS 机直接安装在移动终端实现软件方式支付。
- D2D 通信用户或设备间直接转账，无需网络和服务器端实时介入。
- 区块链记账和电子货币交易。5G 终端计算能力和通信能力，会导引数字货币的发展。分布式记账能力在终端实现成为可能。
- 无钱包无设备支付。借助于生物识别技术，仅需要“人”作为凭证的，无需任何物理载体的支付方式成为可能，例如更安全的人脸支付。

毫无疑问，支付金融类业务需要网络、平台以及终端提供足以信赖的安全性保证。支付金融类业务被攻击成功直接造成个人或企业财务损失。

2.4　政企办公类

即使在移动互联网普及的 LTE 时代，政企的移动办公发展非常缓慢，尤其是核心功能不在移动端开放，须在封闭的内网中部署。其主要原因是网络和设备的公开与封闭的矛盾。在固定网络中，网络边界清晰，防护能力不论从位置上（网关处）还是成本（计算能力、通信能力、实时监控能力）上都容易部署。但是移动端则很难实现网络隔离、软件隔离、可信识别，因此限制了政企办公的发展。

5G 网络提供了网络分片能力，可以从终端到网络、到应用提供一个完整的封闭的网络环境，从而提供与固定网络相似的安全信任等级，政企应用可以在终端安全部署。移动端部署可以扩大政企用户的移动性、可接入性，可以在家、在途操作敏感业务，提高企业效率；可以扩大政府办公的便利性，使得上门服务、街头服务更加普及。

5G 网络的实时性、可靠性，则为政企中的敏感业务提供更加便捷、可靠、安全的服务。消防、公共安全等业务可以通过移动端实现。

随着个人身份电子化、个人生物特征与电子身份绑定的发展，个人原本需要到场面对面办理的业务，转移到移动终端上办理，提高便利性，降低行政成本。

5G 网络还提供广播类业务，与 IoT 系统结合，可以进一步实现行政电子化。例如，通过实时通知到移动用户，通过 IoT 设备（屏、声音）实现无处不在的恶劣天气实时预警等。

政企办公类安全风险涉及比较广。对于企业而言，商业秘密被窃取，造成直接财务损失。对于政府而言，攻击的结果可能是公共安全事件，也可能是个人信息被窃取。

2.5　工业互联网类

工业互联网应用终端种类繁多，涉及的行业众多，部署环境复杂。本文从应用场景和功能两个角度进行分类。

从应用场景的角度看，工业互联网类终端涵盖了增强移动宽带（eMBB）、高可靠低时延通信（uRLLC）、低功耗大连接（mMTC）三大核心应用场景。其中增强移动宽带类终端主要用于视频监控类应用，以及 AR/VR 应用，包括固定式监控摄像头以及移动式视频设备。高可靠低时延类终端主要包括工业控制系统、远程医疗、无人机、自动驾驶车辆等对实时性要求很高的设备。低功耗大连接类终端主要包括各种类型的传感器、数据采集器等低功耗物联网设备。

从终端的功能角度看，工业互联网类终端包括数据采集类、智能控制类、智能业务类、网络通信类等种类。数据采集类终端包括各种类型的传感器、数据采集器、视频设备等，其功能主要以数据回传为主，部分设备有一定的计算和分析能力。智能控制类终端包括各种通过网络控制的阀门、开关等，其功能主要以自动控制为主，通常有一定的实时性和安全可靠要求。智能业务类终端与行业应用相关联，包括固定式、移动式，通常需要一定的人机交互能力。网络通信类终端包括有线通信和无线通信，通常需满足语音、视频等多媒体网络传输需求。

工业互联网应用场景，一般为半开放场景，因此物理攻击和防护非常重要。工业互联网涉及到矿山、制造、物流等行业，一旦被攻击损失重大。

2.6　基础设施联网类

固定网络部署需要有线路铺设，这往往需要大规模的土木施工，有可能影响正常的生活、工作、商务、交通。甚至大多数情况下根本没有施工的可能性。同时，固定网络一旦部署很难改动，而当前电子化、网络化、智能化的急速发展，使得很难完整考虑到未来的演进。

5G 可以提供高覆盖、高容量、高效率、低成本的 IoT 部署方式，提供网络分片和专用网络的网络环境，这些都将促进基础设施通过蜂窝网络进行互联互通的部署。由于 5G 提供了

IoT 联网的低功率设计，不方便部署电源线的低数据量连接点可以通过电池供电进行解决。OTA（Over the Air，空口配置）配置方式，可以降低部署的复杂度和人力成本。D2D 直连通信可为智能设备间的相互协同提供解决方案。

基础设施联网是环境智能化、社会化的基础。基础设施联网提供了人与环境的互动能力，提供了更完善的信息辅助各种人工智能辅助下的“无人化”、“自动化”操作。例如车联网的部署，需要电子化、信息化的道路和交通指示辅助。通过部署无线接入方式，无人区的远郊、乡村道路，可以通过太阳能电源加 5G IoT 终端部署实现基础设施智能化、联网化。

公共基础设施被攻击或被破坏，直接损害公众利益，甚至可能造成公共安全问题。例如交通设施被攻击可能造成交通拥堵，灾害预警设施被攻击可能造成公众恐慌。对基础设施的防护，除了要应对一般的网络攻击外，还须防护物理攻击。例如拆壳后直接对电路和器件攻击，移动通信终端的位置等。

2.7　行业定制专用类

物联网终端具有行业定制化特点。不同行业终端的功能和安全需求差异较大。

（1）能源类

能源类行业包括电力、石油石化、煤炭、新能源等行业。该行业的定制终端包括专用传感器、专用控制器和专用网络设备等。这类终端通常有较高的实时性要求，工作在较为恶劣的工业环境，具有相应的行业技术标准和检测标准。

（2）制造类

制造类行业主要关注智能制造对 5G 终端的需求，包括工业物联网、工业自动化控制、物流追踪、工业 AR、云化机器人等。通过网络切片提供适用于各种制造场景的解决方案，实现实时高效和低能耗。

（3）交通运输类

交通运输类终端包括移动终端（人员、机动车、轨道车辆、船舶、飞行器等）和应用于固定场景的终端（道路、轨道、航运等），这类终端通常有较高的实时性和高带宽要求，实现移动终端与固定终端之间的协同。

2.8　数字钥匙

5G 时代，IoT 联网设备的便利性（低成本、低耗电、海量部署）和可靠性，将普及以 5G 为通信方式的智能门锁。OTA 的部署方式、以及开放平台部署能力，也为快速部署、动态管理提供可能。而 5G 提供的高可靠性、高安全性的通信能力，也为数字门锁提供足够高的用户信赖。D2D 通信的可能，使得无需蓝牙、NFC、WLAN 等局域通信部署，即可实现数字钥匙与数字门禁间的直接通信。使用单一的通信方式，替代多种通信方式，用户将只需携带一个移动终端，即可走遍天下。配合相应的操作系统、平台、软件功能，以及精确定位，实现无需用户操作，临近即识别、验证、开锁的操作。

2.9　终端为中心的 5G 应用

移动宽带和各种应用的发展，终端早已成为个人生活，尤其是信息生活的主体。但传统的业务设计仍以云端为中心，服务用户。以 UE 为中心的模式，即将终端设备经过使用者授权后，作为个人的数字代表，通过网络或临近通信协议，实现自动化操作。5G 的 D2D 通信，以及其他近场通信，给 UE 为中心的应用提供了很大的想象空间。例如，实现自动寻车，自动打开车锁，自动根据终端调整使用者习惯等等。终端可能是移动智能手机，或可穿戴设备，甚至植入人体的设备。若为终端颁发了个人电子身份证或电子护照，可广泛应用于政务、票务、酒店住宿以及移动支付等应用中。

终端设备替代了个人作为认证实体，因此要保证终端设备的安全性，并且要保证个人对终端设备的授权。

3　安全威胁

本章从终端安全威胁、系统安全威胁、通信安全威胁等方面分析 5G 系统的安全威胁。

3.1　终端安全威胁

3.1.1 病毒、蠕虫和木马

随着计算机技术的发展和网络的普及，出现了越来越多的病毒、蠕虫和木马，而且复杂级别持续快速增加，存储方式、隐藏方式、传播方式和活动方式等不断更新，近而越来越难被

检测出来。目前这些恶意传播代码泛滥成灾，危害性和破坏性越来越强，可以轻易使终端速度变慢、内存变小、数据丢失、隐私被盗、芯片被毁以及网络瘫痪，给终端用户造成了严重的经济和心理的压力。

3.1.2 克隆终端

终端多数被放置在不安全的物理环境中，攻击者很容易接触到，而且终端成本不高，攻击者很容易获取。同时终端在芯片、模组或者电路板等硬件上，缺少相应的硬件保护机制，如防篡改、防逆向设计，攻击者就可以对终端实施克隆；通过伪造终端(身份假冒)，发布或传送假数据、监听网络中传输的敏感信息等，可以形成大规模节点伪造/破坏，影响面广、危害较为严重。

3.1.3 带病终端

目前很多终端生产厂商普遍缺乏安全意识和安全能力，在终端操作系统、固件、业务应用等软件的设计和开发过程中，存在编码或者逻辑方面的安全漏洞和缺陷，而且大部分终端没有自动系统升级和漏洞修复机制，这就导致终端存在较高的软件漏洞风险。

不仅软件存在缺陷，硬件也是如此。很多终端在硬件架构设计上缺少安全意识，比如，设备在外壳设计上没有做相应的防拆除设计，攻击者就能很容易查出外壳接触到内部硬件，利用工具从内部硬件组件中提取固件或数据，然后加以分析，寻找可以利用的漏洞进行攻击；设备如果没有响应的电磁信号屏蔽机制，攻击者则可通过侧信道攻击方式来进行密码系统的分析和破解。

由于软件和硬件的漏洞和缺陷，导致终端“先天不足”，带病服役，遗留了极大的安全隐患，为恶意攻击者提供诸多“便利”。

3.1.4 终端劫持

随着网络和终端的发展，越来越多的终端成为攻击者的劫持目标，同时劫持方式也是趋于多元化，其中运用较多的方式是，攻击者通过锁屏、加密等方式劫持终端，从而敲诈用户钱财甚至破坏终端。通常攻击者都是利用系统漏洞或通过网络钓鱼等方式，向受害终端植入恶意程序，加密终端上的数据文件乃至整个终端的存储空间，然后向受害者索要数额不等的赎

金后才予以解密，如果用户未在指定时间缴纳要求的金额，被锁数据文件甚至整个终端将无法正常使用。

3.1.5 DDos 攻击

由于终端种类和数量繁多，目前正逐渐成为 DDoS 攻击的目标。大量终端或因恶意破坏，或因自身存在漏洞，陆续沦为“肉鸡”被黑客远程控制，变成用来发动 DDoS 攻击的工具。例如智能摄像头、网络视频监控设备、数字录像机等终端，都可能沦为 DDoS 攻击的目标。移动智能终端数量庞大，计算能力和通信能力增长迅速。作为个人主要的通信工具，一旦侵入可能追踪其社交网络进行病毒式蔓延传播。

3.1.6 芯片攻击

随着技术的进步，芯片上的晶体管和逻辑门越来越多，压到固件里的指令数量和代码行数也随之暴涨，而随着代码的激增，漏洞也就越来越多；同时多数芯片架构缺少安全防护机制，于此同时攻击方式逐渐成熟，例如代数攻击、故障注入攻击等，从而攻击者可以较轻松的攻破芯片，获取芯片内部数据。

3.1.7 数据窃取

终端上往往会涉及到重要敏感业务数据或者个人的隐私信息，例如智能电表的用电信息、智能家居采集的用户数据、智能穿戴设备采集的个人信息等，由于终端硬件资源限制，或由于成本因子，当前多数终端缺少敏感数据保护机制，这样就导致敏感数据可能被攻击者直接窃取。

3.2　终端应用系统级安全威胁

3.2.1 敏感数据泄露

根据 GB/T 35273，个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。一般包括个人身份信息，生物特征信息，金融相关信息，儿童相关信息等。

越来越多的移动智能终端中引入生物识别作为认证方式，且有逐步向低端终端渗透的趋势，尤其是仅需摄像头+软件设计的人脸识别。终端必须安全地存储和使用这些生物特征数据。生物特征作为人体与生俱来的、无可能修改的个人属性，对个人而言极为重要。一旦泄露将造成不可挽回的损失。

3.2.2 用户隐私泄露和财产损失

互联网时代诞生了一大批“免费”商品，免费游戏、免费咨询、免费社交 APP 等。大部分免费模式依赖于用户点击广告或其他付费服务得以生存甚至盈利。为了提高用户点击率、转换率，免费服务提供者往往会搜集用户的各种隐私数据及行为习惯，精准推送信息。一些服务提供者甚至会将搜集来的用户信息提供给第三方牟利。国内外近年来对用户隐私越来越重视，各国纷纷通过立法、清查等方式保护用户个人信息。

随着用户使用习惯的变化，终端逐渐成为个人生活的中心。近 30%的用户在智能终端上停留的时间占据了非工作时间的近 30%，因此在终端上留下许多敏感、重要的个人数据。在与各个服务提供商签订隐私条款，信息被合法使用外，还可能有如下个人信息泄露情况：

- 操作系统收集个人信息。操作系统作为系统总体控制者和众多传感器的管理者，可能在为应用提供合法使用的同时，拷贝、截留部分信息。
- 软件平台非法手机个人信息。某些多 APP 公用平台、安全软件/管家类平台具有多 APP 的访问权限，后台收集并关联多 APP 收集的个人信息。
- 恶意或流氓软件非法手机个人信息。

而非法收集或非法使用个人信息可能带来的风险包括：

- 心理上个人生活被侵扰。保有隐私是个人的最基本的权利，不愿意被公开的信息会严重破坏个人尊严和独立感。
- 直接经济损失。金融、支付、购物类应用账户和凭据泄露，可能直接造成经济损失。
- 个人电子账户泄露，可能会影响个人形象，甚至造成财产损失。攻击者可能冒充用户去进行信息发布、社交活动，造成自己或家人个人形象受损；甚至可能通过诈骗手段引起经济损失。
- 定向推销或其他市场营销侵扰。
- 社交侵扰。社交网络或联系人信息泄露，可能会为自己的社交圈带来不便，进而影响

个人生活或个人工作。

3.2.3 非法接入和越权使用

非法接入和越权使用是传统网络主要攻击模式。在 5G 系统中，各种传统的封闭网络都对外开放，不再有物理上的封闭和隔离。攻击者只要攻破任何一个单点，都有可能入侵整个网络系统。非封闭的网络使得代理、肉鸡、攻击跳板更容易获取，且难以追踪。BYOD（Bring Your Own Device 自携终端）工作的模式下，终端往往又同时兼生活、工作两个甚至多个用途。这使得终端上限制安装软件、限制操作文件等传统防护手段失效。

3.3 通信安全威胁

终端上对外通信协议（蜂窝，WLAN，蓝牙，NFC 等）都设计了相应的安全协议，但由于协议本身漏洞或使用配置不当可能会受到通信安全攻击。例如，用户随意接入不安全的 WLAN 网络，配置任意蓝牙连接可见等。

3.3.1 位置追踪

终端在 WLAN 常开状态下，会周期性扫描周边的 WLAN 接入点，可能会被网络扫描到其硬件地址。这些接入点可以据此判断用户位置。终端内部安装的软件，可以获取到终端临近的 WLAN 接入点，根据接入点的位置，也可以计算用户的位置。

在 5G 前的网络中，终端在某些情况下会使用明文向网络报告自己的永久通信识别符（IMSI），如果识别符在空口或者在网络种被截获，则可以获取到用户的位置。

3.3.2 伪基站与降阶攻击

2G 的系统设计中，仅设计了网络对终端的单向认证，终端无法判断接入的是否可信的基站和网络。攻击者可以伪冒基站和网络，让用户连接到恶意网络，从而实现进一步攻击。例如，给用户发送短信诱骗用户点击恶意链接、下载恶意软件或者伪冒服务电话对用户实施诈骗等。

3G 和 4G 网络设计时，已经实现了双向认证。但是由于需要与已有网络的配合，一般用户配置允许降级回到 2G 网络。攻击者可以利用这个特性，制造条件让终端降阶接入到 2G 的伪基站，实现相同的攻击。

5G 之前的网络，虽然进行了用户隐私保护，使用用户临时标识替代其永久标识，但仍然存在用户向网络明文发送永久标识的设计。伪基站可以通过向用户请求其永久标识来对特定用户进行定位。5G 中设计了进一步的隐私保护，网络上不会出现永久标识。但是若伪基站对用户实施降阶攻击，使用户降回 4G（5G 不允许降阶接入 2G/3G 网络），则仍然可以实施类似攻击，从而导致用户隐私泄露。5G 初始部署阶段，运营商可能允许用户不更换 USIM 卡直接接入 5G 网络，仍然有可能泄露用户 IMSI（International Mobile Subscriber Identity，国际移动用户识别码）。当前仍有 4G/5G 无法覆盖的地区，而用户接入策略中很难对用户进行区域限制，因此运营商可能不得不允许用户回到 2G/3G 网络，仍然存在降阶攻击的可能。

3.4　终端作为信任根开放后的安全威胁

在以终端为中心的安全系统中，终端的可信作为安全信任的基础存在。终端不仅仅是设备的代表，它成为了人的衍生部分，代表“物理个体”（生物特征识别，“我是”）和“思想个体”（替代“我知”）的认证手段。如不实施可靠的安全保护，终端的遗失、伪冒等，可能造成巨大的损失，甚至是不可挽回的损失。

终端代表“物理个体”，存储了用户的生物特征。生物特征是伴随个人一生、不可更改的特征。若生物特征被获取，甚至被公开，那么作为“物理个人”将失去个人的“物理特征唯一拥有者”的属性。换言之，任何人都可能伪冒个人，导致此个人不可能再将生物特征作为识别自己的可靠凭证。5G 时代，生物特征信息数据将成为的网络安全攻防一个重要战场。

终端遗失或被盗用时，攻击者可以使用终端作为凭证进行各种活动。例如伪冒身份进行商务活动、电子支付、社交活动等，从而造成经济、名誉、心理上的损失。因此，终端上对于“授权”的操作，极为重要。必须通过防护手段，保证终端只有得到自由意志的所有人的授权后才可代表个人。

3.5　　5G 系统安全威胁

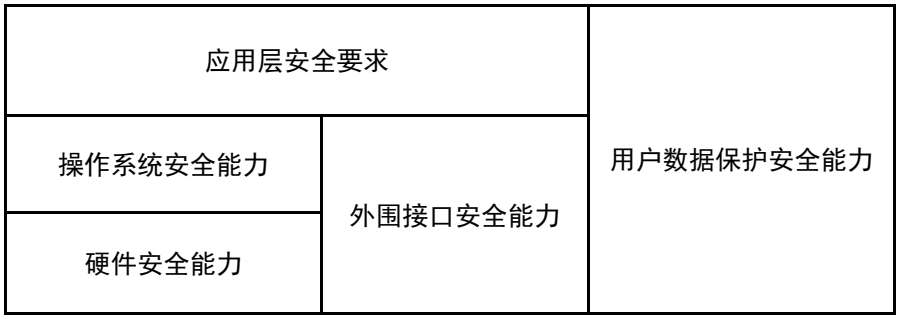
5G 网络系统设计中引入了大量先进技术和理念，例如虚拟化、服务化的核心网，网络能力对外开放，边缘计算与就近服务等，促进了新的业务场景和业务形态的出现，引入了大量新形态的终端。所有的这些变化都会带来新的安全威胁。

5G 中会大量运行敏感业务和高等级安全业务，例如移动支付、警务、救援等。攻击这些业务造成的安全风险不言而喻。5G 系统中业务多样化、开放化，广泛渗透到各个领域，包括工业生产、公共安全等。很多领域的通信之前仅运行在封闭网络环境中，使用特定的终端和软件。这些领域使用公共网络后，会面临来自开放网络的威胁。

5G 中终端形态多样化。从低成本低功耗低管理的物联网终端，到普通用户的移动智能终端，到工业应用终端（机器人、车辆、产线等），联网的基础设施，到高度专业化的终端（医疗器械，警用终端等），有不同的计算和通信能力，不同的数据和业务流程。攻击者会根据终端的业务特征、数据敏感度、业务失效后的影响，以及终端的不同能力进行攻击。5G 系统中对终端和业务的防护应综合考虑进行计划和部署。

4　安全解决方案

终端的安全架构如下图所示（参考[6]和[7]）：



移动终端的安全，目的是保护用户的应用和数据、终端的功能不被侵害。终端须从硬件、操作系统、软件、通信和数据等实现全方位保护。除此之外，终端系统设计还应满足用户对终端的知情权和控制权。即所有对用户个人数据和敏感功能的操作，须通知用户，并且得到用户许可后方可执行。

本章描述的安全解决方案对应于上述终端安全架构，具体如下表：

应用层安全	• 用户认证授权 • 部署防火墙
操作系统安全	• 杀毒软件（软件/硬件） • 虚拟机隔离
硬件安全	• 可信环境 • 硬件杀毒
外围接口安全	• 通信加密完整性保护 • 5G SUCI • 5G 终端认证 • 5G ME 认证 • 伪基站防护
用户数据保护安全	• 杀毒软件 • 可信环境 • 虚拟机隔离

4.1　传统方案

4.1.1 用户认证和授权

传统方案中，采用分层+端到端认证授权的方式。网络访问的第一跳对用户进行接入验证和授权，网络层则在核心网与终端实现端到端认证，以及在非安全区域进行 IPsec 分段保护，传输层实现端到端的认证、授权。

认证和授权包括管理流程和协议流程 2 个部分。通过管理流程，将服务器和客户端标识配置到可信列表中，并为每一个可信的对端分别设定相应的验证凭据，为此对端设置相应的授权信息。管理流程中还必须保证，所配置的标识和标识所代表的角色之间对应关系。为相应的组织颁发数字证书，为个人分发认证令牌前，必须对组织和个人进行相应的验证，例如查看组织的营业证书、个人身份证等。认证流程一般通过凭据比对、挑战-应答、非对称密钥

计算等方式完成。认证结束后，两端/多端根据配置的授权信息，对请求的数据或服务进行相应的过滤，仅提供其有权访问的服务和数据。

对于个人的认证，所使用的凭据一般分为“我知（knowledge factor）”、“我是（inherent factor）”、“我有（possession factor）”的形式。“我知”指的是用户口令类，通过头脑记录的信息或知识，代表“思想个体”；“我是”则一般使用自然人的生物特征，代表“物理个体”；“我有”则是配发相应的设备，例如使用的终端、电子门禁卡、令牌卡等来承载“逻辑个体”。

为提高认证的安全性，大部分敏感业务 APP 采用了多因子（multifactor）认证方式，用户须提供上述 3 类中的 2 类凭据完整认证。一些敏感业务 APP 将用户与设备绑定，仅允许被授权设备运行的 APP 接入。通过发送短信或语音验证码也常常用于 “我持有合法终端”的证明方式。为进一步保证安全性，某些 APP 对终端的地理位置进行识别和限制（“我在”）。相比于传统的 PC 通过 IP 地址的识别，移动智能终端可通过 LBS（Location based service）或 GPS 的辅助对用户进行访问地认证。如果用户脱离了其日常活动区，则需要其提供更多的凭据信息。一些购物网站会采用购物历史或浏览历史作为“我知”的挑战内容，以此保持了用户知识的动态更新，提高其安全性的同时保证用户的使用便利。

移动智能终端中常使用 SSO（Single Sign on）方式为用户提供便利的认证，即不同的服务提供点仅需认证一次。SSO 可能是同一个服务者内的不同站点，也可能是第三方提供的认证，例如某些 APP 使用微信或淘宝提供的对外认证服务，以及移动运营商对外提供的认证服务（例如 GBA, General Bootstrapping Architecture 或其他方式）。

4.1.2 通信加密和完整性保护

通信加密用来保护通信的保密性。因为只有持有相应的解密密钥才可以访问真正的信息内容，从而实现对信息的访问控制。加解密的密钥分发和协商，通常伴随认证协议的执行而产生，以保证密钥的新鲜性。

完整性保护用来保证信息来源的正确，以及信息在传输、存储、转移过程中未被篡改。完整性保护一般使用终端配置的凭据或在密钥分配/协商过程中产生的密钥，对消息进行电子签名（对称或非对称算法）。接收方可以根据签名通过相应的算法验证数据完整性是否被破坏。

移动智能终端在进行数据的加解密和完整性保护的计算过程中，会提高电能的消耗。而一般加密和完整性保护会增加数据量，从而需要更多的通信流量。出于耗费电量和流量的考虑，

终端 APP 在传送消息时，可以区分信息的敏感程度，对敏感数据进行加密和完整性操作。对于一般数据，例如访问资讯网络的内容，观看网络流媒体等，做简单的加密和完整性保护甚至不做保护。对于某些信息做完整性保护而不做机密性保护（例如软件和配置文件下载）。对于个人相关信息则必须提供机密性和完整性保护，以防止个人信息被泄露或篡改。

4.1.3 终端侧安装杀毒软件

大部分攻击的侵害目标是终端上的软件或信息，因此提高操作系统和软件的防护能力是防护入侵的有效手段。移动操作系统都有严格的隔离和访问控制功能，应用软件访问用户敏感数据和敏感功能，以及跨应用的数据访问须经用户许可。

大部分安卓智能终端允许通过非官方应用商店甚至通过网络链接安装 APP。APP 来源不能保证安全可信，为终端带来安装恶意软件甚至病毒的风险。操作系统在下载可安装文件时、安装不明来源的软件时，会提醒用户安全风险。部分终端内置了自研或第三方病毒查杀工具，禁止安装未通过安全检查的软件。终端通过周期性查杀系统和数据，保证不受恶意软件侵害。

4.1.4 网络和服务器侧部署防火墙

终端的运算能力、存储能力和通信能力限制，很难对抗最新的攻击方式或恶意软件。终端是分布式的节点，相互间很难协同。在网络传送集中点或服务侧服务集中点部署防火墙和入侵检测/入侵防护措施是必要且有效的。

某些漏洞从被攻击者发现到防病毒软件有识别能力需要一定时间。杀毒软件不能仅仅依赖于病毒的特征去判别。大部分杀毒防毒软件，尤其是内置的软件，可以通过非法访问的行为识别去判断病毒。判断结果上报到云端统一处理。云端利用其中心位置，通过大数据处理，可进行安全态势感知，并下发判断规则到未被感染的终端，提前病毒防护的时机。

安全态势感知系统与网络侧联合，在网关处对已识别出的恶意资源 URI 进行过滤，防止有安全隐患的、恶意的文件被下载到终端。网络还可以在网络层对攻击终端的流量进行防护，例如对终端的 DoS 攻击可以在网关处过滤，避免占用终端过多的通信流量和计算能力。

4.2　新兴和附加方案

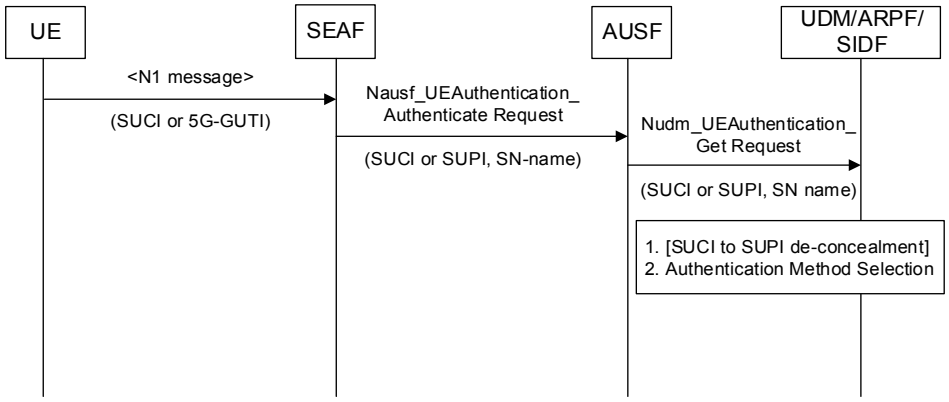
4.2.1　5G SUCI

为了让网络能够识别用户，用户必须发送用户永久标识（Subscription Permanent Identifier，SUPI）。在 LTE 里，与之对应的是国际移动用户识别码（International Mobile Subscriber Identity，IMSI），IMSI 在 LTE 网络中不经过任何加密被清晰地发送，因此 4G 导致了许多与隐私相关的攻击。5G 网络为了增强认证过程中的安全性，发送的是经过非对称加密算法加密的用户隐藏标识（Subscription Concealed Identifier，SUCI），用来保护用户隐私。

在 LTE 系统中，为了避免 IMSI 在空口中的传输，会引入临时移动用户识别码（Temporary Mobile Subscriber Identity，TMSI）。TMSI 由 4G 核心网分配，并且持续更新以确保跟踪者无法确定是同一个使用者。在用户入网之后，IMSI 就被 TMSI 代替在空口中传输，但是 IMSI 仍会有机会暴露在空口中。在用户第一次入网或者 TMSI 的认证失败之后，就需要 IMSI 进行身份认证。目前已经有一种专门用于捕获用户 IMSI 信息的设备，IMSI 捕手。IMSI 捕手利用 4G 网络移动切换中的协议漏洞迫使用户连接到假基站上，然后启动身份认证程序。强行发起初始认证，或发起 IMSI 标识请求，需要 UE 上报 IMSI 进行身份认证，从而完成对用户 IMSI 信息的捕获。捕获用户的 IMSI 信息可以跟踪用户的位置，甚至有可能窃听通话内容或冒充用户进行通话。

在 5G 系统中，引入了非对称加密算法对 SUPI 进行加密。SUPI 用公钥进行加密之后成为 SUCI。公钥放在手机端，私钥放在归属网络的 UDM/ARPF 中，以对 SUPI 进行更加严格的保密。对 SUPI 加密生成 SUCI 时所使用的公钥由归属运营商确定、解密私钥只有归属网络知道。在用户发起鉴权的整个过程中，一直都是 SUCI 充当之前 LTE 系统中 IMSI/TMSI 所扮演的角色。而且每次加密会生成不同的 SUCI，只有在 UDM/ARPF 中才最终解密得到正确的 SUPI。这样即使窃听者获取到 SUCI 也无法解密获取到 SUPI，而每次截取到不同的 SUCI 也让攻击者无法识别是否同一个用户，无法定位和跟踪用户。因此最大程度上保证了 SUPI 的安全，阻止了攻击者通过捕获用户的 SUPI 来跟踪用户位置。

具体的认证程序如下：



认证程序的启动

1) 用户携带 SUCI 或者 5G 全球唯一临时用户标识（5G Globally Unique Temporary UE Identity，5G-GUTI）向安全锚功能（Security Anchor Function，SEAF）发起注册请求。如果使用 SUCI，则用户必须生成新鲜的 SUCI，不得重复使用前次使用过的。
2) SEAF 在接收到信号之后进行解调，查看是 SUCI 还是 GUTI，如果是 GUTI，则匹配到对应的 SUPI，如果是 SUCI，则不进行解密。SEAF 携带 SUCI/SUPI 和对应的网络服务信息 SN-name 向身份验证服务器功能（Authentication Server Function，AUSF）发起鉴权申请。
3) AUSF 通过分析 SEAF 携带的 SN-name，确定手机是否在网路服务范围内，并保存手机所需要的网络服务信息。然后继续将 SUCI/SUPI 和 SN Id 转发给 UDM/ARPF。
4) 在 UDM/ARPF 中调用 SIDF 将 SUCI 解密得到 SUPI，然后通过 SUPI 来配置手机所需要的鉴权算法。
5） AUSF 将 SUPI 告知 SEAF。SEAF 及所在服务网络内部将以 SUPI 作为用户的永久标识。

在服务网络与用户间失去同步时（例如服务网络无法识别终端上报的 5G-GUTI），服务网络会向用户请求其用户标识。用户回复 SUCI，服务网络请求归属网络解密后获得 SUPI，重新与用户获得同步。

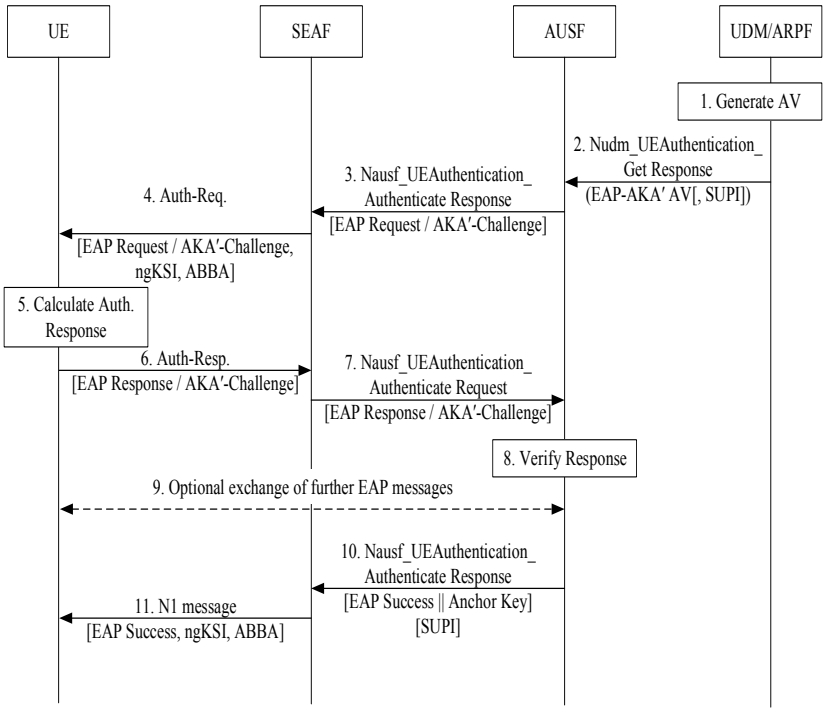
4.2.2 对 5G 终端的认证

在 5G 系统对终端的认证过程中，EAP-AKA 和 5G AKA 是强制性的认证方法。5G AKA 通过向归属地网络提供来自受访网络的 UE 成功认证的证据来增强 4G LTE 的 EPS AKA 协

议。4G 的认证协议是基于对称密钥的，而 5G 的认证协议也可以基于非对称密钥，可以使用通用的 EAP 协议。同时，对 5G 终端的认证不仅仅是对 UE 的认证，更重要的是还可以对移动设备（Mobile Equipment，ME）进行认证。

下面分别给出 EAP-AKA'，5G AKA 以及 5G ME 的简要认证过程。

- **EAP-AKA'身份认证过程**



EAP-AKA'认证程序

1) UDM/ARPF 生成一个认证矢量，然后按照规范计算 CK'和 IK'，并用 CK'和 IK'替换 CK 和 IK。
2) UDM 将转换后的认证矢量 AV'和 SUPI 发送给 AUSF。
3) AUSF 发送 EAP 请求以及 AKA 挑战给 SEAF。
4) SEAF 把收到 EAP 请求以及 AKA 挑战转发给 UE，同时还要将 5G 密钥集标识符 ngKSI 和架构之间的反投标 ABBA 参数一起发送给 UE，这两个参数由 SEAF 生成。
5) UE 根据接收到的信息计算响应（RESponse，RES）。
6) UE 将 EAP 响应和 AKA'挑战消息发送给 SEAF。
7) SEAF 将 EAP 响应和 AKA'挑战消息转发给 AUSF。

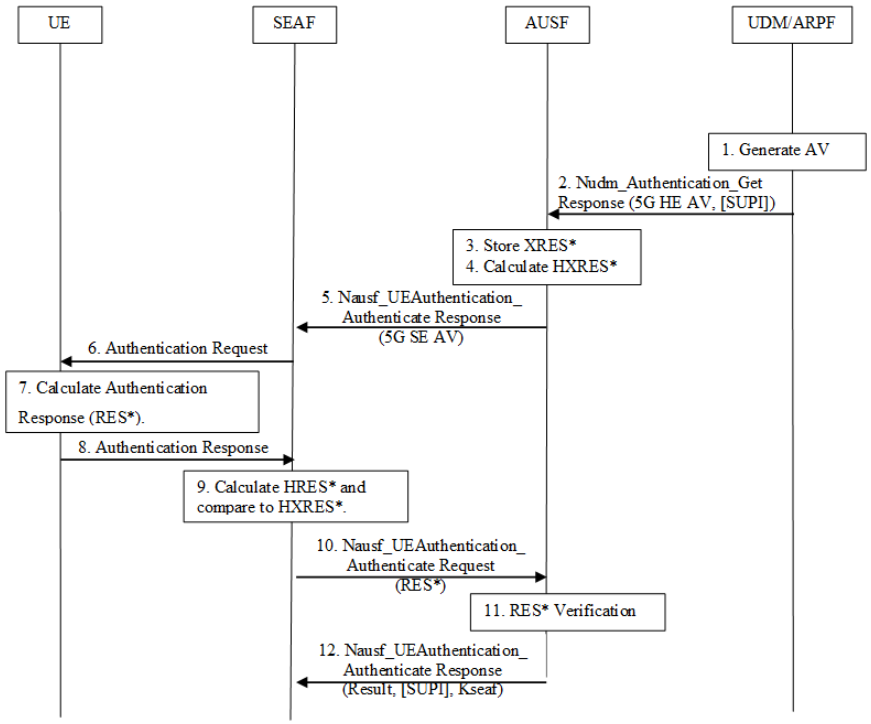
8) AUSF 验证该消息，如果认证失败则返回错误，如果认证成功则继续。并将有关认证结果的信息通知给 UDM。

9) AUSF 和 UE 通过 SEAF 交换 EAP 请求 / AKA'通知和 EAP-响应/ AKA'通知消息。

10) AUSF 计算出 KSEAF。AUSF 向 SEAF 发送 EAP 认证成功消息，并转发给 UE。响应消息中包含 KSEAF 和 SUPI。

11) SEAF 将 EAP 认证成功消息发送给 UE。该消息还应包括 ngKSI 和 ABBA 参数。

- **5G AKA 身份认证过程**



5G AKA 认证程序

1) UDM/ARPF 创建 5G 归属地环境认证向量 5G HE AV。然后导出 K_{AUSF}。

2) UDM 将 5G HE AV 返回到 AUSF，同时指示 5G HE AV 将用于认证响应中的 5G-AKA。如果 SUCI 包含在请求中，则 UDM 将在响应中包含 SUPI。

3) AUSF 应将认证参数 XRES*与收到的 SUPI 一起存储。

4) AUSF 计算归属地认证参数 HXRES*，并生成 5G SE AV。

5) AUSF 将移除 KSEAF，并将 5G SE AV 返回给 SEAF。

6) SEAF 向 UE 发送部分参数、标识 K_{AMF} 的 ngKSI、在身份验证成功时创建的部分安全上

下文以及 ABBA 参数。

7） ME 转发消息至 USIM，计算响应 RES，ME 从 RES 计算 RES*。

8） UE 将 RES*返回到 SEAF。

9） SEAF 从 RES*计算 HRES*，并比较 HRES*和 HXRES*。如果它们一致，则从服务网络的角度考虑认证成功。如果没有，则 SEAF 按照规定进行。如果未到达 UE，并且 SEAF 从未接收到 RES*，则 SEAF 应认为认证失败，并向 AUSF 指示失败。

10）SEAF 应将来自 UE 的 RES*发送给 AUSF。

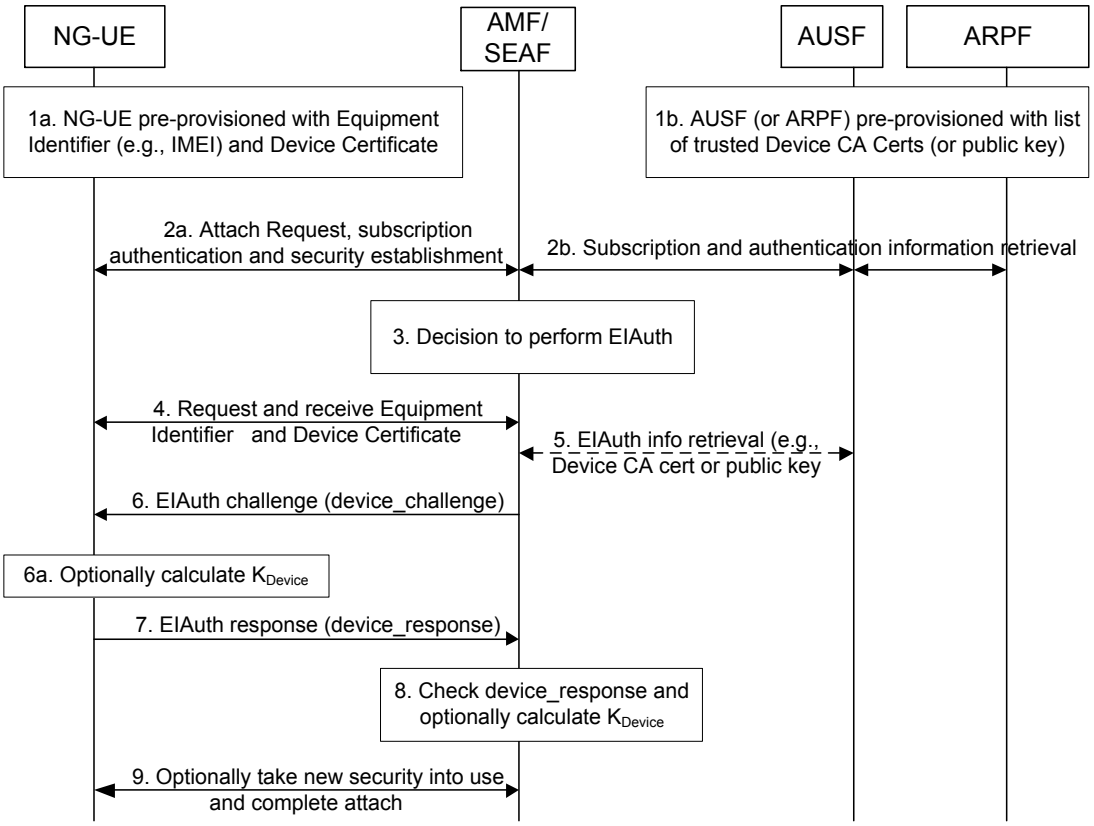
11）AUSF 验证认证向量 AV 是否已经到期。如果 AV 已经过期，则 AUSF 可以认为从归属地网络的角度来看认证是不成功的。 AUSF 将收到的 RES*与存储的 XRES*进行比较。如果相等，则 AUSF 从归属网络的角度考虑认证成功，AUSF 向 UDM 通知认证结果。

12) AUSF 向 SEAF 通知认证结果，如果认证成功，在响应消息中携带 K_{SEAF}。如果 AUSF 在认证请求中从 SEAF 收到 SUCI，则 AUSF 还应在响应消息中添加 SUPI。

注意，上述的认证过程中，SUPI 仅在运营商网络内部出现，不出现在空口或回传网络中。

- 5G ME 认证过程

EAP-AKA 和 5G-AKA 认证的是用户身份，并没有对 ME 做认证。但 5G 需要支持各种类型的终端，这些终端会具有不同的安全能力，5G 也会支持不同的业务，一些业务的提供很可能会依赖于终端的安全能力，但某些安全能力可能并不是所有终端都能支持的。因此，5G 网路除了需要对用户的身份做认证外，很可能还需要对用户正在使用的终端设备做认证，以保证用户正在使用的终端有权或适合接入到所请求的业务中，因此 5G 未来可能会附加地对 ME 进行认证。



5G 终端设备标识的验证

1a. 5G-UE 被预先配置了一个全球唯一的 IMEI 号和可用于认证 IMEI 的设备证书；

1b. 相应地，AUSF/ARPF 被配置了可信终端设备的 CA 证书里列表。归属 PLMN 控制哪些终端需要进行终端认证和使用哪种终端 CA 进行认证 ；

2a. 5G-UE 使用用户的身份 ID 和信任状附着到服务网络;

2b. 服务网络/归属网络和 5G UE 相配合完成用户身份认证；

3. 网络决定需要对终端进行附加的终端 ID 认证；

4. 网络向 5G UE 请求终端 ID，5G UE 返回终端 ID (例如 IMEI)，可能也包含终端的数字证书；

5. 如果需要，AMF/SEAF 向归属地的 AUSF 请求可认证终端的 CA 证书或可信任的公钥；

6. 网络向 5G UE 发生设备 ID 挑战；

7. 5G UE 计算和返回设备 ID 响应；

8. 网络校验 5G UE 返回的设备 ID 响应；

9. 可选地，网络根据已认证的设备 ID 使用特定的安全功能。

设备标识可以唯一标记一个用户，因此在设备认证过程中，要避免明文传送永久标识，以防被窃听后泄露用户的位置隐私。同时，要求 UE 的硬件标识和其认证凭据要实现安全存储，以免被盗用伪冒。

4.2.3 5G 网络安全

5G 通信安全在网络安全传统方案的基础上，着重关注新网络边界、网络切片和边缘计算的安全问题。

1) 5G 新网络边界安全

5G 网络打破传统网络边界，需要新的安全架构。从总体上说，5G 网络由终端侧、接入网、边缘侧、承载网、核心网几部分构成，5G 新网络边界安全需要从终端、边缘侧和核心网三个节点上部署安全防护能力。在终端侧加强设备检测评估、可信标识、认证授权、数据加密和安全 SDK 的部署。在边缘侧加强协议分析、可信接入、流量检测、行为分析、设备发现，以及边缘态势感知（感知神经节点）。在核心网加强虚拟化平台安全防护、数据安全和应用安全防护。

2) 5G 网络切片安全

5G 网络采用 SDN 和 NFV 等技术实现物理网络的灵活划分，应对不同的应用场景。与此同时，SDN 和 NFV 技术也面临新的安全威胁与需求。针对 SDN 网络，加强控制平面和数据平面抵抗网络监听、IP 地址欺骗、DoS/DDoS 攻击和病毒木马攻击的威胁的能力，解决南向和北向外部接口的协议安全和非法访问问题。针对 NFV 网络则重点保护虚拟化基础设施安全以及虚拟网元的安全。

3) 5G 边缘计算安全

多接入边缘计算（MEC）是 5G 网络核心技术。在数据缓存、数据分析、提高应用可靠性等方面具有重要作用，但也面临架构安全、功能安全、信任机制等方面的安全问题。架构安全主要解决 MEC 平台处于相对不安全的物理环境而可能遭到外部和内部网络攻击。功能安全主要解决 MEC 应用下沉带来的用户发生跨节点访问和安全传递问题。信任机制主要解决 MEC 多元化的用户及服务之间跨区域、跨平台、跨行业信任问题。

4.2.4 伪基站防护

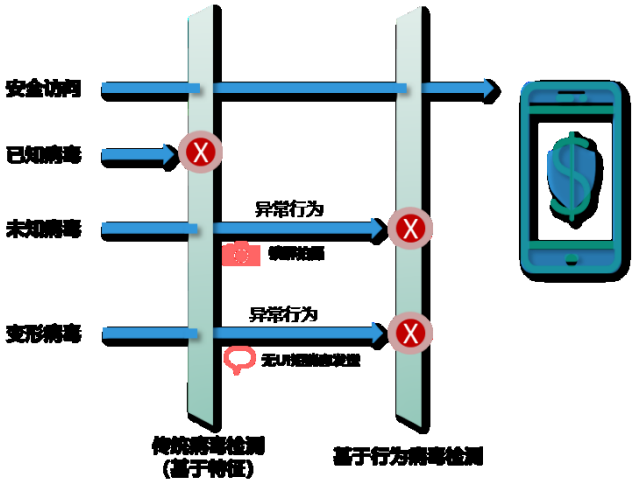
伪基站的目的是干扰正常通信，且伪基站并没有能力接入运营商的可信网络，因此其行为必定有异常之处。可以通过监测异常物理层信号、异常广播消息、异常的位置区信息等方法辨别伪基站。这些检测可以集成在无线收发芯片中或 SoC 中，也可以通过终端上软件实现。终端可以从网络或从可信服务器获取可信基站地理位置列表，排除非列表中的基站。

终端接入伪基站，需要依赖伪基站的广播信息。3GPP 正在研究如何对广播信息进行安全认证，终端如果收到验证失败的信息，则不会发起接入请求。5G 系统中有望彻底消灭未来伪基站的攻击。但在 5G 仍未能实现全覆盖，或在 NSA 中使用 4G 核心网时，降阶攻击仍然有可能成功。

4.2.5 基于终端底层调用监控的病毒和恶意行为检测

传统的病毒查杀软件运行在操作系统层或软件平台层，其识别能力和控制能力基于软件行为特征和软件控制下的信息分类。软件和数据的完整性一般基于对文件的判断。对运行时的数据和代码的运行时完整性保护很难做到，因为 OS 和软件本身运行环境可能受到完整性破坏。通过软件实现的内存完整性验证效率非常低。

为了应对病毒和恶意软件的动态变化，从而实现早发现早防护，基于硬件的防护措施应该是有自学习能力，可以学习设备、软件和用户的使用习惯，根据软件或输入设备的异常行为识别恶意的软件，阻断其访问。例如，在锁屏的情况下启动了拍照功能，或者在用户未操作的情况下发送短信，即可识别为恶意行为。



基于行为的病毒检测

通过底层硬件进行病毒和恶意行为检测，可以提高对恶意行为的检测粒度，可以配合外围的安全外设和安全驱动，对恶意访问行为进行彻底的隔绝。硬件可以高效实现内存中敏感代码和敏感数据的完整性监测，更容易发现病毒的恶意行为。由于其监控粒度更小，行为识别能力更强。硬件中内置的识别能力，其运行不暴露于系统中，很难被外界入侵破坏，从而健壮性和健康得到保证。

以硬件为基础的恶意软件/病毒查杀能力，通过为操作系统和应用 APP 提供相应的访问接口，可以兼得传统方式的优势，提供更灵活有效的查杀机制。同时，单设备的行为学习以及恶意软件/病毒标识，可以为云侧的态势感知系统提供更有效的统计、告警、更新数据的能力。

4.2.6 可信环境和可信终端

5G 是新型基础设施，对推动工业转型升级、加快新型智慧城市建设起到重要作用，它应用连通了物理世界和网络世界。因此 5G 终端工作在复杂的环境下，在安全领域，终端自身的可信需要与网络环境的可信乃至物理环境的可信同步进行可信认证，以防止物理设备与数字身份之间的错位。

（1）可信终端认证

终端可信认证的组件包括：

- 终端可信标识。利用终端可信标识技术，拥有设备级的可信标识，保证终端唯一、可信。
- 终端自身防护。终端环境感知客户端具备自我保护能力，终端在系统驱动层增加可信控制驱动，系统启动后驱动即生效，保证客户端程序目录下的相关文件均是不可以被篡改、注入、拦截、恶意终止，保证客户端程序的可信。
- 通信加密。服务端与客户端传输通信通过加密机制进行加密通信，保障通信安全。
- 身份认证。终端环境感知系统可与访问控制平台、安全应用网关等业务访问控制设备联动，协同完成设备的身份认证工作，构成完整的信任体系。

终端可信认证的技术有许多种类，其安全强度也有所不同，主要包括以下三类技术：

- 芯片级终端安全

  可信机制与芯片/模组厂商的适配，实现硬件级别的物联网设备安全 SDK，快速实现业务同时满足安全信息采集需求。

- 设备级终端安全

  对基于 windows、Android、Linux 的通用客户端进行适配，对设备厂商定制后的的精简操作系统的最大化支持。

- 通用终端安全

  标准 Windows 和 Linux 的设备适配，部署纯软件实现的客户端。

（2）可信环境感知

可信环境感知包括网络环境的感知和物理环境的感知。

1) 网络环境感知

网络环境感知系统具备基础安全感知、系统安全感知、应用合规感知、健康状态感知等四大类系统环境感知能力。

- 基础安全感知是指拥有感知病毒、APT 攻击、系统漏洞等威胁的能力。
- 系统安全感知是指拥有感知有关登陆、帐户、配置等相关的风险能力。
- 应用合规感知是指拥有感知是否存在非合规的软件、进程、注册表键值等风险能力。
- 健康状态感知是指拥有感知是否存在与浏览器相关、文件操作相关、桌面相关的终端健康相关风险能力。

2) 物理环境感知

终端环境感知系统客户端可以通过各种物理环境感知设备来识别操作终端的设备状态和人员操作，从而识别如设备替换、UKEY 插拔、多人围观、授权人离席等物理环境风险的能力。

3) 安全管理

终端管理。能够对安装了终端环境感知系统客户端的电脑进行统一管理，能够对所有终端进行统一分组管理、查看所有终端的状态、并针对终端进行策略统一下发等。

终端策略管理。能够对安装了终端环境感知系统的所有终端进行密码保护策略设置、升级策略设置；能够配置与控制中心的通讯策略、网络流量策略、终端数据上报接口频率设置，并对终端的外观进行自定义。

感知模板管理。能够支持环境感知的模板创建功能，感知模板目前支持基础安全感知、系统安全感知、应用合规感知、健康状况感知等四大感知分类的百余项配置项，能够对所有感知风险进行风险的自定义和扣分规则的自定义，并能够创建多个不同模板。

4) 风险度量

基于终端风险度量技术的度量自定义，形成风险评分和风险报告。风险评分采用“可信加权”原则，将所有风险项产生的权值进行相加，以百分制提供给策略方，策略方再根据不同的权值制定相应的安全策略，主要目的是提供快速终端可信鉴定能力，所有业务安全访问策略可以基于分数的高低来进行设置；风险报告主要目的是提供深度终端可信鉴定能力，所有业务可以基于报告中的具体属性进行细粒度的业务访问控制。

4.2.7 虚拟机隔离

当前主流终端中，同一套硬件下仅允许一套操作系统，不同的 APP 间使用软件沙箱技术隔离。随着虚拟化技术的发展和终端硬件能力的提升，使用 VM（Virtual Machine，虚拟机）隔离多个应用成为可能。使用虚拟机可仍然沿用一套硬件，可以保持终端的便携性。但是对于应用环境的隔离和存储空间的隔离更彻底。当然，随着硬件技术的发展，多套硬件集成化后仍可不降低终端便携性，直接把 VM 建立在独立硬件上可提供更高的安全保护。不同 VM 间的访问必须通过主机间接口才可完成，因此更容易监控，更安全。

虚拟化平台可通过探针的形式对 VM 中的 OS 和 APP 进行监控，进行病毒查杀功能。由于平台与 VM 中的操作系统相互关联度低，独立监控效率更高、识别和查杀能力更高。

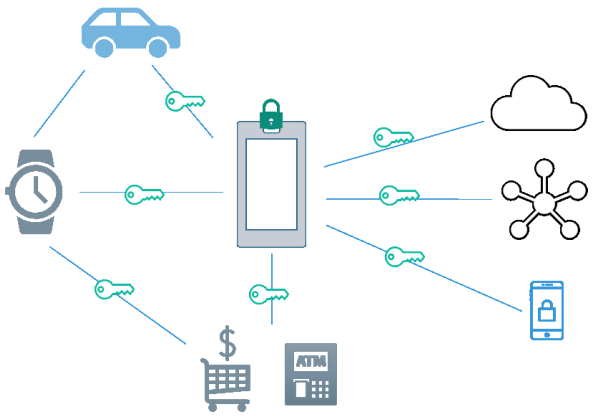
传统终端架构　　虚拟化终端架构

虚拟架构下必须保证虚拟化平台的安全性。必须保证 VM 中的应用不能穿透虚拟机访问虚拟化平台的数据，保护虚拟化平台免遭网络攻击。

虚拟化平台的一个发展趋势，是由硬件平台（例如 SoC）直接提供虚拟化能力，提高虚拟化平台自身的安全保护。

5　终端为中心的安全

5G 带来业务的广度和数量爆炸性增长，个人以终端为中心的工作和生活模式，基础设施和 IoT 的发展，使得 5G 安全具有业务点多，攻击点多，终端能力多元化、安全风险分散的特点。作为通信端节点的通信终端，成为 5G 安全中的重要环节。通过安全技术对终端进行安全加固，保证终端成为一个可信任的根节点，并使用该根节点的“可信”去请求和访问服务和资源，可以保护网络和服务免遭恶意攻击。这种“可信”可以扩展到其他设备，形成以终端为中心的安全体系。



以终端为中心的安全体系

在此体系中，远程证明是网络和服务信任终端的基本方式，终端可信根则为终端实现远程证明提供了安全技术支撑。在此基础上，可以实现终端安全令牌的认证、终端授信外设以及能力开放。终端作为用户个人的身份延伸，必须有机制实现可信的用户认证、授权以及角色隔离和转换。

5.1　终端可信技术

终端可信指的是其设定的属性、宣称的属性和能力与其实际拥有和提供的一致程度。。

5.1.1 可信终端

终端的可信，保证设备是可信赖的厂商提供，当前运行状况是健康的、安全的。包括：

- 硬件可信：
  - 终端硬件是可信的生产厂家生产，通过厂商的质量及可信认证。终端硬件是以合规的方法生产，通过合规部门的认证。厂商可以申请质量和安全体系认证以及入网认证，并获得可信级别证书。每生产一部终端就为此终端生成终端唯一的标识和密钥对（对称或非对称）或证书，并使用厂商数字证书对终端信息进行签名。其中，证书和私钥部分可被安全环境（TEE）或安全模块（SE）保护。
  - 终端已被激活，终端硬件未在报失、锁定状态等。终端应提供访问控制（例如锁屏密码），在丢失遭窃的情况下，可通过远程锁定的方式，限制对终端功能和数据的使用。
  - 若终端硬件与特定的外设或与特定的物理位置、通信网络绑定，则此绑定未被破坏。例如，位于 A 点的红绿灯被移除到 B 处，属于物理绑定破坏。
  - 终端硬件敏感功能、、系统关键模块完整性未遭破坏，无未授权的关键部件替换；硬件间的绑定关系未遭破坏。例如，若硬件指纹传感模块被替换，则原存储的指纹数据不允许被访问，被指纹所控制的敏感功能或敏感数据不允许被访问。终端可提供数据自动删除功能，在硬件模块被未授权替换时，可自动触发删除相关的数据和功能配置。
  - 终端硬件敏感功能模块、系统关键模块间安全通道未被破坏。
  - 终端硬件不在未授权维修、调试状态。如处于授权维修状态，则可能需要对终端功能及某些数据做限制访问。可防止终端被未授权刷机或非法读取数据和运行状态。
  - 终端可提供基于硬件的安全存储能力。
  - 终端可提供纯硬件的安全协议和安全计算能力，并提供相应的接口供操作系统或软件调用。
  - 终端可提供基于硬件保护的传感器、通信模块、人机交互模块等，并提供相应的接口供操作系统或软件调用
  - 终端可提供基于硬件的系统监控、异常行为监测、病毒分析及预警能力，并提供相应的接口供操作系统或软件调用

- 平台可信：
  - 固件系统完整性未遭破坏
  - 操作系统完整性未遭破坏
  - 硬件驱动来自可信提供方，完整性未遭破坏
  - 平台软件来自可信提供方，完整性未遭破坏
  - 硬件驱动和平台软件运行不超越系统授权
  - 操作系统、平台、驱动，有足够的通信、数据、计算保护能力
  - 操作系统、平台有运行环境、存储、接口的隔离和访问控制机制
- 软件可信：
  - 所运行的软件来自可信的、授权的开发者，软件功能不超越其可信的授权范围，不超越操作系统和平台系统授权
  - 软件代码及所依赖的配置、数据未遭完整性破坏
  - 软件无恶意行为
  - 软件执行的功能不超越用户的授权
  - 软件的通信、数据得到足够的安全保护
- 数据可信：
  - 终端上存储的敏感数据具有访问控制机制
  - 终端上存储的敏感数据进行完整性保护
- 可信通信
  - 终端与周边设备的通信使用了适当的安全防护措施，包括技术防护能力和正确的安全配置
  - 终端运行规范的安全通信协议进行远程通信
- 隐私保护
  - 终端有能力保护用户的个人信息不被泄露
  - 终端上对个人信息的操作合乎法律要求，例如告知同意

终端安全必须以可信为基础，继而实现互信、实现业务的可信。

5.1.2 可信存储

可信存储用于存储敏感数据，例如口令、密钥、个人生物特征信息等，并实施访问控制。只有得到授权的访问被允许，从而防止敏感数据被非法泄露、增删改。可信存储实现有几种形式：

- 基于硬件：　将敏感数据，例如密钥、生物特征等数据，存储在硬件中，并且相关的运算也在硬件中进行，对外提供安全加解密、完整性保护和完整性校验，信息比对等工作。做到所有的敏感信息在内存、总线、永久存储中不可见。
- 软硬件结合：　　硬件中存储根密钥，用根密钥来保护其他密钥，其他密钥用于各种不同数据的保护。在永久存储中开辟安全访问区，对此区域的内容进行加密和完整性保护。安全访问区内可存储敏感数据。由于基于硬件的根密钥，因此数据离开本机后无法被恢复、读写。但由于敏感计算由软件完成，因此如不做可信计算的保护，存在信息可能被从内存中窃取等风险。
- 纯软件实现：无硬件辅助的情况下，使用软件对敏感数据进行加密和完整性保护，以及提供访问控制机制。根密钥也必须使用软件保护，因此安全性差。
- 远程可信存储：　敏感数据经过安全保护后存储在远端，例如在公有云或私有云中。用户可以在多终端中分享敏感数据，例如用户无需记忆特定网站的用户名密码，每次使用时从远端获取。远端须对用户和设备进行验证和授权，仅允许授权的设备、授权的 APP 中使用特定的敏感数据。

可信存储一般用加密的手段进行保护，使用基于硬件的加密，加之基于生物特征或用户密码的认证授权保护。加密的密码可以是被硬件根密钥保护的密钥。另一种保护手段是基于用户口令的密钥。在这种保护下，加密的密钥由用户口令加其他材料生成，在终端上完全不保存解密密钥。每次进行加解密操作时，由用户即时输入口令，根据口令即时计算生成密钥（PBE，Password-Based Encryption，基于口令的加密）。结合可信用户界面的保护，密钥生成和数据加密过程完全是硬件完成且不需要保存更无需保护密钥。

5.1.3 可信执行环境

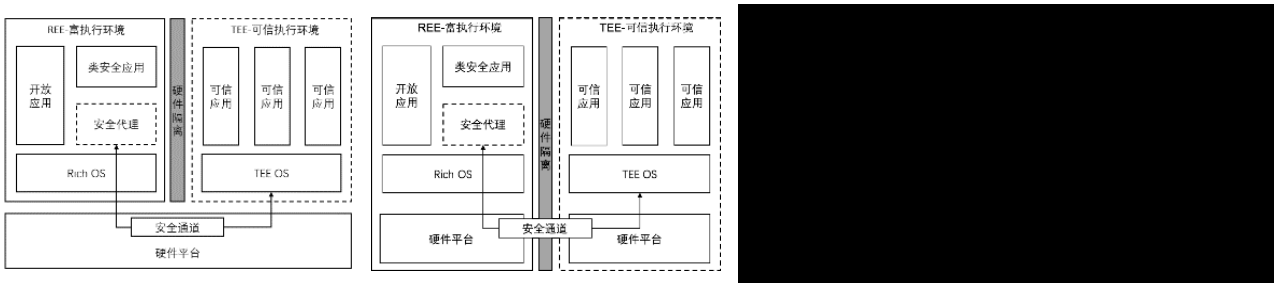
可信执行环境区别于普通执行环境，在其上运行的功能可以保证其安全性。可信执行环境须与普通执行环境隔离，且提供不同可信 APP 间的隔离运行环境。可信环境可以是独立

硬件实施隔离，也可以通过虚拟化或操作系统实施的软隔离。可信执行环境可执行对敏感数据、敏感功能和敏感外设的操作，保护这些数据和功能的安全。

由于可信执行环境的代价较高，因此一般 APP 会将敏感操作部分交由可信执行环境运行，普通操作留在富环境中运行。通过可信环境和富环境间的通信，完成完整的功能。

可信执行环境与可信外设、可信存储等功能结合，可以提供对系统敏感功能的保护。可信执行环境通过可信启动、远程证明、安全生物特征管理、可信用户界面等为系统提供整套的安全解决方案。

可信执行环境根据其软硬件架构，有共用硬件架构、独立硬件架构和虚拟化架构几种。虚拟化架构中的 TVM（可信虚拟机）既允许纯软件隔离，又允许独占硬件（如下图 c 中的 VM3）。前者提供足够的灵活性，后者则可提供更高的安全性。

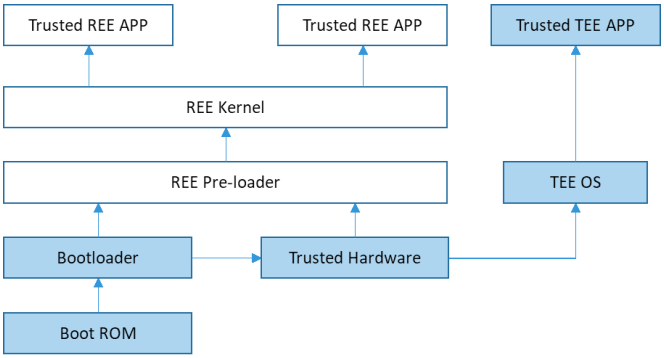


a. 共用硬件平台　　b. 独立硬件平台　　c. 虚拟化架构

5.1.4 可信启动

终端软硬件的完整性保护，可通过可信启动来完成。在可信存储系统中，安全存储了硬件指纹、各级启动软件的完整性保护信息，并用根密钥进行电子签名。

在每次启动时，从底层代码开始，到操作系统，到敏感代码，先验证代码的完整性再运行。如果验证不通过，表示代码可能遭到恶意篡改，停止启动过程并提示用户。一个典型的系统启动过程如下图所示。



可信启动过程

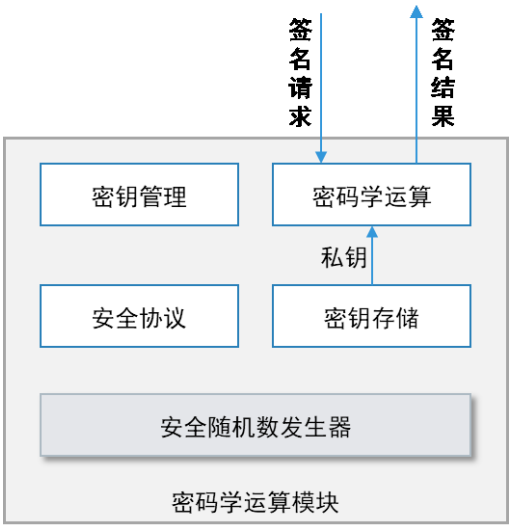
可信启动还可用来验证可信硬件的完整性。例如，可以对摄像头、指纹提取模块进行验证。如发现由部件替换，则提示用户。对于封闭外壳、位置绑定等物理保护的终端，还可以验证配置的绑定参数的完整性，确定是否被暴力打开或移动位置。

当操作系统或其他软件有版本更新时，可以在得到授权的情况下，在可信环境中对存储的完整性校验信息更新，并重新电子签名。

系统可配置仅安装和运行来源可信的软件。这也通过对软件包的完整性保护和电子签名完成。

5.1.5 可信硬件密码运算

传统的加解密、签名及验证、完整性保护运算在内存中完成。恶意软件可能通过内存读取获取到密钥或明文。应用可信环境进行密码学运算可以实现对密码学运算的基本保护，但无法防止直接硬件攻击，例如直接读取总线或硬件读取内存信息。



使用硬件进行密码学运算，可以保证密钥生命中期中密钥仅在芯片内部存在，且对外界不可读。例如可以生产公私钥对，私钥保存在硬件中，仅公钥对外发布。私钥可以用来做签名、身份证实、解密，但所有的运算也都在硬件中执行，仅对外提供功能接口。

硬件支持密码算法，可以提高可信存储的效率，可以支持整个永久存储的加解密操作。硬件实现的密码学运算模块，可以产生更安全的随机数，可以通过控制管理和算法实现防止对芯片的分析功耗、计算时延等侧信道攻击。

5.1.6 可信调试

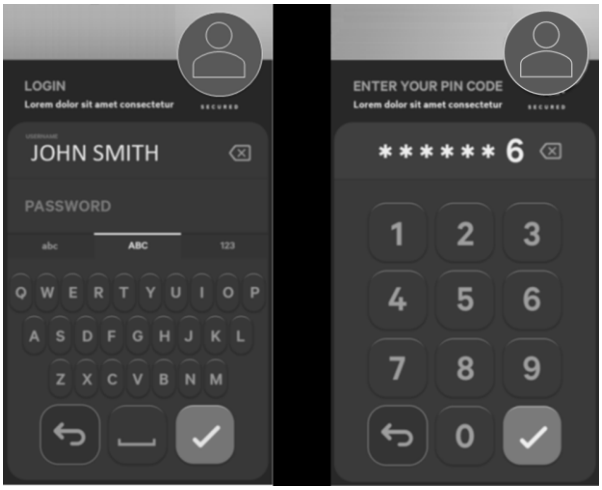
传统的调试模式是在硬件上保留调试接口，调试者通过链接调试接口（例如直接链接芯片管脚），在调试界面中输入默认的用户名密码。用户名密码一般是硬编码的，且所有终端使用相同的密码。由于调试人员众多，使用相同的用户名密码很容易泄露且无法追查。因此为安全起见，逐渐要求商业化终端出厂时要硬件关闭调试接口（例如硬件熔断芯片内调试连接或硬件设定不可复原的开关），即出厂后不再有调试能力。

随着终端设备的安全性进一步提高，用户很多高敏感数据使用硬件相关的安全存储。当设备出现了硬件故障或有物理损坏时，无法正常读取用户数据。如果完全锁死调试接口，读取这部分数据成为不可能，从而造成用户数据丢失。

可信调试保留了一个调试接口，但是设计了安全保护机制保护对此接口的访问。生产商在芯片或终端生产时，每个芯片或终端注入一个信任公钥，还可为每个终端注入不同的访问密钥。只有授权的维修员才可以使用特定的设备，通过适当的安全协议和算法验证，才可以打开调试接口。这样避免了使用相同密钥的泄露风险。调试的过程被严格记录。可信调试既保护了用户数据的可用性，又保护用户数据的安全性。

5.1.7 可信用户界面

在用户输入敏感信息时，可能遇到有其他后台的恶意软件弹出伪冒的用户输入界面，诱骗用户输入敏感数据。使用可信用户界面，则是由可信环境提供一个安全的可信用户界面接口供 APP 调用，APP 调用时由可信环境接管用户界面的显示和输入，保证用户界面是在可信 APP 上运行而非恶意软件。安全用户界面的统一实现还可以防止单个 APP 实现的不安全设计（例如直接显示全部的用户口令）和代码漏洞，从而防止用户敏感信息泄露。



在用户使用口令作为终端解锁和对系统敏感操作的授权场景中，终端不能存储口令的明文，也不推荐存储可逆加密的密文，使用随机盐值和不可逆加密才是安全方案。

需要终端存储网站或 APP 的登录 ID 和口令的场景（即免登录），推荐使用可信存储进行加密存储。或者使用更优的方案，如 5.2 介绍的硬件令牌方式。

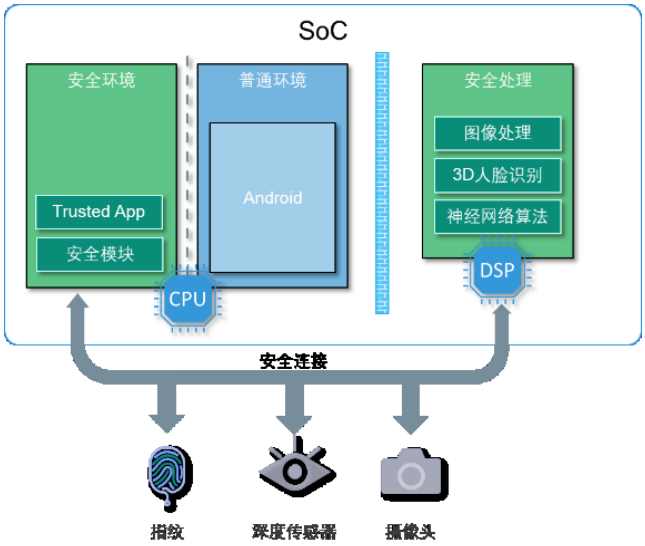
可信用户界面可以是硬件直接支持（免遭恶意软件侵入），并且与可信存储相配合工作，从而实现更安全、可靠的用户接口。

5.1.8 可信传感器

终端的敏感传感器可能被攻击者替换为恶意提供数据或窃取输入数据的硬件，从而为系统提供错误的信息可能造成安全威胁。例如，替换卫星定位传感器可以伪造用户位置绕过对服务位置的限制，替换摄像头可能为人脸识别提供伪冒的图像，替换指纹传感器则可能窃取到个人敏感信息。

可信传感器则通过硬件指纹或密码学方法，将传感器与特定的终端绑定，且在传感器与安全处理器或安全芯片间使用直接通道。

终端仅接受来自指定传感器的信息，并将接收的信息仅在安全环境中处理，以避免敏感数据泄露。例如对于生物特征的注册过程仅对外输出“是否已完成注册”，生物特征识别过程仅对外输出“是否验证通过”，中间过程完全对外不可见。更安全的方法，是将传感器数据直接交给安全硬件计算，所有的计算过程都在硬件芯片中完成，可以防止对内存的分析以及其他相关的硬件攻击，导致算法失效、伪冒成功或造成个人信息泄露。



可信传感器和可信传感计算

5.1.9 隐私保护

终端的隐私保护通过访问控制实现。终端使用可信硬件做基础，通过操作系统实现访问控制。只有通过认证和授权的用户才可对相应的数据和功能进行操作，只有授权的应用才可对个人数据和功能进行操作。例如，拨打电话、使用用户位置、读写用户通讯录等行为须经过用户授权确认才可进行。

可信硬件对用户隐私保护非常重要。终端通过可信传感器和可信界面接受并验证用户的认证凭据（密码或生物特征），通过可信存储实现与设备绑定的安全存储，从而实现未通过验证的本地用户无法操作个人数据，即使将本地存储设备剥离设备也无法操作。

5.2 终端中的基础可信根

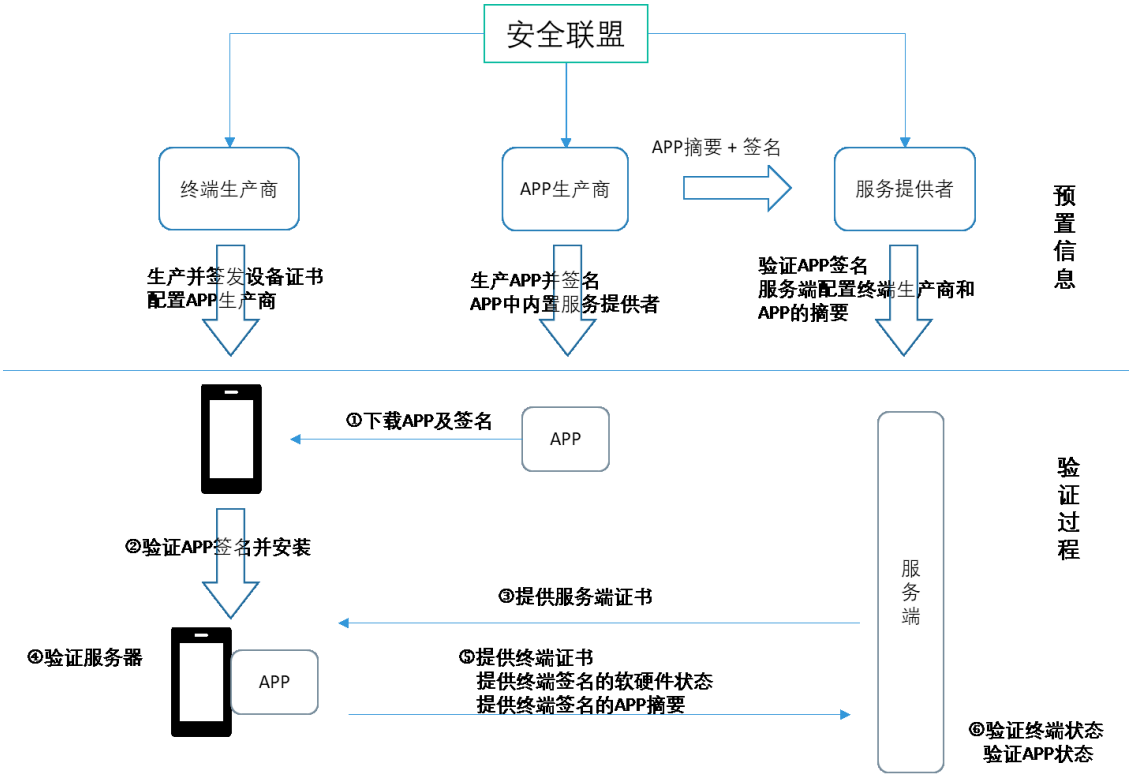
可信启动通过密码技术来验证系统启动过程中每一个阶段软件镜像的完整性和真实性，防止非授权或被恶意篡改的镜像程序被执行。可信启动是后续可信计算、安全防护和一切复杂系统操作安全性的基础。安全启动过程构建了一个信任链，整个过程始于一个可信根（Root of Trust），之后的其它组件通过完整性和真实性验证被执行。可信根包含硬件、代码和数据，是可信执行环境和终端整体系统安全机制建立及运行的基石。

可信根应具备保密性、完整性和真实可靠性三个基本安全特性；同时应具有严格的访问控制机制，保证任何未经授权的用户或厂商不能访问和篡改可信根的数据和代码。5G 终端中可能有多个不同级别或不同用途的可信根，从提高安全性的角度讲，这些可信根宜锚定在一个最基础的可信根基础上，这个最基础的可信根应使用具有高安全级别的独立安全内核，同时应具有最小可访问特性，例如仅能被原始供应商安全访问。

5.3　远程证明

远程证明用于终端向远端服务提供方提交本地的完整性和安全性健康报告，证明本地运行环境是可信的。远端服务可以根据此报告和其配置的策略，决定是否提供某种服务。例如，金融支付软件可以要求终端报告是否有安全运行环境、安全传感器和安全用户界面，所允许的支付软件是否安全可信的。只有符合其策略的终端才可运行敏感服务。

远程证明流程如下：



远程证明依赖于可信执行环境和可信启动。可信执行环境保证其运行安全，可信启动保证其硬件完整性和操作系统的安全性，保证 APP 运行于安全的平台之上，保证 APP 自身启动时是完整的。其中各种信息的完整性，可以靠可信存储实现。

远程证明是生态系统级的解决方案，要求软硬件和服务各提供方有相互承认的可信根。可信根可通过权威测试认证机构颁发，也可通过使用企业证书等手段实现。企业实施可信根可以保证敏感数据仅在有限的范围内产生、处理、存储。

为减少证书链的层级或配置更短的可信列表，生态环境中各方建立相互信任的联盟，实施第三方认证，并且对外开放认证接口，促进终端为中心的安全信任空间，简化各方的配置、部署，增进可信生态的扩展。

远程证明在以终端为中心的安全体系中，扮演重要的角色。远程证明终端的安全呈现给服务提供方，提高了服务的安全性，可以大大降低服务风险，从而可以允许安全级别更高的服务运行于终端上。

5.4　终端安全令牌

终端上运行越来越高敏感度的业务，仅仅通过用户 ID 和口令无法保证足够的安全性，即使使用多因子认证，仍有可能有来自被恶意篡改的操作系统或 APP 的攻击。多因子认证还可能造成使用不便利，例如需要触发发送短信，并切换到短信 APP 中拷贝短信、切换回支付 APP 粘贴再进行认证。使用终端安全令牌，可以在提高安全性的基础上，仍然保证甚至提高用户使用便利性。

5.4.1 基本流程

使用终端硬件令牌认证，须先完成注册过程。流程如下：

R.1　终端下载安装应用客户端 APP。

R.2　用户打开客户端 APP，连接到可信服务端，启动注册。

R.3　服务端对终端发起远程证明，验证终端安全完整性、安全能力、健康程度，并记录相应的信息，例如硬件 ID，操作系统版本等。

R.4　双方协定硬件认证凭据。凭据可以是为每个 APP 的每个用户单独生成的公私钥对或由双方共同签名的证书。

完成注册后，后续的用户登录或使用服务即可通过硬件完成。流程如下：

L.1　　终端上 APP 发起登录或敏感操作，提交硬件令牌和远程证明材料

L.2　　服务端验证终端安全性、健康状态，验证终端硬件令牌

L.3　（可选）服务端向终端发起新鲜性挑战，终端须证明自己持有令牌

L.4　验证通过后登录成功，即可提供服务

服务端对终端发起挑战是防止中间人攻击或重放攻击。完成登录后，服务端可为终端下发有效期限的令牌。终端将此令牌安全存储，可作为一段时间内免认证的凭据。

在实施敏感操作时，终端须对自己发送的数据进行签名。例如实施金融支付时：

S.1　双向认证完成

S.2　服务器生成订单并使用电子签名发送到终端

S.3　终端验证订单来源及内容

S.4　终端向用户提示授权，用户可通过生物特征识别等方法进行认证授权

S.5　终端使用注册时生成的私钥对订单进行签名

S.6　服务端验证订单后，向终端发送交易完成确认

5.4.2 基于本地生物识别的用户认证

安全令牌注册、登录、操作过程，须在用户授权下完成。而此用户授权可以通过用户输入解锁口令或使用生物特征识别完成。

本质上，硬件令牌是将其他认证凭据集中到“我持有终端”的认证方式上，尤其是“我知”的凭据。认证的过程须受安全性保护：

1) 终端是安全的。通过可信计算和可信启动保证。
2) 终端是在可信用户的使用中。通过用户的生物特征识别等实现。
3) 终端的输入是用户的真实意志表现。防止呈现攻击，防止钓鱼。
4) 用户的操作在授权范围内。

5.4.3 安全保护

终端安全令牌解决方案的安全性基于 4.1 中所描述的安全能力来保证。

安全功能	应用场景
可信存储	• 可信对端列表 • 认证凭据

可信执行环境	• 认证流程
可信启动	• 安全健康保证
可信密码运算	• 安全协议 • 验证对端服务器 • 凭据持有证明计算 • 数字签名 • 通信数据安全保护
可信界面	• 账号 ID 及口令
可信传感器	• 生物识别授权
远程证明	• 实时证明终端可信
可信调试	• 保证不在调试状态

5.5　基于 EAT 协议和硬件安全令牌的安全状态证言

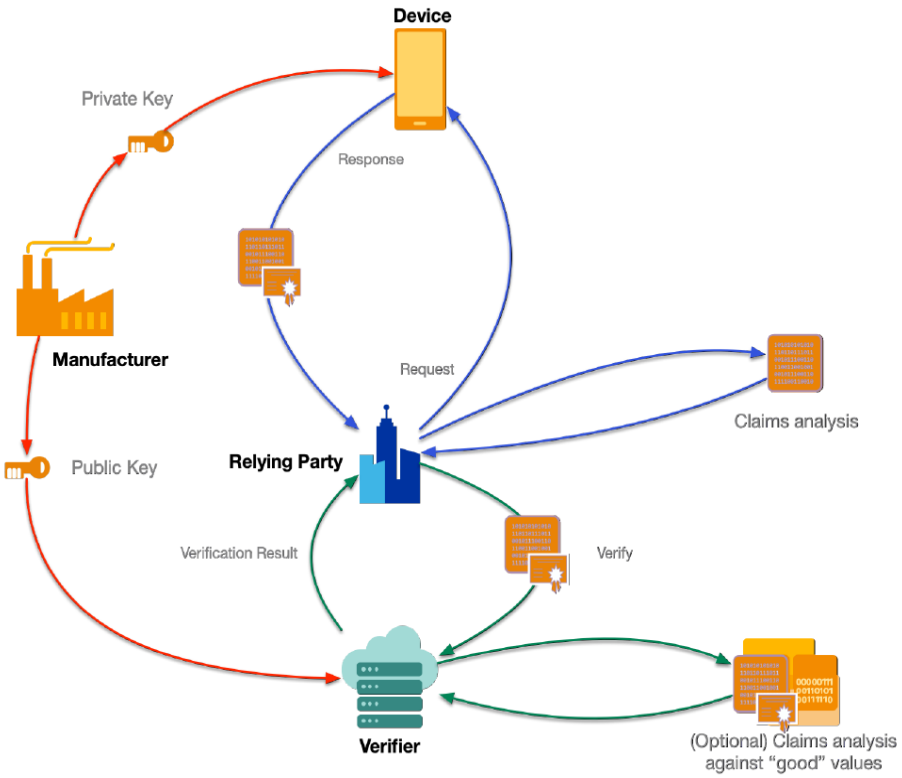
5G 特别是 5G 中的 mMTC 应用场景会实现万物互联，但物联网终端形态丰富多样、通信和安全处理能力参差不齐、部署环境复杂多变，因此会面临更多的安全威胁和更容易受到第 3 章中所描述的各种安全攻击。对 5G 物联网终端按应用场景进行等级化安全防护、对 5G 物联网终端的安全状态进行实时查询和动态跟踪，可以有效保障物联网终端安全、和识别已被攻击或劫持的终端。

IETF RATS（Remote ATtestation ProcedureS，远程证言流程）工作组正在制定 EAT（Entity Attestation Token，实体证言令牌）RFC，其核心功能是定义一个可灵活扩展的、可以可靠描述终端实体安全状态和特征的声明集合，包括终端实体 ID、OEM ID、安全等级、启动状态（安全/普通/rooted）、位置信息、时间戳、子模块名称、子模块安全状态等。EAT 声明集合还可灵活扩展，这通过向 IANA 进行 CWT 注册来实现，EAT 也支持对多个声明的级联或嵌套。EAT 使用硬件安全令牌机制对这些声明进行数字化签名和安全证言，保证声明的真实性和完整性，以供接收应用方或依赖方验签校验后相应使用。

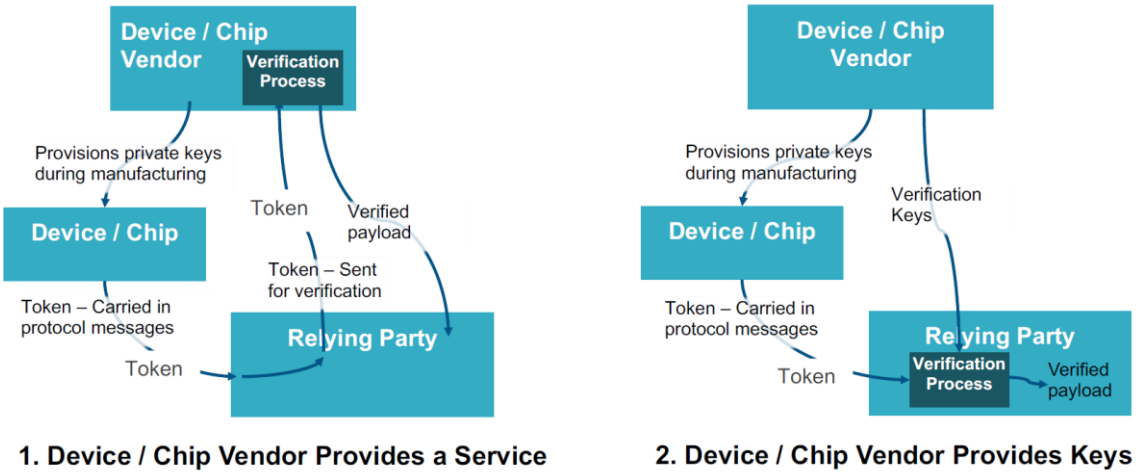
基于 EAT 协议，5G 物联网终端可以根据使用场景或者基于应用方的询问请求，发送终端整体或者终端中特定子模块的实时安全状态，并使用芯片级或模块级的证言私钥和硬件安全机制为状态报告生成安全令牌。

EAT 将可信状态查询、硬件令牌和远程证言相结合，主要工作流程如下图所示，包括：

- 证言私钥在芯片或模组的生产工厂产线上被安全生成，对应的验签公钥由厂商安全共享给 EAT 校验方。
- 需要时，应用使用方或依赖方查询终端的安全状态。
- 终端相应生成安全状态报告，并使用证言私钥对状态报告进行签名，以保证报告的真实性和进行完整性保护。
- 应用使用方或依赖方选择一个可信的 EAT 校验方对所接收的安全状态报告进行校验。
- EAT 校验方返回校验结果，指示安全状态报告是否可信。



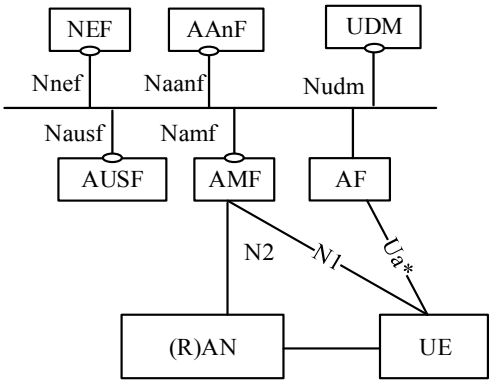
EAT 可支持多种灵活的部署模式，包括终端/芯片厂商直接提供最终校验服务、终端/芯片厂商提供验签公钥给第三方、或者芯片厂商和终端厂商/第三方进行合作式分层校验。



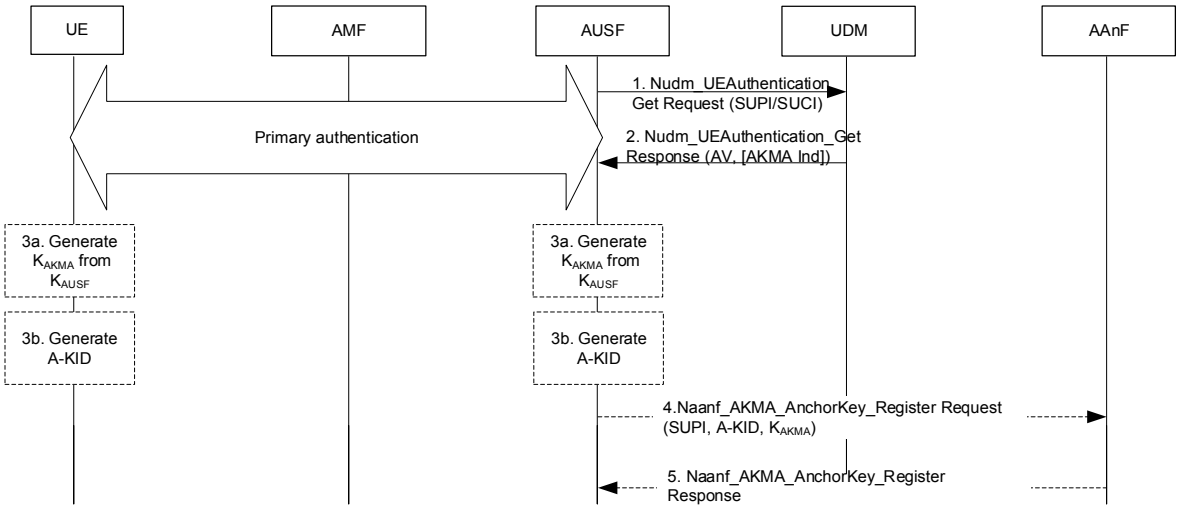
5.6　5G 应用级密钥推衍

5G 有三大使用场景，可以支持不同类型和具有不同安全要求的各种消费类、垂直行业类和政务类、海量物联网类等应用，包括一些尚未出现或处于早期萌芽状态的未来新型应用。这些新增应用有可能需要进行附加的应用级认证、用户授权检查和使用其它安全机制，而这离不开对终端侧和应用服务器或云端应用密钥的灵活可信配置和安全管理，为不同应用生成和配置的密钥还应相互独立，保证隔离安全。

3GPP 在 R16 阶段开展了 5G AKMA（面向 5G 应用的认证和密钥管理）研究和标准化工作，已经完成了 TS 33.535 技术规范[10]。它基于以下系统架构，在网络侧需要引入一个新的逻辑功能实体 AAnF（AKMA 锚点功能）、在 5G 终端和应用功能实体（AF）间支持新的 U_a^*接口。

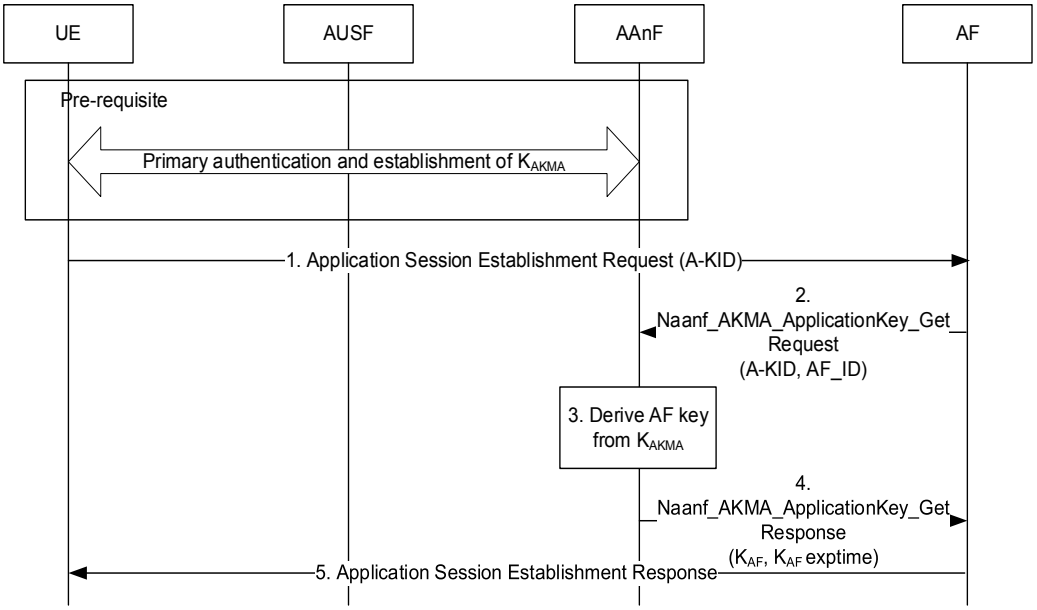


5G AKMA 功能不需要执行额外的 UE 认证，它重用 5G 主认证来实现 UE 和网络的互认证，并利用 5G 主认证成功后在 AUSF 和 UE 中所建立和存储的 K_{AUSF}，来推导 UE 和 AAnF 之间的共享密钥 K_{AKMA}，下图为主要的推衍流程。

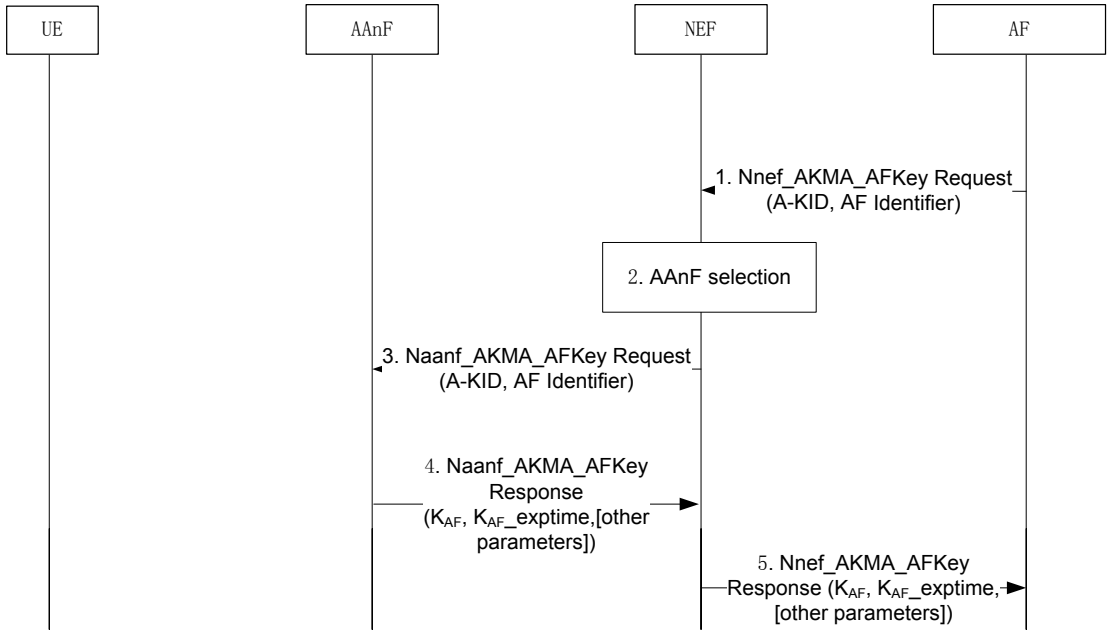


1) 在主认证过程中，AUSF 通过 Nudm_UEAuthentication_Get 请求服务操作获得订阅凭证（例如 AKA 认证向量）和认证方法。
2) 在请求服务操作响应中，UDM 还可以向 AUSF 指示是否需要为 UE 生成 AKMA 密钥。
3) 如果 AUSF 从 UDM 接收到 AKMA 指示，则 AUSF 应存储 K_{AUSF}，并在主认证过程成功完成后由 K_{AUSF} 推衍出 AKMA 锚点密钥（K_{AKMA}）和 A-KID。
   UE 应当在与 AKMA 应用服务器 AF 交互之前，从 K_{AUSF} 推衍出 K_{AKMA} 和 A-KID。
4) 生成 AKMA 密钥材料后，AUSF 应使用 Naanf_AKMA_AnchorKey_Register 请求服务操作将生成的 A-KID、K_{AKMA} 和 UE 的 SUPI 一起发送给 AAnF。AAnF 应存储 AUSF 所发送的最新 AKMA 上下文。
5) AAnF 使用 Naanf_AKMA_AnchorKey_Register Response 服务操作将响应发送给 AUSF。

UE 和 AAnF 再基于 K_{AKMA} 密钥、为特定 5G 应用生成应用密钥（K_{AF}），当 AF 位于运营商网络内部时，AF 直接从 AAnF 请求和获取 K_{AF}，如下图所示。



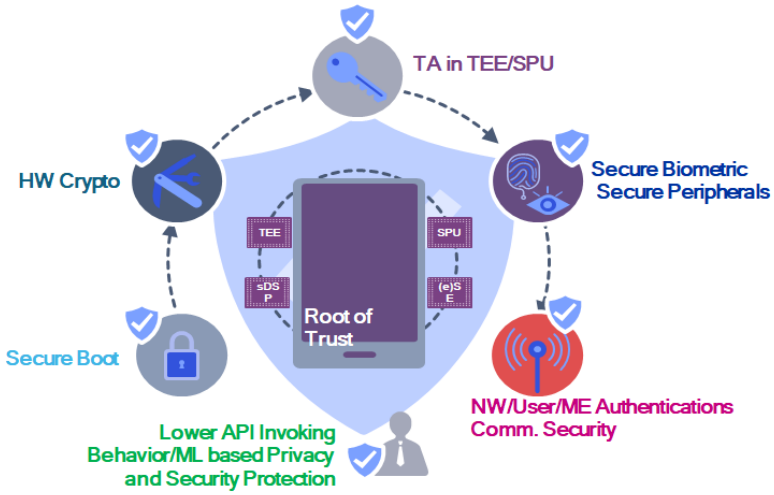
当 AF 位于运营商网络外部时，AF 通过 NEF 向 5GC 请求 AKMA 应用层密钥 K_{AF}，流程如下图所示。



5G 终端可以按照用户选择和业务发展需求、当需要时与不同应用服务器/云端通过 5G AKMA 功能安全建立或者更新共享的业务级密钥 K_{AF}，并基于该密钥派生新的次级业务密钥和进行相应的业务级安全处理，从而为新应用的安全防护建立密钥基础。

5.7　终端作为用户对外操作的新型可信根

在以终端为中心的安全体系中，终端的可信是整个系统安全的基础。基于本章前述小节中介绍的各种终端可信技术、终端状态安全证言技术、动态 5G 应用密钥生成加载技术等，可将已安全验证的 5G 终端整体做为用户对外操作和交互的可信根，并将 5G 终端的安全能力对外开放，实现可信传递和安全能力对外延展。

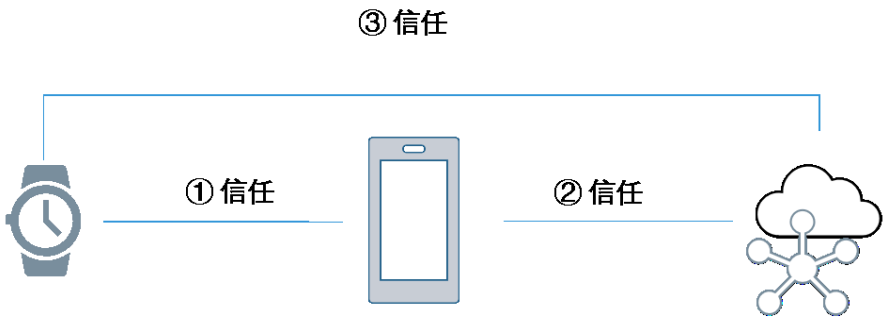


5.8　可信能力开放

当终端与服务/网络形成可信关系后，可以借助于此互信关系，建立进一步的可信和信任传递机制。

5.8.1　终端/用户授权的可信外设

5G 时代是物联网时代。物联网终端可能通过 5G 通信网络或非 5G 通信相互连接或连接至广域网络。物联网终端连接到广域网络中，需要与广域网取得互信，物联网终端连接到 5G 通信网络中，需要配置相应的用户信息和用户凭证。使用可信的终端，可以为物联网设备提供一种认证的凭据和方法，简化物联网设备的配置过程。



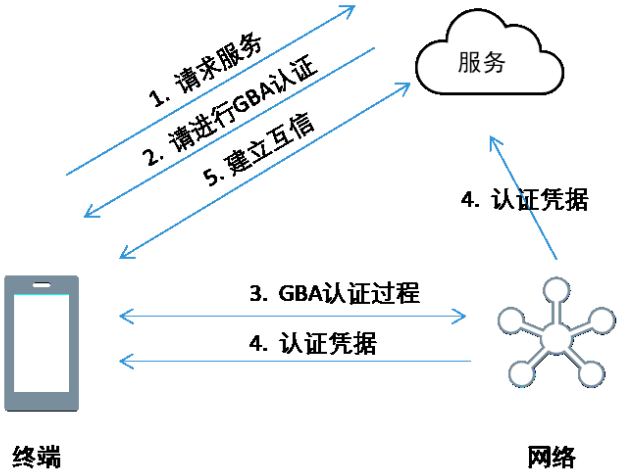
信任传递： 终端与外设可信①，终端与服务可信②，因此外设与服务间可信③

本质上，授信其他外设或终端/设备，是一种信任传递。网络/服务 S 信任终端 A（双向），A 信任 B（双向），则网络/服务 S 可以与 B 建立双向信任。其中 S-A 信任和 A-B 信任均可通过 5.3 所述过程完成。S-B 信任建立后，可以分发给 B 单独的凭据连接到服务/网络中。若操作为敏感操作，则网络/服务可以进一步对 B 进行单独的远程认证以保证操作的安全性。

一个典型的例子是将可穿戴设备甚至植入人体的设备作为终端的授信设备，在无需携带（富）终端的情况下进行门禁、认证、支付等操作，从而扩展其应用场景。在植入式设备场景下，相对于默认开启了多因子认证，即结合了“我有”和“我是”的因子。

5.8.2 网络与服务互信

当终端与网络建立可信关系后（参见 4.2.2 和 4.2.3），网络可以将此可信传递给服务端，建立终端与服务间的互信关系。GBA 框架即实现这种可信的技术方案。



GBA 认证

5G 中支持 EAP 认证（非 EAP-AKA）框架，这意味着终端-服务间的互信可以传递至终端-网络间的互信。借助这种互信，可以实现动态签约。例如，企业与运营商合作，企业可以为其职员的终端做可信安全证明，将信任传递到运营商。运营商则动态与职员的终端签约，允许职员接入网络并访问企业网络。

5.9　多角色隔离与转换

可能同一部终端承担多种角色，接入多个网络，使用多个角色的应用。例如，职员可以使用同一部终端同时接入企业网络和公共网络。为此，5G 应用中提供了专用网络服务，网络层提供了业务分离。

在终端中，如果采用了虚拟架构，则可以实现多业务多角色的隔离。可以为每个角色分配单独的虚拟机，通过虚拟通信接口接入特定的 5G 网络中。企业可以单独管理虚拟机管理而不再使用企业证书去进行管理。终端同时可以在多个虚拟机中开启相同应用的不同实例。例如，同样使用微信，可以设置不同的社交群组、工作群组，且互不干扰。同时，在不同的虚拟机中有不同的数据管理，例如通信录。用户不用担心企业应用会泄露用户的个人信息，企业也无需担心用户会将商业机密信息通过私人通信手段传播。在行业应用中，存在另一种角色转换，即多职员共用专用终端。这种专用终端下，除了上述虚拟化解决方案外，终端上单操作系统实现多用户功能也可。

在以终端为中心的应用中，须注意角色的隔离。如前所述，本质上终端为中心是以“用户个体”为中心。不同的使用者代表不同的个人，需要使用不同的身份，不同的硬件令牌作

为凭据去进行认证。角色的切换，可以通过登入手机的使用时，不同的生物特征，不同的密码，不同的 NFC 工卡等作为角色的 ID 标识。

6 总结和建议

伴随着移动互联网的爆炸式发展，终端逐渐成为个人的生活、社交、工作中心。5G 的业务能力提升、业务多样性扩展、终端形态多样、能力多样、部署环境多元化，以及网络的虚拟化、边缘计算、网络开放等新的特征和技术的引入，5G 安全遇到前所未有的威胁和风险。设计和实施可信技术，打造可信终端，建立以终端为中心的 5G 安全体系，并将可信概念扩展、开放，可以解决 5G 中处于最末端的终端安全以及最高层的应用安全，也可以用 5G 终端的安全能力来加固和赋能用户的周边设备、为 5G 新应用提供灵活可靠的密钥配置管理，实现以 5G 终端为中心的用户域安全联盟。可信终端本质上作为可信用户的扩展和延伸，在得到用户授权后，用“我有”替代了“我知”及“我是”的认证方式，在保证安全的同时可提高用户的便利性。

参考文献

[1] S. Steig, A. Aarnes, T. v. Do and H. T. Nguyen, "A Network Based IMSI Catcher Detection," 2016 6th International Conference on IT Convergence and Security (ICITCS), Prague, 2016, pp. 1-6.

[2] 3GPP TS 33.501. 3GPP System Architecture Evolution (SAE); Security architecture, v16.0.0[S]. 2019.

[3] 3GPP TR 33.899　　Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system. V1.3.0 (2017-08)

[4] NGMN Alliance， 5G White Paper V1.0 2015-02

[5] CCSA, 5G 移动通信网 安全技术要求， 2019

[6] CCSA，YD/T 2407-2013 移动智能终端安全能力技术要求

[7] GB/T 32927-2016 信息安全技术 移动智能终端安全架构

[8] Ovum，《5G 娱乐经济报告》

[9] IETF RFC Draft on EAT，https://datatracker.ietf.org/doc/draft-ietf-rats-eat/

[10] 3GPP TS 33.535 R16. Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS) [S]. 2020

缩略词表

APP	Application （in UE）	（终端）应用
5G	Fifth Generation Of Cellular Network	第五代蜂窝网络系统
AKA	Authentication and Key Agreement	认证和密钥协商
AKMA	Authentication and Key Management for Applications	面向(5G)应用的认证和密钥管理
APT	Advanced Persistent Threat	先进长期威胁
AR	Augmented Reality	增强现实
ARPF	Authentication Credential Repository and Processing Function	认证凭证库和处理功能
AUSF	Authentication Server Function	认证服务器功能
BYOD	Bring Your Own Device	自携终端
CK	Ciphering Key	加密密钥
CoBR	Concise Binary Object Representation	简洁二进制对象表示法
CWT	CoBR Web Token	CoBR 网络令牌
D2D	Device to Device	设备间通信
DDOS	Distributed DOS	分布式拒绝服务攻击
DOS	Deny of Service	拒绝服务攻击
EAT	Entity Attestation Token	实体证言令牌
EAP	Extensible Authentication Protocol	可扩展认证协议
eMBB	enhanced Mobile Broad Band	增强移动宽带
GBA	General Bootstrapping Architecture	通用启动架构
GPS	Global Positioning System	全球定位系统
GUTI	Globally Unique Temporary UE Identity	全球唯一用户临时标识
IK	Integrity Key	完整性保护密钥
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IoT	Internet of Things	物联网
IPsec	IP Security	IETF 定义的 IP 安全机制
LBS	Location Based Service	基于位置的服务
LTE	Long Term Evolution	长期演进（4G）

ME	Mobile Equipment	移动设备（UE 除去用户卡部分）
mMTC	massive MTC	海量机器通信
MTC	Machine Type Communication	机器间通信
NFC	Near Field Communication	近场通信
NFV	Network Function Virtualization	网络功能虚拟化
NG	Next Generation	下一代（指 5G）
NGMN	Next Generation Mobile Network （Alliance）	下一代移动网络（联盟）
NSA	Non-SA	非独立部署
OS	Operating System	操作系统
OTA	Over the Air	空口
PBE	Password-Based Encryption	基于口令的加密
PoS	Point of Sale	收款（设备）
SA	Standalone	独立部署
SDN	Software Defined Network	软件定义网络
SE	Secure Element	安全部件（硬件）
SEAF	SEcurity Anchor Function	安全锚功能
SIDF	Subscription Identifier De-concealing Function	用户标识去隐藏功能
SoC	System on Chip	系统级芯片
SSO	Single Sign On	单点登录
SUCI	Subscription Concealed Identifier	隐藏标识
SUPI	Subscription Permanent Identifier	永久标识
TEE	Trusted Execution Environment	可信执行环境
TMSI	Temporary Mobile Subscriber Identity	临时移动用户识别码
UDM	Unified Data Management	统一数据管理
UE	User Equipment	用户设备（终端）
UI	User Interface	用户界面
URI	Unique Resource Identifier	统一资源标识符
uRLLC	ultra-Reliable Low-latency Communication	高可靠低时延通信
VM	Virtual Machine	虚拟机
VR	Virtual Reality	虚拟现实
WLAN	Wireless Local Access Network	无线本地局域网

关键词

5G，终端，安全，可信

致谢

诚挚的感谢如下人员对本白皮书做出的贡献：

编辑：

高通无线通信技术（中国）有限公司　　杜志敏、王江胜

贡献单位与人员（排名不分先后）：

高通无线通信技术（中国）有限公司　杜志敏、王江胜、李俨

中国信息通信研究院：　　袁琦、王剑

电子科技大学：　　武刚、强奇

奇安信科技集团股份有限公司：　　乔思远、王茜

中国移动通信集团有限公司　　黄晓婷

FuTURE 论坛致力于先进技术和应用的研究，其研究内容相对超前，因而不可避免在某些技术路线和方法上存在争议。论坛鼓励各种观点的充分表述和广泛交流。论坛所发布白皮书中的内容代表参与单位的一致意见，获得论坛多数成员的支持成为共识，进而成为论坛的观点，但不一定代表论坛所有成员的共识。

论坛欢迎各界专家学者踊跃参加 FuTURE 后续各工作组会议及交流研讨活动，诚邀各位积极参与 FuTURE 系列白皮书撰写工作。

未来移动通信论坛

FUTURE MOBILE COMMUNICATION FORUM