大唐电信科技产业集团
DATANG TELECOM TECHNOLOGY & INDUSTRY GROUP

建设安全可信的网络空间

5G网络安全白皮书

大唐电信科技产业集团

2015年12月

目　　录

摘要

5G提供数据、连接和基于场景的服务，人、物与网络高度融合的场景化时代即将来临。现实空间与网络空间交织发展，安全成为支撑5G健康发展的关键要素。

面向信息消费、工业生产、互联网金融、教育医疗、智能交通和公共管理等典型应用场景，5G网络需要提供安全可靠的网络通信和服务平台，并能够保护用户隐私，同时支持国家和社会维护网络空间秩序。在传统接入安全、传输安全基础上，5G需要实现网络空间与现实空间的有效映射，提供满足不同应用场景的多级别安全保证，网络实体自身具备安全免疫能力，构建安全可信的网络空间。

白皮书首先分析了未来5G移动宽带系统的一些典型应用场景，站在用户、网络和服务平台提供者、社会和政府的不同角度分析了5G的安全需求。在此基础上，白皮书提出了5G网络安全的三个核心要素：身份可信、网络可信、实体可信，并对主要的安全技术方向进行了分析探讨。

1. 引言

随着信息通信技术的快速发展和广泛应用，人类与信息网络密不可分。5G作为下一代无线通信技术将支持更加丰富的应用服务，深入融合到人们日常生活、工作、学习、娱乐以及现实社会的运行、管理中，应该站在网络空间的角度审视5G的安全。

建立安全可信[1]网络空间[2]，完成网络空间（Cyberspace）与现实空间（Reality space）[3]的可信对接，将是5G的安全特征。

2. 网络空间5G应用场景与安全需求

从业务和应用的角度来看，5G提供数据、连接和基于场景的服务，5G带来的是一个连接场景的时代。

5G将推动移动互联网、物联网、车联网、工业互联网等聚合型应用，为政府、企业、金融机构、服务行业带来新的业务和管理模式，也将为促进产业转型升级、社会和谐发展创造条件。

图1　5G应用场景

2.1 5G典型应用场景

➢ 信息消费

5G 将推动信息发布、获取、使用、管理方式的根本性变化，公众信息消费将朝着多元化、移动化、在线化方向发展，可实现随时随地信息发布、网络浏览、即时通信、社交娱乐等，带动数字出版、

---

[1]可信——本文中指软硬件运行符合设计预期，或声明与实际相吻合。

[2]网络空间(Cyberspace)——本文中专指由通信网、处理器等连接构成的虚拟环境和空间。

[3]现实空间(Reality space)——与网络空间对应，包括物理世界(Physical world)以及人类社会(Human Society)。

数字互动新媒体、动漫游戏等新型服务发展，提升在线软件商店、地理信息产业、云服务（如PaaS、SaaS）等产业服务品质，满足公众日益增长的信息需求。

在信息消费中，由于缺乏有效的举证通道和调解处理机制，消费者和服务提供者彼此难以有效确认对方的身份和信用，也无法对信息来源及时追溯，这给争议和问题的处理带来了困难。海量的信息增加了信息真实性和有效性辨识的难度，消费者面临更多的网络诈骗、钓鱼网站、软件吸费等安全威胁，其个人信息也面临着被自己使用的设备、网络和应用服务提供商泄漏、盗用的风险。

- **工业生产**

5G网络具有低时延、高可靠等特征，实现5G网络与制造业深度融合，综合高级计算、分析、传感以及网络技术，实现智能化的机器之间、机器与人之间的连接，将推动生产高度数字化、网络化，降低企业生产成本，提高生产效率，推动新一轮工业革命，助力工业制造业良性可持续发展。

与传统计算机网络相同，工业生产系统网络也将面临着病毒、木马的安全风险，也存在被非法控制的威胁。5G网络的泛在化、开放性，对工业生产网络的安全隔离带来了新的挑战。随着工业生产供应链、营销体系等数据管理模式的变化，云计算、云存储等新技术被广泛使用，也带来了越权访问、信息窃取、数据篡改等新的安全威胁。

- **互联网金融**

移动支付、众筹、p2p贷款、电子货币等互联网金融业务正在改变人们的生活，泛在的网络连接将进一步拓展信息技术在金融领域的应用范围，引发银行、电商、零售、投资、保险等多领域业务的变革。在共享开放的互联网中，市场信息不对称的问题将很大程度上得以解决。

互联网金融中，个人、交易平台、银行以及金融监管机构通过网络彼此连接，完成业务处理。指尖操作取代了面对面的交易操作，交易双方的真实身份和信用需要新的确认方式；移动支付与终端绑定，一旦终端设备丢失，即可能面临着账户资金丢失和盗用的风险；大量信息和资金通过计算机网络传输和处理，系统面临被篡改和瘫痪的风险，交易信息和个人信息可能被窃取和盗用。

- **教育和医疗**

5G网络技术将进一步推动信息技术应用，优化教育医疗等公共资源配置，提高资源使用效率。网络在线教育可以提供教师和学生之间远程交流的平台，提供身临其境的教学环境；智能医疗提供远程会诊、健康监控、医疗信息共享等服务，可有效解决医疗资源供给不足、配置不均衡等问题。

在智能医疗系统中，未授权和不具有资质的医生接入和使用远程医疗系统，可能造成病情延误、医患纠纷；不稳定的网络连接会影响远程健康监护、急救指导、远程手术，将直接威胁病人的健康乃至生命安全；病人病历、处方和治疗方案等隐私性信息在采集、存储和传输过程中存在被泄漏、篡改的风险。网络的安全性对于远程教育同样具有重要的意义。服务拥塞、网络中断、设备宕机将会影响教学质量和用户体验。医疗和教育服务对象的特殊性，需要特别注意身份的准确识别、存储数据的完整性和传输内容的安全性。

- **智能交通**

5G网络低时延、高可靠和灵活接入的通信技术将实现车辆、路边设施和行人间实时的网络连接，通过电子传感、信息通信和系统控制等技术的有机结合，实现城市交通的数字化管理。智能交通

在维护城市交通系统高效运转，缓解道路堵塞，优化公共交通资源配置，物流配送智能化等方面具有重要的作用。

智能交通直接关乎道路安全、人身安全和财产安全。永远在线的5G网络中，汽车面临随时随地接收虚假信息的可能，控制信息的延迟、篡改或阻断会直接影响行驶的安全；无线接入设备愈加智能化、小型化、多样化，未经授权的实体[4]可能置入智能交通系统之中，成为控制者，非法操控智能交通系统，而且难以被发现；车辆的位置和行驶轨迹等隐私信息也存在暴露和被非法跟踪使用的风险。

- **公共管理**

信息技术在公共管理中也将发挥越来越大的作用。5G将推动信息化进一步渗透到社会的生产生活之中，人们可以随时随地获得政府的服务，灾害预警、应急处置和公共安全管理更加精准高效。同时，网络空间管理成为公共管理的重要组成部分，个人或组织都可以随时随地成为信息发布者，正确的网络空间信息舆论引导，是社会良性有序的基础。

政府信息平台、网络服务平台和应急响应信息系统受到攻击，将造成政府信息化服务质量的下降甚至中断，影响政府服务职能的提供，影响社会正常的生产生活秩序，并对政府的权威性和公信力造成损害。通过社交网络、微博微信等网络平台传播消极信息、散布谣言，会带来社会骚动；有效身份的缺失，会导致信息无责任的发布、传播，现实社会诸多事件被扭曲、歪曲，将侵蚀广大网民的价值观和道德伦理。全球化的网络在加速信息流动的同时也增加了舆论控制、社会操纵、颠覆政权等危险，对国家、社会安定构成新威胁。

2.2 5G关联方视图

网络与服务平台提供者提供的软硬件、网络物理连接和协议是构成网络空间的基础设施，是网络空间的物质基础；人和组织等作为网络空间用户[5]，在网络空间中发布、传递和消费信息；社会和政府对网络空间进行监督，对网络空间活动加以规范，保障网络空间健康。用户、网络与服务平台提供者、社会和政府，在网络空间中扮演不同的角色，它们对于5G有着不同的安全需求。

2.3 安全需求分析

2.3.1 用户的安全需求

用户希望拥有一个可以信赖的网络空间，信息能够按照自己的预期产生和传递，个人银行账户、网络交易、病历信息等隐私不被泄漏，个人身份信息不被盗用和冒用。手机、电脑、汽车等设备也能正常地工作，不被别人遥控操纵。即使手机等支付终端损丢失，也不至于给自己造成过大的损失。在5G时代，用户希望网络空间：

-- 保证网络空间和现实空间的可信对接，网络空间身份[6]不被冒用，对自身及关联者网络行为能够合法溯源；

---

[4]实体（Entity）——本文专指构成网络和信息系统的各种软件、硬件、协议及其模块或单元。

[5]用户（User）——网络数据、信息的产生者和使用者，包括个人、组织以及连网的物体和机器。

[6]身份（Identity）——本文专指用户身份，即用户对象能被区分、识别的一个或多个信息元素。

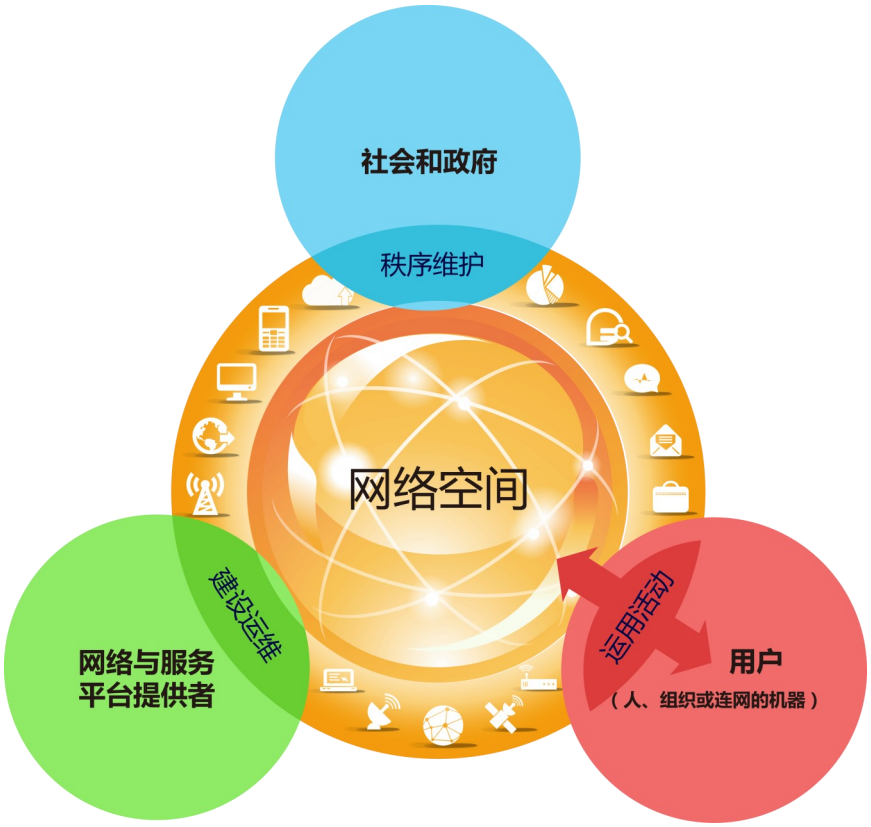

图2　网络空间关联方

-- 可获得稳定可靠的网络空间信息传输、处理等服务；

-- 根据安全需求不同，获得不同防护水平的信息通信服务；

-- 在网络空间的信息和行为等隐私能够得到较好的保护；

-- 使用和操纵的实体安全可信，具有病毒和木马等网络信息攻击的预警和免疫能力。

2.3.2 网络与服务平台提供者的安全需求

网络与服务平台提供者最重要的目标是为用户提供优质的服务，并满足社会监管需要。构建一个让用户信赖而且方便使用的网络，保障其中的实体运转良好，保证使用服务的用户身份真实可信，信息传输安全可靠。网络服务者需要对政府、金融、电力、电信、交通等行业提供相应的安全保障。对于网络与服务平台提供者，希望5G网络：

-- 优化网络资源配置，面向个人、企业、社会团体、物联网节点提供定制化安全服务；

-- 具有用户身份和信用确认的支撑能力；

-- 网络空间基础设施稳定可靠，易于维护管理；

-- 保护用户隐私，防范信息泄漏；

-- 满足网络空间监管要求，协助执法，具有追查信息来源的能力。

2.3.3 社会和政府的安全需求

人类社会需要一个良性的网络空间。随着未来5G网络的广泛应用，网络空间将覆盖人们日常信息消费、金融、交通、教育、医疗、工作等生产生活的方方面面。网络空间需要建立维护网络秩序、净化网络环境的机制，现实社会能够通过法律和道德约束、监督、管理网络空间行为，维护网络空间健康的生态环境。在5G时代，社会和政府希望：

-- 网络活动规范有序，符合法律和道德要求；

-- 提供网络空间和现实空间可信映射，用户对其网络行为可负责；

-- 隐私可以得到有效保护；

-- 网络技术应提升生活品质和社会安全感；

-- 网络空间基础设施应该安全可靠。

3. 5G网络安全架构

3.1 5G网络安全三要素

5G传输速度和连接数量大幅提升，通过移动互联网、物联网、车联网和工业互联网等应用，将现实空间与网络空间广泛地连接在一起。在保障接入安全、通信安全和数据安全的基础上，构建可信的网络空间，5G需要实现网络空间中身份可信、网络可信和实体可信。

图3　5G网络安全三要素

3.2 身份可信，行为可溯

建立可信身份，在网络空间中准确识别网络行为主体，是维护网络空间行为秩序、道德规范和法律制度的基础。通过现实空间中人、设备、应用服务等实体向网络空间的身份可信映射，实现网络空

间与现实空间身份的可信对应，网络空间活动的主体可以准确地追溯到现实空间中的用户，用户为其网络行为负责。

网络空间可信身份的建立依赖于具有公信力的网络身份基础设施。网络身份基础设施为个人、组织和实体分配网络空间标识，支撑软硬件来源可信、用户网络行为规范。基于网络空间可信身份，可建立与现实社会对应的征信机制，为网络和应用安全多样化服务提供可选择的依据。

5G网络采用可信身份框架（如图4所示），不泄露用户隐私信息。

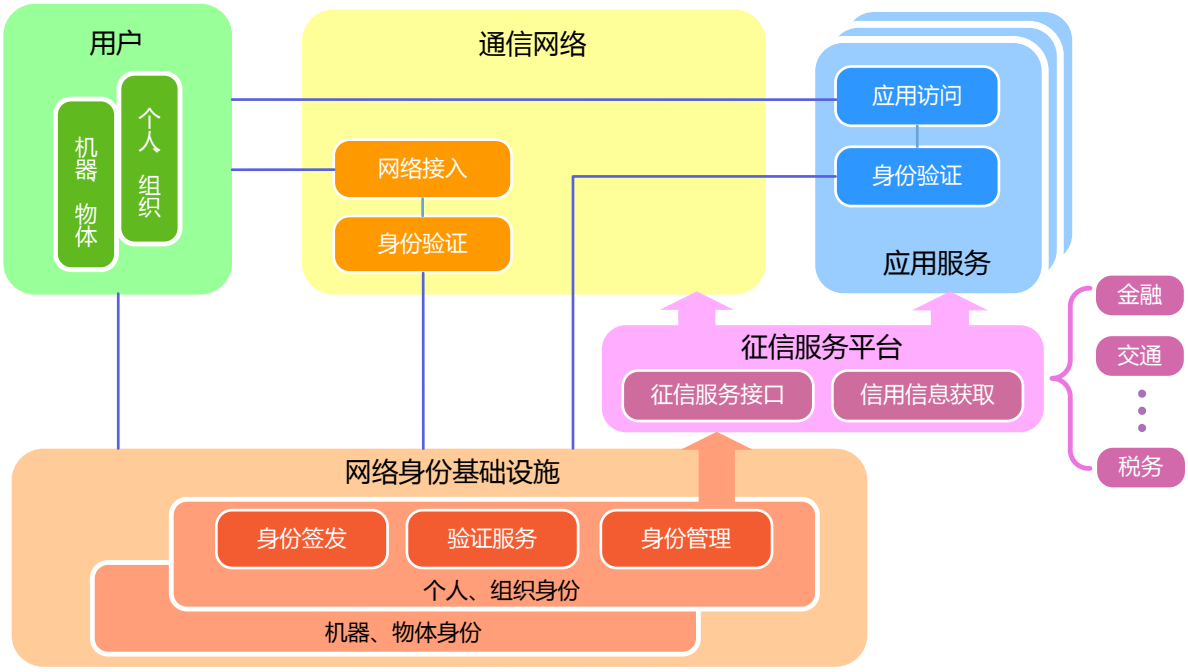

图4　可信身份框架

网络身份基础设施负责现实空间用户身份与网络空间用户身份的连接和映射。基于现实空间用户身份，生成网络空间身份标识，对网络空间身份进行注册、签发及管理。

在网络接入、应用服务连接时，网络身份基础设施支撑对接入的个人、组织、机器、物体等进行身份验证，根据需要实施相应验证策略和验证方法。5G基于连接场景（包括网络连接的大数据、移动设备、传感器、定位系统和社交媒体等）的技术和应用将为身份验证提供重要手段。

依托网络身份基础设施，可以建立征信服务平台，从金融、交通、税务等各类应用获取信用信息。

3.3 网络可信，安全分级

可信网络提供所需即所得的安全通信和应用服务，满足多样化应用场景需求。通过选择使用合适的网络资源切片，不同用户可获得不同安全保证等级的网络服务。高安全等级的用户甚至可获得类似于物理专网的网络隔离度和实时性保证。

可信网络框架如图5所示。

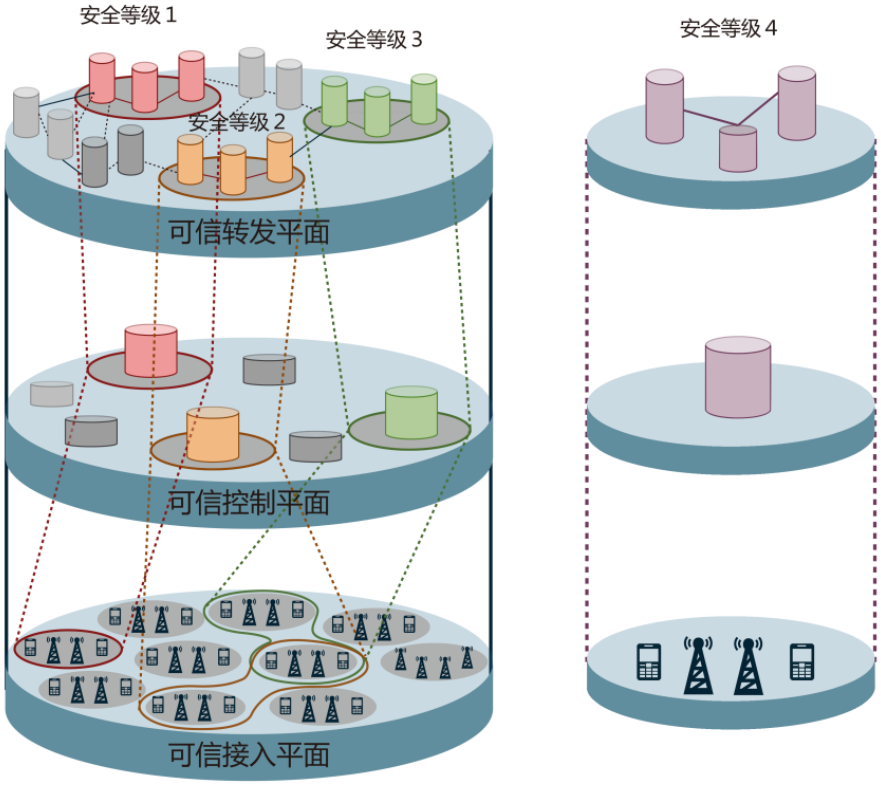

图5　可信网络框架

安全可分级的可信网络通过网络切片技术实现。5G网络引入NFV和SDN技术，将网络物理资源虚拟化为多个相互独立、平行的网络切片，根据安全等级和业务需求进行按需编排。运营商/用户首先根据安全等级需求生成网络切片模板，切片模板包括该等级下所需的网络功能和安全功能，各网络功能模块之间的接口以及这些功能模块所需的网络资源，然后网络编排功能根据该切片模板申请网络资源，并在申请到的资源上进行实例化创建虚拟网络功能模块和接口，或者是建立隔离的网络。

5G网络具有智能场景感知和按策略服务的能力。通过对地理位置、用户偏好、终端状态和网络上下文等场景信息的实时感知和分析，根据服务对象和场景动态选取不同的安全策略进行资源配置，对切片采用认证、加密等方式，提供差异化网络服务。

3.4 实体可信，内建免疫

可信实体是网络和应用安全可靠运行的基石。实体内建可信免疫机制，采用主动方式保证网络和服务正常运行，实现对病毒、木马的主动防御。

可信实体框架如图6所示，在实体平台上植入硬件可信根，构建从运算环境、基础软件到应用及服务的信任链，依托逐级的完整性检查和判断，实现实体软硬件环境的完整性保护。

入网检测认证过程中，对设计、实现的各级可信安全机制进行检测和认证，确保入网软硬件实体可信机制的正确实现。

图6　可信实体框架

4. 5G网络安全重要技术方向

面向网络空间和现实空间安全对接的5G网络，实现身份可信、网络可信和实体可信，需要从网络架构、协议和实体工程实现等多方面进行技术突破。

4.1 灵活可扩展的安全架构

5G网络需要解决安全边界变化、控制转发分离网络架构下的安全问题。支持应用、控制和转发功能的云安全，采取对网络流量进行镜像、阻断和过滤等安全操作，解决服务拒绝攻击、单点失效等安全问题。

5G需要提供异构网络整体的安全措施，为不同网络提供标准的接口进行安全操作，隔离不同类型网络；用户可以根据应用业务安全需求选择不同类型网络。

网络提供安全分级，建立网络切片机制，并制定适应于切片网络的灵活可选的安全服务措施，同时为特殊和应急场景预留一定的资源和扩展接口。

结合大数据技术，研究安全风险特征，实现准确的安全预警和防御。

4.2 新型网络安全机制和协议

5G网络中实体的控制面与转发面分离，5G网络架构产生了应用层、控制层以及转发层，需要重点考虑各层的安全、各层之间连接所对应的安全等。网络新的功能实体、协议、接口将成为新的攻击点，传统安全威胁的形式也会发生改变，如业务可能直接通过与核心网的接口对网络资源进行非法操作。5G业务系统需要从网络中获取更加丰富的信息，采取网络流量镜像、阻断和过滤等手段，对遭

受攻击的网络进行隔离，增强网络安全。

网络集中化控制的控制器是网络的核心，其可靠性和安全性非常重要，存在着负载过大、单点失效、易受网络攻击等问题，如果控制器被攻击，那么控制器覆盖的网络将会瘫痪，因此5G网络需要研究新的安全机制和安全协议保证网络安全。虚拟专用网络（VPN）需要使用统一标准规范，简化配置和使用过程，提供符合未来基于SDN的新型架构网络的操作接口。

4.3 海量网络身份标识与管理

网络身份基础设施应当能够支撑海量用户身份管理，支持超大规模数量的用户身份注册、管理、发布等功能。同时，网络身份基础设施应能够支撑5G多样化的应用场景，支持多安全等级、多类别的身份标识，提供标准化的应用框架和标准化的服务接口。

实现网络空间和现实空间身份的可信对接，需要研究与社会管理相适应的身份注册、登记和身份凭证管理服务体系，完成网络空间中的身份与现实身份的映射。针对个人身份，实现可靠、有效地身份验证服务，需综合运用人证同一验证技术，实现高效、智能验证，还需研究基于生物特征、网络行为、地理轨迹等用户和场景信息的身份识别验证技术。

4.4 网络实体自身安全可信

目前国内可信计算基本上局限于智能终端和计算机使用，在网络设备、嵌入式环境尚未形成标准方法和产业链配套。信任根是网络实体安全可信的源头和核心，为了适应网络设备和嵌入式环境的特定要求，需要研究低功耗、低成本、高性能的硬件可信根实现方式，解决硬件可信根的适应性、可用性问题。同时以信任根为基础，研究适应嵌入式环境定制化、多样化的信任链构建和扩展机制。针对应用模式和网络结构的变化，需要对数据中心和云计算模式开展虚拟化技术中的可信技术研究。

4.5 应用安全开发与可信发布

SDN等重要平台和软件的开发，需要安全的开发环境，避免应用程序存在先天漏洞。应用程序编程接口（API）的调用管理需要由专业管理机构评估和授权，审核应用程序对API的调用和对网络的操作的合理性、合法性，并出具操作边界规范。

5G网络中应用程序将会越来越丰富，为了保证网络安全秩序，需要对开发的应用软件进行认证，建立可信的应用发布机制。

4.6 适应复杂场景的密码算法与密钥管理

5G网络既有计算处理能力强的设备，也存在大量计算能力有限的终端，需要与计算能力相适应的密码算法、协议和密钥管理模式，设计效率高、满足安全性要求的通信协议。

考虑到小微蜂窝密集组网等5G网络应用模式，网络需要提供群签名、多重签名等新型签名机制和

网络协议，支持设备快速在多个小微蜂窝之间切换，支持车联网、D2D等场景网络节点频繁加入和退出时的快速认证和安全认证，减少验证和信令信息开销，保证服务的高效性、连续性和安全性。

4.7 数据与隐私保护

提供数据和隐私保护机制，5G网络需要设计匿名验证、盲签名、零知识验证、属性加密等面向场景的新型防护机制，研究高速加密、同态加密等密码技术，实现大数据、高速网络、云计算等场景的数据保护需求。5G网络通过持续身份验证等技术防止用户设备被诱骗，通过多天线、功率控制等技术降低空口数据被窃听的风险。

5. 总结

网络空间安全可信的三大要素是身份可信、网络可信和实体可信。实现身份可信，提供网络空间与现实空间的有效映射，支持网络行为可追溯，为规范网络空间秩序提供支撑；实现网络可信，面向不同应用场景提供不同安全保证等级的网络服务；实现实体可信，内建网络实体安全免疫能力。随着研究的深入，网络空间安全的内涵将不断丰富，实现机制、方法将不断扩充。

从TD-SCDMA到TD-LTE-Advanced，再到第五代移动通信技术研究，从保密通信、计算机安全、信息安全保障到网络空间安全，大唐电信科技产业集团一直致力于推动通信和网络安全技术的发展与创新，促进经济发展和社会文明进步。大唐将以开放合作的态度，与业界共同创建安全可信的网络空间。

版权所有：