中国联通
China unicom

中国联通 5G 网络商用密码应用白皮书（2023）

中国联通研究院

中国联通网络安全研究院

下一代互联网宽带业务应用国家工程研究中心

2023 年 11 月

版权声明

目　录

前　言

党的十八大以来，以习近平同志为核心的党中央高度重视网络安全工作，习总书记多次发表重要讲话，作出重要指示批示，从党和国家事业发展全局的高度对网络安全工作作出一系列新部署新要求。党的二十大报告指出，“以新安全格局保障新发展格局”，安全在发展中的作用愈发重要。密码是国家网络空间的安全基石与核心技术，也是党的事业和国之重器，密码工作直接关系国家政治安全、经济安全、国防安全和网络安全，直接关系社会组织和公民个人的合法权益，商用密码工作是密码工作的重要组成部分，在维护国家安全、促进经济发展、保护人民群众利益中发挥着不可替代的重要作用。对密码发展进行系统性、体系性的研究和探索，进一步挖掘密码融合创新能力、打造密码生态和发挥密码效能，对践行总体国家安全观，适应国家治理体系和治理能力现代化要求，充分发挥密码在数字经济发展和网络空间安全中的基础支撑作用具有重大意义。

5G 网络是数字经济发展的关键支撑，基于大带宽、低时延、高速率的传输特性，不仅带来更高速、优质的网络体验，也为数字经济发展“修好桥”“铺好路”。随着 5G 网络的飞速发展与行业的不断融合，行业对安全差异化与精细化的需求更加紧迫，密码本身作为安全的重要内核，在 5G 中的作用越来越凸显，尤其近几年来随着国际环境的风云变幻，我国自主可控能力需求进一步提升，更加强调商用密码的应用，特别是重要基础设施行业，纷纷把网络建设与商用密码

应用作为“三同步”的重要要求。此外，随着国家一系列法律法规的出台，《数据安全法》、《个人信息保护法》、《密码法》、《网络安全法》以及《关键基础设施保护条例》等相继实施，有力的指引并推动了商用密码的应用，不断拓宽加深密码在行业应用的广度与深度，更加强调商用密码在促进产业数字化转型、数字产业化等方面的重要作用。为此，加快推进商用密码在 5G 网络中的应用落地，充分激发 5G 与密码应用结合的创新能力，提升运营商和行业用户网络的自主可控、安全合规能力，保障商用密码应用的正确、合规、有效具有重要的价值意义。

目前，5G 网络安全防护主要采用国际密码算法，我国商用密码仅 ZUC 算法在 5G 网络 RRC、NAS 信令面以及空口用户面机密性与完整性保护过程中被作为可选项。在面向工业互联网典型场景和党政军等行业的高安全需求时，5G 网络由于不具备基于商用密码的安全能力，无法满足其高安全需求。随着 5G 网络和业务的发展，亟需推进商用密码技术在 5G 网络中的应用，填补密码技术应用空白，筑牢 5G 网络安全防线。

本白皮书详细阐述了我国商用密码应用发展现状，结合 5G 网络特点，提出了 5G 网络商密应用体系架构，并给出了商用密码在 5G 网络中的应用实践，最终对 5G 网络商用密码应用的未来发展趋势进行了展望，以期为打通商用密码技术产业链上下游，为 5G 网络商密应用提供参考。

编写单位：

中国联通研究院、中国联通网络安全研究院、下一代互联网宽带业务应用国家工程研究中心、联通数字科技有限公司、中国联通广东省分公司、中兴通讯股份有限公司、三未信安科技股份有限公司、渔翁信息技术股份有限公司

编　　委：

中国联通研究院、中国联通网络安全研究院、下一代互联网宽带业务应用国家工程研究中心：李红五、叶晓煜、徐雷、张曼君、陆勰、姚戈、王姗姗、谢泽铖、王蕴实、程筱彪、侯捷、谢中怀、郭新海、傅瑜、陶冶、贾宝军、李强

联通数字科技有限公司：李广聚、朱常波、张建荣、张建桁、周凯、鲁华伟、韩浩

中国联通广东省分公司：潘桂新 李文彬 彭健

中兴通讯股份有限公司：郝振武，关先锋，代九龙，祁娟，魏立平

三未信安科技股份有限公司：鹿淑煜、王华龙、张万涛

渔翁信息技术股份有限公司：刘新田

一、商用密码应用发展现状及挑战

1.1 商用密码概述

根据《商用密码管理条例》中的定义，商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。目前我国自主研发的商用密码算法主要包括：SM1 、SM2、SM3、SM4、SM7、SM9 和 ZUC 算法，其中，SM1 和 SM7 算法不公开，它们的组合可以为各种需要密码技术作为支撑的行业应用提供坚实可靠的基础。

商用密码具有广泛的应用前景，主要面向不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等数据进行加密保护。例如企业敏感信息的传输与存储加密、防止非法第三方获取数据、安全认证与数字签名等。

1.2 商用密码发展现状

党的十八大以来，以习近平总书记为核心的党中央高度重视互联网、发展互联网、治理互联网，形成了网络强国战略思想，走出了一条中国特色治网之道，指引我国网信事业取得历史性成就，商用密码由此得到全面发展。国内密码产业链不断完善，国产密码厂商逐年增加，2020 年《商用密码产品认证目录》颁布后，全国拥有认证商密产品的企业共 551 家。随着近几年的发展，密码产业在法律法规、

标准体系、监管考核、产业应用等方面进展显著，为商用密码更加广泛的应用奠定坚实的基础。

1.2.1 法律法规指引

随着《网络安全法》《密码法》《关键信息基础设施安全保护条例》《个人信息保护法》等一系列法律法规的颁布和实施，我国各领域对商用密码技术和产品的需求将明显增加，应用需求将持续推动技术进步，商用密码产业将迎来长期且持续的发展机遇。

国家在政策法规层面逐步完善现行商用密码管理制度，促进商用密码应用改造，进一步规范商用密码的使用和管理，保障商用密码使用有法可依，引导商用密码产业健康有序发展。

2023 年 4 月 27 日，国务院总理李强签署第 760 号国务院令，公布修订后的《商用密码管理条例》，自 2023 年 7 月 1 日起施行，这就意味着商用密码应用安全性评估正式由“推荐性”转为“强制性”。

1.2.2 标准体系保障

我国高度重视商用密码国际标准化工作，大力推进以我国自主设计研制的 SM 系列算法为代表的中国商用密码标准纳入国际标准，积极参与国际标准化活动，加强国际交流合作。2011 年 9 月，我国设计的祖冲之（ZUC）算法纳入国际第三代合作伙伴计划组织（3GPP）的 4G 移动通信标准，用于移动通信系统空中传输信道的信息加密和完整性保护，这是我国密码算法首次成为国际标准，ZUC 算法也是 5G 网络中的空口机密性与完整性保护的算法之一，目前，我国正推动 256 比特版本的 ZUC 算法进入 5G 通信安全标准。除此之外，从

2015 年 5 月起，我国又陆续向 ISO 提出了将 SM2、SM3、SM4 和 SM9 算法纳入国际标准提案。2017 年，SM2 和 SM9 算法正式成为 ISO/IEC 国际标准；2018 年，SM3 算法正式成为 ISO/IEC 国际标准；2020 年 4 月，ZUC 算法正式成为 ISO/IEC 国际标准；2021 年 3 月，SM9 标识加密算法正式成为 ISO/IEC 国际标准；2021 年 6 月 25 日，SM4 分组密码算法正式成为 ISO/IEC 国际标准；2021 年 10 月，SM9 密钥交换协议作为国际标准 ISO/IEC11770-3:2021《信息技术密钥管理第 3 部分:使用非对称技术的机制》的一部分,由国际标准化组织 ISO/IEC 正式发布。这些标志着我国商用密码算法具有国际领先的技术理论基础，已经具备了可以广泛应用商用密码的条件。

1.2.3 行业监管要求

随着顶层法律法规的逐步健全，标准体系的不断完善，密码应用更加广泛，各行业对密码应用更加强调合规、正确、有效，随之而来的密码相关的监管要求工作也在不断推进。

在重要领域和网络空间推进密码应用，是贯彻落实网络强国战略和密码法，切实防范重要信息系统安全风险的一项重要举措。2019 年年底，国务院办公厅印发了《国家政务信息化项目建设管理办法》，明确要求政务信息化项目应同步规划、同步建设、同步运行密码保障系统并定期进行评估，对于不符合密码应用和网络安全，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统；2021 年 8 月交通运输部发布的

《交通运输领域新型基础设施建设行动方案》中强调推进商用密码技术应用；2022 年 12 月电力行业明确密码应用要求，颁布《电力行业网络安全等级保护管理办法》，其中单列一章（第四章：网络安全等级保护的密码管理）明确密码管理要求；2023 年 3 月交通运输部，国家铁路局，中国民用航空局，国家邮政局，中国国家铁路集团有限公司联合印发《加快建设交通强国五年行动计划(2023-2027 年)》其中第 18 条开展网络和数据安全能力提升行动，明确要求组织实施网络安全实网攻防演练，加强商用密码应用推广。

在通信领域，工业和信息化部高度重视商用密码应用推进工作，2021 年 3 月 11 日成立工业和信息化部商用密码应用产业促进联盟成立。联盟贯彻落实《密码法》有关要求，推动工业和信息化领域商用密码应用和创新发展，进而做大做强商用密码产业，推动商用密码产业健康、高质量发展。当前，商用密码在科技创新、产业发展和应用推广等方面的落实工作已经初见成效。

关键信息基础设施安全是网络安全防护的重中之重，加快推进密码在通信领域关键信息基础设施中的应用，构建更加完善的关基安全体系势在必行。2020 年 4 月，国家密码管理局组织编写出版《商用密码应用与安全性评估》，监管部门在每年的考核中对商用密码应用也作了明确要求，对关键基础设施、等保三级以上的信息系统要求开展商用密码应用安全性评估。2021 年 9 月 1 日起施行《关键信息基础设施安全保护条例》，2022 年 11 月 7 日，全国信安标委公众号发布了《信息安全技术 关键信息基础设施安全保护要求》（GB/T

39204-2022）（简称“《关基安全保护要求》”），该标准于 2023 年 5 月 1 日正式实施，作为关键信息基础设施安全保护标准体系的构建基础，明确了密码技术的应用要求，为运营者开展关键信息基础设施保护工作需求提供了强有力的标准保障。

1.2.4 产业发展助力

近年来，商用密码产业链体系逐步完善，我国商用密码产品自主创新能力持续增强，产业支撑能力不断提升，部分产品性能指标已达到国际先进水平。随着信息技术产业的持续发展和完善，密码产品也随之迭代丰富，现有商用密码产品达到 3,000 余款，其中 2,200 余款产品取得商用密码产品认证证书，品类涵盖了密码芯片、密码板卡、密码整机、密码系统等全产业链条，形成了完整的商用密码产品体系。随着商用密码“放管服”改革的深入推进，预计商用密码从业单位和产品数量将得以进一步增长。从密码技术的产业链成熟度看，上、中、下游的密码技术发展势头强劲。密码产业链上游包括安全芯片、印刷电路板、服务器三大类，基本形成了能够覆盖目前所需的密码相关的技术、产品和服务，技术成熟度越来越高；中游主要是以密码技术为核心的产品，包括密码机/密码卡、数字证书、VPN、令牌、电子签章、量子加密六大类；下游主要是软件、系统集成及应用领域。密码整个产业链具有完整的体系，能够为各行各业提供密码相关的技术、服务和产品。此外，随着我国网络安全政策法规的逐步推进、产业生态日益完善和安全需求的深化演进，我国网络安全产业发展进入快车道。据 IDC 统计，我国 IT 安全产业规模 2023 年预计达 136.26 亿

美元（约 941.16 亿元），同比增长 18.07%，到 2026 年，IT 安全市场投资规模将达到 319 亿美元，其中安全软件的市场占比将超过安全硬件，软件占比在 2026 年将达到 41%。

密码作为网络信任体系的重要基石，涵盖数据加密、身份认证、消息认证三大场景，伴随我国网安建设由“合规驱动”向“事件驱动”转型，密码技术重要性更加凸显，据赛迪研究院预测，2023 年我国商用密码市场规模有望达 985.85 亿元，同比增长 39.32%。

伴随着商用密码应用安全性评估的要求、信创产业的发展，我国商密产业发展速度将持续提升，未来需求将在 ICT 基础设施、物联网、数字经济等更广泛领域渗透，商密市场规模将不断扩大。

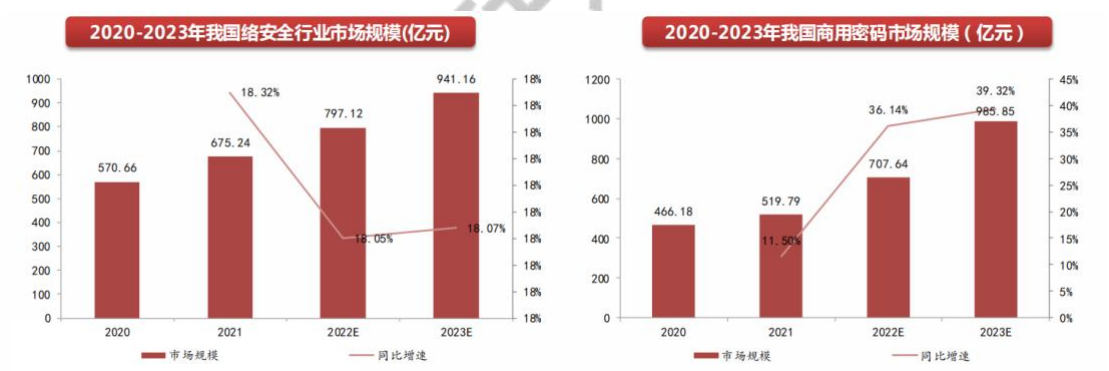

图 1 我国商用密码行业及市场发展规模（数据来源：IDC，赛迪，西南证券）

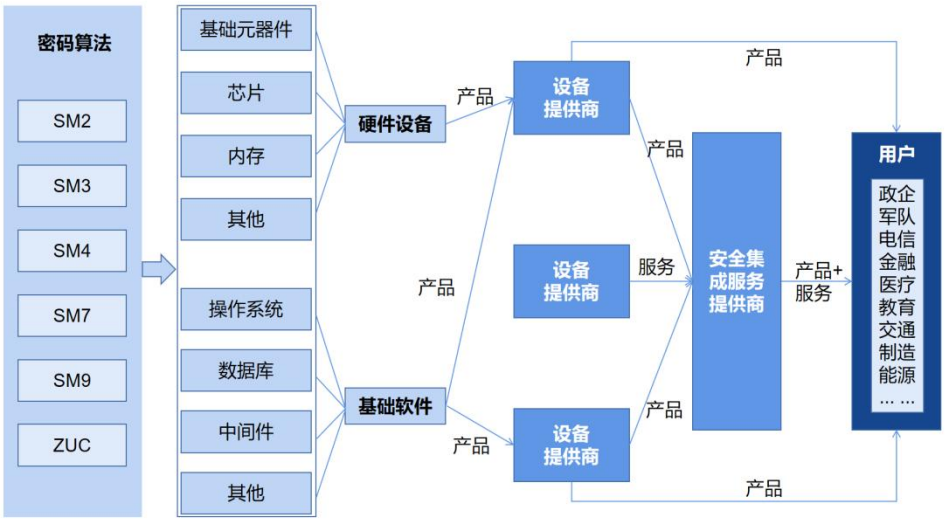

图 2 商用密码产业链（资料来源:《商用密码行业发展机遇报告（2022 年）、国信证券经济研究所》）

1.3 商用密码融合发展的挑战

1.3.1 密码保障能力及信任体系未完全建立

虽然密码的产业链和环境在不断的优化升级，但当下还是面临一些不容小觑的挑战。在一些关键行业，商用密码并未得到有效实施，一些单位重信息化建设、轻安全保护，信息系统密码使用不规范、不正确，密码使用存在不安全情况，在密钥管理、密码系统运维等方面存在风险，密码安全能力建设相对滞后，制度体系不配套等等。总体来说，密码的安全保障能力不足，基于密码完整的信任体系未全面建立。

1.3.2 密码高性能需求与兼容性成为发展瓶颈

随着算力网络、大数据、云计算的不断发展，对密码产品的性能要求逐渐提升，低性能成为密码产品发展受限的瓶颈，传统的、通用密码产品已经越来越难做到“广谱适用”，通用处理器、操作系统、

数据库、中间件等基础软硬件产品，对于密码技术的内生支持尚不充分，兼容性、适配性仍存在问题，这在相当程度上制约了部分复杂场景下商用密码应用的开展。

1.3.3 密码产业链供应链的融合创新能力不够强

目前，密码产业链供应链优质资源分散，缺乏产业级创新发展基地和密码产业聚合效应；密码通用型产品较多，针对行业差异化的需求不能全面满足，按需定制能力不足；科研机构研究成果转化能力不够强，成果落地存在差距。

透过商密应用融合发展面临的挑战棱镜，映射到运营商网络中，主要存在四方面的挑战：

（1）缺乏细粒度的指引性文件

以关基为例，按照现有的管理规定（网络安全法（第三十八条），关保条例（第十七条）），关基商密应用安全性评估检测的周期均为每年至少一次，但在实际开展工作中，由于密评体系不够完善，缺乏通信领域关基商密应用有效、正确、合规的评测抓手，方案应用场景、方案设计、密评机构认证认可等关键环节缺乏指导，导致关基商密应用推广后劲不足。

（2）缺乏成熟案例指引

由于国外算法起步较早，应用范围较广，所以对其替换难度较大，周期较长。目前，国内轻量级的改造方案较少，改造难易程度、性能、兼容性等效果影响需要多方评估，缺乏成熟案例指引。

（3）高性能密码资源不够丰富

运营商拥有种类繁多、格式各异、数量庞大的数据资源，对数据全生命周期的安全要求较高，随着网络的高速发展，算力、网络、数据、安全密不可分，相应对设备的要求也越来越高，而密码产品、技术、服务与运营商需求有着明显差距，导致密码产品在运营商网络应用不够深，不够广，响应机制不足。

（4）产业上下游耦合度较低

针对商用密码在运营商应用的情况来看，目前存在设备厂商、密码厂商、安全厂商在密码技术应用产业链各环节缺乏联动。密码厂商对通信网络和运营商的需求不了解，设备厂商对商密算法支持度低，支持商用密码算法的产品体系不丰富，安全厂商兼顾设备商和密码厂商产品特性，但商密产品体系不完善，产业联动性不足。

基于此，亟需加快推动商用密码在基础电信企业中的应用，针对 5G 网络的商密应用，需要打通商用密码在 5G 网络中的应用壁垒，畅通商密应用交流渠道，构建面向 5G 网络的商用密码应用能力体系，打造 5G 商密应用“硬实力”，面向行业实际业务场景，为行业提供自主可控、灵活高效、安全合规的 5G 商密应用能力，锻造基础电信企业 5G 商密原子能力，筑牢 5G 网络和行业用户安全防线。

二、5G 网络商密应用体系架构及方案

2.1 5G 网络密码应用情况

密码技术是信息安全的核心技术，是网络安全与信任体系的基石，也同样是 5G 网络安全机制的关键基础。

在 5G 标准制定过程，国内外标准化组织持续推进密码技术在 5G 中的的应用，满足用户接入安全和用户隐私保护、信令和数据传输的机密性和完整性保护、数据存储的机密性和完整性保护等安全需求，防范空口安全威胁、终端安全威胁、通信网络安全威胁、基础设施安全威胁等方面。

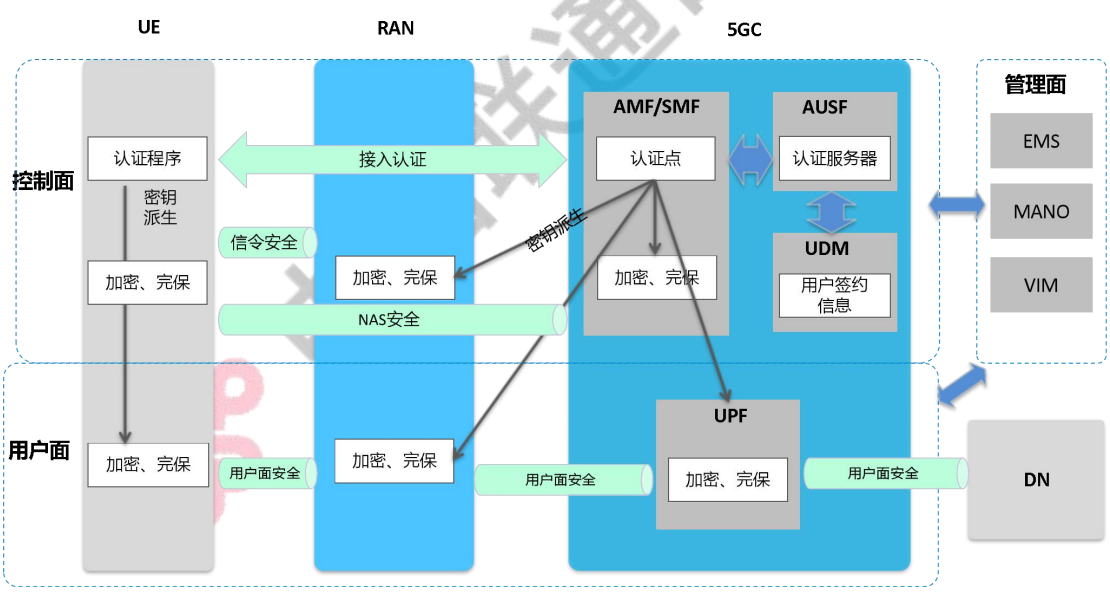

图 3 5G 网络密码技术应用概况

5G 网络密码技术主要用于以下方面：

（1）5G 用户可信接入

隐私保护：用户设备 UE 接入网络时，应用非对称等算法对用户

标识 SUPI 进行加密保护，生成 SUCI 标识，防止在空口暴露 SUPI 信息。

用户主认证：用户设备 UE 接入网络时，使用对称算法在入网附着过程中与核心网网元 UDM 之间进行双向认证，防止非授权用户设备 UE 接入网络，或者用户设备 UE 接入伪基站或假冒网络。

用户二次认证：5G 二次认证支持 EAP 认证协议，有很强的扩展性，对应的认证方式和密码算法由终端和 AAA 认证服务器协商决定。

密钥派生：在用户认证成功后，应用散列函数算法进行多层次的密钥派生，用于密钥的分发、数据的完整性和机密性保护，以保护根密钥。

（2）数据传输安全

空口安全：基于派生密钥，使用 SNOW 3G、AES、ZUC 对称密码算法，对用户设备和基站之间的 AS 层信令和数据，以及对用户设备和核心网之间的 NAS 层信令和数据进行完整性和机密性保护。其中，国产祖冲之算法 ZUC 在网络中优先级配置低于 SNOW 3G 和 AES 算法。

用户面安全：在用户面接口（N3：gNB-UPF，N6：UPF-DN，N9：UPF-UPF）通过密码技术建立 IPSec 安全传输通道，保证用户数据传输的机密性和完整性。

控制面安全：在 5GC 服务化架构中，5GC 网络功能（AMF/SMF/UDM/NRF/NEF/AUSF 等）之间采用 SBI 接口，建

立 HTTPS 安全传输通，对控制信令进行完整性和机密性保护；在基站/UPF 与 5GC 控制面之间的 N2、N4 接口建立 IPSec 安全传输通信，对控制信令进行完整性和机密性保护。

（3）运维安全

设备证书：由运营商为基站、核心网网元签发证书，支持设备级认证，实现设备准入、设备间认证、设备生命周期管理等功能。

管理接口安全：在 EMS/VIM/MANO 等提供运维管理界面的网元中，客户端使用 HTTPS 接入。

在上述场景中，涵盖终端、基站、核心网设备，其中涉及到终端安全的，如用户可信接入、空口安全、NAS 安全，3GPP 详细定义了流程和算法，而对于网元域间安全、运维安全，3GPP 只是给出了安全建议，并没有定义具体算法。从标准定义和具体的实践看，5G 网络普遍使用国际通用密码算法，迫切需要加强国产密码在 5G 行业专网网络中的研究和应用。

另外，国家已经出台了 GB/T 39786《信息安全技术 信息系统密码应用基本要求》、《GMT0115 信息系统密码应用测评要求》、《GMT0116 信息系统密码应用测评过程指南》等密码应用标准规范，需要基于上述标准，指导 5G 网络国产密码应用，从而使得其应用最终能够满足密码应用的要求。

2.2 5G 网络商用密码应用体系架构及方案

在 5G 网络中应用商用密码技术，总体需要遵循 3GPP、CCSA

等国内外标准组织发布的 5G 网络标准、5G 安全标准、专网标准等要求，面向智能电网、工业互联网、物联网等垂直行业，结合具体不同场景的安全需求，在不影响基本业务流程和业务要求的情况下，引入商用密码技术和产品，从网络层提供商用密码防护能力，在密码算法层面实现对 5G 网络的自主可控。

在 5G 专网网络环境下，以商用密码和配套软硬件平台为核心，面向多种垂直行业安全需求，实现基于商用密码 5G 专网模式，在 5G 网络空口侧、控制面、用户面的身份认证、密钥派生、数据加密、安全通道等功能涉及的密码算法均采用商用密码算法，构建一套端到端完全独立的 5G 商用密码专网。

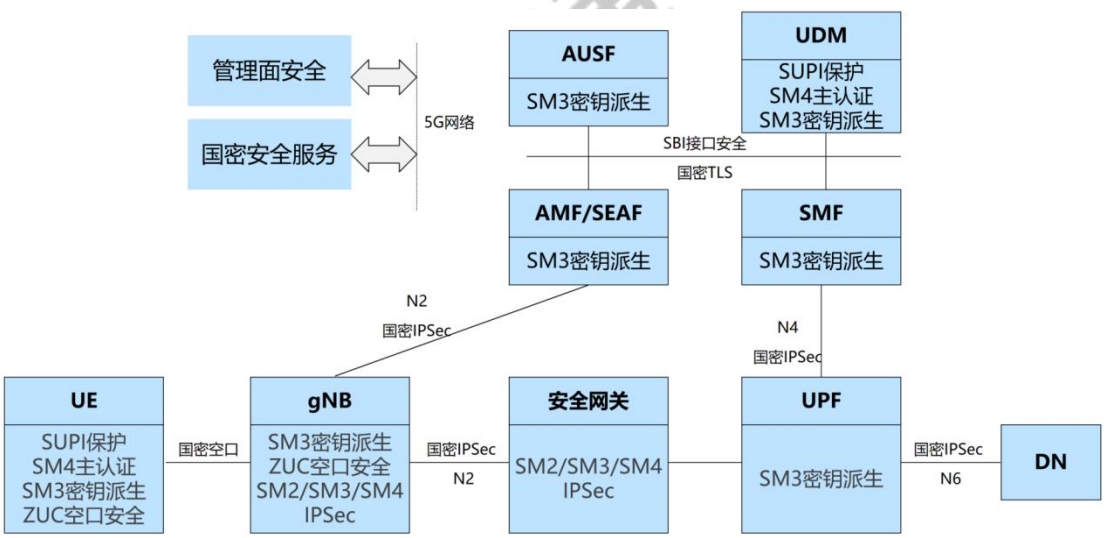

图 4 5G 网络国产商用密码应用架构

（1）用户可信接入：

1）隐私保护：基于 SM2 算法，辅之以 SM3/SM4 算法对终端 SUPI 加密生成 SUCI，实现用户身份标识的保护。

2）用户主认证：基于 SM4 算法实现终端与网络的双向认证，

保证用户接入的可信性，并基于认证进行密钥派生。

3）密钥派生：基于 SM3 算法实现分层密钥派生，密码算法派生的相关网元有 UDM、AUSF、SEAF、AMF、gNB 及 UE 等，可进一步优化，实现关键环节的密钥派生。

（2）数据通信安全：

1）空口安全：使用商用密码 ZUC 算法进行空口的安全防护，具体包括，UE 与 gNB 之间 AS 层 ZUC128 信令和数据完整性和机密性保护，UE 与 AMF 之间 NAS 层 ZUC128 信令完整性和机密性保护。

2）用户面安全：在 gNB-UPF、UPF-DN、UPF-UPF 等安全传输网元之间，基于 SM2/SM3/SM4 算法在网元间建立 IPSec 通道，实现用户数据传输的完整性和机密性。

3）控制面安全：在支持 SBI 接口的 5G 核心网网元之间，基于 SM2/SM3/SM4 算法在网元间建立 TLS 安全传输通道，保证控制信息的安全传输；在 gNB-AMF 、UPF-SMF 等关键接口，建立商用密码 IPSec 通道。

（3）管理和存储安全：

1）管理面安全：EMS、OMC、MANO、VIM 均为 B/S 架构，这些管理设备与网元之间也多采用 B/S 架构，这些接口可进一步采用商用密码浏览器、商用密码 TLS 安全传输等技术，进行身份认证、数据安全传输，保证用户可信接入安全，防范数据被窃取和篡改的风险。

2）设备管理：启动商用密码证书，支持设备认证、数据签名、数据机密等功能。

3）数据存储安全：网络有管理数据、配置数据、工作参数、操作日志等，存在窃取和串改的风险，引入商用密码技术，保证这些重要数据的安全存储和使用。

目前 5G 网络密码应用方面缺少体系性设计指引，尚未建立密码应用标准体系，中国信息通信研究院牵头制定 5G 独立专网场景密码应用与安全性评估实施指南等规范，可填补这方面的空白。

为了使 5G 商用密码专网满足国家密码技术要求，可借鉴成熟的密码平台技术框架与技术理念，将国产商用密码技术融入 5G 基础网络，建设 5G 商用密码专网服务体系，不断创新，为 5G 行业用户提供密评合规、密评整改、商用密码整改、商用密码数据加密提供统一的密码安全服务和综合安全解决方案。

通过在不同环节、不同层面引入国产密码技术，可以根据实际需求，局部或全部引入国产密码技术，增强 5G 专网的安全。其中管理和存储安全，主要采用 IT 领域成熟技术，构建管理和数据存储方面的安全能力。

2.3 用户可信接入

2.3.1 基于商用密码的用户隐私保护

在 3GPP 标准中，UE 首次接入网络时，5G 网络支持使用 ECIES 算法框架，采用椭圆曲线集成加密等算法实现 SUPI 加密隐藏生成

SUCI。商用密码用户隐私保护方法将使用相应的国产密码算法进行替换，实现对 SUPI 的隐藏。5G 商用密码专网中 ECIES 算法框架中涉及密钥生成算法、密钥协商算法、密钥派生算法、SUPI 加密算法、消息鉴权码算法等，能够对应采用 SM2、SM3、SM4 算法，如表 1 方案 Profile <C>所示。

表 1 SUCI 的保护方案

方案	标识符	采用算法
null-scheme	0x0	NULL
Profile <A>	0x1	Curve25519；SHA-256；HMAC－SHA-256；AES－128 in CTR mode
Profile <B>	0x2	secp256r1；SHA-256；HMAC－SHA-256；AES－128 in CTR mode
Profile <C>	0x3-0xB（需要标准化）	SM2；SM3-256; HMAC－SM3-256; SM4－128 in CTR mode
未来标准化保护方案	0x4-0xB	\
运营商专有保护方案	0xC-0xF	\

2.3.2 基于商用密码的认证流程

5G 商用密码专网采用商用密码算法进行认证向量的生成，在设备和核心网之间进行双向身份认证，以实现设备安全接入网络，保护设备与网络的安全。

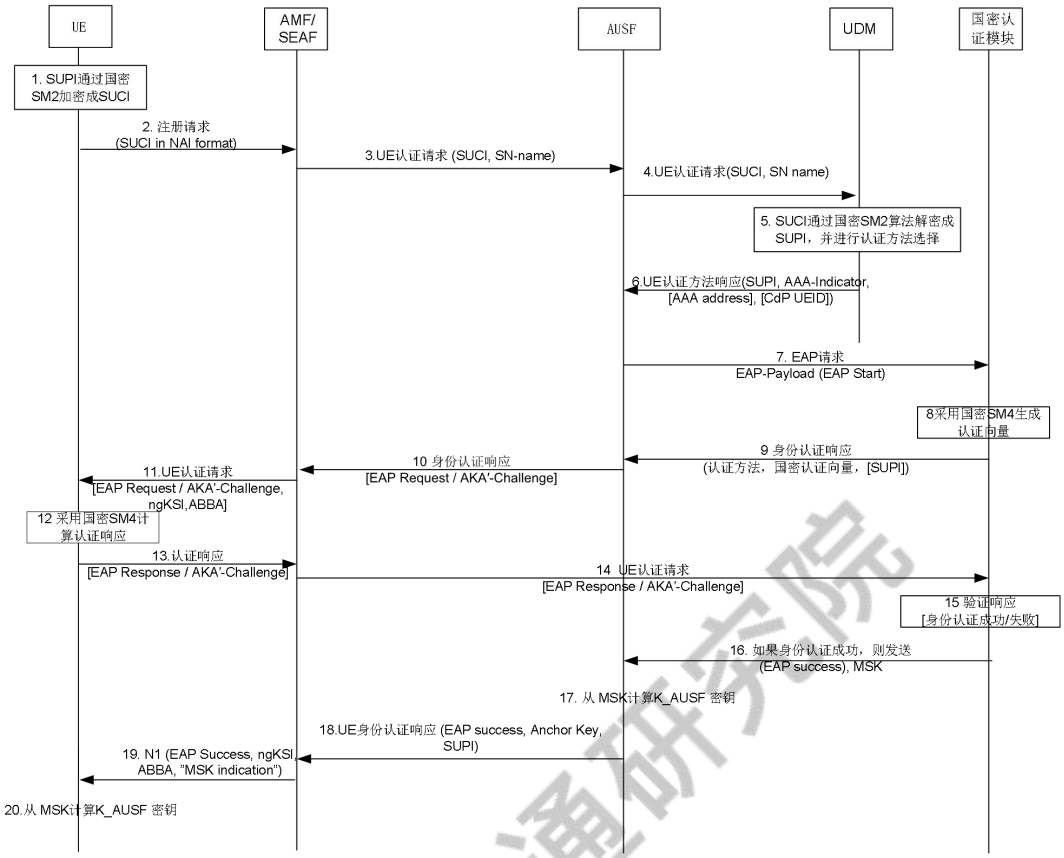

图 5 基于国产商用密码的主认证流程

5G 终端入网主认证过程如图 5 所示，当终端向核心网发起入网注册请求时，首先由核心网 UDM/ARPF 网元为其生成认证向量 AV，通过 AUSF、SEAF 网元发送到 UE 中，然后 UE 对核心网进行认证并在通过认证后计算 RES*返回给核心网，最后 SEAF、AUSF 网元根据接收到的 RES*对终端进行认证，完成主认证过程。

主认证过程中，核心网网元 UDM/ARPF 网元生成认证向量 AV，以及用户设备 UE 对核心网进行认证并计算 RES*时，如图 6 所示，其中 EK 为对称加密算法，在 3GPP 标准中规定为 AES 算法，在构建高安全 5G 独立专网时，将 EK 由 AES 替换成我国商用密码算法 SM4 即可。

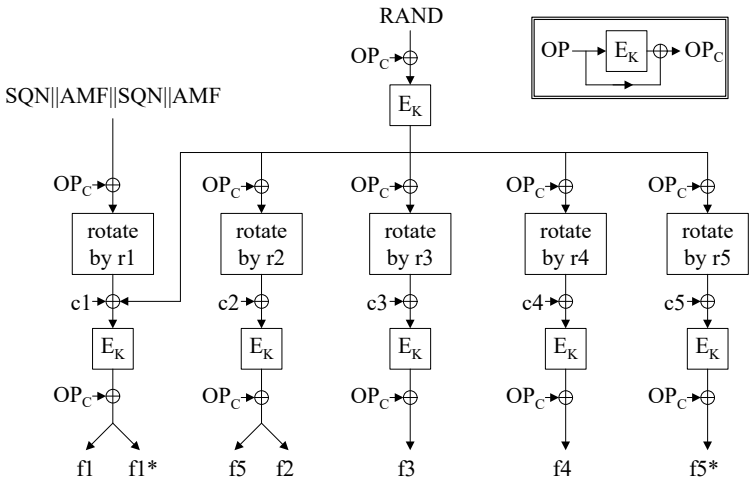

图 6 5G 身份认证向量计算

2.3.3 基于商用密码的密钥派生

基于 5G 标准密钥派生架构，采用 SM3 算法替代原有国外算法，实现密钥派生函数商用密码化改造，为主认证、空口安全、AKMA 认证等提供相关密钥。

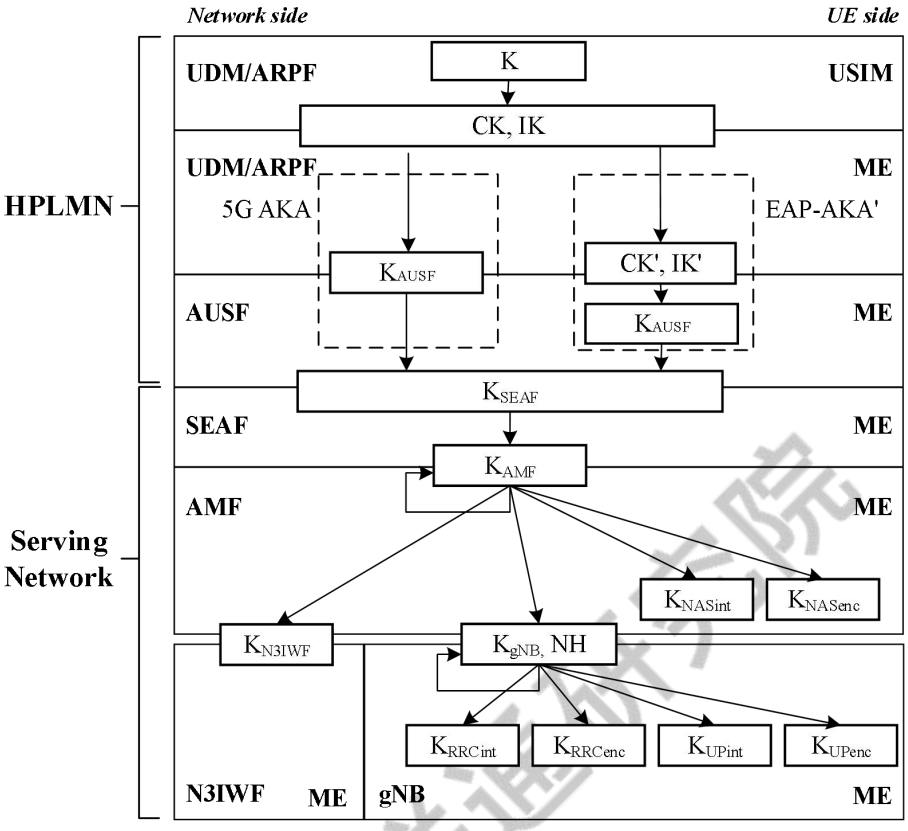

图 7 5G 密钥派生层级

5G 基本延续了 4G 的密钥派生方式，其中根密钥 K 为用户(UE)与核心网络的统一认证数据管理(UDM)共享的长期密钥，整个密钥派生系统依赖于这一密钥。密钥层级的第 2 层是加密算法密钥(confidentiality key，简称 CK)和完整性保护算法密钥(integrity key，简称 IK),在 CK 和 IK 的基础上,具体的派生密钥包括: K_{AUSF}，K_{SEAF}，K_{AMF}，K_{NASint}，K_{NASenc}，K_{N3IWF}，K_{gNB}，K_{RRCint}，K_{RRCenc}，K_{UPint} 和 K_{UPenc}。

针对密钥派生，采用 HMAC SM3 256 算法代替 HMAC SHA 256 算法，代替方法有两种方式：

方式一：在密钥派生每个环节都使用 SM3 算法，涉及 USIM、

UE 和 UDM、AUSF、SMF、AMF、gNB 等网元，该方式改造彻底，但工作量大，另外需要专网内的所有网元同步升级，以保证密钥派生的正确性。

方式二：在关键环节使用 SM3 算法派生，如在关键密钥 K_{AUSF} 派生过程中使用 SM3 算法，这时只涉及 UDM 和 ME。这种方式只需要对归属网络进行改造，不需要对拜访网络进行改造，部署方便，并采用两种异构的派生算法，在一定程度上能够提升派生密钥的安全性。

2.4 数据通信安全

2.4.1 基于 ZUC 算法的空口安全

ZUC 算法在 4G 时代已经被 3GPP 国际标准采纳，现在的 5G 终端和网络设备均已支持 ZUC 算法，已经具备规模应用条件。具体地，在基站上配置 ZUC 算法的优先级最高，开启 AS 层信令和数据保护，通过 gNB 与 UE 派生出的密钥实现 ZUC-128 完整性和机密性保护能力，并进一步在 AMF 上配置 ZUC 算法优先级最高，开启 NAS 层信令保护，通过 AMF 与 UE 派生的密钥实现 ZUC-128 完整性和机密性保护。

同时，我国加强运营商、设备制造商、终端、芯片企业及科研院校等的紧密合作，深化国际合作，积极推动 ZUC-256 密码算法在 5G 系统以及未来移动网络中应用。IMT-2020（5G）推进组密码算法特设组发布了《ZUC-256 算法实现评估报告》，对 ZUC-256 密

码算法设计进行了详细分析和评估；中国信息通信研究院牵头信息通信芯片开发、设备研制、运营服务等产业单位，对 ZUC-256 算法的工程实现进行了研究评估、推动 ZUC-256 密码算法成熟、标准化及应用。

2.4.2 基于商用密码的用户面分段传输安全

5G 网络用户数据在用户面进行传输，在用户终端和目标 DN 网络中传输，除了上述的空口安全，还包括基站-UPF、UPF-DN 等环节，数据经过不同的安全域，这其中包括 N3、N6、N9 等接口。

在 5G 行业专网中，引入商用密码 IPSec 能力，对 5G 用户面实施分段保护机制。

对于 N3 接口，通常在基站内置商用密码 IPSec 软硬件功能，在 UPF 前置 IPSec 安全网关，或在 UPF 内置 IPSec 安全网关功能，在基站和 IPSec 安全网关之间建立 IPSec 通道，将需要加密传输的数据流在 IPSec 通道中传输。

对于 N6、N9 接口，需要与对端建立 IPSec 通道，这时可以使用 UPF 配套或内置的 IPSec 安全，也可利用部署在边界的防火墙的 IPSec 功能。

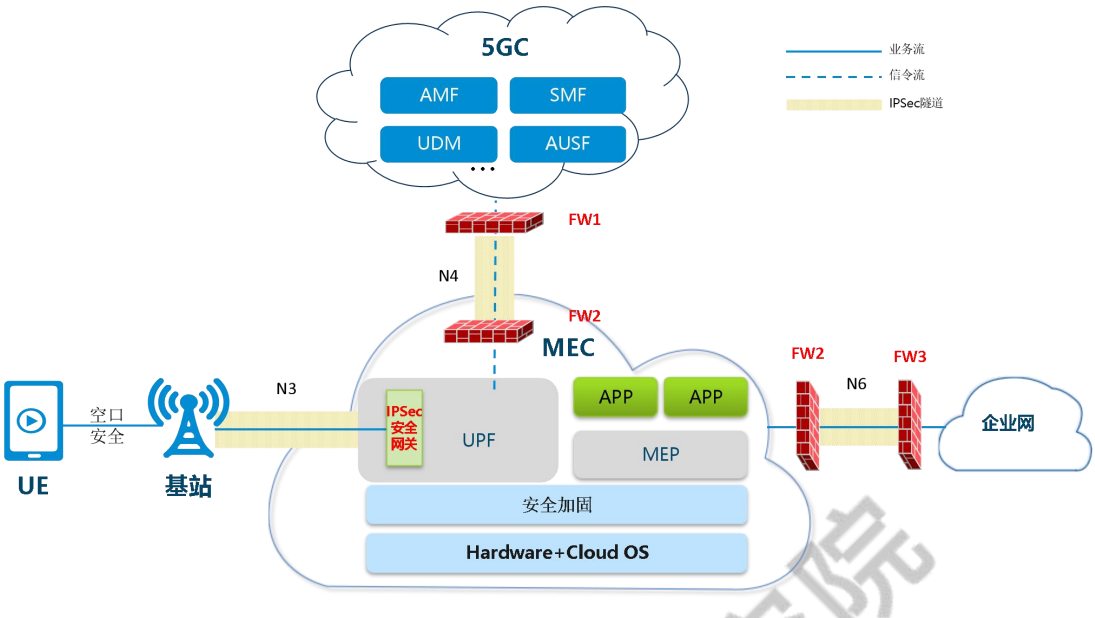

图 8 用户面分段安全传输

2.4.3 基于商用密码的控制面传输安全

5G 控制面接口主要有两类：

一类是 SBI 接口，基于 HTTP2.0，主要用于 5GC 控制面网络功能网元之间，《RFC 8998 ShangMi (SM) Cipher Suites for TLS 1.3》定义了商用密码密码算法在 TLS 中的应用。具体实施时，可以使网元自身支持商用密码 TLS，也可以部署专用商用密码代理网关。

一类是 Diameter 接口，用于基站/UPF 与 5GC 控制面之间，与用户面安全传输类似，根据安全需求可以部署独立或内置 IPSec 安全网关，实现不同网元或不同区域之间的数据安全传输。

2.5 管理面安全和设备数据安全

对于管理面，采用合规的密码产品和系统，通过数字证书、UKEY、商用密码浏览器、SSL VPN、签名验签服务器等实现对网络层及应

用层身份认证，以及对管理服务器的安全访问。通过 SSL VPN 安全网关实现 HTTPS 的安全访问，可卸载 HTTPS 对网元设备资源的占用，提升网元的业务处理性能。

对于重要数据，可以引入服务器密码机等实现重要数据存储机密性及完整性，并满足合规要求。

2.6 商用密码安全服务

为了更好的支持 5G 行业专网国产密码和应用，可借鉴 IT 领域和云计算领域成熟的密码服务体系，建立 5G 行业专网国产密码服务体系，满足密码测评的技术要求。逐步建立支持国产密码的密钥管理系统、密码机、CA 中心，以及支持商用密码的云或边缘云基础设施。

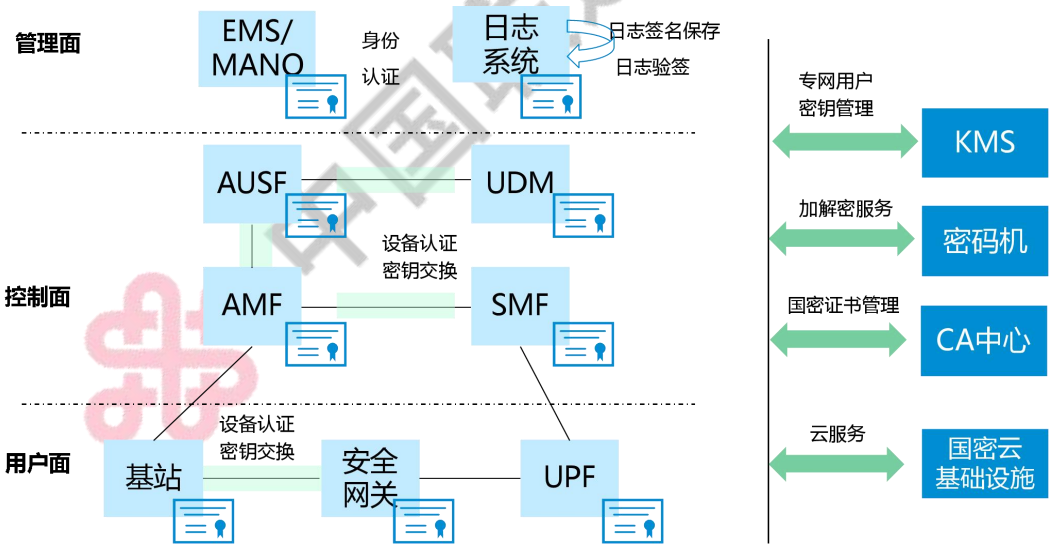

图 9 5G 网络商用密码安全服务

目前这方面缺少体系性设计指引，需要协同产业界各方共同努力，开展标准规划研究，指导相关体系的建立和技术实践，逐步建立和完善 5G 商用密码行业专网技术体系。

2.7 商用密码 5G 专网建设模式

根据网络建设模式，5G 行业专网可分为虚拟专网模式、混合专网模式和独立专网模式三类，覆盖行业用户的局域和广域业务需求。5G 网络国产密码方案支持不同的建设模式，适应不同场景的安全需求。

（1）独立专网模式

独立专网模式全部为企业独占网络设备，为行业建立与公网完全隔离的行业专网，适用于高精制造、电力等专属需求大、安全要求高、业务连续性要求高等场景。在这种场景下，可以在用户可信接入、控制面、用户面、管理面全部采用商用密码算法，建立一套独立的端到端 5G 商用密码专网，独立建设，独立演进。

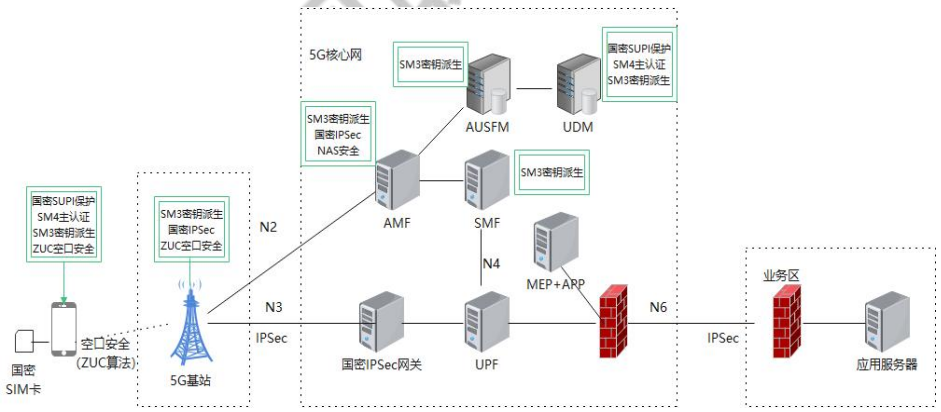

图 10 5G 基于商用密码的独立专网

（2）混合专网模式

混合共用专网模式是指复用部分公网资源，并根据行业用户需求将部分网络资源由行业客户独享的 5G 专用网络，适用于政务、工业

园区、工厂等有时延要求和数据安全隔离要求的垂直行业领域。在这种场景下，在用户认证、空口安全、下沉网元用户面安全采用商用密码算法，实现用户的可信接入、从 UE 到 DN 用户面的商用密码安全传输通道。

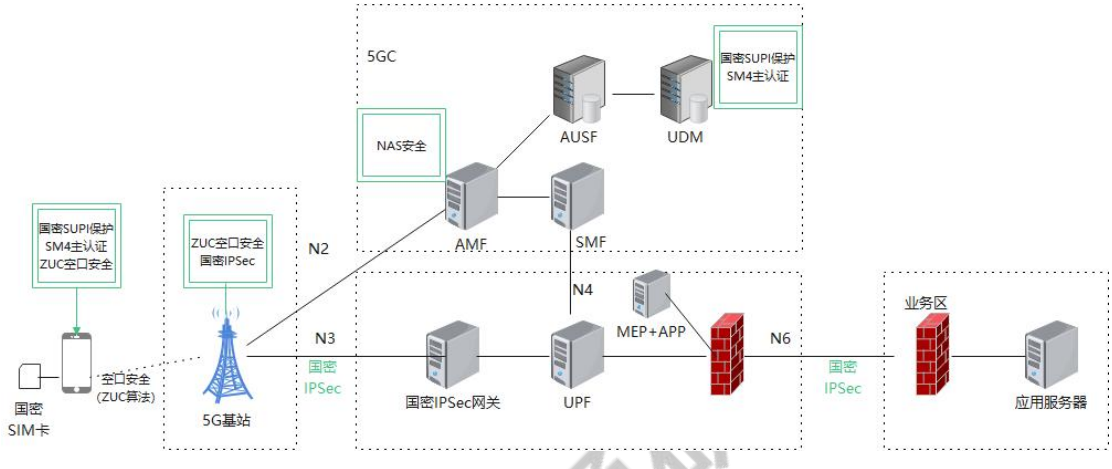

图 11 5G 基于商用密码的混合专网

（3）虚拟专网模式

虚拟专网模式利用 5G 公共网络资源，通过网络切片、边缘计算等技术，向行业用户提供的能满足其业务及安全需求的高质量专用虚拟网络，智慧城市、新媒体、智能交通等场景。在这种场景下，在用户认证、空口安全、UPF-DN 用户面安全采用商用密码算法，实现用户的可信接入、5G 网络到企业网络之间用户面的商用密码安全传输通道。

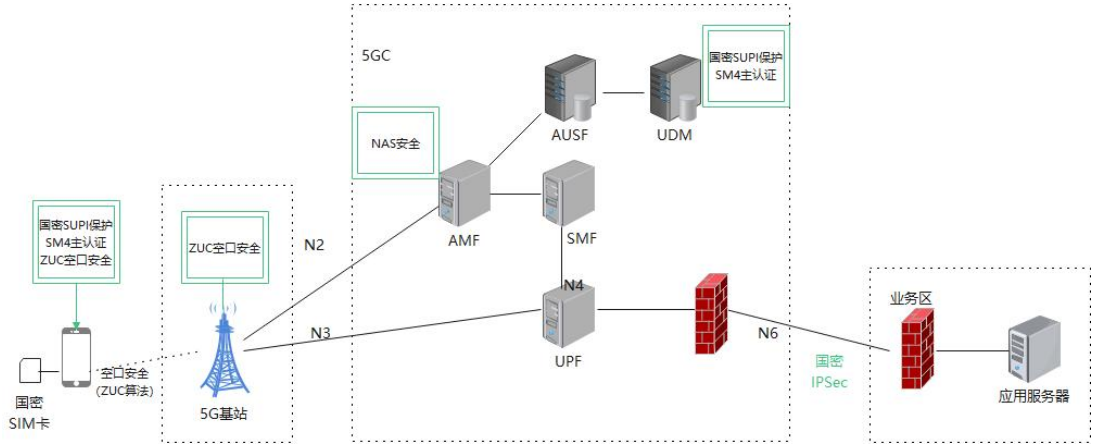

图 12 5G 基于商用密码的虚拟专网

依托不同的专网模式，为不同的行业用户按需提供自主可控、安全合规的 5G 商用密码应用服务，打造基于商用密码的 5G 网络安全创新能力和模式，赋能行业高质量发展。

三、商用密码在 5G 网络中的应用实践

3.1 5G 网络商用密码服务基础设施

5G 网络在面向垂直行业时，呈现出业务系统云化、用户接入多样化、场景移动化、管理复杂化的特征，使得密码应用体系极其繁杂，密码产品数量、种类繁多，容易产生网络安全漏洞和隐患。此外，随着《密码法》等相关法律法规的颁布和实施，对信息系统密码应用提出了规范化要求和密评的规定，针对运营商行业，关基和等保三级以上系统需满足密评有关要求，然而，目前自身难以对密码应用体系的合规性和安全性进行评估。为了满足 5G 网络和行业用户在新时代、新场景下的安全需求，建立面向 5G 网络的商用密码服务基础设施，可以为系统和业务应用提供统一、集约的密码服务，同时满足 5G 面

向行业用户在安全能力建设过程中的自主可控和安全合规需求。

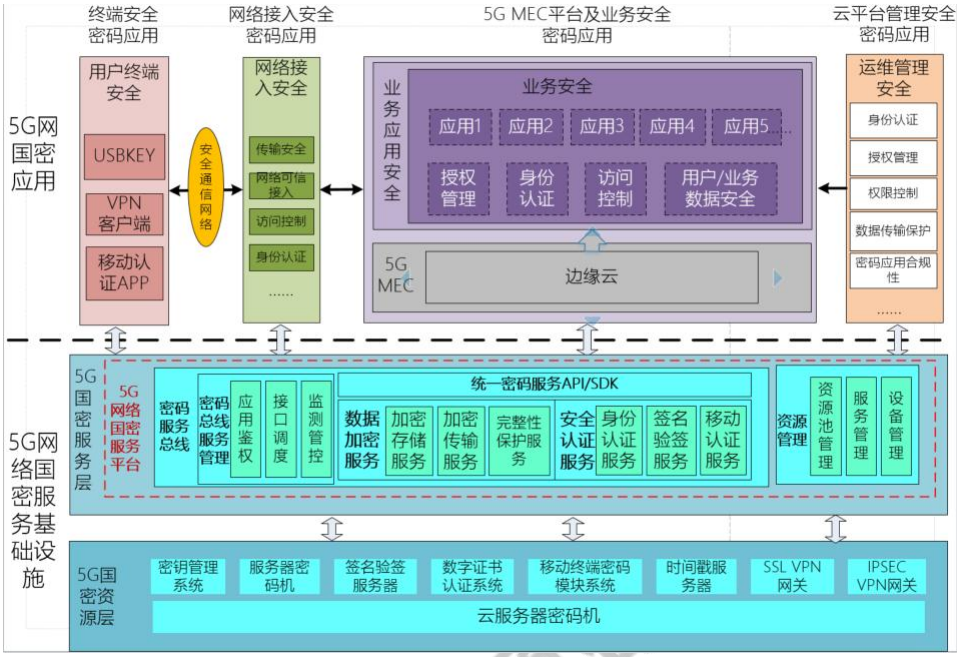

图 13 5G 网络商用密码服务基础设施

5G 网络商用密码服务基础设施由 5G 商用密码资源池和 5G 网络商用密码服务平台两部分组成。5G 商用密码资源池提供统一的商用密码基础能力，由基础密码服务单元组成，包含云服务器密码机、签名验签服务器、时间戳服务器、SSL VPN 网关、IPSEC VPN 网关、数字证书认证系统等；5G 网络商用密码服务平台基于 5G 商用密码资源池通过统一的密码服务总线，对 5G MEC 平台及平台上的业务应用提供统一的商用密码服务，能够面向 5G 网络数据加解密、安全接入、身份认证等场景提供商用密码服务能力。

5G MEC 与 5G 网络在结构深度绑定，5G 网络密码应用包括 5G 终端安全、网络接入安全、5G MEC 平台及业务安全、平台管理

四部分。依托于 5G 网络商用密码服务基础设施，提供身份认证、数字签名、签名验证、数据加密、完整性保护等商用密码服务能力，从而实现身份认证、传输加密、存储加密等国产商用密码应用。

（1）密码服务总线

把密码调用接口进行业务级封装形成统一密码服务 API 和 SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。支持业务应用的鉴别和密码服务权限控制；支持密码服务接口调度，匹配到对应的密码服务资源；支持日志采集，记录调用密码服务的详细日志。

1)身份认证服务

提供基于数字证书和密码技术的身份认证接口类服务，支持手机扫码认证、USBKey 证书认证等。

2)数据加密服务

对存储到数据库中的个人敏感数据、隐私数据、重要数据进行加密、解密。

3)签名验签服务

提供数字签名、签名验证、证书验证等密码服务。支持数据签名与验证、支持文件签名与验证；支持证书有效期验证、CA 根验证、CRL 验证等服务，支持证书/证书链的导入，支持多 CA 验证，为业务应用提供专用接口；支持 SM2/SM3/SM4 等商用密码算法。实现基于 SM2 算法的数字签名和验证功能，支持对数据、文件制作数字签名，签名结构符合 PKCS#1/PKCS#7 标准；支持验证符合

PKCS#1/PKCS#7 标准的签名结果，包括 RAW 签名/验签，Attached 签名/验签，Detached 签名/验签等多种签名验签方式。

4)完整性保护服务

面向重要数据在传输以及存储的完整性保护需求，结合数字证书、签名验签、云密码机提供完整性保护服务。提供基于消息鉴别码的完整性保护（HMAC-SM3）算法和基于数字签名的完整性保护（SM2-SM3）算法，支持数据完整性保护、文件完整性保护服务等。对外提供数据完整性保护接口协议，业务系统可以通过 Restful 接口方式或 SDK 方式调用数据完整性保护服务。

5)数字信封及密码运算服务

基于商用密码算法提供制作与解析数字信封、数据加密解密、数据摘要运算、数据签名、公钥加密、私钥解密等相关密码运算服务，为应用提供统一的密码调用方式，支持为云平台和云上业务系统提供基于数字信封的应用数据加密传输及基础密码运算服务。

（2）密码平台管理服务

实现对各类密码服务接口、服务订购、应用调用、应用认证、平台运行等的管理。支持租户信息管理及服务订购；支持租户密码资源配置与信息管理；支持系统管理员、安全管理员、安全审计员等的系统管理；支持密码资源状态监控、统计展示和告警管理。

（3）租户密码管理服务

为租户提供密码资源与应用管理服务门户。支持租户密码资源查看与管理；支持租户应用配置管理与权限控制；支持密码服务配置管

理与监测管控。

（4）密码资源管理服务

负责接入和管理密码资源池的所有硬件密码设备和软件密码产品。支持密码资源池和密码产品配置管理；支持密码镜像管理，实现密码产品虚拟镜像的制作和管理；支持与云平台对接，实现密码镜像启停；支持云服务器密码机资源管理，实现对多台云服务器密码机的配置管理和密码资源编排。

3.2 5G+车联网商用密码应用实践

5G 网络安全是车联网系统中至关重要的部分，随着车联网的业务场景的不断丰富，信息篡改、隐私泄漏等问题层出不穷，给汽车的安全性带来极大的挑战。在车联网中，车辆与平台之间的认证、车与车之间的认证，车辆涉及数据交换问题，各智能设备实时进行的数据传输问题，都需要密码技术提供安全保障。密码算法作为安全领域的底层技术，在车联网安全防护技术架构中起着决定性作用。

立足于此，基于 5G 网络“云网边端业”融合特点，以车联网基础设施车路+MEC+中心云为基础，构建车联网“云网边端业”一体化商用密码保障体系，提供身份鉴别、安全通道加密、数据加密等商用密码服务以及跨域互认，实现全方位的商用密码安全防护。在车辆网的场景中存在两类密码应用场景。

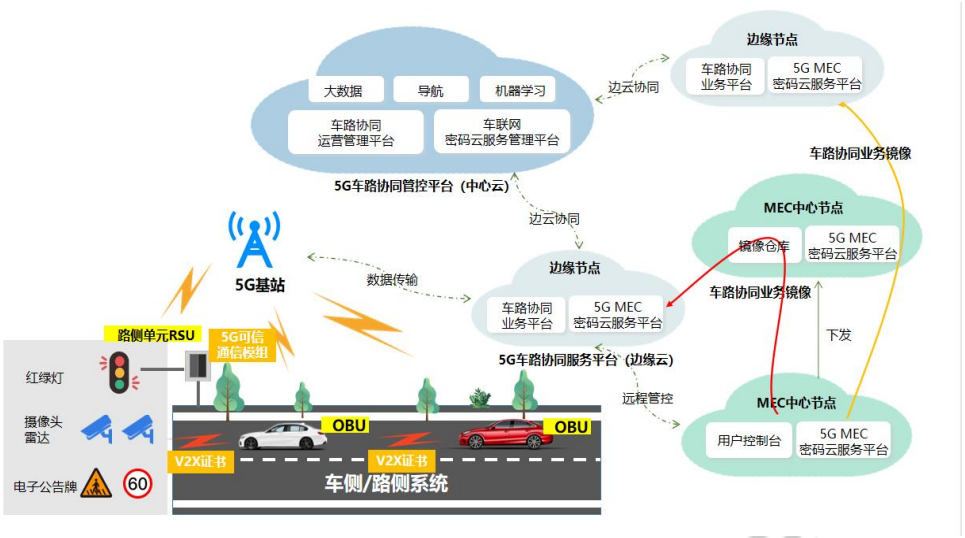

图 14 5G+车联网商用密码应用

（1）云平台侧和端侧互联

在云平台侧和端侧互联场景中，存在中心云节点、边缘云节点、车侧系统、路侧系统等应用主体。通过构建密码云服务平台，实现云平台和云平台上业务系统对不同关键的重要数据、敏感信息、审计日志等重要的数据信息安全的机密性和完整性保护。端侧和云平台侧之间的通信过程采用基于数字证书的方式，通过构建端侧和云平台侧之间通信数据的机密性和完整性保护，建立基于商用密码技术的安全通道，解决端侧和云平台侧数据传输过程中安全不足等问题。中心云平台和边缘云平台之间通信过程，基于 GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》的 IPSec VPN，对进行数据备份的设备在通信前进行身份鉴别，并建立安全的数据备份传输通道，保障数据传输的机密性和完整性保护。

（2）端侧与端侧互联

车联网场景中最核心的是保护车侧系统和路侧系统在网络通信

过程中的数据安全。在车侧系统与路侧系统间采用 V2X 证书为车侧系统和路侧系统签发所需的注册证书、假名证书和应用证书，实现基于商用密码技术的身份认证，建立安全通道链路，保障身份的真实性和数据传输过程中的机密性和完整性。基于工信部可信根证书列表和可信域证书列表验证响应通信双方的证书，实现跨信任域的身份认证。

3.3 5G 专网 MANO 商用密码应用实践

面向管理面，5G 专网 MANO 实现了 5G 专网的管理和编排，独立实现网络部署、更新和扩容等网络编排能力，在 5G 专网 MANO 管理中使用到密码的需求包括：

（1）身份认证

对 MANO 应用人员和用户进行基于密码技术的身份鉴别，防止身份被假冒，保证 MANO 应用人员和用户身份真实性。

（2）数据传输安全

基于密码技术建立安全的 MANO 管理数据安全传输通道，实现 MANO 管理数据和指令的安全传输，防止被窃取和篡改。

（3）日志安全存储

采用密码技术实现 MANO 管理日志完整性保护，防止被篡改。

（4）重要数据存储安全

NFVO、VNFM、VIM 等各管理单元存储的管理数据、配置数据、工参数据采用明文存储，存在被窃取和篡改的风险，采用密码技术对存储的数据进行加密，防止被窃取和篡改。

（1）总体应用框架

针对 5G 专网 MANO 密码技术应用需求，提出的总体架构部署图如图 15 所示：

图 15 5G 专网 MANO 密码应用总体架构图

（2）身份认证

在 MANO 应用客户端侧安装商用密码浏览器，为 MANO 用户分配智能密码钥匙（内置数字证书），基于数字证书技术实现 MANO 用户的身份识别。

MANO 各用户通过智能密码钥匙进行身份鉴别，智能密码钥匙内存放第三方 CA 颁发的个人数字证书。MANO 各管理网元对接签名验签服务器实现 MANO 用户人员身份的真实性进行鉴别。

用户登录身份鉴别实现密码应用中，涉及的密钥为 SM2 签名算法公私钥，涉及的设备为智能密码钥匙和签名验签服务器，不存在私钥明文出现的情况。

（3）数据安全传输

5G 专网 MANO 服务端部署 SSL VPN 安全网关，和商用密码浏览器配合完成商用密码 SSL 安全通道的建立，所有的数据均在此通

道内传输，实现 MANO 配置和管理数据传输的机密性和完整性保护，防止被窃取和篡改。

对从 PC 端传输到 MANO 应用系统的重要数据如管理数据、配置数据、工参数据等在安全浏览器、USB Key 和 SSL VPN 安全网关之间建立的安全传输通道中传输，通过符合要求的密码技术保障数据传输的机密性、完整性。

（4）日志完整性保护

在 MANO 各网元所在网络内部署服务器密码机、签名验签服务器等密码计算资源池，对 MANO 所产生的系统日志、管理日志、操作日志、业务日志等进行完整性保护。

在 MANO 各管理单元部署国家密码管理部门认可的服务器密码机、签名验签服务器，使用 HMAC-SM3 在日志记录写入时进行完整性保护，并在读取和使用时进行验证其完整性。

（5）数据存储安全

对 5G 专网 MANO 各管理单元（NFVO、VNFM、VIM 等）所存储的管理数据、配置数据、工参数据等进行加密和完整性保护。对 MANO 各管理单元存储在数据库中的敏感数据、业务数据等都可通过服务器密码机实现存储的机密性和完整性，防止恶意拖库、被篡改等风险事件发生。

四、展望

密码技术正在以前所未有的广度和深度与信息技术相互促进、融合发展,为网络空间的云计算、大数据、物联网等应用保驾护航。密码技术的发展已经不再是单一的领域需求，而是国家、行业、市场及自身发展的切实之需。此外，“放管服”改革将极大拓宽商用密码市场规模，整个密码产业面临一个大发展的机遇，面临一个蓝海空间。5G 作为推动数字经济高质量发展的重要引擎，安全作为数字经济健康发展的重要保障，统筹推进 5G+商用密码应用，协同创新，强化商用密码需求侧与供给侧互动对接，推出一批具有基础性、引领性、创新性、示范性、特色鲜明的优秀 5G 商用密码应用方案，逐步扩大 5G 网络赋能行业的蓝海市场是当下 5G 与商用密码应用的必然发展。坚持 5G+商用密码应用助力行业用户高质量数字经济发展换挡提速是整个产业链共同追求的目标，也是壮大生态链、提升价值链、增强产业链的必由之路。

目前面向基础电信企业网络的商用密码应用需求日趋细化，联通将充分发挥网络安全现代产业链链长的融通带动作用，携手业界各方，共同推动商用密码在基础电信网络中的应用，坚持政府主导、产业联动，共同打通商用密码应用产业链，畅通商密应用交流渠道，拓宽商密应用范围，壮大商密应用全景图，做强做优商密应用能力。

面向新征程，未来基于 5G 网络商用密码应用发展需要行业产学研用各方力量凝心聚力，通力协作。联通愿与行业伙伴一起携手并进，共创未来。

附录 A：缩略语

缩略语	全称	释义
5G	5th Generation	第五代移动通信
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5GC	5th Generation Core Network	5G 核心网
AAA	Authentication Authorization Accounting	认证授权计费
AKMA	Authentication and Key Management for Applications	应用层认证和密钥管理
AMF	Access and Mobility Management Function	接入与移动性管理功能
ARPF	Authentication Credential Repository and Processing Function	认证凭据存储和处理功能
AS	Access Stratum	接入层
AUSF	Authentication Server Function	鉴权服务器功能
CA	Certificate Authority	证书机构
CCSA	China Communications	中国通信标准化协会

	Standards Association	
CRL	Certificate Revocation List	证书吊销列表
DN	Data Network	数据网络
EAP	Extensible Authentication Protocol	可扩展认证协议
EMS	Element Management System	网元管理系统
gNB	next Generation Node B	下一代 B 节点
ICT	Information Communication Technology	信息通信技术
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission	国际标准化组织/国际电工委员会
KMS	Key Management System	密钥管理系统
MANO	Management and Orchestration	管理和编排
MEC	Multi-Access Edge Computing	多接入边缘计算
NAS	Non Access Stratum	非接入控制

NEF	Network Exposure Function	网络开放功能
NFVO	Network Function Virtualisation Orchestration	网络功能虚拟化编排
NRF	Network Repository Function	网络存储功能
OMC	Operations&Maintenance Center	操作和运维中心
PKCS	Public-Key Cryptography Standards	公钥密码学标准
RAN	Radio Access Network	无线接入网
RRC	Radios Resource Control	无线资源控制
SBI	Service Based Interface	服务化接口
SEAF	Security Anchor Function	安全锚功能
SMF	Session Management Function	会话管理功能
SUCI	Subscription Concealed Identifier	签约用户隐式标识
SUPI	Subscriber Permanent Identifier	签约用户永久标识
TLS	Transport Layer Security	传输层安全
UDM	Unified Data Management	统一数据管理

UE	User Equipment	用户设备
UPF	User Plane Function	用户面功能
USIM	Universal Subscriber Identity Module	通用用户身份识别模块
VIM	Virtualised Infrastructure Manager	虚拟基础设施管理
VNFM	Virtualised Network Function Manager	虚拟化网络功能管理

参考文献

[1] 3GPP TS 23.501:System Architecture for the 5G System.

[2] 3GPP TS 33.501: Security architecture and procedures for the 5G system.

[3] YD/T 3628-2019，5G 移动通信网安全技术要求.

[4] 赛迪研究院.2021-2022 年中国商用密码行业发展白皮书[R]北京：中国赛迪研究院, 2022.

[5] 数观天下. 2021-2022 商用密码行业分析报告[R].北京：数观天下, 2022.

[6] 北京商用密码行业协会 .云密码服务技术白皮书[R]北京：北京商用密码行业协会, 2019.

中国联通研究院是根植于联通集团（中国联通直属二级机构），服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展引领者、产业发展助推者，是原创技术策源地主力军和数字技术融合创新排头兵。联通研究院致力于提高核心竞争力和增强核心功能，紧密围绕联网通信、算网数智两大类主业，按照 4+2+X 研发布局，开展面向 C3 网络、大数据赋能运营、端网边业协同创新、网络与信息安全等方向的前沿技术研发，承担高质量决策报告研究和专精特新核心技术攻关，致力于成为服务国家发展的高端智库、代表行业产业的发言人、助推数字化转型的参谋部，多方位参与网络强国、数字中国建设，大力发展战略性新兴产业，加快形成新质生产力。联通研究院现有员工 700 余人，85%以上为硕士、博士研究生，以“三度三有”企业文化为根基，发展成为一支高素质、高活力、专业化、具有行业影响力的人才队伍。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路 1 号
电话：010-87926100
邮编：100176

中国联通研究院

中国联通泛终端技术