辽宁省商用密码
产业发展报告

（2026年）

辽宁省工业和信息化厅
辽宁省国家密码管理局
辽宁省商用密码协会

版权申明

辽宁省商用密码产业发展报告（以下简称本报告）著作权归辽宁省工业和信息化厅、辽宁省国家密码管理局、辽宁省商用密码协会共同所有，并受《中华人民共和国著作权法》及相关法律法规保护。

凡转载、摘编或以其他方式使用本报告文字内容、观点及相关数据的，均须注明来源。

违反上述申明，擅自使用本报告内容且未履行标注义务的，将依法追究其相应法律责任。

编写组名单

（排名不分先后）

主编单位：

辽宁省工业和信息化厅

辽宁省国家密码管理局

辽宁省商用密码协会

参编单位：

中国科学院沈阳计算技术研究所有限公司

中国科学院沈阳自动化研究所

华为技术有限公司

龙芯中科技术股份有限公司

曙光信息产业股份有限公司

联通（辽宁）产业互联网有限公司

中国移动通信集团辽宁有限公司

北方实验室（沈阳）股份有限公司

北京数字认证股份有限公司

北京信安世纪科技股份有限公司

长春吉大正元股份有限公司

辽宁数字证书认证管理有限公司

大连秘阵科技有限公司

辽宁航天信息有限公司

沈阳问天量子科技有限公司

沈阳赛宝科技服务有限公司

辽宁广烁科技有限公司

沈阳安创信息科技有限公司

辽宁公信安全信息科技有限公司

目 录

前　言

百年变局与数字浪潮交织，网络空间作为国家主权的组成部分，已经成为冲突与博弈的重要战场。作为网络安全的“基因密码”，在捍卫网络空间国家主权的斗争中，密码技术的战略价值愈发凸显，它既承载保障国家网络主权、经济安全与社会稳定的使命，也担负守护社会组织与公民权益的责任。

2019 年《中华人民共和国密码法》（以下简称《密码法》）颁布实施后，《商用密码管理条例》等法规相继出台，相关的法规与制度框架不断完善，为商用密码产业的发展奠定了良好的基础。近五年来，商用密码产业驶入快车道，市场规模趋近千亿元。然而，迄今为止，商用密码技术对多数行业仍是“熟悉的陌生人”，场景落地不足、技术适配欠缺等问题仍然客观存在。这些问题既是挑战，更蕴含广阔的产业发展空间。

作为东北振兴的战略支点，我省以“数字辽宁、智造强省”为契机，将商用密码融入振兴发展大局，依托深厚工业底蕴，推动密码技术与高端装备制造、石油化工等传统产业及工业互联网等新兴产业深度融合，为将工业优势转化为数字产业竞争力保驾护航。同时通过强化司法保护、完善相关政策、营造法治环境等，促进商用密码技术成为关键信息基础设施安全与产业转型的核心支撑。

本报告立足辽宁实践，全景呈现区域产业发展；梳理技术创新、产业生态等基础成果，剖析新形势下的机遇挑战；展示密码在工业互联网、智慧能源等特色场景的应用案例；解读“政产学研用”协同路径，并提出密码技术与地方经济协同发展的策略。

未来已来，商密先行。我们期待本产业发展报告成为凝聚共识的宣言、普及知识的媒介、构筑安全屏障的载体，让密码基因深植辽宁沃土，为习近平新时代中国特色社会主义思想的辽宁实践贡献“密码力量”。辽宁商密人必将在这场数字化征程中，书写“无负时代、无负历史、无负人民”的答卷。

编写组

2026 年 3 月

第一章 政策法规

数字时代下，商用密码已成为守护国家安全、社会公共利益与公民信息安全的核心技术支撑，更是辽宁省数字经济高质量发展的重要安全基石。政策法规作为商用密码产业规范有序发展的根本保障，构建起多层次、全方位的制度体系。

本章聚焦商用密码领域核心制度框架，系统梳理整合商用密码国家法律法规、政策文件、国家标准、行业标准与指导文件，全面呈现政策法规的演进脉络与实践要求，为全省商用密码应用推广、产业发展与安全监管提供坚实法治遵循。

（一）商用密码概览

1. 商用密码的核心概念与范畴

商用密码是指用于保护不属于国家秘密的信息，由国家密码管理部门批准使用的密码技术、密码产品和密码服务的统称，是保障数字经济安全、社会公共利益、公民个人信息安全的关键技术支撑，与国家秘密密码共同构成我国密码保障体系的两大支柱。

从技术范畴来看，商用密码涵盖对称密码、非对称密码、哈希函数等核心技术类型：对称密码以“加密密钥与解密密钥相同”为特征，具有加密速度快、运算效率高的优势，广泛应用于金融交易、数据存储等场景；非对称密码采用“公钥加密、私钥解密”的模式，解决了对称密码中密钥传递的安全问题，主要用于数字签名、身份认证等领域；哈希函数则能将任意长度的输入数据转换为固定长度的哈希值，可快速验证数据的完整性，常用于电子文档防伪、数据篡改检测。从产品与服务范畴来看，商用密码产品包括密码芯片、密码模块、密码机等硬件产品，以及密码软件、密码系统等软件产品；商用密码服务则涵盖密码评估、密码咨询、密码运维等，形成“技术－产品－服务”一体化的产业生态。

2. 商用密码的多元应用场景

在数字经济深度发展的背景下，商用密码已渗透到商业、政务、民生等多个领域，成为保障信息安全、维护市场秩序、提升服务效率的基础设施，是平衡安全与发展的关键。

商用密码是金融交易、电子商务、企业数据保护的安全基石、是推动数字政府建设、保障政务信息安全的关键支撑、为人民提供安全服务、保障个人信息安全的核心手段。

商用密码既是信息安全的守护者，更是数字经济高质量发展的赋能者，为我国商业模式创新、政务升级、民生优化提供坚实保障。

3. 密码的重要性

密码是保障网络安全和数据安全的基因技术，其重要性随着时代变迁不断升级，从革命时期的“生存保障”，逐步演进为和平建设时期的“安全基石”，再到数字时代的“发展支撑”，始终与国家战略、社会需求同频共振。

随着信息技术的飞速发展，数据成为核心生产要素，密码的重要性实现“质的飞跃”，从“安全保障工具”升级为“数字经济发展的核心基础设施”。无论是数字金融、电子商务等新业态的发展，还是工业互联网、人工智能等新技术的应用，都离不开密码的安全支撑，密码工作不仅关乎安全，更关乎发展，是推动信息化高质量发展、建设网络强国的战略支撑。

密码的重要性不仅体现在技术支撑与发展赋能上，更通过法律法规的刚性约束形成制度保障，让密码应用从“自愿选择”走向“法定责任”，为数字时代的安全与发展筑牢法治根基。

（二）法律法规

《中华人民共和国密码法》2019 年 10 月 26 日，正式颁布，自 2020 年 1 月 1 日起实施。第二十七条（节选）法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

《中华人民共和国网络安全法》2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行。第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。

《中华人民共和国电子签名法》2004 年 8 月 28 日通过，2015 年 4 月 24 日第一次修正，2019 年 4 月 23 日第二次修正，自 2005 年 4 月 1 日起施行。第二

十二条 电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。

《中华人民共和国数据安全法》2021 年 6 月 10 日通过，自 2021 年 9 月 1 日起施行。第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、法人和其他组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

《中华人民共和国个人信息保护法》2021 年 8 月 20 日通过，自 2021 年 11 月 1 日起施行。第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。

《商用密码管理条例》2023 年 4 月 27 日修订通过，自 2023 年 7 月 1 日起施行。第三十八条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。

《关键信息基础设施安全保护条例》2021 年 7 月 30 日公布，自 2021 年 9 月 1 日起施行。第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

（三）政策文件

近年来，国家层面与地方政府相继出台一系列政策文件，从重点领域管理到区域落地实施等多个维度，构建起全方位、多层次的密码应用促进体系，为密码技术落地、合规使用提供了明确指引与坚实保障。

《电子印章管理办法》（国办发〔2025〕33 号）于 2025 年 9 月 27 日由国务院办公厅印发，自发布之日起施行。办法共五章二十六条，以密码技术为核心

支撑，明确了电子印章管理的总体框架、职责分工、全流程规范及互信互认要求。核心内容包括界定电子印章的法律属性（与实物印章具有同等法律效力），明确国家密码管理局等部门的监管职责，规范电子印章制作、备案、注销的全流程管理，要求电子印章制作符合国家密码标准和数据格式规范。同时，强调电子印章使用遵循“谁所有、谁控制，谁签章、谁负责”原则，明确电子签章数据需保证真实完整可追溯，并推动跨地区跨部门电子印章互信互认。

《关键信息基础设施商用密码使用管理规定》（国家密码管理局、国家网信办、公安部令第5号）2025年6月11日发布，2025年8月1日起施行。规定共25条，明确了关键信息基础设施商用密码使用的总体要求，包括适用范围、管理部门职责和保护工作部门职责等。规定要求运营者落实关键信息基础设施商用密码使用“三同步一评估”原则，即同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。同时，对商用密码技术、产品、服务使用要求，数据安全保护、个人信息保护要求等方面做出了具体规定，还明确了监督检查及法律责任等内容。

《辽宁省数字政府建设实施方案（2025—2027年）》2025年7月11日发布。商用密码相关要求：在“完善网络安全保障体系”部分明确提出，需“落实关键信息基础设施保护、网络安全等级保护等制度，推进政务系统商用密码应用改造和密码应用评估工作”。

实施方向：辽宁省将推动省级、市级政务信息系统（如政务服务平台、数据共享平台等）的商用密码应用改造，确保符合《信息安全技术 信息系统密码应用基本要求》（GB/T 39786—2021）等标准；同时，将密码应用评估纳入政务系统建设与运维的必要环节，未通过密评的政务系统将影响运行维护经费安排，与《国家政务信息化项目建设管理办法》《辽宁省省级政务信息化项目管理办法》等要求衔接。

《国家政务信息化项目建设管理办法》2020年8月28日印发，自2020年10月1日起施行。第二十八条 加强国家政务信息化项目建设投资和运行维护经费协同联动，坚持“联网通办是原则，孤网是例外”。部门已建的政务信息化项目需升级改造，或者拟新建政务信息化项目，能够按要求进行信息共享的，由国家发展改革委会同有关部门进行审核；如果部门认为根据有关法律法规和党中央、国务院要求不能进行信息共享，但确有必要建设或者保留的，由国家发展改革委报国务院，由国务院办公厅会同有关部门进行审核，经国务院批准后方可建设或者保留。

（一）对于未按要求共享数据资源或者重复采集数据的政务信息系统，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。

（二）对于未纳入国家政务信息系统总目录的系统，不安排运行维护经费。

（三）对于不符合密码应用和网络安全要求，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。

《商用密码应用安全性评估管理办法》2023 年 9 月 26 日公布，自 2023 年 11 月 1 日起施行。第六条 法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统（以下简称重要网络与信息系统），其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

第九条 重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。未通过商用密码应用安全性评估的，运营者应当进行改造，并在改造期间采取必要措施保证网络与信息系统运行安全。

《商用密码检测机构管理办法》2023 年 9 月 26 日公布，2023 年 11 月 1 日起施行。第三条 从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理局认定，依法取得商用密码检测机构资质。

第二十条 商用密码检测机构应当于每年 1 月 15 日前通过所在地省、自治区、直辖市密码管理部门向国家密码管理局报送上一年度工作报告以及相关统计数据，包括持续符合资质认定条件和要求、遵守从业规范、开展检测活动、实施标准等情况。

《电子政务电子认证服务管理办法》自 2024 年 11 月 1 日起施行 。第三条 本办法所称电子政务电子认证服务，是指采用商用密码技术为政务活动提供电子签名认证服务，保证电子签名的真实性和可靠性的活动。

第二十一条 电子政务电子认证服务机构应当遵守国家有关密码管理要求，保障电子政务电子认证服务使用密码安全。

《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》2020 年 7 月 22 日印发。二、深入贯彻实施国家网络安全等级保护制度

（四）落实密码安全防护要求。网络运营者应当贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

（四）国家标准

GB/T 15843.1—2017 《信息技术 安全技术 实体鉴别 第 1 部分：总则》

GB/T 15843.2—2017 《信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制》

GB/T 15843.3—2023 《信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制》

GB/T 15843.4—2024 《网络安全技术 实体鉴别 第4部分：采用密码校验函数的机制》

GB/T 15843.5—2005 《信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制》

GB/T 15843.6—2018 《信息技术 安全技术 实体鉴别 第6部分：采用人工数据传递的机制》

GB/T 15851.3—2018 《信息技术 安全技术 带消息恢复的数字签名方案 第3部分：基于离散对数的机制》

GB/T 15852.1—2020 《信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制》

GB/T 15852.2—2012 《信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制》

GB/T 15852.3—2019 《信息技术 安全技术 消息鉴别码 第3部分：采用泛杂凑函数的机制》

GB/T 16264.8—2005 《信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架》

GB/T 16649.15—2010 《识别卡 集成电路卡 第15部分：密码信息应用》

GB/T 17901.1—2020 《信息技术 安全技术 密钥管理 第1部分：框架》

GB/T 17901.3—2021 《信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制》

GB/T 17902.1—2023 《信息技术 安全技术 带附录的数字签名 第1部分：概述》

GB/T 17902.2—2005 《信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制》

GB/T 17902.3—2005 《信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制》

GB/T 17903.1—2008 《信息技术 安全技术 抗抵赖 第1部分：概述》

GB/T 17903.2—2021 《信息技术 安全技术 抗抵赖 第2部分：采用对称技术的机制》

GB/T 17903.3—2008 《信息技术 安全技术 抗抵赖 第3部分：采用非对称技术的机制》

GB/T 17964—2021 《信息安全技术 分组密码算法的工作模式》

GB/T 18238.1—2000 《信息技术 安全技术 散列函数 第1部分：概述》

GB/T 18238.2－2024 《网络安全技术 杂凑函数 第2部分：采用分组密码的杂凑函数》

GB/T 18238.3—2002 《信息技术 安全技术 散列函数 第3部分：专用散列函数》

GB/T 19713—2005 《信息技术 安全技术 公钥基础设施 在线证书状态协议》

GB/T 19714—2005 《信息技术 安全技术 公钥基础设施 证书管理协议》

GB/T 19771—2005 《信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范》

GB/T 20518—2018 《信息安全技术 公钥基础设施 数字证书格式》

GB/T 20520—2006 《信息安全技术 公钥基础设施 时间戳规范》

GB/T 21053—2023 《信息安全技术 公钥基础设施 PKI 系统安全技术要求》

GB/T 21054—2023 《信息安全技术 公钥基础设施 PKI 系统安全测评方法》

GB/T 21082.4—2007 《银行业务 密钥管理（零售） 第4部分：使用公开密钥密码的密钥管理技术》

GB/T 25056—2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》

GB/T 25061—2020 《信息安全技术 XML 数字签名语法与处理规范》

GB/T 25064—2010 《信息安全技术 公钥基础设施 电子签名格式规范》

GB/T 25065—2010 《信息安全技术 公钥基础设施 签名生成应用程序的安全要求》

GB/T 26855—2011 《信息安全技术 公钥基础设施 证书策略与认证业务声明框架》

GB/T 27909.2—2011 《银行业务 密钥管理（零售） 第2部分：对称密码及其密钥管理和生命周期》

GB/T 27909.3—2011 《银行业务 密钥管理（零售） 第3部分：非对称密码系统及其密钥管理和生命周期》

GB/T 28456—2012 《IPsec 协议应用测试规范》

GB/T 28457—2012 《SSL 协议应用测试规范》

GB/T 29241—2012 《信息安全技术 公钥基础设施 PKI 互操作性评估准则》

GB/T 29243—2012 《信息安全技术 数字证书代理认证路径构造和代理验证规范》

GB/T 29767—2013《信息安全技术 公钥基础设施 桥CA体系证书分级规范》

GB/T 29829—2022 《信息安全技术 可信计算密码支撑平台功能与接口规范》

GB/T 30272—2021 《信息安全技术 公钥基础设施 标准符合性测评》

GB/T 30275—2013 《信息安全技术 鉴别与授权认证中间件框架与接口规范》

GB/T 32905—2016 《信息安全技术 SM3 密码杂凑算法》

GB/T 32907—2016 《信息安全技术 SM4 分组密码算法》

GB/T 32915—2016 《信息安全技术 二元序列随机性检测方法》

GB/T 32918.1—2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则》

GB/T 32918.2—2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分：数字签名算法》

GB/T 32918.3—2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分：密钥交换协议》

GB/T 32918.4—2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法》

GB/T 32918.5—2017《信息安全技术 SM2 椭圆曲线公钥密码算法 第 5 部分：参数定义》

GB/T 32922—2023 《信息安全技术 IPSec VPN 安全接入基本要求与实施指南》

GB/T 33133.1—2016 《信息安全技术 祖冲之序列密码算法 第 1 部分：算法描述》

GB/T 33133.2—2021 《信息安全技术 祖冲之序列密码算法 第 2 部分：保密性算法》

GB/T 33133.3—2021 《信息安全技术 祖冲之序列密码算法 第 3 部分：完整性算法》

GB/T 33560—2017 《信息安全技术 密码应用标识规范》

GB/T 34953.1—2017《信息技术 安全技术 匿名实体鉴别 第 1 部分：总则》

GB/T 34953.2—2018 《信息技术 安全技术 匿名实体鉴别 第 2 部分：基于群组公钥签名的机制》

GB/T 34953.3 《信息技术 安全技术 匿名实体鉴别 第 3 部分：基于盲签名的机制》

GB/T 34953.4—2020 《信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制》

GB/T 35275—2017 《信息安全技术 SM2 密码算法加密签名消息语法规范》

GB/T 35276—2017 《信息安全技术 SM2 密码算法使用规范》

GB/T 35285—2017 《信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求》

GB/T 35291—2017 《信息安全技术 智能密码钥匙应用接口规范》

GB/T 36322—2018 《信息安全技术 密码设备应用接口规范》

GB/T 36624—2018 《信息技术 安全技术 可鉴别的加密机制》

GB/T 36631—2018 《信息安全技术 时间戳策略和时间戳业务操作规则》

GB/T 36644—2018 《信息安全技术 数字签名应用安全证明获取方法》

GB/T 36968—2018 《信息安全技术 IPSec VPN 技术规范》

GB/T 37033.1—2018 《信息安全技术 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别》

GB/T 37033.2—2018 《信息安全技术 射频识别系统密码应用技术要求 第2部分：电子标签与读写器及其通信密码应用技术要求》

GB/T 37033.3—2018 《信息安全技术 射频识别系统密码应用技术要求 第3部分：密钥管理技术要求》

GB/T 37092—2018 《信息安全技术 密码模块安全要求》

GB/T 38540—2020 《信息安全技术 安全电子签章密码技术规范》

GB/T 38541—2020 《信息安全技术 电子文件密码应用指南》

GB/T 38556—2020 《信息安全技术 动态口令密码应用技术规范》

GB/T 38625—2020 《信息安全技术 密码模块安全检测要求》

GB/T 38629—2020 《信息安全技术 签名验签服务器技术规范》

GB/T 38635.1—2020 《信息安全技术 SM9 标识密码算法 第1部分：总则》

GB/T 38635.2—2020 《信息安全技术 SM9 标识密码算法 第2部分：算法》

GB/T 38636—2020 《信息安全技术 传输层密码协议（TLCP）》

GB/T 38647.1—2020 《信息技术 安全技术 匿名数字签名 第1部分：总则》

GB/T 38647.2—2020 《信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制》

GB/T 39786—2021 《信息安全技术 信息系统密码应用基本要求》

GB/T 41389—2022 《信息安全技术 SM9 密码算法使用规范》

GB/T 42564—2023 《信息安全技术 边缘计算 安全技术要求》

GB/T 42570—2023 《信息安全技术 区块链技术安全框架》

GB/T 42571—2023 《信息安全技术 区块链信息服务安全规范》

GB/T 43206—2023 《信息安全技术 信息系统密码应用测评要求》

GB/T 43207—2023 《信息安全技术 信息系统密码应用设计指南》

GB/T 43578—2023 《信息安全技术 通用密码服务接口规范》

GB/T 43779—2024 《网络安全技术 基于密码令牌的主叫用户可信身份鉴别技术规范》

（五）行业标准

GM/T 0001.1—2012 《祖冲之序列密码算法 第1部分：算法描述》

GM/T 0001.2—2012 《祖冲之序列密码算法 第2部分：基于祖冲之算法的机密性算法》

GM/T 0001.3—2012 《祖冲之序列密码算法 第3部分：基于祖冲之算法的完整性算法》

GM/T 0001.4—2024 《祖冲之序列密码算法 第4部分：鉴别式加密机制》

GM/T 0002—2012 《SM4分组密码算法》

GM/T 0003.1—2012 《SM2椭圆曲线公钥密码算法 第1部分：总则》

GM/T 0003.2—2012 《SM2椭圆曲线公钥密码算法 第2部分：数字签名算法》

GM/T 0003.3—2012 《SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议》

GM/T 0003.4—2012 《SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法》

GM/T 0004—2012 《SM3密码杂凑算法》

GM/T 0005—2010 《随机性检测规范》

GM/T 0006—2023 《密码应用标识规范》

GM/T 0008—2012 《安全芯片密码检测准则》

GM/T 0009—2023 《SM2密码算法使用规范》

GM/T 0010—2023 《SM2密码算法加密签名消息语法规范》

GM/T 0011—2023 《可信计算 可信密码支撑平台功能与接口规范》

GM/T 0012—2012 《可信计算可信密码模块接口规范》

GM/T 0013—2012 《可信计算可信密码模块接口符合性测试规范》

GM/T 0014—2023 《数字证书认证系统密码协议规范》

GM/T 0015—2023 《数字证书格式》

GM/T 0016—2023 《智能密码钥匙密码应用接口规范》

GM/T 0017—2023 《智能密码钥匙密码应用接口数据格式规范》

GM/T 0018—2023 《密码设备应用接口规范》

GM/T 0019—2023 《通用密码服务接口规范》

GM/T 0020—2023 《证书应用综合服务接口规范》

GM/T 0021—2023 《动态口令密码应用技术规范》

GM/T 0022—2023 《IPSec VPN技术规范》

GM/T 0023—2023 《IPSec VPN网关产品规范》

GM/T 0024—2023 《SSL VPN技术规范》

GM/T 0025—2023 《SSL VPN 网关产品规范》

GM/T 0026—2023 《安全认证网关产品规范》

GM/T 0027—2014 《智能密码钥匙技术规范》

GM/T 0028—2024 《密码模块安全要求》

GM/T 0029—2014 《签名验签服务器技术规范》

GM/T 0030—2014 《服务器密码机技术规范》

GM/T 0031—2014 《安全电子签章密码技术规范》

GM/T 0032—2014 《基于角色的授权与访问控制技术规范》

GM/T 0033—2023 《时间戳接口规范》

GM/T 0034—2014 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》

GM/T 0035—2014 《射频识别系统密码应用技术要求》

GM/T 0036—2014 《采用非接触卡的门禁系统密码应用技术指南》

GM/T 0037—2014 《证书认证系统检测规范》

GM/T 0038—2014 《证书认证密钥管理系统检测规范》

GM/T 0039—2024 《密码模块安全检测要求》

GM/T 0040—2024 《射频识别标签模块密码检测规范》

GM/T 0041—2024 《智能 IC 卡密码检测规范》

GM/T 0042—2015 《三元对等密码安全协议测试规范》

GM/T 0043—2024 《数字证书互操作检测规范》

GM/T 0044—2016 《SM9 标识密码算法》

GM/T 0045—2016 《金融数据密码机技术规范》

GM/T 0046—2024 《金融数据密码机检测规范》

GM/T 0047—2024 《安全电子签章密码检测规范》

GM/T 0048—2016 《智能密码钥匙密码检测规范》

GM/T 0049—2016 《密码键盘密码检测规范》

GM/T 0050—2016 《密码设备管理设备管理技术规范》

GM/T 0051—2016 《密码设备管理对称密钥管理技术规范》

GM/T 0052—2016 《密码设备管理 VPN 设备监察管理规范》

GM/T 0053—2016 《密码设备管理远程监控与合规性检验接口数据规范》

GM/T 0054—2018 《信息系统密码应用基本要求》

GM/T 0055—2018 《电子文件密码应用技术规范》

GM/T 0056—2018 《多应用载体密码应用接口规范》

GM/T 0057—2018 《基于 IBC 技术的身份鉴别规范》

GM/T 0058—2018 《可信计算 TCM 服务模块接口规范》

GM/T 0059—2018 《服务器密码机检测规范》
GM/T 0060—2018 《签名验签服务器检测规范》
GM/T 0061—2018 《动态口令密码应用检测规范》
GM/T 0062—2018 《密码产品随机数检测要求》
GM/T 0063—2018 《智能密码钥匙密码应用接口检测规范》
GM/T 0064—2018 《限域通信（RCC）密码检测要求》
GM/T 0065—2019 《商用密码产品生产和保障能力建设规范》
GM/T 0066—2019 《商用密码产品生产和保障能力建设实施指南》
GM/T 0067—2019 《基于数字证书的身份鉴别接口规范》
GM/T 0068—2019 《开放的第三方资源授权协议框架》
GM/T 0069—2019 《开放的身份鉴别框架》
GM/T 0070—2019 《电子保单密码应用技术要求》
GM/T 0071—2019 《电子文件密码应用指南》
GM/T 0072—2019 《远程移动支付密码应用技术要求》
GM/T 0073—2019 《手机银行信息系统密码应用技术要求》
GM/T 0074—2019 《网上银行密码应用技术要求》
GM/T 0075—2019 《银行信贷信息系统密码应用技术要求》
GM/T 0076—2019 《银行卡信息系统密码应用技术要求》
GM/T 0077—2019 《银行核心信息系统密码应用技术要求》
GM/T 0078—2020 《密码随机数生成模块设计指南》
GM/T 0079—2020 《可信计算平台直接匿名证明规范》
GM/T 0080—2020 《SM9 密码算法使用规范》
GM/T 0081—2020 《SM9 密码算法加密签名消息语法规范》
GM/T 0082—2020 《可信密码模块保护轮廓》
GM/T 0083—2020 《密码模块非入侵式攻击缓解技术指南》
GM/T 0084—2020 《密码模块物理攻击缓解技术指南》
GM/T 0085—2020 《基于 SM9 标识密码算法的技术体系框架》
GM/T 0086—2020 《基于 SM9 标识密码算法的密钥管理系统技术规范》
GM/T 0087—2020 《浏览器密码应用接口规范》
GM/T 0088—2020 《云服务器密码机管理接口规范》
GM/T 0089—2020 《简单证书注册协议规范》
GM/T 0090—2020 《标识密码应用标识格式规范》
GM/T 0091—2020 《基于口令的密钥派生规范》
GM/T 0092—2020 《基于 SM2 算法的证书申请语法规范》
GM/T 0093—2020 《证书与密钥交换格式规范》

GM/T 0094—2020 《公钥密码应用技术体系框架规范》
GM/T 0095—2020 《电子招投标密码应用技术要求》
GM/T 0096—2020 《射频识别防伪系统密码应用指南》
GM/T 0097—2020 《射频识别电子标签统一名称解析服务安全技术规范》
GM/T 0098—2020 《基于 IP 网络的加密语音通信密码技术规范》
GM/T 0099—2020 《开放式版式文档密码应用技术规范》
GM/T 0100—2020 《人工确权型数字签名密码应用技术要求》
GM/T 0101—2020 《近场通信密码安全协议检测规范》
GM/T 0102—2020 《密码设备应用接口符合性检测规范》
GM/T 0103—2021 《随机数发生器总体框架》
GM/T 0104—2021 《云服务器密码机技术规范》
GM/T 0105—2021 《软件随机数发生器设计指南》
GM/T 0106—2021 《银行卡终端产品密码应用技术要求》
GM/T 0107—2021 《智能 IC 卡密钥管理系统基本技术要求》
GM/T 0108—2021 《诱骗态 84 量子密钥分配产品技术规范》
GM/T 0109—2021 《基于云计算的电子签名服务技术要求》
GM/T 0110—2021 《密钥管理互操作协议规范》
GM/T 0111—2021 《区块链密码应用技术要求》
GM/T 0112—2021 《PDF 格式文档的密码应用技术要求》
GM/T 0113—2021 《在线快捷身份鉴别协议》
GM/T 0114—2021 《诱骗态 BB84 量子密钥分配产品检测规范》
GM/T 0115—2021 《信息系统密码应用测评要求》
GM/T 0116—2021 《信息系统密码应用测评过程指南》
GM/T 0117—2022 《网络身份服务密码应用技术要求》
GM/T 0118—2022 《浏览器数字证书应用接口规范》
GM/T 0119—2022 《PLC 控制系统及 PLC 控制器密码应用技术规范》
GM/T 0120—2022 《基于云计算的电子签名服务技术实施指南》
GM/T 0121—2022 《密码卡检测规范》
GM/T 0122—2022 《区块链密码检测规范》
GM/T 0123—2022 《时间戳服务器密码检测规范》
GM/T 0124—2022 《安全隔离与信息交换产品密码检测规范》
GM/T 0125.1—2022 《JSON Web 密码应用语法规范第 1 部分：算法标识》
GM/T 0125.2—2022 《JSON Web 密码应用语法规范第 2 部分：数字签名》
GM/T 0125.3—2022 《JSON Web 密码应用语法规范第 3 部分：数据加密》
GM/T 0125.4—2022 《JSON Web 密码应用语法规范第 4 部分：密钥》

GM/T 0126—2023 《HTML 密码应用置标语法》

GM/T 0127—2023 《移动终端密码模块应用接口规范》

GM/T 0128—2023 《数据报传输层密码协议规范》

GM/T 0129—2023 《SSH 密码协议规范》

GM/T 0130—2023 《基于 SM2 算法的无证书及隐式证书公钥机制》

GM/T 0131—2023 《电子签章应用接口规范》

GM/T 0132—2023 《信息系统密码应用实施指南》

GM/T 0133—2024 《关键信息基础设施密码应用要求》

GM/T 0134—2024 《密码模块安全设计指南》

GM/T 0135—2024 《多方安全计算技术框架》

GM/T 0136—2024 《密码应用 HTTP 接口规范》

GM/T 0137—2024 《密码卡技术规范》

GM/T 0138—2024 《C-V2X 车联网证书策略与认证业务声明框架》

GM/T 0139—2024 《信息系统密码应用安全管理体系》

GM/T 0140—2024 《支付系统个人可信确认密码应用技术规范》

GM/T 0141—2024 《V2X 证书认证系统检测规范》

GM/T 0142—2024 《云服务器密码机检测规范》

GM/T 0143—2024 《对称密钥管理系统检测规范》

GM/Z 4001—2013 《密码术语》

GM/Y 5001—2023 《密码标准使用指南》

GM/Y 5003—2024 《多方安全计算密码技术研究》

GM/Y 5004—2024 《数据安全密码技术应用研究》

GM/Y 5005—2024 《密码功能服务安全要求及评估标准研究》

GM/Y 5006—2024 《信息系统密钥生命周期选取研究》

GM/Y 5007—2024 《基于 SM4 密码算法的保留格式加密技术研究》

GM/Y 5008—2024 《基于可信执行环境的密码模块技术研究》

GM/Y 5009—2024 《区块链隐私保护机制中的范围证明算法和环签名算法研究》

GM/Y 5010—2024 《秘密分享技术研究》

GM/Y 5011—2024 《车联网密码应用标准体系研究》

GM/Y 5012—2024 《北斗短报文密码技术应用研究》

GM/Y 5013—2024 《电子合同服务平台密码应用技术研究》

GM/Y 5014—2024 《涉及身份管理的个人信息保护技术研究》

GM/Y 5015—2024 《政务云密码应用安全性测评研究》

GM/Y 5016—2024 《车载 SoC 密码模块保护轮廓与测评要求研究》

GM/Y 5002—2018 《云计算身份鉴别服务密码标准体系》

（六）指导性文件

《商用密码应用安全性评估 FAQ（第三版）》

发布单位：中国密码学会密评联委会

《信息系统密码应用高风险判定指引》

发布单位：中国密码学会密评联委会

《商用密码应用安全性评估量化评估规则》（2023 版）

发布单位：中国密码学会密评联委会

《商用密码应用安全性评估测评实施指引》

发布单位：中国密码学会密评联委会

《政务领域政务服务平台密码应用与安全性评估实施指南》

发布单位：中国密码学会密评联委会

《政务领域政务云密码应用与安全性评估实施指南》

发布单位：中国密码学会密评联委会

第二章 商用密码发展态势

本章全面分析了国内外商用密码产业的发展现状，重点探讨了美国、欧盟、俄罗斯等国家和地区在商用密码领域的政策法规、产业格局等多个方面的现状。

深入剖析了我国商用密码产业在《密码法》实施后的新进展，从保护数字资产、维护经济社会秩序到推动数字中国建设，并展望了商用密码技术在新质生产力构建、产业数字化转型、数字中国建设中的重要作用和未来发展目标。

（一）国内外发展现状

1. 国际商用密码发展现状

随着数字化进程的深入和量子计算技术的崛起，商用密码作为网络安全的基础核心技术，已成为各国数字主权与国家安全的战略必争之地。美国、俄罗斯和欧盟作为全球重要的经济体和技术发展中心，在商用密码领域采取了各有侧重的发展路径。本节将基于最新信息，从政策法规与产业格局两个维度，对这三个国家/地区的商用密码发展现状进行梳理。

1.1 美国商用密码发展现状

美国的商用密码发展呈现出战略引领、法规保障、产业联动的鲜明特点。

美国在商用密码的管理上采取了分散与集中相结合的模式。国家安全局（NSA）作为密码工作的领导机构，自 1952 年成立以来，其职能已经从最初的国防部和国务院的密码和保密通信活动，扩展到了包括编制通信密码方案、领导民商界通信保密标准政策制定、协调保密设备的制造使用、密码破译和网络监控等多个方面。2022 年 9 月 7 日，NSA 通过其发布的 CNSA2.0，展示了美国在商用密码领域的顶层规划设计和应对量子计算威胁的战略布局。在法律法规方面，美国没有独立的密码法或通用的信息安全法律法规，但美国联邦政府通过一系列政策对政府部门的密码应用进行了规范。这些政策不仅涵盖了密码使用的层面，还涉及了信息安全测评与密码检测认证的架构体系。美国政府还推出了与密码应用相关的政策，如“托管加密标准”（EES），要求加密产品加入密钥恢复机制，以便执法部门在必要时能够获取明文。

美国在密码产品和密码应用方面，一直走在世界前列。NSA 在密码产品制造方面，主要提供需求标准和产品认证，而研发工作则由美国的商业公司如 Motorola、AT&T、Harris 等完成。在密码应用方面，美国政府要求处理机密和敏感信息的办公自动化系统采用传输和存储加密等手段，同时，涉密系统还需采用 NSA 核准的包括密码设备在内的通信安全措施。此外，美国政府还加强对电子商务的支持，逐步放宽密码产品出口，并允许美国公司向世界大多数国家出售强加密产品，供本国总公司与跨国子公司之间的保密通信使用。

美国商用密码的发展趋势指向了量子安全算法的采用、密码技术的持续创新、密码人才的培养和教育，以及全球密码市场的参与和影响力扩大。综上所述，美国在商用密码领域的现状和发展趋势表明，该国正通过一系列前瞻性的政策和技术创新，积极构建一个更加安全、可靠和具有全球竞争力的密码生态系统。通过顶层设计、政策引导、技术创新和人才培养等多方面的努力，美国在这一关键领域保持了其优势地位，并为全球密码学和信息安全领域的发展提供了重要的参考和借鉴。

1.2 俄罗斯商用密码发展现状

俄罗斯的商用密码发展路径则体现出严格管控、进口替代、安全优先的突出特征，强调通过国家主导保障网络安全和数字主权。

俄罗斯很早就着手密码算法的标准化工作，并创立了俄罗斯联邦密码委员会，负责监管和推动俄罗斯国家密码标准化工作，统一规范俄罗斯在信息安全领域的加密算法等技术。对于俄罗斯的密码算法标准化文件和技术，在俄罗斯政府批准后方可在国家范围内广泛使用。在法律法规方面，俄罗斯通过了《俄罗斯联邦信息、信息化和信息保护法》，该法律对信息安全和密码使用提出了基本要求。此外，俄罗斯还制定了《俄罗斯联邦个人数据法》，要求对个人数据进行加密处理，以防止未授权访问。

俄罗斯在密码产品的研发和应用方面具有一定基础。俄罗斯的密码产品包括加密软件、安全芯片、密码卡等，广泛应用于政府通信、金融服务、交通控制等领域。在密码应用方面，俄罗斯政府积极推动密码技术在公共服务和关键基础设施中的使用。在检测认证方面，俄罗斯非常重视密码算法的测试和评估。对密码算法的测试和评估主要有以下两种形式。一是国家级测试，俄罗斯联邦政府的安全机构负责对新算法进行安全性和可靠性测试。如果一种新算法被认为是安全、可靠的并且符合俄罗斯政府的加密标准，它可能就会被确定为俄罗斯联邦密码算法标准的一部分。除了政府级别的测试外，一些独立的安全机构也会对俄罗斯的密码算法进行评估和测试。这些测试的结果往往会严格审查算法的安全性、可靠性和性能，并根据评估结果提出建议或改进建议。俄罗斯的密码算法因其独特的特点和高强度的安全级别而在国际上备受关注，这也促进了俄罗斯密码算法的良性发展和推广应用。

1.3 欧盟商用密码发展现状

欧盟在商用密码领域的发展则体现出寻求平衡、协同发展的特点，试图在维护网络安全与促进数字单一市场之间找到合适的路径。

欧盟的商用密码管理涉及多个机构，包括欧盟网络安全局（ENISA）、欧盟执法合作署（Europol）以及各成员国的国家网络安全机构。ENISA 作为欧盟网络安全的主要机构，负责提供网络安全战略、政策和标准的建议，并推动成员国

之间的合作。在法律法规方面，欧盟通过了一系列重要的法规来规范密码产品和服务的使用，其中最为关键的是《通用数据保护条例》（GDPR）。GDPR 对个人数据的保护提出了严格要求，包括数据加密和泄露通知等，从而间接推动了商用密码技术的发展和应用。此外，欧盟还通过了《电子隐私指令》（ePrivacy Directive）和《网络安全法案》（Cybersecurity Act），这些法规进一步强化了对商用密码的需求。

欧盟在密码产品的研发和应用方面具有显著的成就。欧盟资助的地平线2020（Horizon2020）研究与创新计划支持了多个密码学项目，包括抗量子密码学和云计算安全等。欧洲标准化委员会(CEN)和欧洲电工标准化委员会(CENELEC)，与 ENISA 合作，制定了一系列网络安全和密码技术的标准。2023 年，CEN 和 CENELEC 联合发布了世界上首个量子技术综合标准化路线图。在监督管理方面，欧盟通过其网络安全监管框架对商用密码的使用进行监督和管理。2024 年 1 月，欧盟《网络安全条例》已正式生效。

2. 国内商用密码发展现状

2.1 政策环境

我国密码行业已构建起以《密码法》为根本准则，以《商用密码管理条例》等法规规章为重要支撑的密码法律法规体系，为行业的健康发展奠定了坚实的法治基础。

《密码法》为商用密码的管理、应用和发展提供了坚实的法律基础。随着相关配套法规的陆续出台，商用密码的法律体系更加完善。《商用密码管理条例》要求关键信息基础设施使用商用密码进行保护的单位必须开展商用密码应用安全性评估，这标志着商用密码的合规性和安全性要求达到了新的高度。同时，在《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规的持续驱动下，商用密码支撑体系也得到进一步完善。

2.2 产业规模

在政策法规和市场需求的共同推动下，我国商用密码产业展现出强劲的发展活力，产业生态日益繁荣。市场规模保持高速增长态势。我国商用密码行业市场规模呈现出稳定增长的态势，已达千亿元规模。

近年来商用密码产业较高的增速主要归因于政务、金融等关键领域密码应用的深度渗透，以及《密码法》和《商用密码管理条例》的政策驱动。

《密码法》降低了商用密码产业的准入门槛，商用密码企业数量不断增多，大大促进了商用密码产业的发展。商用密码产业的技术创新持续活跃，新产品和新服务不断涌现。量子密码、人工智能安全、大数据加密等前沿技术成为研究热点。产业规模方面，在政策环境与市场需求的共同作用下，商用密码产业规模将

迎来较快增长，随后逐步趋于成熟。根据最新数据，我国商用密码产业规模显示出强劲的增长势头。

2.3 技术融合

当前，以区块链、云计算、物联网、大数据、5G、量子技术、人工智能等为代表的新技术新应用蓬勃发展，为实现数据资产安全与隐私保护带来了机遇和挑战。以密码为基础的安全技术体系将与前沿技术深度融合和协同创新，引领信息领域关键核心技术的创新突破。在数据信息存储、传输、共享等多个环节采用加密技术，强化信息技术产品研发应用过程中的密码技术应用，将共同保障信息网络和信息系统的安全。密码芯片、密码模块、密码硬件产品、密码软件系统、密码管理服务平台、密码运营服务中心等将实现与新技术、新模式的应用场景适应和技术深度融合，以满足用户企业密码管理安全可靠、密码使用优质高效的发展要求。

2.4 应用范围

商用密码产业的地域分布集中在科技和经济发展水平较高的地区。这些地区聚集了大量的商用密码企业，形成了产业集群效应。在行业应用方面，目前，商用密码在金融、通信、工业互联网、物联网、交通等领域已经开展诸多场景应用，并将在未来构建起更加完善的密码支撑体系。新兴领域，随着云计算、大数据、区块链等新业态的蓬勃发展，国家鼓励重点行业企业加大网络安全投入，单独列支网络安全预算，推动了商用密码技术、产品和服务的深入融合与拓展应用。

2.5 生态环境

面向重点领域逐步构建起与密码深度协同的融合产业生态，密码前瞻性技术沙龙和创新论坛将会百花齐放，深入研究探讨密码技术与新一代移动通信、云计算、区块链等技术融合发展，推进密码在“新基建”中的规范化发展和规模化应用。通过密码行业协会、产业联盟等社会团体整合产业力量，促进商用密码产品和服务供需对接，形成优势互补、布局合理、自治共管的产业体系。通过构建商用密码科技创新和产业发展的统一平台，形成合作共赢、高效协同的良性市场环境，以及健康、有序的密码产业生态。

（二）我国商用密码发展趋势

1. 我国商用密码发展新目标

我国密码产业规划以总体国家安全观为根本遵循，构建了以《密码法》为核心、以配套法规规章为支撑的密码法律法规体系，为产业发展奠定了坚实的法治基础，也预示着商用密码将进入一个新的发展阶段。在这一阶段，商用密码不仅是保护数据资产、维护经济社会秩序的关键技术，也是推动数字中国建设的核心

动力。

在技术层面，规划强调以创新驱动技术与产业发展的现代密码产业体系。商用密码产业长远发展核心目标是技术自主和高水平的自强自立。我国商用密码产业将致力于标准体系完备、产业链和国际合作与交流，以实现高水平的自强自立。推动商用密码技术和产品的广泛应用，减少对外部技术的依赖，确保产业链的稳定性和安全性。标准制定方面，开展新兴数字产业及新业务场景下密码标准制定，积极参与国际标准的制定，推动我国商用密码标准在促进云、物、移、大、智等新兴场景密码应用和我国商用密码标准和技术国际化方面充分发挥作用。国际合作与交流将在保持自主发展的同时，加强与国际密码学界的交流与合作，提升我国商用密码技术的国际影响力。进一步健全和完善商用密码检测认证以及运行安全保障体系，建立密码应急响应机制以提高对网络安全威胁的应对能力，是保障国家网络安全和数据安全，支撑商用密码高质量发展的重要举措。

进一步深化商用密码与网络信息化融合发展，建设国家网络安全和数据安全密码保障体系。规划着力推动密码在各领域的深度应用，实现密码与经济社会发展的深度融合。促进商用密码在金融、政务、民生、工业等关键行业以及区块链等新兴领域的应用，满足不断增长的市场需求，通过加密、认证等手段，防止数据泄露和篡改。法规与标准的制定将为数据安全密码保障提供规范性指导，在推进重要行业领域密码高质量应用的同时，推动密码应用与各行业网络与信息系统建设的“三同步一评估”。同时，密码技术的普及教育将提升全民的网络安全意识和密码保护能力，构建全社会共同维护网络安全的良好氛围。

在人才培养方面，教育部已将“密码科学与技术”列入普通高等学校本科专业目录，多所高校开始招收密码专业本科生。截至 2025 年 4 月，我国开设“密码科学与技术”本科专业的高校增至 22 所，分别为南开大学、山东大学、华中科技大学、西安电子科技大学、北京电子科技学院、北京理工大学、海南大学、北京邮电大学、东南大学、暨南大学、湖北大学、华南师范大学、西安邮电大学、武汉大学、郑州大学、宁波工程学院、河南大学、广东技术师范大学、桂林电子科技大学、甘肃政法大学、河南师范大学、成都信息工程大学。“密码技术应用”也已纳入职业教育专业目录。人力资源社会保障部将“密码技术应用员”确定为新职业，发布的《密码技术应用员职业技能标准（2023 版）》将密码技术应用员共设为四个等级，分别为四级/中级工、三级/高级工、二级/技师、一级/高级技师，建立了密码职业人才分类分级评价体系。

在数字中国建设的新时期，商用密码技术面临着新的发展机遇和挑战。通过加强技术创新、推动密码与网络信息化的深度融合，我国商用密码将在保护数据资产、维护经济社会秩序、推动数字经济发展等方面发挥更加重要的作用。在政府的支持和引导，以及企业的积极参与和创新和全社会的共同努力下，商用密码

技术将为数字中国建设提供更加坚实的安全保障，为实现网络强国战略目标做出更大的贡献。

这一系列从战略、技术到产业再到人才和价值的新发展，共同确立了商用密码作为推动新质生产力加速发展的核心助推器与赋能引擎的全新历史定位，标志着我国密码事业进入了一个能动的、与数字经济核心发展脉络深度融合的新纪元。

2. 商用密码与新质生产力

新质生产力核心在于以颠覆性技术和前沿科技创新驱动生产要素的革新性配置，而数字化、网络化、智能化正是其实现的关键路径。在这一深刻变革中，数据作为新的核心生产要素，其安全、可信、有序地流动与利用成为生命线。商用密码，作为保障网络与信息安全的核心技术和基础支撑，正是守护这条生命线的关键环节。它不仅是新质生产力赖以发展的底层安全基座，更深度融合于智能制造、智慧政务、数字金融等各类新业态、新模式之中，通过加密保护、身份认证、安全通信等手段，为新质生产力的蓬勃发展构建起一个可信的数字空间，确保科技创新在安全轨道上释放最大效能。

因此，发展新质生产力与强化商用密码应用，是实现高质量发展和高水平安全动态平衡、一体推进的战略抉择。

2.1 新质生产力的意义

新质生产力的培育与发展，是引领国家迈向现代化新征程的核心引擎。从国家战略高度看，它关乎我国能否在全球科技革命与产业变革中抢占制高点，提升产业链供应链的韧性与安全水平，从而在国际竞争格局中塑造全新优势，这既是高质量发展的内在要求，也是保障国家安全的战略基石。具体到经济发展层面，新质生产力通过科技创新赋能传统产业升级、催生战略性新兴产业和未来产业，彻底改变了依赖传统要素投入的增长模式，成为驱动经济实现质突破的有效提升和量突破的合理增长的根本动力。

进一步看，这种以创新为主导的生产力具有鲜明的绿色底色，是实现可持续发展的关键路径。它推动经济增长与碳排放脱钩，借助智能化、绿色化技术大幅提升资源利用效率，为达成“双碳”目标、建设人与自然和谐共生的现代化社会提供了坚实的科技支撑。

最终，所有这些变革的成效将切实惠及于民。新质生产力在创造巨大社会财富的同时，也深刻重塑了就业创业格局：一方面，它催生了大量高技能、创新性的职业岗位，对劳动者素质提出了更高要求，倒逼人力资源结构优化；另一方面，它降低了技术应用和创新创业的门槛，为各类市场主体尤其是科技型中小企业提供了广阔舞台，激发了社会创造活力，形成了发展为了人民、发展依靠人民、发展成果由人民共享的良性循环。

2.2 新质生产力与密码技术融合

新质生产力，以科技创新为核心，通过信息化、数字化、智能化等手段，正在深刻改变传统的生产和生活方式，推动经济社会进入一个新的发展阶段。在这一进程中，商用密码技术和产业作为新质生产力的重要组成部分，正受到多方面的推动和促进。

一方面，AI 技术的发展为商用密码领域带来了新的设计理念。通过机器学习和深度学习，可以设计出更加复杂和安全的密码算法，同时自动化的密码破解尝试也对现有密码系统的安全性提出了挑战，促使密码技术不断进化。量子通信技术的安全性、高效性和准确性为商用密码技术提供了新的发展方向。同时，量子计算的发展也对现有密码体系构成了潜在威胁，促使密码学界研究抗量子密码技术。

另外一方面，随着各行各业数字化转型的加速，对数据安全的需求日益增长，这直接推动了商用密码产业的发展。在线教育、互联网医疗、线上办公、数字化治理等新业态的出现，为商用密码技术提供了新的应用场景。国家对新质生产力的重视和支持，通过政策引导和资金投入，为商用密码技术和产业的发展提供了良好的外部环境。同时，随着数据价值的日益凸显，企业和个人对数据安全保护的需求不断增长，推动了商用密码市场的扩大。

商用密码的应用并非单一算法或产品的堆砌，而是基于场景需求的技术组合方案，即通过算法的特性适配、密码产品的部署落地、密钥管理的全生命周期管控，最终实现数据安全、业务可信、合规达标的核心目标，成为数字经济时代的安全基石。

3. 商用密码与数字中国

在数字化浪潮的推动下，中国正致力于构建一个全面数字化的社会，即“数字中国”。这一宏伟蓝图涉及金融、政务、民生保障等多个领域，数据作为新型生产要素，其安全可信流通是关乎全局的基石。商用密码技术正是浇筑这一基石，激活数据潜能的核心力量。商用密码不仅保障了信息的机密性、完整性和可用性，而且对于维护国家政治安全、经济安全、文化安全、社会安全、生态安全和国防安全具有重要意义。

3.1 数字中国的安全基座

商用密码是数据安全防护的核心技术。在数字化时代，数据已成为一种极其重要的资产，其安全防护变得尤为关键。密码技术，作为信息安全的核心技术，为数据安全提供了坚实的保障。它不仅能够保障数据的理论安全，而且在数据的整个生命周期中发挥着至关重要的作用。此外，随着数据价值的日益凸显，密码技术的创新已成为推动数据流通和发挥其价值的关键因素。密码技术的设计基于

数学原理和计算复杂性理论，能够为数据提供机密性、完整性、真实性和不可否认性的保护。理论上，只要密码算法足够强大，密钥管理得当，且密码系统的实现没有漏洞，密码技术就能够抵御各种已知攻击，从而保障数据的安全性。

商用密码是保障国家关键信息基础设施安全的基础。国家关键信息基础设施是指对于国家经济、政治、社会稳定和人民生活至关重要的信息系统和网络设施。这些基础设施一旦遭受破坏或功能失效，可能会对国家安全、经济运行和社会秩序造成严重影响。

密码技术在保护关键信息基础设施中发挥着核心作用，其作用和意义主要体现在以下几个方面：通过加密技术，可以确保存储和传输的数据安全，即使在数据被截获的情况下也无法被解读；密码技术提供身份验证机制，确保只有授权用户才能访问关键系统和数据；通过使用数字签名和消息认证码，密码技术确保数据在传输过程中未被篡改；密码技术确保数据的发送方和接收方无法否认其参与过的数据交换行为；有效的密钥管理是密码系统安全性的关键，包括密钥的生成、分发、存储、更新和销毁；密码技术的发展，如抗量子密码算法，有助于应对未来可能出现的量子计算威胁；密码技术帮助关键信息基础设施的运营者满足各种法律和行业标准要求，确保数据保护符合法律法规；通过展示强大的密码保护措施，增强公众对关键信息基础设施服务的信任。

密码技术是保护国家关键信息基础设施免受内部和外部威胁的基石。随着技术的发展和新威胁的出现，密码技术必须不断演进，以保持其有效性。国家需要投资于密码学研究、人才培养和技术创新，以确保关键信息基础设施的长期安全和韧性。同时，制定和实施全面的网络安全策略，包括密码技术的应用，对于保护国家的关键资产和推动社会经济发展具有重要意义。

商用密码是安全基石的保障。2020 年 4 月 20 日，国家发展改革委在新闻发布会上首次明确了新型基础设施的范围。新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系。新型基础设施主要包括三方面内容：一是信息基础设施，包括以 5G、工业互联网、卫星互联网为代表的通信网络基础设施，以人工智能、云计算、区块链等为代表的新技术基础设施，以数据中心、智能计算中心为代表的算力基础设施等。二是融合基础设施，主要指深度应用大数据、人工智能等技术，支撑传统基础设施转型升级，进而形成的融合基础设施，比如，智能交通基础设施、智慧能源基础设施等。三是创新基础设施。主要是指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施，比如，重大科技基础设施、科教基础设施、产业技术创新基础设施等。新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系。

3.2 护航数字经济

数字经济是新兴产业，在数字经济发展之初，就要以系统性、整体性和协同性为原则，同步规划建设以密码保障系统为核心的信息安全保护系统，推动商用密码与数字经济的融合发展，切实提升数字经济的安全防护能力。密码是支撑数字经济发展、护航数字经济发展的基础。数据就是财富，安全才有价值；融合就是机遇，信任才有基础。密码将在数字经济发展中发挥不可替代的重要作用。

数字经济高质量发展离不开安全可靠的运行环境。利用基于密码技术的身份鉴别、信任管理、访问控制、数据加密、可信计算、密文计算、数据脱敏等措施，可以有效解决数据产生、传输、存储、处理、分析、使用等全生命周期安全问题，解决网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端等全体系平台安全问题，解决技术融合、产业融合中的全产业链条安全问题，为数字经济提供系统性、全方位的安全防护。

数字经济时代，一方面，密码助力打通数据融通的信任瓶颈，实现信息资源开放共享。利用基于密码的数据标识、数字签名、数字内容和产权保护等技术，构建起真实不可抵赖的“数字契约”，为数据资源确权、开放、流通、交易提供信任基础。另一方面，密码助力疏通资金融通的信任梗阻，促进融资便利化。

新型计算、网络攻防和密码技术的交替演变、融合发展，成为推动社会科技进步的强大动力。一方面，密码与信息技术的融合催生信息科技创新。近年来基于密码的区块链技术的广泛应用，为电子商务、数字金融等带来新的机遇。另一方面，信息科技创新推动密码创新。量子计算的快速发展，使得抗量子密码算法设计成为新的发展方向；云计算推动密码理论研究进入同态时代；物联网技术对终端环境实现密码计算安全提出新挑战。数字经济本质是一种创新经济，核心动力是信息技术创新，在数字经济发展过程中，始终存在着密码与信息技术的协同创新。

利用密码技术和数据标识、数字签名、网络身份认证等技术的结合，在确保数据安全有序流动的同时，为数据溯源、行为追踪、隐私保护提供有效支撑，为数字经济领域的监管提供司法证据，为部门监管和打击犯罪提供有力武器，为提升国家治理体系和治理能力现代化水平、完善监督保障体系建设提供技术手段。

3.3 建设数字社会

商用密码技术是推动国家数字化发展的核心技术之一。在电子政务、社会治理、民生保障等方面，商用密码技术的应用有助于提升国家治理能力，保护公民隐私。通过构建以密码为核心的安全防护架构，可以实现身份鉴别、访问控制、权限管理等安全措施，保障数据共享的安全。此外，商用密码技术还可以为政务移动办公构建安全传输通道，提升电子政务的安全性与灵活性。在社会治理方面，密码技术可以构建统一的网络信任体系，为网络身份认证与实体鉴别提供技术支

撑。在民生保障信息系统中，商用密码技术则可以提供身份认证、数据保护和隐私保护，确保教育、医疗和社会保障等关键信息系统的安全。

商用密码技术是数字中国建设的核心支撑，对于保障国家关键信息基础设施的安全、推动数字经济的发展和促进国家数字化转型具有至关重要的作用。随着数字技术的不断进步和数字应用的日益广泛，商用密码技术将面临更多的挑战和机遇。未来，需要进一步加强商用密码技术的研发和应用，完善相关的法律法规和标准体系，培养更多的密码技术人才，以适应数字中国建设的需要。通过全社会的共同努力，商用密码技术将为数字中国的全面发展提供坚实的安全保障。

第三章 辽宁商用密码产业发展情况

在“十四五”期间，辽宁省商用密码发展紧扣国家发展战略，构建与法律法规相匹配的商用密码标准体系，推动商用密码应用向纵深发展，深化商用密码在关键信息基础设施和新兴领域的应用，加强商用密码技术与新一代信息技术，丰富算法种类、优化供给形态、提升服务水平。

本章聚焦辽宁省内的商用密码产业，立足商用密码的辽宁实践，旨在系统梳理辽宁省商用密码产业的发展现状及趋势。首先以本地商用密码产业图谱入手进行梳理，并介绍了省内的代表企业平台及相关基础设施。之后列出省内商用密码领域的重要规划举措。总的来说本章从产业现状和重要规划举措两个方面宏观介绍了我省商用密码产业的整体发展概况。

（一）辽宁省商用密码产业建设现状

1. 辽宁省密码产业简况

截至 2025 年 11 月，辽宁省内 6 家密码生产研发企业获得商用密码认证产品证书产品共 12 款，其中辽宁公信安全信息科技有限公司 5 款、沈阳东软系统集成工程有限公司 2 款、大连秘阵科技有限公司 2 款、辽宁广烁科技有限公司 1 款、中国科学院沈阳自动化研究所 1 款、大连凌一科技发展公司 1 款。

辽宁省内密码生产研发企业及商用密码产品介绍：

1.1 辽宁公信安全信息科技有限公司

办公地址：辽宁省沈阳市浑南区天赐街 7-3 号 1104-1109

公司介绍：辽宁公信安全信息科技有限公司成立于 2019 年 6 月，主要从事商用密码产品的研发、生产、销售及信息系统集成服务。是辽宁省重点扶持的国家级高新技术企业、商用密码产品生产单位：拥有自主知识产权的核心技术及产品，先后取得多款商用密码产品认证型号证书及相关软件著作权 20 项。是“天津滨海 CA”“东软集团”的战略合作伙伴，是其商用密码产品的主要供货商和电子签名服务解决方案的技术支撑单位。

公司团队核心人员均具有硕士以上学历，具有多年密码行业的从业经验，精准把握行业发展方向，熟练运用相关的核心技术，为客户提供医疗、教育、电子劳动合同、智慧房产、招投标等领域电子签名服务完整解决方案。

公司在沈阳、郑州设立两个研发中心，在全国主要省会城市设立运营服务中心，并已经为全国 60 多家医疗机构和卫健委，1 个省级电子劳动合同平台提供电子签名服务，累计颁发数字证书 2 万张。

优势行业：政务、医疗、教育

商用密码认证产品信息：

产品名称	证书编号	应用行业或领域
签名验签服务器	GM002111120210017	医疗、教育、政务
时间戳服务器	GM002111220202046	医疗、教育、政务
公信签密钥协同服务端密码模块	GM002112220220699	医疗、教育、政务
公信签密钥协同客户端密码模块	GM002112220220701	医疗、教育、政务
电子签章系统	GM002111520202238	医疗、教育、政务

1.2 沈阳东软系统集成工程有限公司

办公地址：辽宁省沈阳市浑南新区创新路 175 号 B3 座 5 层

公司介绍：沈阳东软系统集成工程有限公司成立于 1997 年 3 月，成立伊始就开始了优秀软件技术成果的转化，致力于面向国民经济关键领域与重点行业的信息系统研制开发与自主创新。目前已建立了辐射全国 66 个骨干城市的营销网络与本地化客户服务体系。近三年业绩达到 20 亿元，拥有员工 400 余人。公司承担主要业务的专业技术人员 350 人，其中本科学历以上 90%，具有较为成熟的研发、生产、管理体系。

优势行业：政务、金融、医疗、通信、教育、能源、交通、税务

商用密码认证产品信息：

产品名称	证书编号	应用行业或领域
东软 NetEye 防火墙 FW5200V3.2	GM002110520220388	医疗、教育、政务、能源
东软 NetEyeSSLVPN 网关 VPNV3.0	GM002110620220607	医疗、教育、政务、能源

1.3 大连秘阵科技有限公司

办公地址：辽宁省大连市高新园区火炬路 1 号创业园 A 座

公司介绍：大连秘阵科技有限公司，是一家专注于网络与信息安全领域，深耕网络身份与数据安全及密码技术的研发与应用的国家级高新技术企业。

公司致力于为用户提供从移动端（APP、智能终端等）→到客户端（PC，瘦客户机等）→到云平台，从应用到数据，从物联网（IoT）到工业互联网，从软件算法到智能硬件的跨终端、多平台、全场景的强身份认证服务与定制化开发，为客户提供基于“零信任”体系的密码安全管理平台的解决方案、终端安全密码技术解决方案、区块链密码技术应用及网络安全相关的全流程密码技术应用解决方案和产品服务。

2017 年，公司取得了“国家商用密码生产定点单位”（国密局产字 SSC2167 号）的涉密企业资质。通过自主创新和技术攻关先后完成多项商用密码安全产品

的研发，现已取得包括 3 项国家发明专利、4 项国际发明专利、2 项外观设计专利，以及多达 30 余项软件著作权在内的一系列自主知识产权，并通过了国家密码管理局的权威检测。

秘阵科技现已通过 ISO90001、ISO27001 体系认证。作为国内密码技术研发与创新应用的新领军企业，公司先后多次承担国家工信部、科技部和省、市级的网络安全重点项目的研发工作，现为国家工信部“商用密码应用标准委员会”的委员单位。秘阵科技的事迹曾先后被中央广播电视总台、新华社、《人民日报》和香港《大公报》等国内外主流权威媒体所报道。2019 年，秘阵科技的创业事迹和产品优势，还被中央电视台一套的“焦点访谈”栏目所报道。

商用密码认证产品信息：

产品名称	证书编号	应用行业或领域
秘盾密码动态令牌密码模块	GM002112220230608	信息安全
秘阵认证管理系统密码模块	GM002112220231058	信息安全

1.4 中国科学院沈阳自动化研究所

办公地址：辽宁省沈阳市沈河区南塔街 114 号

公司介绍：中国科学院沈阳自动化研究所成立于 1958 年，主要研究方向是机器人、智能制造与光电信息技术。研究所拥有正式员工 1400 余人，其中中国工程院院士 3 人，高级职称的技术人员 600 多人，拥有博士培养点 5 个、硕士培养点 8 个，博士后流动站 2 个。有南塔街和创新路两处所区，是“机器人学国家重点实验室”“机器人技术国家工程研究中心”“国家机器人创新中心”“国家机器人质量监督检验中心（辽宁）”等十多个国家和省部级平台的依托单位，主办中国科技核心刊物《机器人》和《信息与控制》。

六十多年来，沈阳自动化所着眼国民经济和国家安全重大战略需求，凝练研究方向，在机器人与智能制造领域着重开展创新研究，在机器人学、工业机器人、水下机器人、空间机器人及自动化、特种机器人、先进光电技术与系统、无线传感与通信技术、机器人化工艺装备及智能产线等研究与开发方面取得大批成果，形成技术领先优势。为国民经济、社会发展和国家安全作出了突出贡献，获得国家、中国科学院、各部委及地方奖励 300 余项。沈阳自动化所以为国家战略高技术及其产业发展提供技术基础为发展理念，向着成为具有强大自主创新能力和可持续发展能力，向着建设成为具有中国特色、国际知名的科研机构为目标奋进。

优势行业：通信、能源

商用密码认证产品信息：

产品名称	证书编号	应用行业或领域
沈自所 USB 密码模块	GM002112220230443	装备制造

1.5 辽宁广烁科技有限公司

办公地址：辽宁省大连市中山区华乐街滨景园 1 号

公司介绍：辽宁广烁科技有限公司成立于2015年，注册资金3000万元，是大连软件行业协会会员单位、高新技术企业、双软认证企业、国家ISO9001质量管理体系认证企业，鲲鹏网络安全产学研联盟成员单位，也是辽宁省唯一进入国家信创名录的商密产品研发公司。全部产品均为自主研发，有电子签章、电子证照、统一身份认证等主力产品，以及相关应用平台，手机端、智慧云端等产品，著作权有38项，国家级检测报告5项，国产和非国产平台国家级认证资质2项，平台符合等保三级要求。

公司承建了辽宁省一体化政务服务平台统一电子印章系统、省物电一体印章治安管理信息系统、新办企业“一网通办”平台印章缴费统一支付系统等省级平台，各系统实现互通互认，与国家平台电子公章系统、公安部三所的全国电子公章管理与服务平台、3个国家级系统、完成近200个全省业务系统对接、全省政务部门覆盖度达到了100%，累计调用次数达到1.2亿次。

优势行业：政务、金融、医疗、通信、教育、能源、交通、税务

商用密码认证产品信息：

产品名称	证书编号	应用行业或领域
广烁电子签章系统V3.0	GM002111520210147	政务

1.6 大连凌一科技发展公司

办公地址：辽宁省沈阳市浑南区东湖街道南屏东路36号16号楼5门

公司介绍：凌一科技在网络信息安全与终端接入安全方面有着长期的积累，一直以来主要为中央部委、政府部门，央企集团、科研院所、事业单位、行业企业承担信息化项目建设、信息技术服务。自公司成立以来，每年的研发投入比例不断增大，注重基础核心技术积累和应用创新，逐步形成了一系列具有自主版权的软件产品和先进的行业解决方案。软件产品主要包括业务自适应统一安全接入平台、安全智能接入终端、客户端运维综合管理平台和网络应用性能分析系统等。近年来，公司积极参与推动信息化软件核心技术的国产化，广泛与业界同行开展战略合作，为我国民族软件的快速发展贡献力量。

优势行业：政务、金融

产品名称	证书编号	应用行业或领域
无线接入终端密码模块USEC1500V3.0	GM002112220230767	金融行业

2. 代表企业平台及基础设施

省内已具备电子认证服务机构（CA）、密码测评机构、政务云密码资源池等基础配套能力资源。按照辽宁省数字政府建设规划对信息化产业信创和国产化的政策指导方针，加快实现密码技术应用创新，充分发挥密码技术对网络和信息安全的基础支撑和核心技术的作用，推动密码技术在各行业中深度融合应用，不断

丰富和完善密码技术的应用场景。

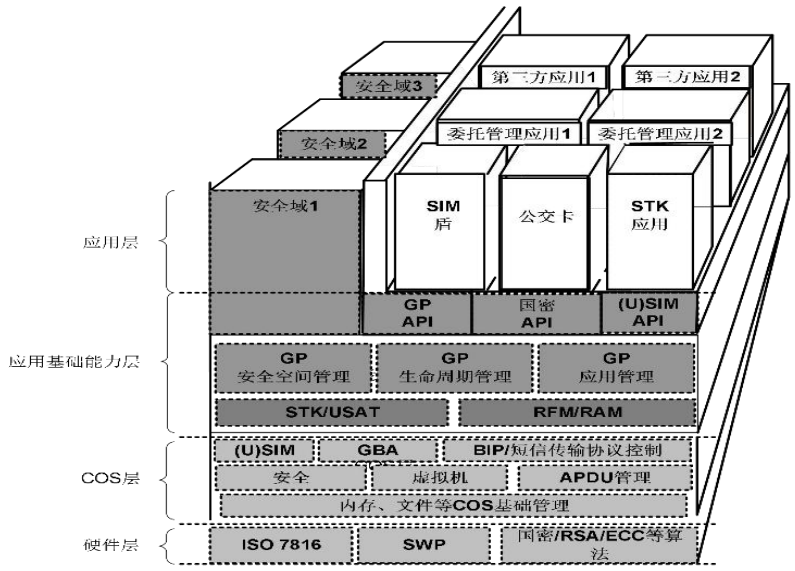
2.1 电子认证服务

辽宁数字证书认证管理有限公司是辽宁省唯一拥有电子认证服务全资质的服务机构，资质包括国家密码管理局颁发的《电子认证服务使用密码许可证》《电子政务电子认证服务机构》、工业和信息化部颁发的《电子认证服务许可证》、卫生部颁发的《医疗卫生电子认证服务机构》、国家信息中心颁发的《国家电子政务外网辽宁省电子认证服务分中心（LRA）》资质。长期以来，辽宁数字证书认证管理有限公司面向辽宁省政务、医疗、商业等领域，提供安全、高效、稳定的电子认证服务。

辽宁数字证书认证管理有限公司大力推动电子认证服务升级工作，基于 PKI 技术框架体系和国密算法，利用移动智能终端设备普及性、便携性、易用性的特点，提供安全、便捷、高效的电子认证签名印章移动一体化服务。

2.1.1 全民证书移动超级 SIM 基础设施

超级 SIM 卡是 5G 时代重点打造的号、卡、消息三大基础入口之一，集存储功能、通信服务与智能应用于一体，内置金融级安全芯片，大幅提升数据存储的安全性和可靠性。2022 年，中国移动超级 SIM 卡作为数字证书新式硬件载体已通过商用密码产品密码模块二级认证，数字证书安全存储在超级 SIM 卡中，在主体充分知晓并同意下，通过中国移动专有信令安全通道，实现电子认证、电子签名等功能。



图三-1 移动超级 SIM 卡技术架构

中国移动通信集团辽宁有限公司按照全民证书项目建设规划，已建设完成全民证书超级 SIM 平台，实现对超级 SIM 卡的集中管理和权限分配。第三方应用通过对接全民证书能力开放平台，与 SIM 卡平台进行信息交互，应用在完成授权验证后，获取数字证书使用权限，从而确保数字证书使用的安全性。支持数字证书

使用记录全过程可追溯，便于数字证书的主体全面了解数字证书使用情况，当存在争议时，可作为具有法律效力的证据提供给用户。

2.1.2 全民证书电子认证集群基础设施

辽宁数字证书认证管理有限公司按照《商用密码应用安全性评估管理办法》中关于电子认证的相关要求，采取集约化部署模式，搭建覆盖全省的电子认证集群基础设施，面向政务领域和商务领域业务系统提供安全合规的电子认证、电子签名服务。

采用“多层架构+智能调度”方式进行部署，打破各单位信息壁垒，实现电子认证“全域互通、高可用、低延时”。具体包括以下功能：

多层冗余架构：采用多层架构，省级节点部署主备双机，地市节点配置至少2个冗余实例，从硬件、网络、数据层面构建三重冗余，避免单点故障导致电子认证服务中断。

跨节点自动切换：系统内置“故障检测－自动分流”机制，当某个地市节点出现硬件故障或网络中断时，500ms内自动将该节点的电子认证请求分流至邻近健康节点，确保政务业务“7×24小时不中断”。

就近访问调度：基于用户地理位置自动匹配最近节点，减少跨区域数据传输耗时，将电子认证响应时间从“跨节点平均300ms”压缩至“就近访问80ms以内”，提升操作体验。

动态算力调配：搭建省级算力调度中心，实时监控各地市、各部门的算力需求，自动将闲置算力调配至需求旺盛的单位，使整体算力利用率从不足20%提升至65%以上。

全民证书电子认证集群基础设施有助于政务云集中部署电子政务系统和各委办厅局自建电子政务系统完成密评密改工作，为数字政府建设提供坚实的电子认证安全基础，支持跨部门的高效协同，切实保障电子政务服务连续性和数据安全性。

2.1.3 全民证书个人和企业电子印章云签服务

2025年9月国务院办公厅印发《电子印章管理办法》，电子印章服务基于密码技术和相关数字技术表征印章的特定格式数据，实现电子文件的可靠电子签名，符合规定的电子印章与实物印章具有同等法律效力。全民证书个人和企业电子印章云签服务提供电子印章的申请、制作、备案、使用、注销等服务，全过程保障电子印章使用安全合规和管理规范有序。

全民证书个人和企业电子印章与主体数字证书进行唯一绑定，主体在全民证书专用APP完成身份认证后，可进行电子印章申请、使用、注销等操作。全民证书个人和企业电子签章过程信息被记录并保存，实现电子签章行为可追溯、可定责。电子签章验证时，按照国家有关标准规范核验电子签章数据的真实性、完整

性、机密性和不可否认性，并提供电子印章状态信息查询服务，核验电子印章在电子签章时的有效性。

全民证书个人和企业电子印章云签服务可大幅提升个人和企业办公效率，打破地域限制，简化办公流程，显著降低企业运营成本，充分保障电子印章使用的安全性，稳步推进电子印章深入融合应用工作。

2.2 密码服务能力

为筑牢省级政务云密码安全底座，构建全场景、标准化、集约化的密码服务体系。政务云密码服务支撑平台立足政务场景合规需求，提供坚实的底层密码技术支撑；密码资源池化服务与全场景应用支撑通过资源整合与弹性调度，实现基础及扩展类密码服务的全域覆盖；密码服务一体化管理运营平台则聚焦多角色协同与全流程管控，打通自助服务、运营管理、运维监测与态势感知的全链路闭环，全面赋能政务数字化转型与安全保障。

2.2.1 政务云密码服务支撑平台

省级政务云已建成统一的密码云支撑平台，三大运营商联通、移动、电信已建设政务云密码资源池，为云上各委办局业务系统提供按需、弹性的密码服务。采用国产密码算法和通过国密认证的密码产品，为政务云平台及云上业务系统提供身份鉴别、数据保护、重要数据完整性、机密性保护等密码服务，具体包括数字证书服务、国密 SSL 证书服务、政务外网安全接入服务、浏览器密码服务、软件密码模块服务、加解密安全服务、时间戳服务、签名验签服务、身份认证服务、数据加密服务、电子签章服务、动态令牌身份认证服务等。辽宁在电子认证、电子印章、政务云密码资源池等方面迈出坚实步伐，全面支撑“一网通办”等政务服务。

2.2.2 密码资源池化服务与全场景应用支撑

统一密码服务通过部署服务器密码机、签名服务器等密码资源构成密码资源池，以密码资源池为硬件支撑，对各信息系统提供微服务形式的、标准化的独立密码服务及接口。支持丰富的密码算法、密码运算接口，能够为各业务系统提供标准合规的密码基础服务及多种类型密码应用服务。提供微服务形式的、标准化的独立密码服务及接口，涵盖加解密、签名验签等密码服务资源。支持使用经国家密码管理局批准的密码设备及 SM 系列密码算法并提供完善的对称密钥和非对称密钥管理应用体系，保障密钥管理生命周期中各环节的安全。

基础类密码服务：基于密码资源池和密钥管理服务基础设施，为租户提供基于业务场景如敏感文字加解密服务、签名验签服务、完整性保护服务等基础类密码服务，保证关键业务信息的机密性、真实性、完整性和不可否认性。

扩展类密码服务：除基础类密码服务之外，还提供扩展类密码服务，包括：

协同签名服务：为用户提供用户密钥、用户证书的统一管理、协同签名等服

务。通过密钥分割技术，保障移动端密钥安全。

电子签章服务：提供制章、盖章、验章等服务，为用户的 PDF、OFD 文档完成电子签章。将传统的实物印章转变为电子化防伪印章，保障文件的完整性、真实性、有效性和防篡改性。

时间戳服务：为单位/个人等用户提供精准、安全和可信的时间戳生成、验证、解析时间戳等服务。

数据库透明加密服务：提供应用免改造、灵活部署、安全性能高的数据加解密服务，解决数据库敏感数据面临的信息安全问题，实现数据库中数据机密性和完整性保护。

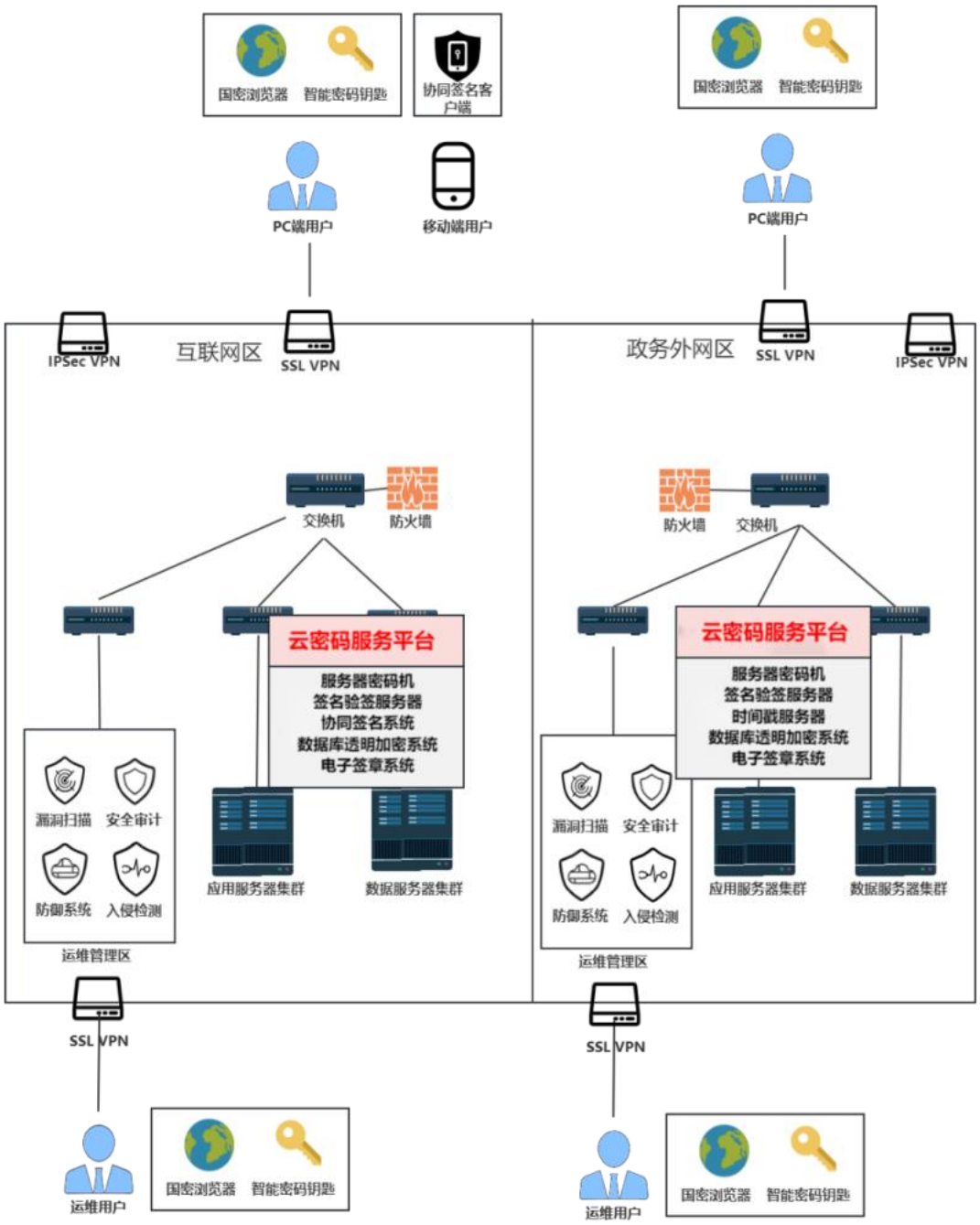
密码设备管理：密码设备管理主要包括云服务器密码机等密码设备的管理。采用密码资源池的概念通过管理系统实现对各类密码资源的统一设备管理。

密码资源配置：通过订单形式管理密码服务的申请信息，实现密码服务申请的资源统一配置管理。

密钥全生命周期管理：密钥管理服务提供密钥全生命周期管理服务，记录密钥全生命周期的操作管理日志，支持多维度的密钥管理。提供密钥的多重、多种方式分隔服务集。

订单管理：主要包括查询订单列表，为密码服务管理流转下来的订单进行密码服务申请的资源配置、密钥配置、服务反馈及详情查看、并反馈日志。

2.2.3 密码服务一体化管理运营平台



图三-2 密码服务管理平台

租户自助服务子系统：面向云租户，根据租户自身业务发展的需要，针对租户各类等级保护、安全保护、密评改造需求，一站式自助申请所需密码基础类服务及多类型扩展类密码服务，待分配资源后，通过标准的 RestfulAPI 文档进行系统对接，获取相应密码服务。

密码服务运营子系统：面向运营人员。解决日常租户密码服务订单申请及处理，包括快速响应、运营预警、售后服务和运营数据分析。

密码服务管理子系统：面向系统管理人员。系统初始化业务，包括计费方案

配置管理，预警模板、指标及推送方式管理，云密码服务平台录入管理和系统管理等。

密码服务运维子系统：面向运维人员，主要实现“监测、预警、管理、控制”。全面对系统进行监测、管理和业务控制，保障系统运行正常服务。加强了可视化仪表盘和可视化数据分析。

密码服务态势感知子系统：面向监管机构管理人员。密码态势感知系统目标实现事前持续预警、事中协同响应、事后回溯优化。通过数据采集，进行数据分析；及时响应处置；实时安全监测，提升密评密改的实际应用效能，充分发挥模型建模能力，基于大数据、人工智能技术，对指标建模分析、进行综合分析评估，生成密码应用综合态势感知指数，进行预测感知。

2.3 测评机构

省内国家授权的商用密码应用安全性评估（密评）机构情况。

按照国家密码管理局公告（第 53 号），辽宁省取得商用密码检测机构（商用密码应用安全性评估）资质的单位如下（排名不分先后）：

北方实验室（沈阳）股份有限公司　　联系人：韩晓娜 18602425836

沈阳赛宝科技服务有限责任公司　　联系人：王海洋 15640330085

辽宁牧龙科技有限公司　　联系人：周　菊 15640161677

大商所飞泰测试技术有限公司　　联系人：李婷婷 15041126359

（二）辽宁省密码产业发展重要举措

1. 我省政策引领产业发展

《辽宁省工业领域数据安全能力提升实施方案（2024—2026 年）》：由辽宁省工业和信息化厅印发，以推动辽宁省工业高质量发展为出发点，以构建完善工业领域数据安全保障体系为主线，提出了提升工业企业数据保护能力、提升数据安全监管能力、提升数据安全产业支撑能力等十项重点任务。其中明确推动各行业企业加强商用密码应用保护数据安全，鼓励数据安全服务商、基础电信运营商、工业互联网平台企业、专业测评机构、科研院所、密码企业等加强协作，开展产品研发和服务创新，推动工业企业开展密码应用安全性检测与评估，增强密码技术保障工业领域数据安全能力。

《2025 年辽宁省重点研发计划项目申报指南》：由辽宁省科学技术厅组织实施，以突破关键核心技术、培育创新型产业生态为目标，以支撑数字经济安全发展为核心导向，布局多项密码与数据安全领域重点研发任务。其中明确支持密态计算集群系统、密码智能化测评平台两大关键技术产品研发，通过“揭榜挂帅”模式引导创新资源集聚。密态计算集群系统项目揭榜成功，将构建基于密码学与可信硬件的全链路安全计算体系，实现数据“可用不可见”的跨主体可信流通，

破解高敏感数据融合利用难题，为金融、医疗、工业等领域提供低成本、规模化的数据安全处理能力。密码智能化测评平台项目揭榜成功，将融合人工智能与密码学专业技术，打造覆盖算法分析、协议设计、工程实现的全流程智能测评体系，提升密码产品安全性验证效率与精准度，降低密码技术应用门槛。两项技术成果的落地，将推动辽宁省密码产业从传统防护向智能安全升级，强化“政产学研用”协同创新机制，助力构建自主创新、安全可靠的密码与数据安全产业生态，为数字辽宁建设筑牢技术根基。

《辽宁省商用密码应用和安全性评估工作指南（试行）》（2025 年 4 月印发）：由辽宁省国家密码管理局牵头编制，联合多地市密码管理部门及省内密评机构、密码企业共同起草。该指南以国家相关法律法规和标准为依据，明确了重要网络与信息系统密码应用和安全性评估的范围、政策要求、建设流程、密评备案程序，细化了物理环境、网络通信、设备计算、应用数据等层面的密码应用措施，提供了常用密码产品应用指引、密评实施规范及常见问题解决方案，配套密码应用方案模板、备案信息表等实用工具，为省内各单位落实密码应用要求、密评机构开展评估工作提供全面操作指引。

《关于开展重要信息系统密码应用安全性评估工作的通知》〔辽密局发〔2019〕6 号〕：由辽宁省国家密码管理局印发，落实国家密码管理局专项检查要求，明确重要信息系统密码应用安全性评估的责任主体、实施流程和监管要求。规定关键信息基础设施、网络安全等级保护第三级及以上信息系统每年至少评估一次，责任单位需委托国家认定的测评机构开展评估，评估结果需向省密码管理局和公安厅备案，为省内密码应用评估工作划定操作规范。

《关于进一步加强政务信息化系统密码应用与安全性评估工作的通知》（辽密局发〔2020〕26 号）：由辽宁省国家密码管理局、辽宁省发展和改革委员会联合印发，聚焦非涉密政务信息系统安全防护。要求政务信息化项目落实密码应用“三同步”原则，项目审批阶段需提交密码应用方案并通过合规性审核，验收阶段需提供密码应用安全性评估报告，运行后定期开展评估，市级预算内资金建设项目参照执行，强化政务领域密码应用管理。

2. 政府统筹协调助力产业生态构建

辽宁省以政府统筹协调为核心抓手，围绕商用密码产业发展全链条，通过调研对接、会议交流、培训赋能、政企研学协同等多元举措，全方位搭建产业发展支撑体系，助力构建安全高效的商用密码产业生态。

2.1 搭建交流平台，促进产业协同联动

（1）成立辽宁省商用密码协会：辽宁省商用密码协会由北方实验室（沈阳）股份有限公司、沈阳东软系统集成工程有限公司、辽宁省信息产业发展公司、大连秘阵科技有限公司、丹东华通测控有限公司五家单位联合发起，于 2021 年 9

月获得辽宁省民政厅批准成立，业务主管部门为辽宁省国家密码管理局。

协会现有会员单位 127 家，已形成覆盖密码生产研发、咨询评估、电子认证、科研创新等多领域的会员体系。

协会秉持开放包容、合作共赢的理念，致力于为会员单位搭建优质高效的交流服务平台；积极宣传贯彻党和国家相关方针政策、法律法规，推动全省密码行业规范健康发展，维护公平有序的行业市场秩序；在业务主管单位指导下，协会搭建政企协同、产学研融合的沟通桥梁，构建辽宁商用密码协同发展生态圈，为辽宁省密码产业高质量发展注入强劲动力、贡献坚实力量。

图三-3 辽宁省商用密码协会成立大会

（2）商用密码应用推广交流会：2023 年 4 月 27 日，由省国家密码管理局指导，省商用密码协会主办的全省商用密码应用推广交流会在沈阳召开。会议以“国家安全、密码护航，助力辽宁全面振兴新突破三年行动”为主题，由国内密码领域专家、学者就密码政策、密码发展趋势、密码应用成效及密码应用安全性评估等方面作主题报告，密码应用服务单位结合密码应用场景作专题交流发言。各市国家密码管理局局长、相关业务部门负责同志和省（中）直各重要信息系统主管单位业务负责同志共计 120 余人参加会议。

图三-4 辽宁省商用密码应用推广交流会现场

（3）2023 商用密码大会参展：2023 年商用密码大会期间，辽宁省商用密码协会组织会员单位共同参展，本次大会集中展示我省在商用密码技术研发、产品创新、行业应用、统筹服务等领域的特色成果，与业内领军企业、权威专家展开深入交流，精准把握行业发展趋势与市场需求。此次参会有效拓宽了会员单位的发展视野，强化了省内外行业联动，为推动我省商用密码产业创新升级奠定了坚实基础。

图三-5 2023 全国商用密码大会

（4）“工业互联网+商用密码”专题论坛：2024 年 9 月 12 日，在全球工业互联网大会活动期间，由辽宁省国家密码管理局、省工业和信息化厅联合指导，省商用密码协会承办“工业互联网+商用密码”专题论坛沈阳举办，论坛以“密码技术赋能工业企业数字蝶变”，旨在推动密码技术与工业互联网深度融合，解决工业互联网核心安全问题。论坛紧扣当前工业互联网向新型工业化深度演进的核心需求，精准锚定工业企业数字化转型中的安全痛点，旨在以商用密码这一网络安全核心技术为抓手，推动其与工业互联网设备接入、数据传输、应用管理等全场景深度融合。与会嘉宾通过政策解读、技术分享、案例剖析等多种形式，深入探讨商用密码赋能工业互联网安全升级的路径与方案，为破解工业互联网核心安全问题提供思路借鉴，助力为工业企业数字化转型筑牢安全基因，护航区域工业经济高质量发展。

图三-6　2024“工业互联网+商用密码”专题论坛

2025 年 9 月 7 日，“2025 全球工业互联网大会—密码应用创新专题论坛”在辽宁沈阳成功举办，论坛以“筑牢密码安全防线，护航新型工业化”为主题，聚焦新型工业化进程中的核心安全需求，深入探讨商用密码应用技术创新与最佳实践，推动商用密码技术与新型工业化场景的深度融合。

图三-7　2025 辽宁省“工业互联网+商用密码”专题论坛

2.2 强化政策落地，完善行业规范体系

（1）关基单位专项培训：组织开展“关基单位网络安全能力建设与推进商用密码应用培训班”，邀请公安部关键信息基础设施保护中心、公安部保密科技测评中心等权威机构专家授课，围绕《关键信息基础设施安全保护条例》《密码法》等核心法规，从政策解读、合规要求、技术落地等维度开展系统培训。

图三-8　辽宁省关基单位商用密码应用培训班活动

（2）商密应用安全性评估实施指南研讨会：由辽宁省国家密码管理局牵头召开《辽宁省商密应用安全性评估实施指南（试行）》专题研讨会，本次会议聚焦商用密码应用安全性评估工作的痛点、难点问题，邀请沈阳市国家密码管理局、

大连市国家密码管理局、鞍山市国家密码管理局相关领导与技术骨干，以及商用密码领域权威专家、行业骨干企业代表共聚一堂。会议紧扣国家商用密码相关法规标准要求，深度结合辽宁省产业发展实际与企业应用需求，围绕评估流程优化、评估要点细化、评估标准落地等核心议题展开深入研讨。

图三-9　辽宁省商密应用安全性评估实施指南研讨会

2.3 推动产教融合，筑牢人才支撑根基

（1）校企合作交流座谈会：辽宁省国家密码管理局联合省教育厅组织座谈会，汇聚东北大学、大连理工大学等 11 所高校与 10 余家重点密码企业代表，围绕密码专业人才培养、科技创新协同、现代产业学院共建，探索“教学－科研－产业”一体化产教融合模式。

（2）商用密码研讨会：辽宁省国家密码管理局主办研讨会，张民局长主持，汇聚政企研学多方力量（7 所高校、16 家重点企业及省市密码管理局领导），聚焦“密码产业发展行动计划落地”“密码学科建设优化”“专项人才培养模式创新”三大议题，推动校企协同育人，破解人才缺口难题。

图三-10　辽宁省商用密码校企合作交流座谈会

2.4 加强宣传科普，营造良好发展氛围

（1）打造密码宣传教育平台（密码科普与红色教育展厅）：在辽宁省国家密码管理局指导下，省商用密码协会牵头筹建密码科普与红色教育展厅，展厅以“普及密码知识、筑牢安全防线、传承红色基因”为核心，整合政策解读、技术科普、红色教育、互动体验功能，普及密码重要作用，厚植爱国主义情怀。

图三-11　辽宁省密码科普与红色教育展厅

图三-12　辽宁省密码科普与红色教育展厅

（2）2025 物联网密码学术会议落地辽宁：2025 年 8 月，中国密码学会物联网专委会“2025 物联网密码学术会议”在沈阳举办，本次会议聚焦人工智能、低空经济、车联网等领域密码应用，邀请知名院士、专家、学者齐聚辽宁，共同推动学术成果向产业转化，强化辽宁在物联网密码领域的学术氛围与产业竞争力。

图三-13　2025 物联网密码学术会议

图三-14　2025 物联网密码学术会议合影

（3）2025 密码应用与创新发展高级研修班：2025 年 12 月 10 日—12 日，由辽宁省国家密码管理局指导，辽宁省商用密码协会主办的 2025 密码应用与创新发展高级研修班在沈阳开班，本次研修班是辽宁省人力资源和社会保障厅“2025 年专业技术人才知识更新工程高级研修项目”，是实施专业技术人才知识更新工程的重要内容，是培养造就高素质专业技术人才队伍的重要平台，是提升专业技术人才能力的重要抓手。

研修班紧扣研修主题，邀请行业权威专家授课，采用专题授课、案例研讨、攻防场景演示等多种形式进行研修，充分发挥高级研修项目的示范引领作用。来自辽宁省内企事业单位、高校、医疗、金融、关键信息基础设施运营单位等 90 余家单位的 130 余名专业技术人员参加研修，共有 121 名学员成绩合格，并获得《辽宁省专业技术人员继续教育证书》，该证书作为其个人专业技术经历和接受继续教育的重要证明。

图三-15　2025 密码应用与科技创新发展高级研修班合影

第四章 商用密码应用及案例

本章介绍商用密码应用及案例，包括政务云建设模式，我省商用密码从重要行业领域应用到与新技术的融合应用情况，最后提供行业领域典型案例为开展密码应用工作提供参考。不同行业的业务特性决定了该领域下商用密码的算法选型、产品形态、部署架构存在差异。

（一）商用密码应用指引

1. 各方职责

商用密码建设实施主要由监管方（密码管理部门）、需求方、网络运营者（供给方）和检测方四类主体构成。其中，监管方依据国家政策法规对商用密码产品与服务进行合规监管；需求方指网络与信息系统运营者，负责使用商用密码保障信息安全；供给方提供密码产品与技术服务的各类企业；检测方则负责对密码产品及系统进行检测与评估，确保符合国家标准。

1.1 监管方

监管方主要指国家及地方各级密码管理部门。根据《密码法》和《商用密码管理条例》，国家密码管理部门负责管理全国的密码工作，县级以上地方各级密码管理部门则负责管理本行政区域的密码工作。

辽宁省国家密码管理局是负责全省商用密码工作的主管机构，其主要职责包括：拟定全省商用密码工作规划，向社会提供商用密码法律和政策服务，负责全省商用密码的科研、生产、销售、测评认证、使用及进出口等相关工作，并监督管理全省商用密码工作，查处违法行为。辽宁省内各市，如大连、鞍山、抚顺等地均设有市级密码管理局，共同构成覆盖全省的商用密码管理网络。

密码管理部门会同网信、商务、市场监管等有关部门建立协作机制，推进商用密码监督管理与社会信用体系相衔接，并依法对商用密码活动进行监督检查。

1.2 需求方

需求方是指网络与信息系统的运营者，特别是关键信息基础设施的运营者。他们有责任依法使用商用密码保护其系统安全。

需求方的主要义务体现在网络与信息系统的规划、建设、运行三个阶段，并需落实三同步一评估原则：

规划阶段：运营者需制定商用密码应用方案，并自行或委托检测机构对该方案进行安全性评估。评估通过后，方案才能作为建设依据。

建设阶段：应严格按照通过评估的密码应用方案进行建设。系统建成后、投入运行前，必须再次进行商用密码应用安全性评估，评估不通过不得投入运行。

运行阶段：系统运行后，每年至少开展一次商用密码应用安全性评估。评估

结果需按国家规定向主管部门及所在地密码管理部门备案。发生涉及密码的重大安全事件或系统重大调整时，也需及时开展评估。

此外，运营者还需建立健全密码使用管理制度，配备必要的密码专业人员进行密钥管理、密码操作和安全审计，并对这些人员进行安全背景审查和定期培训，同时落实相关经费保障。

1.3 供给方

供给方是指提供商用密码产品、服务和集成建设的各类企业，主要包括密码产品开发生产商、密码系统集成商和密码服务提供商。

密码产品开发生产商：从事密码软件、密码芯片、密码模块、密码整机等产品的开发、生产和销售。其产品品种和型号需经国家密码管理局批准，所采用的密码算法需为国家密码管理局认可的算法。产品需经检测认证合格后方可销售。

密码系统集成商：负责按照通过密评的密码应用方案，为用户实施密码保障系统的集成建设，确保密码应用的正确性和有效性。

密码服务提供商：典型代表是电子认证服务机构，需依法取得相应资质，为政务活动、企业和个人提供电子签名、身份认证等服务。

辽宁省密码管理局会对本省的商用密码企业进行调研和指导。供给方积极参与行业协会交流，提升技术能力，并可申报政府专项密码建设工作，促进商用密码产业发展。

1.4 检测方

检测方是指经国家密码管理部门认定，取得商用密码检测机构资质的专业机构。它们负责对商用密码产品进行检测，并对信息系统进行商用密码应用安全性评估（密评）。

检测机构须具备法人资格，拥有相适应的资金、场所、设备设施、专业人员和专业能力，以及有效的管理体系。其主要工作包括：

含有密码技术的产品密码检测：依据标准对商用密码产品的功能、性能、合规性等进行检测。

商用密码应用安全性评估：对信息系统的密码应用方案进行评估，并对建设完成的信息系统进行现场测评，评估其密码应用的合规性、正确性和有效性。

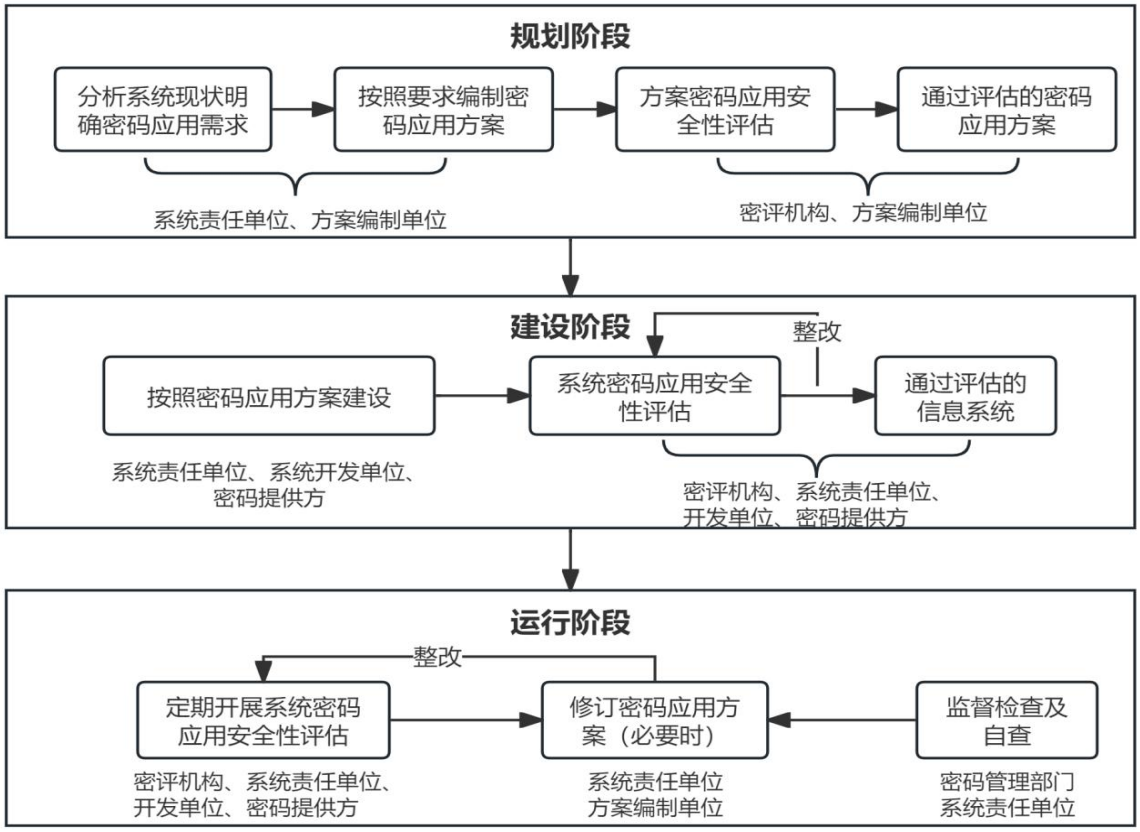
其他工作：参与制定检测标准、研制检测工具、提供密码技术咨询与培训等。

检测机构独立、公正、科学、诚信地开展检测评估活动，并对结果负责，同时承担保密义务。密码管理部门会对检测机构及其活动进行监督管理。

2. 商用密码应用实施过程

重要网络与信息系统商用密码应用工作包括三个阶段：规划阶段、建设阶段、运行阶段。同时，密评工作贯穿系统的规划、建设和运行各阶段。实施过程如下

图所示。



图四-1 商用密码应用实施过程

密码应用安全建设过程涉及的各方包括信息系统责任单位、密码管理部门、密评机构等。

信息系统责任单位是指信息系统运营者，包括信息系统建设、使用、管理单位。作为信息系统密码应用安全的责任主体，应负责信息系统密码应用安全的规划、建设、运行等总体工作；

国家密码管理部门负责监督、指导和检查全国的商用密码应用安全工作；省（部）密码管理部门负责监督、指导和检查本地区、本部门、本行业（系统）的密评工作；

密评机构是商用密码检测机构（商用密码应用安全性评估业务）的简称，具体是密评的承担单位，应当按照有关法律法规和标准要求科学、公正地开展评估；

密码提供方是指密码基础设施、密码服务等密码技术资源提供者，可供给信息系统密码应用建设、密码应用改造的各类密码资源，为信息系统的密码应用安全提供充足的密码服务类型。

2.1 规划阶段

（1）密码应用方案编制

信息系统责任单位在编制项目建议书、可行性研究报告与初步设计方案时，应当按照 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以

下简称《密码应用基本要求》）、GB/T 43207-2023《信息安全技术 信息系统密码应用设计指南》（以下简称《密码应用设计指南》）和密码应用方案模板，同步编制单独的密码应用方案。密码应用方案的质量直接影响密码应用效果，各单位应选择专业服务机构进行密码应用方案的编制。

（2）密码应用方案的评估

信息系统责任单位应当委托密评机构对密码应用方案进行评估。密码应用方案通过密评并完成备案，为项目立项的前置审核条件。密码应用方案未通过密评的，不得作为商用密码保障系统的建设依据。

2.2 建设阶段

（1）系统建设实施

信息系统责任单位按照通过密评的密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。密码设备选型应选择通过国家密码管理部门检测认证的商用密码产品及许可的密码服务。

（2）系统密评和验收

在重要网络与信息系统运行前，信息系统责任单位应当委托密评机构对系统进行密评，并完成密评结果材料备案，密评结果与备案回执作为项目验收的前置审核材料。如系统未通过密评，信息系统责任单位应针对评估中发现的安全问题及时整改，整改期间不得投入运行。整改完成后需进行复评，复评仍未通过的，则该项目不得进行验收。

2.3 运行阶段

（1）定期评估

重要网络与信息系统建成后的运行阶段，信息系统责任单位应定期（每年至少一次）开展密评，对于通过密评的系统，信息系统责任单位应及时完成密评结果材料备案；对于未通过密评的系统，信息系统责任单位应针对评估中发现的安全问题及时整改，整改完成后进行复评与初评结果材料备案。通过密评是项目运维经费审批的重要条件。

（2）应急评估

在系统运行期间，信息系统发现密码相关重大安全事件、重大密码安全隐患或者特殊紧急情况的，信息系统责任单位应当及时向所在地区密码管理部门报告，并启动应急处置方案，必要时需重新开展密评。

（二）政务云建设模式

随着信息技术的发展，云计算已经被广泛应用。为降低系统成本，打通数据融合，越来越多的政府及事业单位的系统选择部署在云上。云计算技术融合了软硬件资源，采用了虚拟化技术，主机边界和网络边界相对于传统数据中心来讲变

得非常模糊，风险不但来自南北流量，还来自东西流量，部署在云平台上的系统，其安全风险也随之增加。

政务云是数字政府建设的核心基础设施，在政务领域全面推行商用密码应用，是保障数字政府安全基座、维护国家网络空间主权的关键举措，《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）要求项目建设单位应当充分依托云服务资源开展集约化建设。《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）要求，强化政务云平台支撑能力，将国务院各部门政务云纳入全国一体化政务云平台体系统筹管理；各地区按照省级统筹原则开展政务云建设，集约提供政务云服务。

政务云的密码应用建设模式，直接关系到密码保障体系的整体效能、管理成本与长期可持续性。其密码应用模式根据系统部署方式的不同，可分为云集中部署与自建系统两种典型模式。二者在建设思路、实施路径和运营效果上存在显著差异。

1. 云集中部署模式

该模式遵循“统一规划、集约建设、服务化供给”的核心原则，将密码资源作为政务云的基础公共能力进行集中建设与管理。其核心是将密码硬件资源在云数据中心层面进行物理集中与虚拟化池化，形成统一的密码资源池。在此基础上，通过开发标准化的服务接口，向云上各业务部门提供按需申请、弹性伸缩的密码服务，实现密码能力的即开即用。该模式特别适用于省、市级大型政务云平台，以及追求高标准安全、强协同效应和低成本高效运营的数字化应用场景。

该部署模式主要特点包括：（1）效能最大化：避免了各部门重复采购密码设备，极大地提升了高端密码设备的利用率，降低了总体投资成本；（2）安全性强：由云运营方组建专业团队进行统一的密码设备运维、密钥全生命周期管理和策略制定，能够实施最高标准、全局一致的安全防护与合规性审计；（3）促进业务协同：为跨部门、跨层级的数据安全共享与业务协同提供了统一的信任基础，所有基于该平台的服务使用统一的密码标准与信任体系，天然打破了信任孤岛；（4）简化应用开发：业务应用部门无需关注底层复杂的密码技术实现，只需调用标准化服务接口即可快速获得高等级密码保护，显著降低了应用系统的开发门槛与集成难度。

2. 应用自建模式

该模式表现为“谁建设、谁管理”，由各业务应用单位自行采购、部署和管理所需的密码设备与服务。在此模式下，密码能力并非作为云平台的底层公共服务，而是作为业务系统的一个独立组成部分。每个业务系统根据自身的安全等级保护要求和功能需求，独立规划密码应用方案，单独采购并维护专用的密码硬件

或软件，以满足其特定的身份认证、数据传输加密等安全需求。该模式通常出现在政务云发展早期、对密码有极端特殊需求（如涉及国家秘密的特定专网系统），或尚未被全面纳入集约化云平台管理的遗留系统中。

该部署模式主要特点包括：（1）灵活性与自主性高：业务部门对自身密码系统的选型、部署和运维拥有完全自主权，能够快速响应某些特殊或临时的业务需求；（2）权责边界清晰：密码安全的责任主体明确，与应用系统的责任主体一致，避免了可能出现的责任推诿；（3）易形成资源浪费与安全短板：容易导致密码设备分散采购、利用率低下，造成财政资金浪费。同时，各部门技术能力不均，密码配置和管理水平参差不齐，容易形成安全短板，整体安全水位由最薄弱的环节决定；（4）加剧信任壁垒：各系统采用不同的密码技术路线和信任根，密钥管理体系互不相通，为跨系统、跨部门的数据安全流通与业务协同制造了巨大的技术障碍。

（三）电子印章应用

1. 政务场景下电子印章应用

在政务场景下应用场景纵向覆盖省、市、县、乡、村五级政务用印场景的密码服务下沉；横向覆盖行政审批、公文流转、公共服务、电子证照签发等核心业务的密码应用。系统通过商用密码应用安全性评估的关键整改与优化措施。

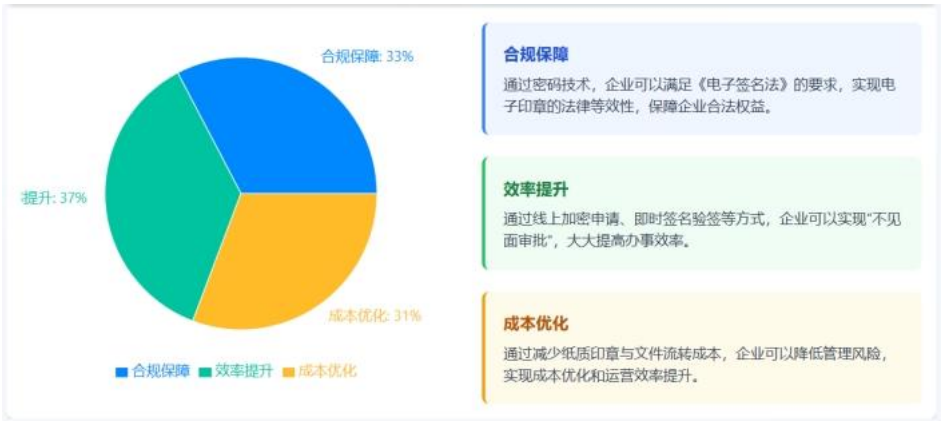
关键环节密码技术落地包括：（1）身份认证：基于数字证书的机构与人员强身份核验流程，防止身份假冒；（2）申请制作：印章信息加密传输、模板数据签名保护，确保源头安全；（3）签章使用：数字签名与时间戳结合，保障电子文件不可篡改、来源可追溯；（4）备案监管：与公安厅系统实时同步加密的印章全生命周期数据，实现闭环管控。

图四-2　系统通过商用密码应用安全性评估的关键整改与优化措施

2. 企业场景下电子印章应用

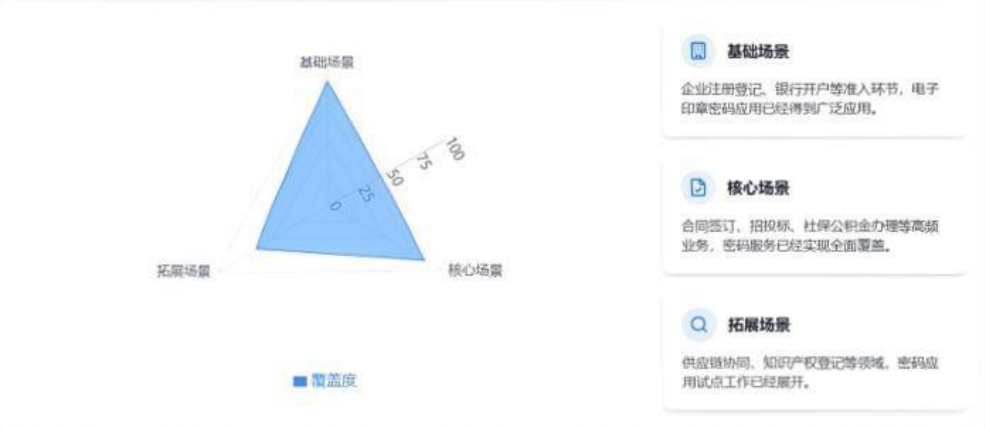
针对中小微企业的特点，电子印章应用在企业场景设计了轻量化、低成本的密码应用接入模式。中小微企业可以以较低的成本接入密码应用，享受到密码技术带来的便利和效益。一方面将印章备案纳入“一网通办”，新办企业可以同步在线申领印章，节约了时间成本。企业可以更加便捷地完成开办手续，提高了企业的开办效率。另一方面开发 APP、服务平台等查验功能，支持政府、金融机构、企业等主体的印章真伪核验，为打击印章违法犯罪奠定了基础。这样可以有效防范印章违法犯罪行为，保障了企业的合法权益。

通过密码技术，企业可以满足《中华人民共和国电子签名法》的要求，实现电子印章的法律等效性。企业在进行电子合同签订、电子招投标等活动时，可以确保电子印章的法律效力，保障了企业的合法权益。通过线上加密申请、即时签名验签等方式，企业可以实现“不见面审批”，大大提高了办事效率。这样，企业可以节省大量的时间和人力成本，提高了企业的运营效率。通过减少纸质印章与文件流转成本，企业可以降低管理风险，实现成本优化。企业可以减少大量的纸质文件存储和管理成本，降低了企业的运营成本。



图四-3　电子印章应用价值示意

电子认证服务在企业场景下应用包括：（1）基础场景：在企业注册登记、银行开户等准入环节，电子印章密码应用已经得到广泛应用。通过密码技术，企业可以在线完成注册登记、银行开户等手续，提高了办事效率，降低了办事成本；（2）核心场景：合同签订、招投标、社保公积金办理等高频业务，密码服务已经实现全面覆盖。企业可以通过线上加密申请、即时签名验签等方式，实现不见面审批，大大提高了办事效率；（3）拓展场景：在供应链协同、知识产权登记等领域，密码应用试点工作已经展开。通过密码技术，企业可以实现供应链协同、知识产权登记等业务的在线办理，进一步提高了办事效率，降低了办事成本。



图四-4　电子认证服务应用场景覆盖度

（四）新技术与商用密码融合应用

随着数字化进程的深入，商用密码技术与云计算、区块链、零信任等新兴技术的融合已成为保障网络空间安全的必然要求。这种融合不仅带来了技术革新，也面临着从技术、产品、部署、运维到监管各个层面的挑战。本文将系统探讨商用密码与主要新兴技术的融合路径、实践案例与发展趋势。

1. 云计算与商用密码

云计算掀起了信息产业变革的浪潮，它的快速发展给政府、企业和个人带来了巨大的创新潜力，但浪潮背后也面临着一些新的障碍和挑战，其中安全方面的挑战是目前云计算在大规模推广、部署过程中用户关注的首要问题。由于计算模式的差异和新技术的采用，云计算面临着技术、管理和法律风险三个方面的新挑战。

在云端，由于 IT 资源高度集中，会导致风险的集中甚至放大，事故一旦发生影响范围广，后果严重。此外，在云中，因为虚拟化技术的大量应用，使得传统基于物理安全边界的防护机制在云计算的环境中难以得到有效的应用，这些都将带来一系列突出的安全风险。由于云计算数据的管理权和所有权是分离的，这就对客户和服务提供商之间在安全协同和管理方面提出了新的挑战。地域及监管方面的问题导致法律风险的存在。云计算应用数据的特点是对地域依赖性弱，信息流动性大，使得在信息安全监管、隐私保护等方面产生了新的需求。

云密码服务的发展是伴随着云计算应用的不断推进而不断发展。在公有云发展和逐步成熟的进程中，公有云运营商首先提供了密钥管理、数据加密等云密码服务；随着 SaaS 服务的兴起，一些面向公众的以密码技术为安全基础的 SaaS 服务被推出，如身份认证服务、电子合同服务等；另外，传统的密码产品厂商也顺应产品云服务化的需要，推出了一些适合云中部署的产品和服务，为云运营商或云用户提供密码技术解决方案，如密码资源池、云安全访问代理（CASB）服务等。目前主要云密码服务有传输加密、存储加密、单点登录、安全隔离/交换、

数据签名、云电子签名服务等。

辽宁省级政务云已建成统一密码云平台，通过国产密码算法和认证产品构建资源池，为云上政务系统提供数字证书、国密 SSL 等多元密码服务，支撑“一网通办”等政务服务安全落地。

2. 大数据与商用密码

在大数据环境中，商用密码技术为数据全生命周期安全提供了保障。通过数据加密、数字签名、访问控制等措施，商用密码有效保护了大数据在采集、传输、存储和使用过程中的安全性。基于密码学的隐私计算技术（如安全多方计算、同态加密等）可以在不共享明文数据的情况下实现多方数据联合计算，促进数据要素的安全流通与价值释放。

在大数据背景下，可信数字身份认证成为一种重要的安全认证手段。利用商用密码可以实现多种数字身份认证技术，如智能 IC 卡、移动手机盾、智能密码钥匙 USBKEY 等，为用户提供安全、便捷的身份认证方式。对于电子商务、移动支付等领域的安全保障至关重要。

3. 区块链与商用密码

区块链技术是一种被称为分布式账本技术的互联网数据库技术，是又一项颠覆性的应用技术。区块链结合密码学技术，可以保证交易的可追溯性、不可篡改性、不可否认性和不可伪造性，支持数据安全共享和大规模协同计算，也可实现对用户身份和机密数据的隐私保护，更适用于需要高隐私性和安全性的分布式应用场景中。

其中可追溯性是指交易的每次变更都会按照时间顺序记录在区块链上，前后关联，可以查询交易从发布源头到最新状态间的整个变更流程。不可篡改性和不可否认性指交易等数据一经验证达成共识被写入区块链后，任何人无法对数据进行修改和抵赖。不可伪造性指任何人无法通过有效手段伪造可通过矿工验证的交易，更无法伪造整笔交易变更记录。相比传统的中心化数据库，利用哈希函数的单向性和耐碰撞性、数字签名的防伪认证功能和分布式共识的容错能力，区块链极大增加了攻击者恶意篡改、伪造和否认数据操作的攻击难度和成本，有效提升数据的安全性。

4. 零信任架构与商用密码

零信任是一种全新的安全理念，它对网络安全进行了范式上的颠覆，打破了网络边界的概念，引导网络安全体系架构从网络中心化向身份中心化的转变，实现对用户、设备和应用的全面、动态、智能访问控制，建立应用层面的安全防护体系。

零信任总体架构的核心是密码支撑体系，对其不同对象提供基于国产商用密

码算法支撑的数字证书管理服务，依托密码支撑体系，通过身份认证管理中心，对不同对象进行规范化统一管理，从而实现颗粒度授权管理与鉴权，并实现安全审计服务。在零信任网络环境下，以密码支撑体系和可信身份管控平台对接网关管理平台，实现安全控制服务。通过基于密码态势感知服务，建设安全管理中心。

5. 人工智能与商用密码

人工智能（AI）是新一轮科技革命和产业变革的重要驱动力量，是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。人工智能的研究范围十分广泛，包括机器人、语言识别、图像识别、自然语言处理、专家系统、机器学习，计算机视觉等。人工智能应用已经发展到计算机科学、金融贸易、医药、诊断、重工业、运输、远程通讯、在线和电话服务、法律、科学发现、玩具和游戏、音乐等诸多领域。

人工智能与商用密码呈现双向赋能趋势。一方面，密码技术为 AI 模型训练数据和核心算法提供安全加固和隐私保护，如同态加密技术可在密文状态下进行模型训练，有效防止原始数据泄露。另一方面，AI 技术也可用于增强密码系统的安全性，如通过机器学习提升异常检测能力，或利用神经网络改进密码算法的实现效率。随着大模型技术的快速发展，商用密码在保护训练数据隐私和模型安全方面的重要性日益凸显，预示着两者深度融合的未来发展方向。

6. 5G与商用密码

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。商用密码作为安全的重要内核，在 5G 中的作用越来越凸显。5G 网络与各行业的深度融合对密码技术提出了新的需求。5G 环境中的海量物联网设备连接、网络切片安全以及低时延高可靠通信场景，需要轻量化、高性能的商用密码算法支持。

中国电信研究院等机构已发布基于国密算法的 5G 专网方案，探索了商用密码在独立、下沉、虚拟三种专网模式下的应用，实现了国产商用密码在 5G 关键环节的全覆盖。未来，商用密码在 5G 中的应用将继续深入发展。随着技术的不断进步和应用场景的不断拓展，商用密码将在保障 5G 网络安全、促进产业数字化转型、数字产业化等方面发挥更加重要的作用。

中国移动辽宁公司打造基于国密算法的 5G 可信专网，实现终端与核心网双向认证，通过 ZUC 算法保障信令和数据传输安全，已为党政机关、科研院所等提供高安全通信服务。

7. 二维码与商用密码

二维码是一种用特定几何图形按规律在二维平面上分布的图形，用来记录数据符号信息，可将文字、网址、数字等信息通过特定的编码转换成二维码图案，

成为连接物理世界和数字世界的超级桥梁，已经深刻地改变了我们的生活方式和社会运行模式。同时随着二维码深入融入生活和工作的方方面面，安全问题也日益凸显。

二维码安全问题成因从技术层面分析，现有二维码技术国家标准主要聚焦于二维码的数据结构和编码规范，并未考虑安全性设计。目前，大多数二维码采用通用编码格式，没有强制要求使用密码技术进行保护，任何人都可以通过网络免费生成。从管理层面分析，目前我国尚未建立统一的二维码安全国家标准。同时，二维码的使用场景复杂多样，涉及多个部门和领域，监管职责分散，存在监管空白和交叉问题，使得一些安全问题难以及时发现和处理。从用户层面分析，由于肉眼无法分辨二维码内容的技术特性，伪造的二维码与正品码在图形呈现上完全一致，许多用户在扫描二维码时缺乏警惕性、容易受到虚假信息和利益诱惑的欺骗。

密码作为维护网络和信息安全的关键核心技术，能够在构建二维码可信性、真实性和安全性等方面发挥重要作用。在商用密码与二维码融合的新兴领域，我省企业沈阳安创信息科技有限公司正在应用其具有完全自主知识产权的新一代安全二维码 Security2image 技术（以下简称 S2i 码），在数字内容保护与信息安全防伪追溯方面积极探索与密码技术融合应用，推动产品迭代，适应行业变化，符合未来二维码市场的安全性需求。

沈阳安创信息科技有限公司将 S2i 码与国密算法结合，开发新一代安全二维码技术，在跨境电商防伪溯源、政务证件认证等场景应用，实现二维码生成、使用、监管全生命周期安全防护。

8. 低空经济与商用密码

商用密码技术是低空经济安全发展的核心保障。低空经济以无人机、电动垂直起降飞行器等航空器为载体，涵盖物流配送、巡检监测、农业植保等多元化场景，其通信链路、控制指令和采集数据均面临篡改、劫持或泄漏风险。商用密码通过数字证书和 PKI 体系为无人机、地面站及操作人员提供身份认证与访问控制，确保只有合法实体能接入系统；同时利用加密算法保护传输数据的机密性与完整性，防止敏感信息被窃取或篡改。例如，在物流无人机场景中，密码技术可加密货物信息并验证配送路线指令；在电力巡检等工业场景中，它能保障采集数据的安全可靠。

低空经济的本质是空域资源数字化，而地理空间信息等核心数据涉及国家安全，需构建全链条防护体系。在具体应用中，密码技术助力应对低空经济发展中通信安全、数据加密、身份认证和空域协同方面的更高要求。随着低空经济规模持续扩大，商用密码的应用将进一步拓展至城市空中交通等复杂场景，为产业健康发展筑牢安全基石。

辽宁正探索商用密码在低空经济领域的应用，通过数字证书和 PKI 体系为无人机、地面站提供身份认证，利用加密算法保护通信链路和采集数据，为物流配送、电力巡检等低空场景筑牢安全防线。

（五）商用密码在各领域应用

1. 政务领域

商用密码在政务领域案例以高安全合规为核心，构建政务数据可信体系。政务领域的核心风险是“敏感数据泄露、业务身份伪造、数据篡改”，需依托商用密码实现“身份可信、数据加密、操作可追溯”，且需符合《电子政务电子认证服务管理办法》等合规要求。

电子政务网安全应用通过 SM4 加密以及 SM2 身份认证，保障传输与接入安全。具体来说，政务内网（处理涉密信息）、外网（处理非涉密公开信息）的传输层安全，需通过商用密码 VPN 实现：（1）数据传输加密：采用 SM4 分组密码对传输的政务数据进行加密，加密模式选用 CBC 模式，避免数据在传输中被窃听；（2）设备身份认证：采用 SM2 椭圆曲线密码实现政务终端与网络的双向认证，终端内置商用密码 USBKey，接入网络时向网关发送 SM2 签名的身份信息，网关通过 SM2 公钥验证签名，拒绝非法设备接入。

电子证照与电子印章应用体系，采用 SM2 椭圆曲线公钥密码算法实施数字签名，依托 SM3 密码杂凑算法开展哈希校验，从技术底层构建可信认证机制，确保电子证照生成、传输、存储全生命周期的完整性与不可篡改性。具体来说，电子证照的核心需求是“来源真实、内容未改、责任可追”，技术方案需结合密码签名与哈希算法：（1）电子证照生成：先对证照原文用 SM3 密码哈希算法计算哈希值，再用政务部门的 SM2 私钥对哈希值签名，最终将“证照原文+数字签名+SM2 公钥”打包为电子证照；（2）电子证照验证：接收方先提取 SM2 公钥，对数字签名解密得到哈希值，再对证照原文重新计算 SM2 哈希值，两者一致则证明来自合法机构、内容未被篡改；（3）电子印章：本质是绑定印章主体身份的数字签名，其中印章图像需用 SM2 私钥签名，且印章使用时需通过商用密码印章服务器校验使用权限，防止印章伪造或滥用。

政务云安全应用通过 SM4 存储加密以及密钥管理系统，保障云端数据隔离。具体来说，政务数据存储在政务云时，需解决“云服务商越权访问、物理硬盘被盗”的风险：（1）数据存储加密：采用 SM4 模式对政务数据进行加密存储，每个数据块生成独立的加密密钥，云服务商仅能管理密文数据，无法获取明文；（2）密钥安全管理：SM4 加密密钥需存储在硬件安全模块 HSM（符合 GM/T0013 标准的密码硬件，防物理破解）中，调用密钥时需通过 SM2 身份认证，避免密钥泄露导致加密失效。

2. 金融保险领域

商用密码在金融领域案例以高可用、低延迟为核心，守护资金与交易安全。金融领域的业务特点是“交易频次高、对延迟敏感（如支付需≤100ms）、容错率低”，商用密码需要在安全与性能间平衡，核心采用“对称算法为主、非对称算法为辅”的架构。

支付结算安全应用通过 SM4 会话加密以及 SM2 身份认证，实现交易端到端安全。具体来说不同支付场景的密码技术选型差异显著，需结合交易规模与安全需求适配。在银行卡交易方面，芯片卡内置商用密码安全芯片（符合 GM/T 0016 标准），采用 SM4 对称算法加密存储持卡人敏感信息。交易时首先卡片与 POS 机通过 SM2 实现双向认证，生成临时 SM4 会话密钥。之后交易数据用 SM4 加密后传输，避免克隆卡盗刷。在移动支付（扫码/NFC）方面，支付指令需经过两层加密首先应用层用 SM4 加密支付指令（对称算法，满足低延迟），与之对应的传输层通过“商用密码 SSL 证书”（基于 SM2 算法）实现 HTTPS 加密（替代传统 RSA 证书），防止支付指令在网络中被篡改。支付完成后，用户手机的 SM2 私钥对交易记录签名，作为用户确认支付的法律依据（符合《中华人民共和国电子签名法》）。

金融数据安全通过 SM4 存储加密以及 SM3 完整性校验，保护客户敏感信息。具体来说，银行、证券等机构的核心数据需满足《个人金融信息保护技术规范》，技术方案需覆盖“传输－存储－使用”全环节。当客户通过手机银行查询账户时，数据（如余额、流水）用 SM4 加密传输（搭配 TLS1.3 协议，基于 SM2 证书），防止 Wi-Fi 窃听。当存储加密时核心数据库采用 SM4 透明加密，敏感字段加密存储，仅授权查询时解密。当每日对账时，对交易流水用 SM3 计算哈希值，与总行备份的哈希值比对，若不一致则定位篡改记录。

金融设备安全应用通过 SM1 硬件加密以及身份认证，防范设备被劫持。具体来说，ATM 机、自助终端、加密机等专用设备需通过硬件级密码防护防止物理或逻辑攻击。对于 TM 机，密码键盘内置 SM1 对称算法（非公开算法，仅用于硬件加密，安全性高于 SM4），用户输入 PIN 码时直接在键盘内加密，加密后的密文传输至 ATM 主机，避免 PIN 码被键盘劫持软件窃取。对于金融加密机，符合 GM/T 0028 标准，内置 HSM 模块，所有交易的 SM4 密钥生成、SM2 签名均在加密机内完成，外部系统无法接触密钥。

3. 教育领域

教育领域的核心安全需求集中在师生身份认证、学籍与科研数据保护、在线教学与考试安全等场景。

身份认证与系统访问安全，教育行业的网络培训平台、学籍管理系统等常服务于海量用户，身份冒用风险突出。通过构建基于国密算法的数字证书认证体系，

可实现多端安全登录与跨平台身份互认。为业务系统用户配置国密数字证书后，PC 端与移动端均能完成安全登录，移动端用户还可通过扫码认证替代传统硬件介质，在提升登录便捷性的同时，通过强身份认证杜绝账号盗用，满足教育行业多系统协同的安全需求。

学籍与科研数据安全防护，学籍信息、招生录取数据、科研成果等核心敏感数据，需通过全流程加密保障机密性与完整性。采用数据库加密设备、服务器密码机等产品，可对学籍数据库的敏感字段进行加密存储，仅授权人员查询时解密，不影响日常教学管理业务；针对科研项目数据，通过硬件级加密能力实现实验数据、研究成果的加密传输与存储，防止数据泄露或篡改。

在线教学与考试安全保障，线上教学、远程考试等场景需兼顾数据传输安全与操作不可否认性。通过“加密传输+电子签名”组合方案，可筑牢安全防线。考生登录远程考试系统时，通过数字证书完成身份核验，答题数据经 SM4 算法加密传输，避免窃听或篡改；考试结束后，考生提交的试卷通过 SM2 算法电子签名，作为答题行为的不可否认凭证，保障考试公平性。这类方案已在高校在线考试、职业技能培训等场景广泛应用，实现了便捷性与安全性的平衡。

4. 医疗领域

医疗卫生领域的敏感数据承载着生命健康与隐私价值，电子病历篡改、患者信息泄露等风险日益凸显。密码技术作为信息安全的核心手段，正从数据存储、传输到业务操作的全流程，为医疗安全筑牢防线，其应用场景与解决方案已成为行业刚需。

电子病历与处方管理是密码应用的核心场景。病历与处方的真实性、完整性直接关系诊疗安全，传统纸质方式已难以适配数字化需求。通过非对称加密算法进行数字签名，医生签署诊断报告或处方时，算法会生成专属加密标识，接收方凭公钥即可验证内容未被篡改；同时结合哈希函数对数据进行处理，生成固定长度的哈希值，一旦数据被修改，哈希值将发生显著变化，可快速发现异常，确保医疗文件的法律有效性与可信度。

远程医疗与数据传输场景则迫切需要密码技术保障隐私。患者向远程医生传输健康信息、医院与医保系统交互数据时，数据在网络中易被窃取。对称加密算法因效率高的特性，可对海量传输数据进行实时加密；配合数字证书建立安全通信通道，实现双方身份的严格核验，确保只有授权方才能解密查看数据，既保障诊疗连续性，又守住患者隐私底线。

医疗数据存储与设备安全同样离不开密码防护。医院数据库中存储的海量患者信息，需通过对称加密算法进行加密存储，防止未授权访问导致的泄露。在医疗影像设备、智能监护设备等终端，安全芯片可硬件级存储加密密钥，从数据采集源头进行加密处理，即便设备被非法获取，数据也无法被轻易读取，形成全链

路安全保障。

在政策合规层面，《密码法》《医疗卫生机构网络安全管理办法》等已明确要求医疗行业应用密码技术。无论是在线挂号的身份认证，还是电子签约的抗抵赖需求，密码技术都通过加密保护、身份核验等核心能力，实现医疗数据“防泄露、防篡改、防假冒”，既守护公众健康权益，也为智慧医疗发展提供安全底座。

5. 电信与互联网领域

商用密码在电信与互联网领域案例以泛在化、轻量化为核心，保障网络与隐私安全。电信（5G/物联网）与互联网场景的特点是“设备数量多、资源受限、用户隐私敏感”，商用密码需适配“轻量化算法+分布式部署”。

通信网络安全应用通过SM4简化算法以及SM2身份认证,适配资源受限设备。具体来说,在5G网络方面,用户终端与基站的空口传输需通过5G商用密码套件。首先用SM2实现终端（UE）与核心网设备（AMF）的双向身份认证，防止伪基站伪装成合法基站窃取通信内容。用户面数据用SM4-CCM模式加密，控制面数据用SM2签名，保障通信机密性与完整性。物联网（IoT）由于智能摄像头、智能家电等设备算力低、内存小，需采用SM4轻量化算法，数据上传时用SM4加密，设备身份用SM2精简版认证，避免设备被劫持。

互联网服务安全应用通过SM2证书以及SM4加密，构建可信应用环境。具体来说，网站/APP HTTPS加密使用传统HTTPS基于RSA/ECC证书，现在需要替换为商用密码证书（基于SM2算法，符合GM/T 0024标准）。首先网站部署SM2服务器证书，用户访问时，浏览器与服务器通过SM2协商生成SM4会话密钥。之后网页内容用SM4加密传输，同时用SM2签名验证网站身份，防止钓鱼网站。APP收集的个人信息需用SM4加密存储在手机本地或云端，密钥由设备安全芯片管理，仅用户授权时才能调用密钥解密，符合《中华人民共和国个人信息保护法》中“最小必要+加密保护”的要求。

6. 工业领域

商用密码在工业领域案例以高可靠、抗干扰为核心，筑牢工业控制系统安全。工业领域的核心风险是“控制指令被篡改、生产数据泄露、设备被干扰”，商用密码需适配工业协议、恶劣环境，且需满足无间断运行要求。

工业控制系统（ICS）安全应用通过SM2签名以及SM4加密，保障控制指令可信。具体来说，在电力调度、油气管道控制等场景中，控制指令的篡改可能导致重大事故，需要通过密码技术实现“指令不可篡改、来源可追溯”。调度中心发送指令前，用SM2私钥对指令签名，同时用SM3计算哈希值。指令与签名用SM4加密后，通过工业以太网传输至现场设备，SM4密钥由“工业密码网关”动态分发。现场设备接收后，先解密得到指令与签名，使用调度中心的SM2公钥验

证签名，确认指令合法后再执行，避免黑客伪造指令导致电网瘫痪。

工业数据安全应用通过 SM4 加密以及 SM3 哈希，保障核心数据不泄露。具体来说，工业设计图纸、生产工艺参数、质量检测数据等核心数据，需防止内部人员泄露及外部黑客窃取。设计图纸从研发部门传输至生产车间时，使用 SM4 加密（基于工业专用 VPN，符合 GM/T 0026 标准），防止数据在工厂内网被窃取。生产工艺参数存储在工业服务器时，使用 SM4-XTS 模式加密硬盘，密钥由工业密钥管理系统管理。质量检测数据上传至云端后，用 SM3 计算哈希值并存储在本地服务器，后续审计时比对哈希值，确认数据未被篡改。

7. 新兴领域

商用密码在车联网、低空经济、海量视频监控等新兴领域，以“场景适配、高效协同”为核心，结合业务高动态、广连接、高敏感的特点，构建“算法选型差异化、防护全链覆盖”的安全体系，已经成为新兴产业高质量发展的核心安全保障。

车联网业务具有“实时交互性强、数据量级大、安全后果严重”的特征，密码应用需平衡实时性与安全性，采用“SM2+SM4+硬件加密”的核心架构。在身份认证层面，数字钥匙内置 SM2 算法实现车与人、车与设备的双向认证，替代传统物理钥匙防范非法启动。通信安全方面，V2X（车与万物）通信采用 SM4 加密传输传感器数据与控制指令，搭配基于 SM2 的商用密码 SSL 证书构建安全通道，防止指令被篡改或劫持。数据安全上，高精度地图、用户行为数据通过 SM4 加密存储，关键操作经 SM3 哈希校验保障完整性，符合《汽车密码应用技术要求》标准。车载 T-box、自动驾驶控制器等核心部件内置安全芯片，实现密钥全生命周期硬件级防护。

低空经济（无人机、eVTOL 等）面临飞行劫持、数据泄露等风险，密码应用聚焦“空-天-地”全链路防护。设备端采用 SM2 算法完成无人机与管控平台的身份核验，飞控系统内置硬件加密模块保障控制指令安全。通信链路通过 SM4 加密飞行数据与导航信息，在关键场景引入量子密钥分发技术杜绝窃听风险。数据安全方面，采集的地理信息、敏感图像经 SM4 加密传输，利用 SM3 实现飞行日志完整性校验，结合区块链技术完成数据存证。针对集群作业场景，采用联邦学习与同态加密结合的方案，实现“数据可用不可见”，符合《民用无人驾驶航空器系统安全要求》。

海量视频监控具有“终端分散、数据敏感、存储量大”的特点，密码应用以“隐私保护+数据安全”为核心。前端设备通过 SM2 完成接入认证，防止非法设备接入网络。视频传输采用 SM4 实时加密，搭配商用密码 TLS 协议保障传输安全。存储环节对人脸、车牌等敏感信息采用 SM4 透明加密，仅授权用户可解密查看，符合个人信息保护相关法规。数据使用时，通过 SM3 哈希校验防止视频篡改，关

键场景叠加数字签名实现操作可追溯。采用密码服务平台实现海量终端的密钥统一管理，兼顾加密效率与运维便捷性。

（六）行业领域典型案例

1. 政务领域

案例1. 电子政务电子认证（辽宁CA & 辽宁广烁）

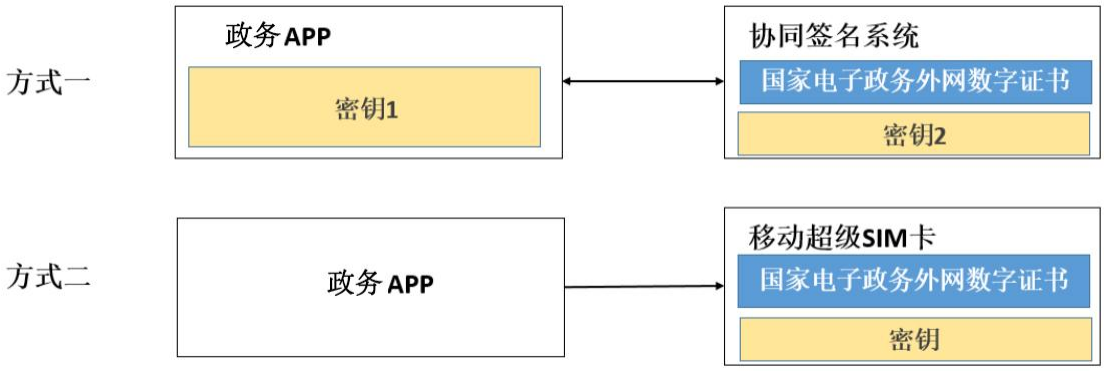
- **案例背景：**

在数字政府建设的进程中，政务云占据着举足轻重的地位，已成为关键的数字基础设施。随着云计算技术的飞速发展以及政府对数字化转型的大力推动，政务云在各级政府部门中得到了广泛应用。此时政务云的安全性显得尤为重要，在众多的信息安全技术中，密码技术是保障政务云的网络与信息安全的基础支撑和核心技术。

在政务云大力推广应用和密码技术持续迭代升级的背景下，为满足电子政务移动端用户办公需求，按照《GM/T 0109—2021 基于云计算的电子签名服务技术要求》标准和国家相关法律法规要求，电子认证、电子签名和电子印章服务，启动从 PC 端向移动端、云计算平台迁移升级。

- **电子政务移动电子签名服务**

电子政务外网采用政务 APP 和超级 SIM 卡两种方式搭载国家电子政务外网数字证书，满足用户移动办公可信电子签名需求。



图四-5　数字证书搭载方式

区别于以往 Ukey 在 PC 端的使用方式，政务 APP 采用协同签名的方式使用国家电子政务外网数字证书。在政务 APP 和协同签名系统中各自保留密钥的一部分，用户使用数字证书完成电子认证、电子签名等操作，既节省 Ukey 密码模块投入成本，又大幅提升国家电子政务外网数字证书的使用率和应用范围。为进一步提升用户使用国家电子政务外网数字证书的安全性和用户体验，采用超级 SIM 卡安全存储国家电子政务外网数字证书，政务 APP 从超级 SIM 卡中获取数字证书使用权限，保障电子政务数据流转过程中的真实性、完整性、机密性和不

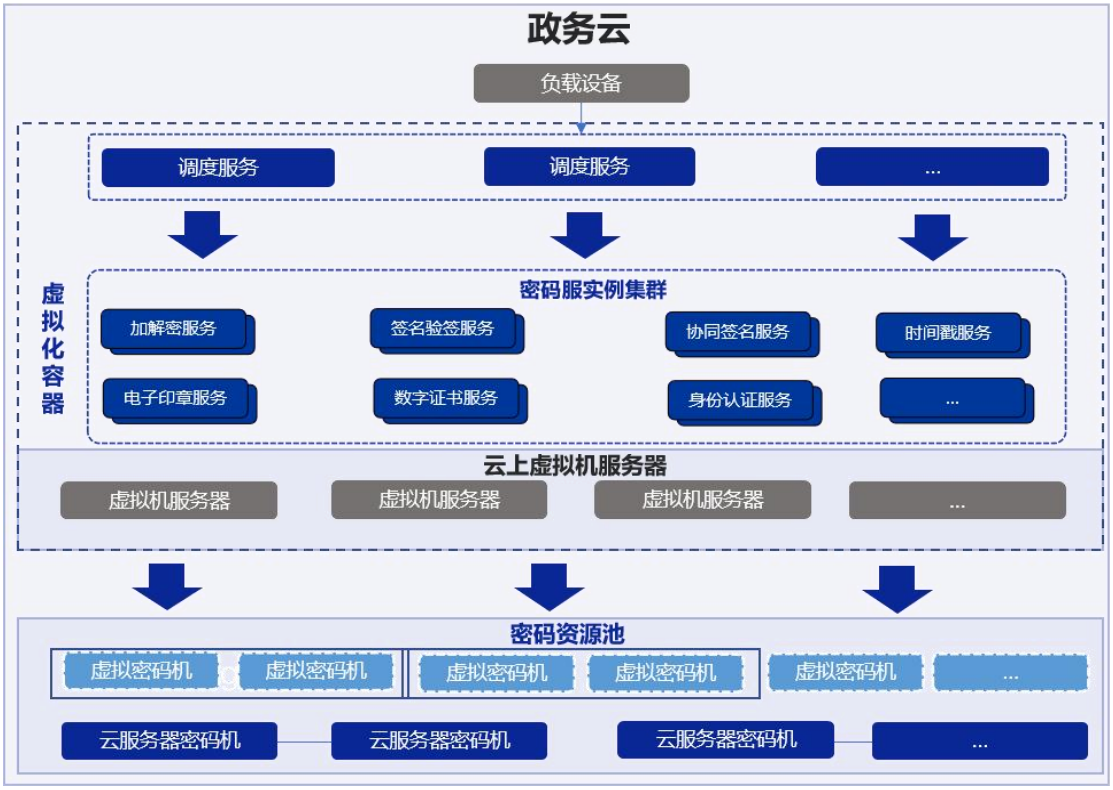
可抵赖性。

- **电子政务电子印章云签服务**

电子印章基于密码技术和数字技术的特定格式数据，用于实现电子文件的可靠签名，与实物印章具有同等法律效力。电子政务电子印章在全国率先实现“同章同模”“物电同源”“公安备案”的印章服务体系，符合国办和公安部三所技术标准，并构建印章全生命周期数据链，全面支持电子政务电子印章云签服务。电子印章的普及推广应用，有效提升电子政务工作办事效率，积极响应政府无纸化办公需求，充分保障“零伪造、零篡改”的安全电子印章应用环境。

电子印章技术原理

案例2. 政务云密码资源池（吉大正元）



图四-6　政务云密码资源池架构图

- **平台能力**

基于云上虚拟机，构建虚拟化容器；

虚拟化容器内组建多节点调度服务；

各类密码服务在容器内组建集群实例，密码服务以多节点方式保障高可用；

由调度服务根据租户资源分配策略，实现动态负载调用。

➢ **创新亮点**

形成密码资源池，统一支撑云上业务的密码应用需求，避免重复建设和投入；

优化应用开发过程，应用开发只需要针对标准接口进行开发，避免满足不同厂家的不同标准；监督责任方的密码应用改造进度，充分发挥密码在政务云环境中的核心支撑作用，指导、监督商用密码应用安全性评估工作。

案例3. 政务系统密码应用解决方案（辽宁移动）

➢ **案例背景**

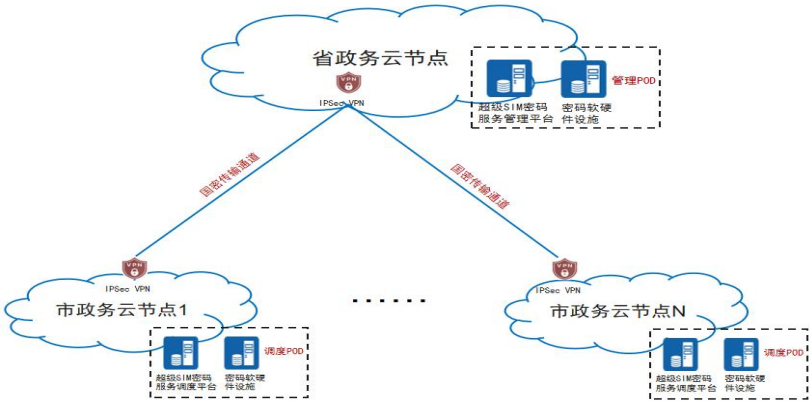
随着数字化政务战略的深入推进，政务云作为数字政府基础设施，已成为各级政府、企事业单位数字化转型的核心平台。然而，传统政务云在安全基座上存在显著短板，不具备成熟的商用密码服务能力。这一能力的缺失无法满足《密码法》与网络安全等级保护 2.0 等相关要求。另外也无法保障业务数据本质安全，在云计算环境下，所有数据都在共享的资源池中流转。没有内置的、体系化的密码服务，意味着用户数据的机密性和完整性无法得到有效保障，面临被窃取、篡改和泄露的风险。

此外，在数字化转型浪潮下，各省份与地市的各类业务对密码应用的需求呈现“井喷式”增长。然而，过去的建设模式缺乏顶层设计，导致了“密码资源缺乏统一规划”的困境。

因此，中国移动提出二级平台架构的密码资源池建设方案，通过构建“1+N”的集约化架构—即 1 个中心密码资源池作为统一管理核心，N 个节点作为服务延伸和边缘算力补充。实现对全省密码资源的统一规划、统一建设、统一运营。

➢ **方案架构**

本方案中，在省政务云节点部署密码资源池管理 POD，为省政务云上的政务应用提供密码服务，在地市政务云部署密码资源池调度 POD，为市政务云上的政务应用提供属地密码服务。其中，省政务云和市政务云之间的数据传输通过国密 IPSec VPN 组网封包，打通省－市节点超级 SIM 密码服务平台的管理通道，实现全省地市政务租户密码服务、系统密码改造信息统一管理，密评信息统一管理。



图四-7　密码资源池架二级架构图

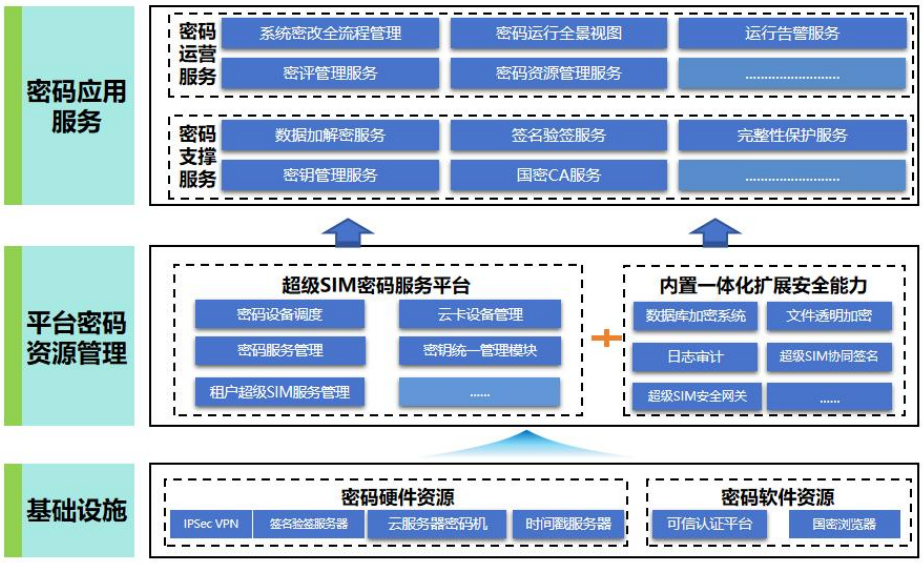
密码资源池包含超级 SIM 密码服务平台、密码软硬件设施两个部分。

超级 SIM 密码服务平台：实现密码硬件的云化管理、服务，根据应用系统密码业务需求合理分配、调度密码资源，按需分配密码服务能力；运用容器技术和密码安全中台概念，实现密码运算能力动态负载均衡，面向业务应用系统提供可靠的密码运算服务。

密码软硬件设施：为云上多样化密码应用需求提供支撑，包括云服务器密码机、签名验签服务器、时间戳服务器、数据库加解密、电子签章系统、数字证书等密码基础设施资源。

- **主要功能**

超级 SIM 密码服务平台采用通过商用密码产品认证的密码产品作为算力支撑以及密钥管理安全根，平台本身支持基于国密算法的 PKI 体系，支持 SM2、SM3、SM4 等国产密码算法，并在云南、广东、辽宁等多地省政务云通过了密评。



图四-8　超级 SIM 密码服务平台功能图

（1）终端超级 SIM 智能密码钥匙服务：基于超级 SIM 卡提供端侧硬介质密钥载体，兼容协同签名软模块，满足移动端、PC 客户端、web 端等多端业务的签名验签、数据加解密密码应用的需求。

（2）系统国密改造信息全流程跟进：对现有需要进行国产商用密码应用改造系统进行信息登记，包含系统名称、管理部门、管理人、系统描述等保等级、国密等级等信息；

（3）系统密评信息统计：对租户系统的密码应用数据、密码资产数据、密码应用安全性评估过程等统计数据和报表，以文件、接口、大屏展示等方式，可以供上层监管系统查询，调用和展示。

（4）分布式密码服务架构：采用省、市二级平台管理架构，二级平台之间的通讯支持 Https 加密协议（RSA-2048 位以上），可更安全地实现统一管理、

统一运营，可降低建设成本。

- **适用领域**

本方案围绕信创国产商用密码体系，构筑“安全与网络共生”的电子政务系统安全防御体系，不仅有力支撑国家网络空间安全战略体系建设，高效守护网络数据安全，支持海量的上层政务应用，助力电子政务领域密码改造。

- **方案特色**

（1）行业首个实现以超级 SIM 卡作为密钥安全载体，集成安全芯片为卡应用提供安全的运行环境，芯片通过 EAL4+以上安全认证、EMVCo 安全认证及国密二级以上认证，对比行业内通用的 USBKEY、TF 卡、贴膜卡等，是密钥的最佳安全硬件载体，同时开发出协同签名软件密码模块并获得国密认证，满足各类场景的身份认证需求。

（2）建设多级密码服务调度体系，市面上常见的国密资源池多采用单点建设，面对多节点资源统一管理的实际需求，多级政务云亟需降低建设与管理成本，提升云上密码服务效能。超级 SIM 国密资源池实现了“接入－运营－运维－监控”全过程的多级国密调度体系，可实时分析系统负载、数据安全风险等因素，自动调整密码服务的调度策略，确保在保障安全的前提下，最大化发挥系统性能。

（3）创新打造超级 SIM 国密门禁卡，遵循 GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》设计。将 IC 卡替换超级 SIM 卡，存储卡片密钥 Keyc，内置 SM1/SM4 国密算法，并开发超级 SIM 卡门禁应用，解决了传统 IC 卡易丢失，难管理的场景，降低了机房密改成本，将密码应用场景从 B 端推向了 C 端。

案例4. 省级一体化数据平台密码解决方案（航天信息）

- **案例背景**

某省积极推进省级数字化建设，省第十一次党代会提出全面建设省级数字化体系，发挥数字技术对经济发展的放大、叠加、倍增作用。相关实施方案明确提出建成覆盖全省、集约高效、安全可靠、开放兼容的一体化数据支撑体系，作为省级数字化建设的重要基石。根据省政府年度重点工作通知，在推进重点领域改革中明确要求建设全省一体化数据基础平台。

为满足《密码法》、GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，规范平台基础信息安全建设，满足平台在应用过程中的数据完整性、数据机密性以及抗抵赖等方面的基础密码服务需求，结合全省一体化数据支撑的特点，开展密码服务设施建设的规划和设计，构建适用于省级一体化数据基础平台的完善的密码防护体系，实现机密性、完整性、真实性、不可否认等安全目标。

- **方案概述**

某省已建成覆盖全省、集约高效、安全可靠、开放兼容的一体化数据支撑体

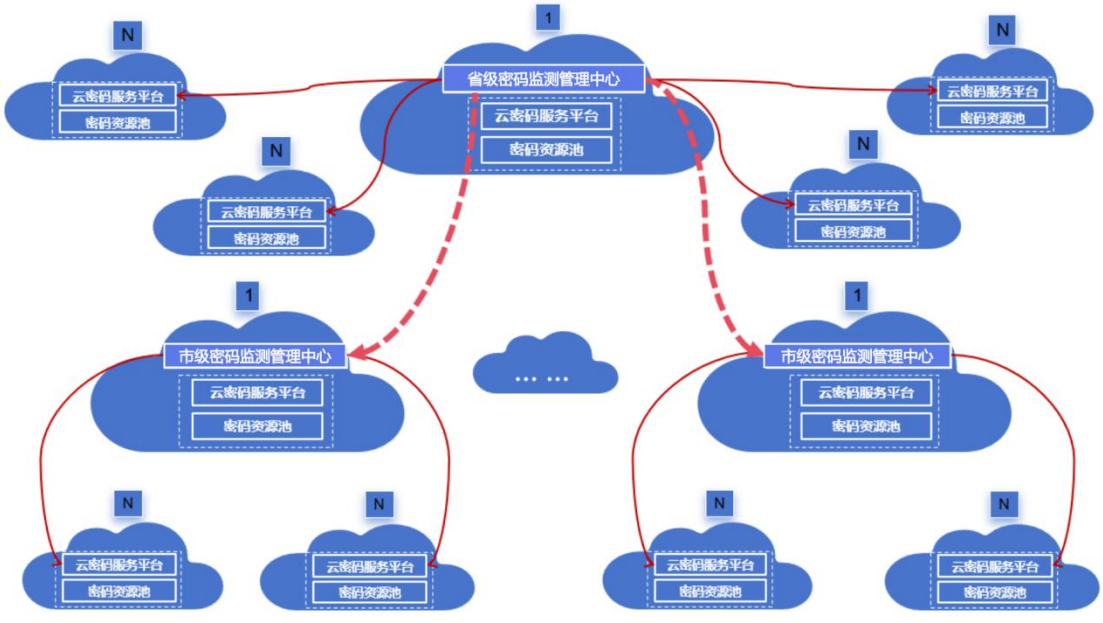
系，包含密码防护体系，实现机密性、完整性、真实性、不可否认等安全目标。项目采用分级部署体系，将管理平台和密码服务平台分开建设，打造了“1+N”云密码综合服务平台，实现了一套高效、可靠、易扩展、可统管的全省云密码基础设施。管理层的“1”是密码监测管理中心，作为密码资源顶层管理调度平台，与省级政务一体化服务平台集成，为政务应用提供一体化密码资源申请和密码态势监测感知服务。业务层部署“N”个云密码服务平台，为所在政务云上信息系统提供集约化密码服务。截至 2025 年上半年，平台已经为省内 30 余家单位近 200 多个业务应用提供服务，累计提供各类密码服务 30 亿次。

- **需求分析**

省级一体化数据平台的密码基础设施建设需要规划新模式统筹建设，以应对一体化管理和未来的各类密码应用需求。考虑统一管理、统一接入接口标准、自助申请密码资源等模式，且政务应用和密码资源分布在多个机房的多个网络区域，分布式的密码应用需求和一体化管理需求均要满足。

- **设计方案**

设计思路：针对政务应用在多个网络区域部署的实际情况，以及未来省市多级部署建设的扩展需求，创新性地设计了“1+N”多级云密码服务平台，从逻辑架构上分为密码监测管理中心、云密码服务平台、密码资源池三个部分。在每个网络区域建立一个云密码服务平台，接受密码监测管理中心的统一监管，形成管理一体化、服务规范化的密码服务体系。



图四-9　“1+N”云密码综合服务平台部署示意图

管理层的“1”是密码监测管理中心，作为密码资源顶层统一管理平台，实现密码设施统一管理与调度、密码服务统一管控等功能。省级密码监测管理中心

与省级政务一体化服务平台集成，为政务应用提供一体化密码资源申请和密码态势监测感知服务。

业务层分网络区域部署“N”个云密码服务平台，为本网络区域政务云上的信息系统提供集约化密码服务。云密码服务平台以云密码资源池为计算资源支撑、实现对多种密码资源的统一调度和弹性分配，面向所在域的云上信息系统可以按照统一的服务目录提供多样化、场景化、可扩展的密码应用服务。对云上信息系统屏蔽后台密码设备的多样性、指令的复杂性，降低其对密码设备调度的技术难度，将密码能力全面融入各云上信息系统，实现密评各个层面的安全要求。

“1+N”部署模式既对多云跨域异构云密码服务平台进行统一纳管，又可支持在省市多级部署统筹管理。省级密码监测管理中心能够向市级密码监测管理中心下发市级平台根密钥、密钥管理策略、平台管理策略等，市级密码监测管理中心将各纳管云密码服务平台的业务应用情况、服务调用情况、运维服务等数据上传，实现省级平台对市级平台安全有效的管理、指挥、数据交换，全面掌握密码建设和运行情况，形成在全省统一指挥，联防联控的有效机制。

- **主要功能**

一站式密码资源申请。本项目建设的云密码基础设施与政务一体化平台深度融合，制定了密码服务标准业务流程和对接规范，实现了密码监测管理平台与一体化平台基于密码服务与业务的有机整合，密码服务作为业务资源包可同云资源、安全资源等一起申请，为政务应用提供一站式密码资源申请。

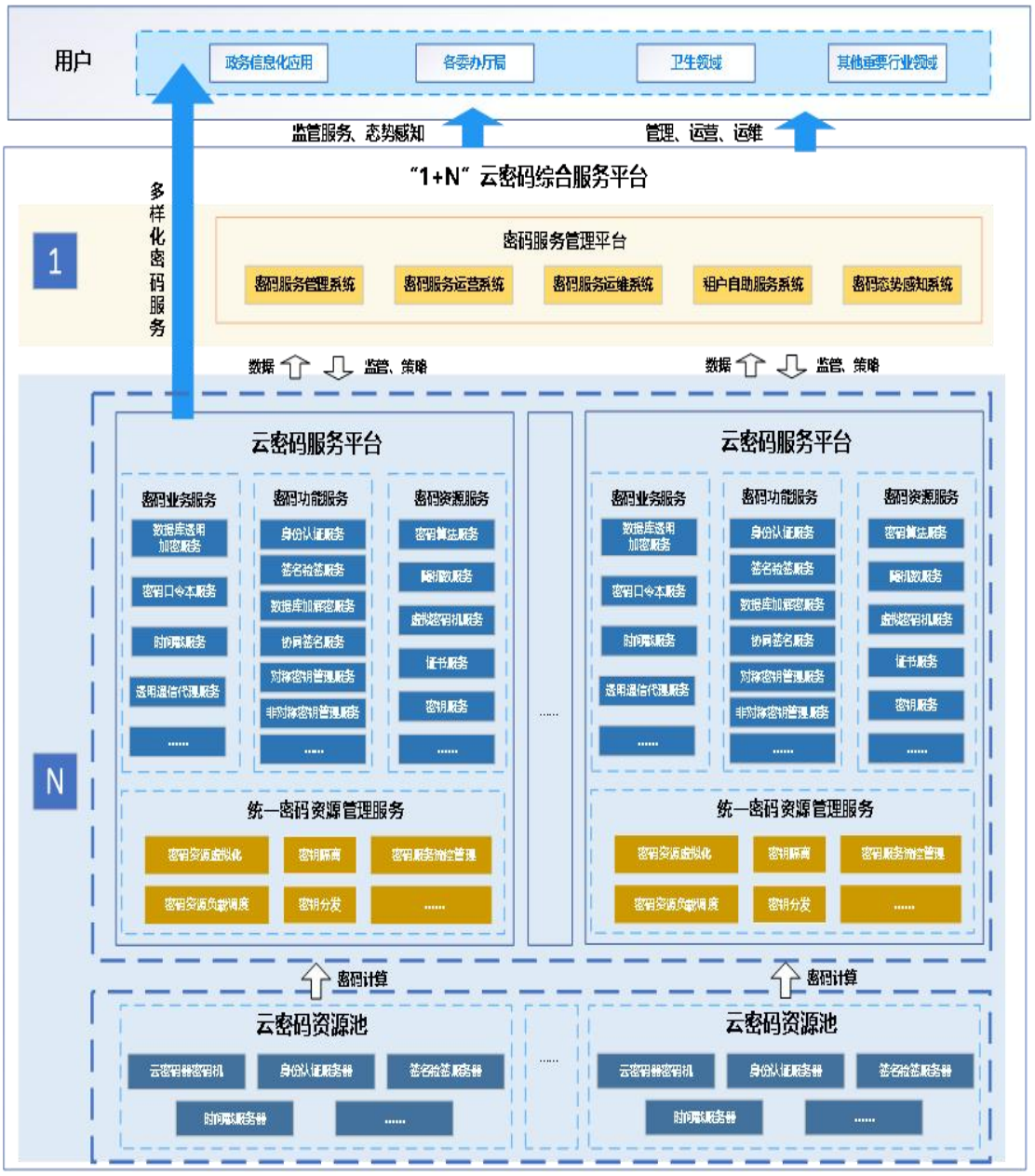
密码态势监测全感知，服务统一监管。各数据中心的密码服务调度平台将业务应用的密码服务调用情况、运维服务等数据上传，以多维度数据分析助力精细化运营，实现省级密码监测管理平台对各数据中心安全有效地管理、指挥、数据交换，全面掌握密码建设和运行情况。

多类型密码资源支撑，提供统一高效的密码服务。密码服务调度平台为各业务系统提供微服务形式的、标准化的密码服务，满足业务多场景、多形态的密码应用需求，应用改造少、改造易、便捷用。

主要技术指标：系统上线后已持续稳定运行 2 年，密码服务性能达万级 tps。高效使用资源，扩展性强，可应对突发业务请求峰值，密码服务日请求量峰值约 4000 万次，业务峰值期间一小时请求量达 400 万次，系统均运行平稳。

核心产品：本方案用到的核心产品是云密码服务平台，具体内容如下。

技术架构：云密码服务平台包括密码监测管理平台、云密码服务子平台以及密码资源池三部分。支持省市分级部署，并可纳管多个垂直行业及第三方平台，提供密码运算能力和密码统一管理，实现网络、云、终端、应用、数据等领域密码应用安全全覆盖，形成统一指挥，联防联控的有效机制。



图四-10　方案建设架构图

案例5. 政务应用自建系统密码应用改造（辽宁联通）

➢ 案例背景

为落实相关法律法规对于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》《政务信息系统政务采购管理暂行办法》等规范性依据，现需要将我省“一号台”系统进行密码应用改造。

“一号台”目前部署于自有机房，为领导同志和机关单位提供电话服务。覆盖全省县级以上党政机关、企事业单位的通信指挥系统，实现快速指挥、及时调度、高效督办，提升政务处理、机关管理效能，加快工作节奏，提高工作效率，助力辽宁全面振兴全方位振兴。

➢ **方案设计**

图四-11　系统示意图

根据系统部署方式和需要实现的业务功能，在访问终端部署国密浏览器，并给业务用户、管理员和运维人员派发 USBKey。在“一号台”网络边界部署 SSL VPN 安全网关实现基于 SSL/TLS 协议的安全通道建立。新建密码资源区部署服务器密码机和签名验签服务器，实现加解密、签名验签功能。

➢ **技术方案**

（1）物理和环境安全：本系统所在机房目前采用基于生物识别技术（人脸、指纹）对进入人员进行身份鉴别，并在重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控。本系统计划明年将迁移到辽宁省政务云平台。

（2）网络和通信安全：在访问终端部署国密浏览器，并给业务人员派发 USBKey，实现基于数字证书的强身份认证登录方式，在访问终端与平台侧签名验签服务器进行身份鉴别，防止与假冒实体进行通信。

在“一号台”网络边界部署国密 SSL VPN，建立与访问终端的国密 SM2 算法 https 通道，保证重要数据传输的机密性、完整性，以及用户访问控制信息完整性，防止数据被非授权篡改，防止重要数据泄露。

（3）设备和计算安全：在远程运维终端部署国密浏览器，并向运维人员配发 USBKey，对访问堡垒机的用户进行身份鉴别，使用 SSL VPN 安全网关建立安全的远程管理信息传输通道。

调用部署在密码资源区中的服务器密码机使用 HMAC-SM3 算法对服务器、数据库等设备的系统资源访问控制信息进行完整性保护。密码设备日志记录和访问控制信息的完整性保护由设备自身实现。

调用部署在密码资源区中的服务器密码机使用 HMAC-SM3 算法对服务器、数据库等设备日志进行完整性保护。

（4）应用和数据安全：在访问终端部署国密浏览器，并向业务人员配发 USBKey，对访问业务系统的用户使用签名验签服务器进行身份鉴别。

调用部署在密码资源区中的服务器密码机使用 HMAC-SM3 算法对系统应用用户访问控制列表进行完整性保护。

调用部署在密码资源区中的服务器密码机对访问用户身份鉴别数据、姓名、身份证号、联系方式等重要业务数据进行完整性和机密性存储保护。

（5）安全管理：GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》从制度管理、人员管理、建设运行、应急处置、密钥管理等层面进行制度的编制并执行。

案例6. 某部委密码保障系统（北京数字认证）

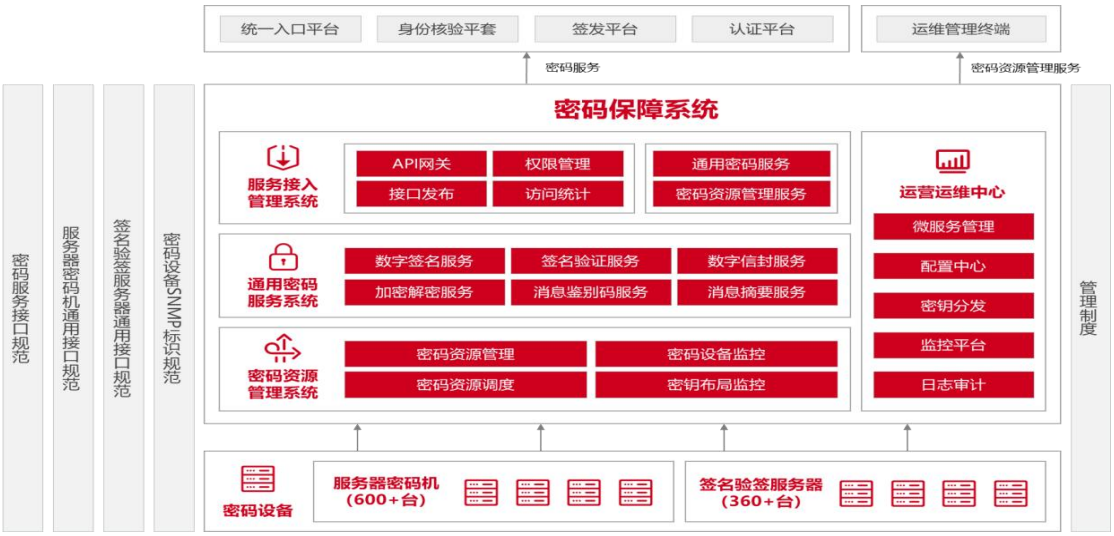
➢ 建设背景

某部委为满足全国网络身份认证业务，已购数百台来自不同厂商、不同型号的密码设备，各厂商密码设备间存在标准不统一、接口不统一、参数格式不统一等问题，不仅给运维工作带来巨大的压力，而且无法实现密码服务的快速应用。运营期间，时常出现密码设备损坏、宕机、证书过期等情况，需要频繁开展巡检工作，当遇到业务高峰时，密码服务时常达到性能上限，极易引发业务运转事故。因此，某部委亟须探索新的密码应用模式，面向业务应用提供统一的密码服务，为业务运维管理提供集中密码资源集中运维管理能力。

➢ 建设目标

某部委规划建设密码保障系统，可以作为衔接密码基础设施和各业务系统的纽带，实现密码设备的集中管理，对业务系统屏蔽密码设备的多样性，降低密码安全管理的复杂性，提供针对密码资源的统一调度能力和集中管理视图；同时，统一规范接口设计，减小适配难度，提高研发工作效率。

➢ 建设方案



图四-12　密码保障系统架构图

某部委密码保障系统基于云容器技术，将密码资源进行虚拟化，提供统一的密码资源管理视图，实现了对不同厂商、不同类型密码设备的统一纳管，将密码设备作为密码资源，以池化方式进行统一调度，有效屏蔽密码资源差异性。同时，支持根据密码服务请求进行密码资源动态扩展，确保提供的密码服务灵活且高效。

- **应用效果**

（1）实现海量设备集中管理：实现 600+台密码机、360+台签名服务器统一调度和管理，面向业务应用提供统一、合规的密码计算及密钥管理服务。支撑 50 万 TPS 业务签名和加密需求。

（2）具备服务扩展能力：面对海量的资源、服务规模，极高的业务并发、吞吐量时，提供全自动按需分配、动态扩展/缩减密码服务的能力。

案例7. 政务云部署平台（辽宁联通）

- **案例思路**

保障云平台通过密评产品包括：服务器密码机、签名验签服务器、SSL VPN 安全网关、国密浏览器、智能密码钥匙、个人数字证书和 SSL 证书。

针对互联网区云平台和公共服务区云平台，根据密码测评中应用与数据部分要求，需通过签名验签服务器和服务器密码机提供的服务接口分别为互联网区云平台和公共服务区云平台提供签名验签服务和加解密服务；根据密评中网络与通信、设备与计算相关要求，应采用个人数字证书+智能密码钥匙、SSL VPN 安全网关配备 SSL 证书和国密浏览器，实现身份认证及链路加密，配合堡垒机管控方式，确保云平台的访问与控制安全合规。

为云租户提供密码服务设备包括：密码服务平台、云服务器密码机、SSL VPN 安全网关、国密浏览器、智能密码钥匙、个人数字证书和应用国密证书。

建设密码服务平台，提供统一的密码安全能力和密码集中化的管控服务，密码服务能力需要必须满足租户隔离、资源计费统计、弹性扩容。密码服务平台部署建设，独立于政务云平台的计算资源和存储资源，确保底层密码服务（加解密服务、签名验签服务、身份认证服务、密钥管理服务）可以通过密码服务平台按需分配给云租户，满足业务系统密码应用需要。

- **建设目标及内容**

政务云密码应用建设最终目标是，落实国家政策及标准规范，围绕商用密码应用安全性评估要求，建设符合国家要求的密码云平台，保障政务云平台和云上业务系统的密码应用安全合规。该项目建成后，密码云平台可为政务云平台及云上的业务应用系统提供实体身份真实性、重要数据机密性和完整性、操作行为的不可否认性等方面的密码防护，为政务云及云上的应用系统的安全可靠运行提供全面高效的密码支撑。项目密码安全应用建设以下内容：

（1）建设密码云平台，采用国产密码算法 SM2、SM3、SM4 和通过符合国密

认证的密码产品及密码服务，为政务云提供统一密码资源服务，包括：密码服务平台、云服务器密码机等密码产品构建的云密码资源池，提供身份鉴别、数据保护、重要数据完整性、机密性保护等能力。云上业务系统密码应用对接，各委办局业务信息系统上云通过调用云密码资源池能力，从应用和数据层面，对用户身份鉴别、重要数据保护、完整性保护以及操作不可否认性进行密码安全改造，保障云上业务满足密码测评要求。

（2）建设完善密码安全管理相关制度建设，根据 GB/T39786-2021 中安全管理制度方面的要求，制定政务云密码安全管理制度和操作规范，内容至少包含密码建设、运维、人员、设备、密钥等 6 个方面。

- **服务要求**

基于国产密码标准体系和密码管理体系，参考《政务云密码支撑方案及应用方案设计要点》中的政务云密码应用参考模型，建设以保护云上业务系统的身份认证及数据资产为中心的辽宁省政务云密码服务平台，通过核心的云密码技术、密码模块、云密码产品、密码基础设施等产品服务，为网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端、设备控制等提供身份鉴别、访问控制、机密性、完整性、抗抵赖的密码服务。

具体服务内容如下：

（1）数字证书服务（含介质）：服务提供一个支持 SM2、SM3、SM4 算法的个人专属标识，具有身份认证、加/解密、签名/验签等服务。

（2）国密 SSL 证书服务：服务提供保护一个域名下所有的子域名网站，保证了网站的信息从用户浏览器到服务器之间的传输是高强度加密传输的，是不会被窃取和篡改的。确保网站身份真实可靠。

（3）政务外网安全接入服务：支持 IPv6/IPv4 双栈协议，提供政务用户通过 SSL-VPN 安全接入电子政务外网的业务流程办理及 VPN 系统运行维护以及 VPN 用户的技术支持、故障处理等服务。

（4）浏览器密码服务：服务主要通过浏览器内核、SSL 安全协议模块、渲染进程、插件进程等提供支持 SM2、SM3、SM4 算法，提供与 Web 服务器之间建立安全通道，实现 Web 网页安全访问功能。

（5）软件密码模块服务：服务主要通过动态库文件和配置文件两部分，支持 SM2、SM3、SM4、ZUC 算法，提供数据加密/解密、签名/验签、消息鉴别等内容。

（6）加解密安全服务：服务支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证等功能。

（7）时间戳服务：服务支持 SM2、SM3、SM4 算法，具有时间戳生成、应答、验证等功能。

（8）签名验签服务：服务支持 SM2、SM3、SM4 算法，具有签名验签、身份认证等功能。

（9）身份认证服务：服务支持 SM2、SM3、SM4 算法，具有证书管理、密钥管理、用户授权管理等功能。

（10）数据加密服务：服务支持 SM2、SM3、SM4 算法，提供密钥管理、密码运算、数据库加密和文档加密等服务。

（11）电子签章服务：服务由电子印章制作系统、电子印章服务系统、电子签章客户端软件等组成，支持 SM2、SM3、SM4 算法，具有电子印章制作、印章管理、对 OFD 格式等文档进行签章及验证等。

（12）动态令牌和数字证书身份认证服务：服务主要通过证书管理系统、动态口令生成及验证系统等提供支持 SM2、SM3、SM4 算法的动态口令认证、证书管理、安全审计等。

（13）动态令牌身份认证服务：服务主要通过密钥管理系统、动态口令生成及验证系统等提供支持 SM2、SM3、SM4 算法的动态口令认证、密钥管理、安全审计等。

（14）密码方案咨询设计服务：服务针对有商用密码测评需求的委办局，提供针对具体业务系统的密码应用方案咨询、设计服务，确保密码应用方案通过评审。

（15）业务系统对接技术支持服务：服务针对有密码资源使用需求的应用开发商，提供基于云密码服务平台的密码计算服务的对接技术支持，确保密码改造快捷合规。

（16）密码管理制度优化服务：对组织架构按照《密码法》及实际需要进行重新规划设计，确保组织架构的工作条线清晰、规范，弥补组织架构缺陷，增加业务衔接流畅度；协助用户满足密码测评对管理的相关要求。

案例8. 某防洪排涝调度系统商用密码应用（沈阳市水务局）

➢ 建设背景

随着气候变化和城市化进程的加快，洪涝灾害的频率和影响范围正在逐渐扩大，给人民群众的生命财产安全和社会经济发展带来了严重威胁。因此，建设防洪排涝调度系统具有重要意义。

首先，防洪排涝调度系统有助于提升防洪排涝能力。通过对气象、水文、水位等数据的实时监测，系统能够准确评估洪水风险和水涝情况，及时采取相应的防洪措施。系统还能进行模拟和预报，帮助决策者制定科学合理的防洪排涝方案，提高防洪排涝能力，减少洪涝灾害的损失。

其次，防洪排涝调度系统能够提高调度效率和减少人力资源投入。传统的防洪排涝工作主要依靠人工经验和判断，工作效率低下且容易出现误判。而建设防

洪排涝调度系统可以自动化地进行数据采集、分析和处理，实现对洪涝情况的实时监测和评估，提高调度的准确性和效率。这样可以减少人力资源的投入，提高工作效率，降低防洪排涝工作的成本。

再次，防洪排涝调度系统有助于提高社会安全和稳定。洪涝灾害是一种常见的自然灾害，对人民群众的生命财产安全和社会稳定造成严重威胁。建设防洪排涝调度系统可以提升防洪排涝能力，减轻洪涝灾害的影响，保障人民群众的生命安全和财产安全，维护社会的安定和谐。

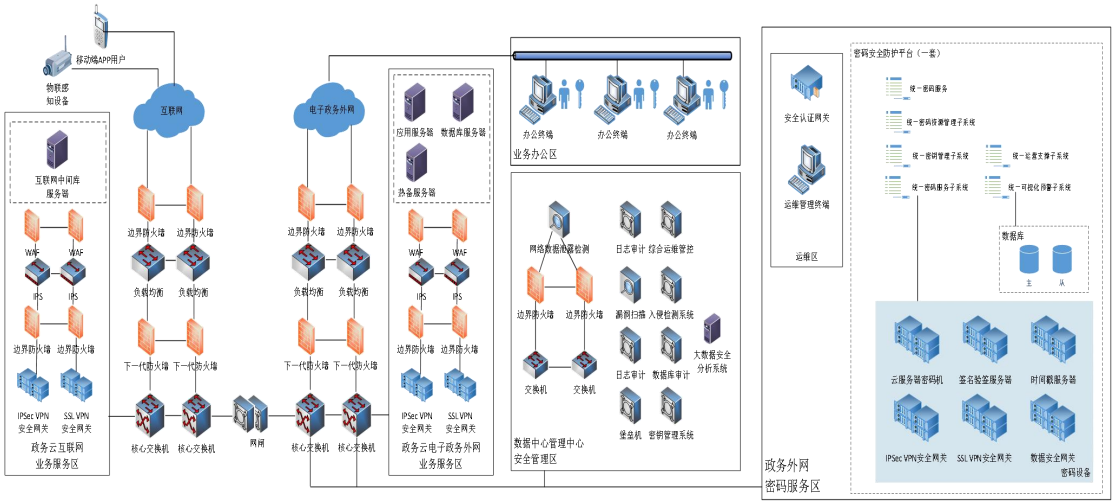
此外，防洪排涝调度系统还对城市规划和建设具有重要意义。随着城市化进程的加快，城市面积不断扩大，水泥化程度不断提高，城市排水系统的建设和管理面临更大的挑战。建设防洪排涝调度系统可以对城市排水系统进行科学规划和布局，合理配置排水设施，提高城市排水能力，确保城市基础设施的可持续发展。

总之，建设防洪排涝调度系统对于提升防洪排涝能力，提高调度效率，保障社会安全和稳定，以及推动城市规划和建设具有重要意义。随着科技的不断进步和应用，防洪排涝调度系统将发挥越来越重要的作用，提供更加准确、高效、可靠的防洪排涝服务。这将为人民群众的生命财产安全和社会经济发展提供有力保障。

同时，防洪排涝调度系统作为网络安全等级保护三级系统，承载着承载业务运转与公众利益的重要数据，其安全防护体系需严格对标《数据安全法》《密码法》等法律法规要求，系统需落实数据分类分级管理，对核心敏感数据开展全生命周期防护，杜绝数据外泄风险。需采用 SM4、SM2 等国密算法实现重要数据存储与传输加密，守护重要数据安全。

➢ 方案架构

系统部署于政务云，依托于沈阳市政务云提供的标准密码服务进行建设，使用了包括：签名验签服务、加密解密服务、时间戳服务、协同签名服务、数字证书服务、SSL 安全传输服务等。相关部署图如下：



图四-13　密码应用部署图

➢ **方案特色**

在物理和环境安全方面：系统物理机房在系统所在区域部署符合 GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的安全门禁系统，使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行鉴别；门禁一体机将刷卡记录通过国密 SSL 协议加密传输至管理平台，管理平台使用基于 SM3 的消息鉴别码（MAC）技术对电子门禁系统进出记录进行数据完整性保护并与对应的消息鉴别码一并写入数据库。

在网络和通信安全方面：互联网部分通过应用安全网关加载了 RSA 证书，采用 TLS 协议构建访问通道；政务外网部分系统通过应用安全网关加载了国密证书，采用 GMTLS 协议进行访，对重要数据传输机密性和完整性进行保护。同时系统相关运维人员使用具有国密证书的 AG 安全网关构建安全的运维通道。

在设备和计算安全方面：系统的运维人员使用符合 GM/T 0027-2014《智能密码钥匙技术规范》的智能密码钥匙登录堡垒机、云服务器密码机，采用基于 SM2、SM3 等密码算法的数字签名机制对登录设备的用户进行身份鉴别，保证用户身份的真实性。

在应用和数据安全方面：系统管理员使用合规 UKey 登录，采用基于 SM2 算法的签名验签技术实现身份鉴别；业务用户和移动 App 用户通过用户名、口令+动态口令的方式登录，实现用户身份的有效鉴别。系统相关的口令等鉴别数据、电话号等个人信息通过调用密码资源采用 SM4 算法进行加密存储，系统相关的重要日志、水源水文等重要业务数据通过调用密码资源采用 SM4-GCM 算法实现完整性保护。

2. 金融保险领域

案例1. 数据要素流通基础设施主体授权方案（辽宁移动）

➢ **案例背景**

当前，数据作为关键生产要素的地位已成国家共识。随着国家数据局的成立及相关政策文件的密集出台，国家正全力推动数据要素市场化配置改革。然而，企业在数据流通中普遍面临“不敢共享、不愿共享、不会共享”的核心痛点，根源在于数据权属不清、安全体系不健全与跨域流通困难。

在此背景下，沈阳市数据局携手中国移动辽宁公司，积极响应国家号召，成功打造了东北首个可信数据空间。此举旨在构建一个低成本、高效率、可信赖的数据流通基础设施，确保数据“供得出、流得动、用得好、保安全”，为城市全域数字化转型开辟了新路径，也为本项目提供了坚实的实践基础。

➢ **方案架构**

本方案旨在构建安全可信的数据流通基础设施。我们以高速可靠的数据专属

服务网络为底座，集成连接器、可信空间服务平台与主体授权系统三大核心组件，并融合区块链、隐私计算与数据沙箱等共性服务能力，实现数据使用控制、产品融合开发与交易流通的全流程可信保障，推动形成主体接入可信、资源统一共享、价值融合共创的数据流通新范式。

图四-14　数据要素流通基础设施架构图

在此基础上，方案进一步构建完整的运营与信任体系：通过“软、硬、云”多元化连接器实现“一点接入、即插即用”，大幅降低参与门槛；依托可信空间服务平台整合全域数据目录与多源隐私计算能力，形成闭环的数据服务生态；并以密码技术为核心，融合主体授权与超级 SIM 数字身份，建立“确权—授权—鉴权”一体化可信机制，通过“认证免费、签名收费”的普惠模式，为全社会数据要素流通提供普适性信任基础。

- **主要功能**

本方案具备四大核心功能，保障数据从接入到使用的全链路安全与合规。

（1）可信身份与无缝接入，通过多元化连接器与超级 SIM 证书，为每个参与方提供安全、便捷的身份认证与接入服务。

（2）数据主权与精细管控，数据提供方可通过策略自定义，对数据的使用目的、范围、次数和有效期进行精准控制，实现“我的数据我做主”。

（3）隐私保护与价值融合，内置隐私计算（如联邦学习、安全多方计算）和数据沙箱等技术，支持数据“可用不可见”，实现数据价值的安全融合与挖掘。

（4）全景审计与合规监管，利用区块链技术对数据流通过程进行全链路存证，生成不可篡改的审计轨迹，满足日益严格的合规与监管要求。

- **适用领域**

本方案适用于多个关键领域，通过可信数据流通推动价值实现：在公共数据领域支撑金融风控、医保核验、群租房识别等场景的政务数据开放，释放公共数据价值；在普惠金融领域打通银政企信息壁垒，构建中小企业信用风控体系；在

医疗健康领域实现临床科研、疾病防控等场景的隐私保护数据共享；在工业互联网领域促进产业链数据可信流通，赋能协同制造与预测性维护；在商业智能领域为零售、咨询等行业提供合规数据支持，助力精准决策与区域洞察。

- **方案特点**

（1）网络筑基，接入便捷：依托中国移动独有的“数据专属服务网络”，提供业界领先的“数据快递”服务，实现低成本、高效率的广泛接入。

（2）主权明晰，管控精细：通过创新的主体授权系统，将数据控制权真正交还给提供方，破解“不愿共享”的难题。

（3）技术融合，开箱即用：并非单一技术堆砌，而是将区块链、隐私计算、数据沙箱等能力深度融合，提供一站式、组件化的价值解决方案。

（4）生态开放，标准引领：平台设计遵循国家标准，具备强大的跨域互联和第三方能力纳管功能，避免形成新的“数据孤岛”。

（5）模式创新，普惠全民：首创“超级 SIM 全民证书”模式，以普适性技术手段降低全社会信任成本，为构建广泛的数据要素生态奠定基础。

案例2. 可信数据流通的医疗保险快速核保方案（辽宁移动）

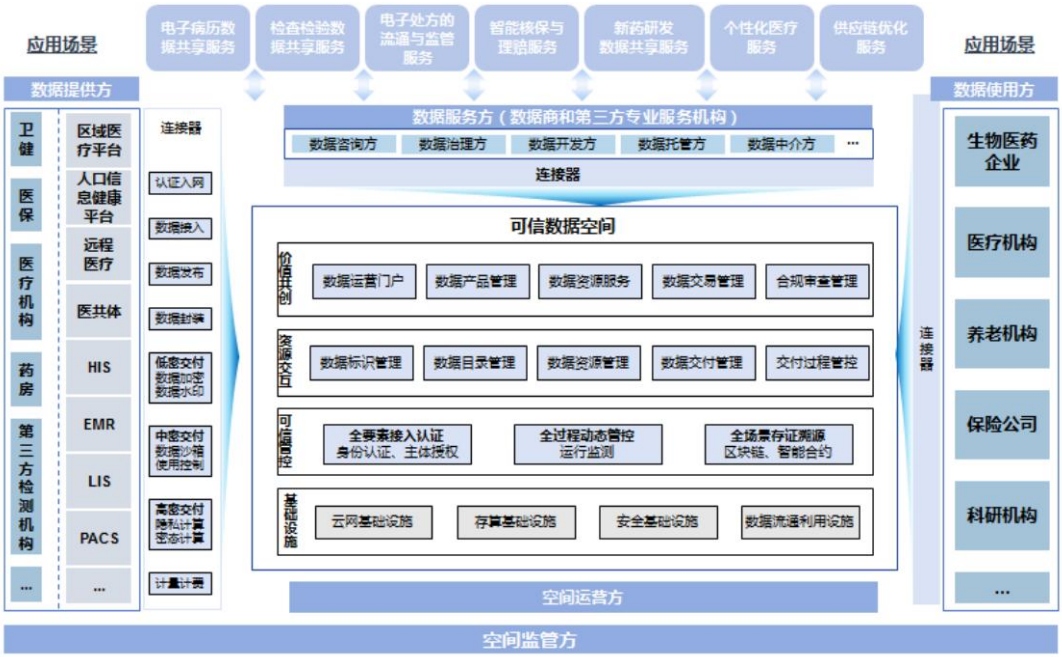
- **案例背景**

在保险业数字化转型进程中，核保与理赔的效率与风控是核心竞争点。传统模式下，保险公司为核实被保险人的健康状况，需要人工传递和审核纸质病历资料，流程烦琐、周期长（通常长达 1-2 周），且存在个人敏感信息泄露、授权不清、追溯困难等数据安全与合规风险。《数据安全法》《个人信息保护法》等法规的深入实施，对保险业数据处理的合法性、最小必要性和安全性提出了更高要求。

为解决上述痛点，锦州市数据局、医保局、卫健委携手辽宁移动建设基于主体授权的锦州医疗可信数据空间，构建了一个以商用密码技术为信任基石，以“数据可用不可见”为核心的保险快速核保与理赔解决方案。该方案旨在确保医疗数据安全合规流通的前提下，将核保周期从数周缩短至近实时，极大提升了保险服务效率与用户体验，为保险行业的可信数据应用提供了创新范式。

- **方案架构**

本案例基于“分层解耦、场景驱动”的理念，构建了“平台+场景+生态”的一体化技术架构，为核心业务场景提供全方位、全生命周期的安全保障。



图四-15　空间架构图

（1）可信管控层：构建全域可追溯信任基座

作为安全治理核心，通过“全要素接入认证”与“全过程动态管控”双引擎全要素接入认证，依托区块链构建分布式数字身份体系，为医疗机构、企业等参与方颁发唯一可信数字身份，所有数据流通请求均需经数字证书与强身份认证主体授权，确保接入主体真实可信。全过程动态管控：基于智能合约建立细粒度动态权限模型，嵌入数据敏感度、用户角色、操作场景等要素，实现数据全链路授权与实时策略执行；所有访问行为均由区块链存证，保障“事前可授权、事中可控制、事后可审计”。

（2）资源交互层：提供安全的数据融合环境

以“标准化连接器+分级数据沙箱”为核心，满足不同密级数据交互需求：

标准化数据连接器：开发统一接入与交换组件，支持医疗机构异构系统（HIS、PACS 等）标准化接入，实现数据自动化清洗、加密转换与格式统一，从源头保障合规。分级数据沙箱：按密级提供差异化环境——高密级采用多方安全计算、联邦学习，实现数据不出域联合建模；中密级用密态交付技术确保全程加密；低密级施加数据水印，泄露可溯源追责。

（3）价值共创层：保障协同公平与合规

聚焦安全前提下的价值最大化，依托联邦学习与智能合约：安全协同计算：部署医疗联邦学习平台，支持医院、药企在本地数据不出场的情况下共同训练 AI 模型，仅交换加密模型参数，杜绝原始数据泄露。可信价值分配：通过智能合约将收益分配规则代码化，交易或模型使用后自动执行分配，确保公平公正。

（4）贯穿全域的安全管理体系：技术+规则+运营

安全能力贯穿上述所有层次，形成纵深防御体系。技术保障：采用国密算法

对数据全生命周期进行加密。部署安全探针实时监测数据流量与访问行为，对异常操作进行自动告警与阻断。规则嵌入：将数据分类分级标准、脱敏规则、合规要求等预先嵌入到平台的技术流程中，实现安全策略的自动化执行，减少人为干预风险。运营保障：建立 7×24 小时安全监控与应急响应中心，定期开展渗透测试与风险评估。

- **主要功能**

案例围绕“保险快速核保”核心场景展开，其数据流转遵循“授权启动、安全计算、可控交付”的核心原则。

保险快速核保业务流程旨在帮助保险公司在获得用户授权后，快速、合规地完成理赔核保决策。具体流程如下：

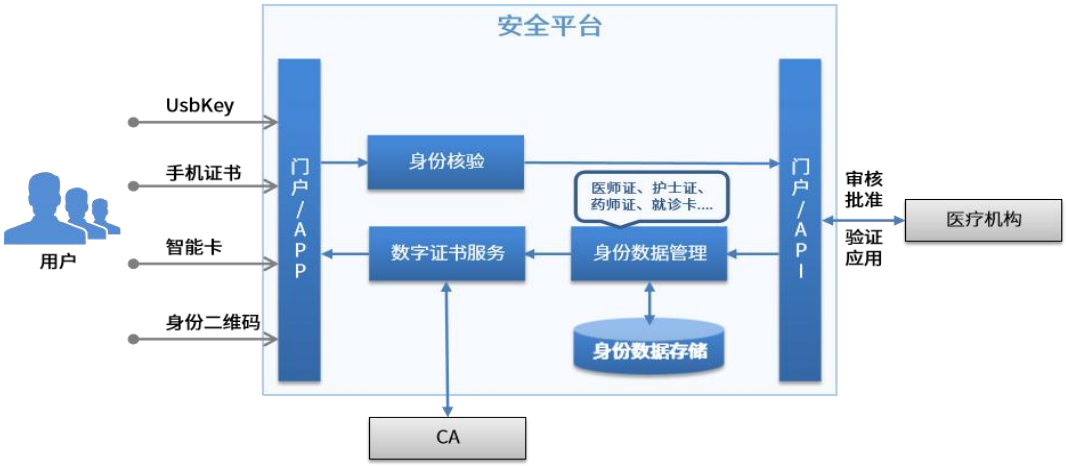
申请与授权：投保用户（患者）在保险公司 App 端提交理赔申请，并通过电子签名方式明确授权保险公司向“医疗可信数据空间”查询其相关的脱敏诊疗数据。

发起请求：保险公司业务系统在获得用户授权后，通过标准化接口向可信数据空间运营平台发起数据查询请求，请求中附带用户授权凭证与待核验的诊疗信息标识。

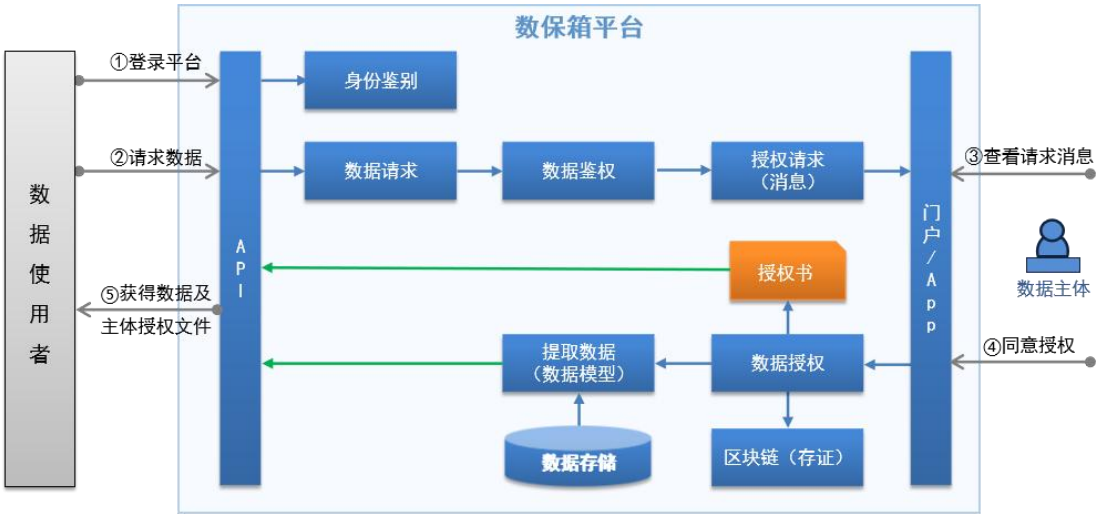
安全计算与反馈：数据空间平台接收到请求后，首先验证授权链的真实性与有效性。随后，在平台内部调度隐私计算引擎，在不输出原始数据的前提下，对存储在医疗机构数据节点中的相关数据进行联合计算，生成核保所需的特征指标或风险评估结果。

结果交付：计算产生的加密结果被返回至保险公司。保险公司获得结果为“是/否”或风险评分等非原始数据形式的结论，并据此完成自动化核保与理赔流程。所有请求、授权及计算行为均被区块链记录存证。

图四-16　快速核保



图四-17　用户授权



图四-18　数据使用流程图

➢ 适用领域

人身保险核保与理赔：尤其适用于健康险、寿险、意外险等需要快速核实被保险人健康状况的场景。

互联网保险业务：为线上销售的保险产品提供实时、可信的风控能力，提升用户体验。

保险反欺诈：在合法授权前提下，通过安全多方计算等技术，在不暴露个人隐私的情况下，联合多方数据源进行欺诈行为分析。

3. 教育领域

案例1. 某高校可信校园密码服务平台（北京数字认证）

➢ 案例背景

2018 年，某高校率先实施并应用了基于电子签名技术实现的可信电子成绩单解决方案，面向本科生、研究生签发可信电子成绩单，受到广大学生的认可。然而，随着某高校信息化建设进程逐步推进，校方逐步在电子合同在线签署、电子招投标、电子文件签章等方面，产生了密码技术应用的迫切需求。此外，校方

意识到现有的独立分散的电子印章基础设施已使用多年，出现了性能和稳定性等相关问题。基于现状分析，结合国家及教育部相关文件工作要求，某高校拟依托密码技术建设统一的密码服务平台。

➢ **建设目标**

某高校旨在通过本项目建成体系完整、安全稳定、高效可用的学校电子签章应用支撑体系，夯实密码应用和运营管理的基石，落实国产密码在重要校园信息系统中的应用，基于密码技术的安全支持，构建基于密码技术的安全可信教育网络空间，实现电子签章的全面应用，并根据后期情况进行推广，有效提升校园业务电子化办理程度，增强校园信息化服务能力，实现信息系统可信运行，提升教育服务满意度，促进办学效益提升。

➢ **建设方案**

图四-19　高校密码服务平台架构图

某高校密码服务平台采用组件化、模块化方式进行构建，可支持不同密码算法、不同类型的密码设备和服务，充分考虑密码资源利旧需求，统一纳管已购签名验签服务器、服务器密码机以及 PDF 签章服务器，同时具有高度扩展性，能够实现密码服务的统一规划与管理、汇聚各业务系统的密码服务相关数据，有效解决校园密码应用统一支撑问题。

案例2. 高校5G专网国密二次鉴权解决方案（辽宁移动）

➢ **案例背景**

在教育行业的数字化浪潮下，传统基于物理边界的校园网络安全模型，在混合教学、海量设备接入和移动办公的新常态下已然失效。为保障核心教学科研数据安全，并满足高性能、灵活接入的网络需求，构建一个无处不在安全的新型网络环境成为迫在眉睫的任务。

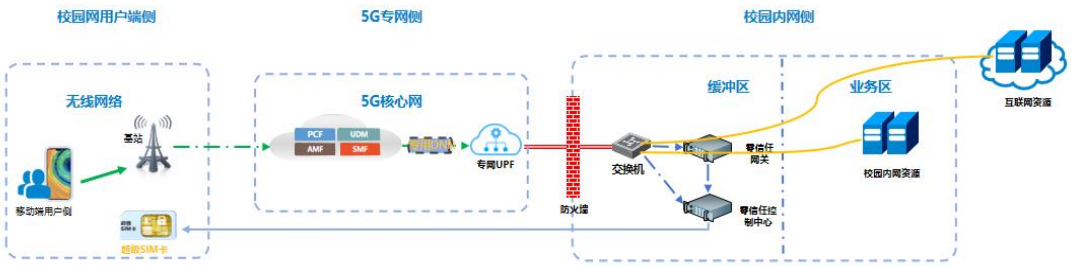
校园网 5G 专网融合国密零信任技术的应用，根本上是为应对高等教育数字

化转型带来的深刻挑战。5G 专网以其大带宽、低时延和网络切片能力，为校园提供了高质量的连接底座；而零信任架构则以“永不信任，始终验证”为核心，实现了以身份为中心的动态、细粒度访问控制。二者融合，共同构筑了一个“访问便捷、权限最小、风险可控”的智能安全体系，这不仅是对网络性能的升级，更是从传统静态防御向自适应安全免疫系统的根本性转变，为智慧校园的可持续发展奠定了坚实根基。

- **方案架构**

在充分利用 5G 专网安全技术的基础上，在校园网 DMZ 区部署超级 SIM 国密零信任安全网关，实现校园网用户网络接入的安全管控。本方案中，用户终端通过超级 SIM 卡与 5G 核心网进行第一次双向认证，超级 SIM 卡安全存储用户唯一身份（SUPI）和根密钥，确保只有合法卡和用户才能接入网络。超级 SIM 卡及网络侧全面支持 3GPP 标准定义的国密 ZUC 算法。在认证和密钥协商过程中，可使用 ZUC 算法生成加密和完整性保护所需的密钥，显著提升核心信令流程安全性。

在第二次认证中，超级 SIM 卡集成了支持国密公钥机制的硬件密码模块，访问国密零信任网关时由终端发起签名，国密零信任控制中心完成验签，整个二次鉴权过程在专网内完成，用户证书与密钥数据不出公网。有效构建无法抵赖、无法篡改、动态访问控制安全边界，实现内网、互联网访问流量的全程审计，根据用户的行为进行动态访问控制。



图四-20　5G 专网国密二次鉴权架构图

5G 专网国密二次鉴权包含 5G 专网、超级 SIM 国密零信任网关、超级 SIM 卡。

5G 专网：5G 专网提供专属 UPF 接入，业务从 5G 接入点－基站－传输网－核心网－外网全链路与互联网、其他用户隔离。在无线基站侧提供专属空口资源，与公众、其他政务 5G 终端在无线接入环节即物理层隔离，该资源仅政务专属应用场景使用。在运营商承载网传输过程中，提供物理级隔离专属通道。切片隔离“硬切片”本质上是在移动终端－政务外网的运营商链路中，运营商进行了物理层资源专属隔离，保障端到端数据传输的安全性。

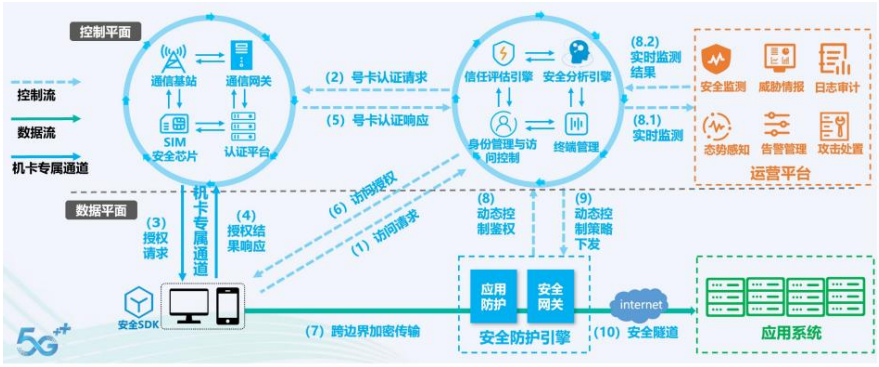
超级 SIM 国密零信任网关：基于 SPA 单包授权技术与 UDP 复合敲门，强制实施“先认证、后连接”的访问模式，实现用户终端网络准入。以零信任技术为核

心，将控制平面与数据平面分离，构建集动态可信边界、全局态势感知为一体的网络安全防护体系。

超级 SIM 卡：集成安全芯片和密钥存储能力，结合 PKI 非对称加密技术，功能集成在零信任网关上，实现便捷的身份鉴权服务。基于号卡身份，可实现网络访问行为的实名化审计。

➢ **主要功能**

超级 SIM 国密零信任网关以号卡身份为“安全大脑”，基于接入安全、身份安全、行为安全、访问安全、自身安全等多个维度构建安全接入防护能力，最大程度缩减系统暴露面、助力纵深防御与终端数据保护，整体实现全方位立体的业务安全访问体系。



图四-21　超级 SIM 零信任网关功能图

（1）层次化认证体系：依托国密超级 SIM 卡，针对不同安全等级的业务系统和应用场景，提供基于手机号码的号认证、基于号卡的 SIM 快捷认证、基于数字证书的 SIM 盾认证和 SIMKEY 认证等不同认证方式，符合 GW 0202-2024《国家电子政务外网 5G 专用网络接入规范与安全要求》。

（2）AI 敏感词管控：安全网关支持企业接入 AI 应用，包含号卡认证能力、单点登录、动态风险识别与访问控制等功能。对 AI 应用提供敏感词防护能力，支持敏感词策略灵活配置，支持自定义敏感词组和类别，可叠加组合检测。支持智能语义识别，精准识别敏感内容。支持变体绕过检测，以及多类型内容分析，包含文本、图片、文档内容检测，可提取其中文字进行风险识别。对大模型代答内容进行动态脱敏处理，防止敏感信息泄露。记录触发敏感词策略的用户行为，提供完整日志，支持事后溯源分析，保障企业 AI 应用的安全使用，防范数据泄露和违规风险。

（3）安全沙箱：集成安全沙箱功能，支持用户在一台计算机上建立逻辑隔离空间，创建沙箱为工作空间，本地为个人空间，工作空间和个人空间之间通过数据隔离、进程隔离、网络隔离、文件隔离等保障一切工作行为在安全沙箱内完成。

（4）国密双算法引擎：内置安全加密芯片，并通过国家密码管理局商用密

码检测认证中心二级认证。支持国际国密双算法，可以根据用户需求选择不同的安全协议及安全套件。

- **适用领域**

本方案适用于教育、政务、医疗等行业访问内网资源、网络安全管控的场景。

- **方案特色**

（1）提高了业务访问效率，为师生用户打造了一个无缝、高效且资源丰富的数字化学习环境。消除了反复登录认证各类校园网资源的烦琐，实现了从课堂到宿舍，从校内到校外的一次登录、多维度检测的便捷接入体验。同时，配合5G 校园专网专用 DNN 切片技术，以及 5G 高宽带、低时延的特性，让师生用户能够随时随地一键直达所需的教学平台与学术资源，保障了直播课、学术资料下载等关键应用的高速流畅，极大减少了网络卡顿对教学进度的干扰。

（2）构建智能的内容安全与合规性屏障，本方案通过敏感词实时检测技术与终端沙箱的深度结合，实现了从用户终端到网络资源的一体化内容安全治理。它能主动识别并阻断通过外网（如社交媒体、邮件）泄露内部敏感信息的行为，同时也能监控并审计对内网知识资源的违规下载与传播，将数据泄漏风险进行闭环的管控。用户访问校园内网资源与互联网资源所有流量统一纳入代理，实现了对网络访问行为的可视与精细化管控。

4.医疗领域

案例1. 某三甲医院密码服务平台（北京数字认证）

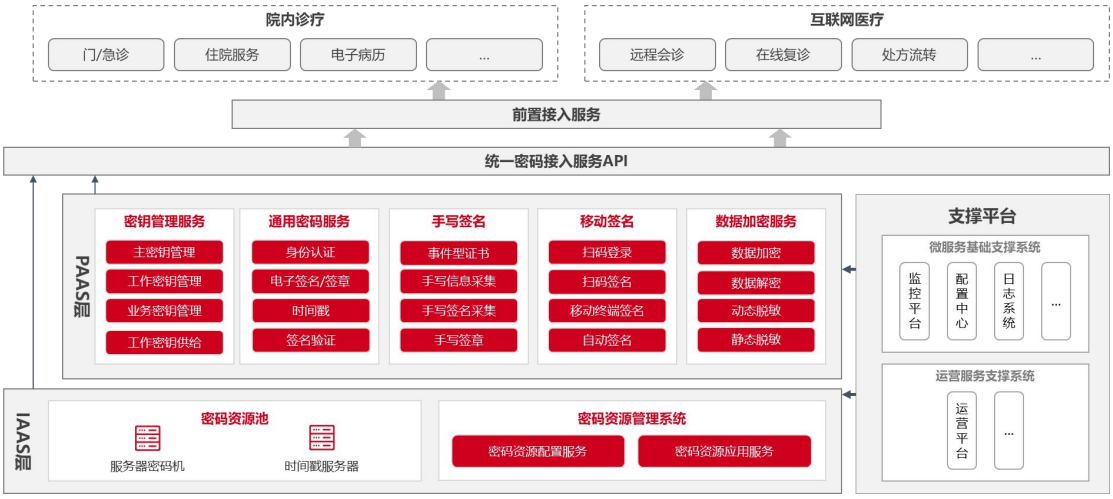
- **案例背景**

2018 年，某三甲医院主要的医疗业务系统已分别集成电子签名、可信时间戳加盖、患者签名的应用，实现了对医疗文书、检验医疗文书、检查检验报告等电子文件进行电子签名和可信时间戳处理。近年来，随着政策法规陆续颁布，以及业务和技术的不断发展，某三甲医院面临着密码设备到期、密码上云迁移难、密码服务扩展难、密码应用合规难等问题，亟须探索新的密码应用模式。

- **建设目标**

依托医院云环境，建设医院密码服务平台。构建医院密码基础设施，为医院HIS、电子病历系统等 10 余个业务系统提供密码服务，主要解决医院医技护、患者电子签名，以及互联网医疗业务密码应用。此外，建设病案归档模块，解决医院病案电子签章，实现病案归档无纸化，满足合规性要求。

➢ 建设方案



图四-22　医院密码服务平台架构图

某三甲医院密码服务平台主要包括签名验签服务、时间戳服务、加解密服务、协同签名服务、手写签名服务、数据脱敏等服务，以及配套的密码服务支撑系统等，密码硬件为服务器密码机、时间戳服务器以及安全认证网关，用于解决医院医技护、患者签名、移动签名、数据加密/脱敏等业务场景，满足多院区医疗业务系统密码应用，并为医院关键业务系统密评奠定基础。

案例2. 隐私计算的数据流通利用基础设施方案（辽宁移动）

➢ 案例背景

当前，数据作为关键生产要素的价值日益凸显。国家《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）等政策，正推动建立“可用不可见、可控可计量”的数据流通新范式，为隐私计算技术的规模化应用提供了明确的政策指引与广阔的市场空间。

面对金融、政务、医疗等行业迫切的跨域数据协作需求，以及传统数据共享模式带来的安全与合规挑战，市场亟须能够打破“数据孤岛”的破局之道。

中国移动不仅是这一趋势的响应者，更是行业的引领者。我们凭借顶级的隐私计算研发团队，深度主导并参与多项国际国内核心标准的制定，技术实力与行业影响力屡获权威认可。基于此，中国移动适时推出隐私计算解决方案，通过先进的密码学与分布式技术，在确保数据“不出域、不外泄”的前提下，实现“数据不动价值动”，为千行百业构建安全、可信的数据协作基础设施，赋能数字化转型新征程。

➢ 方案架构

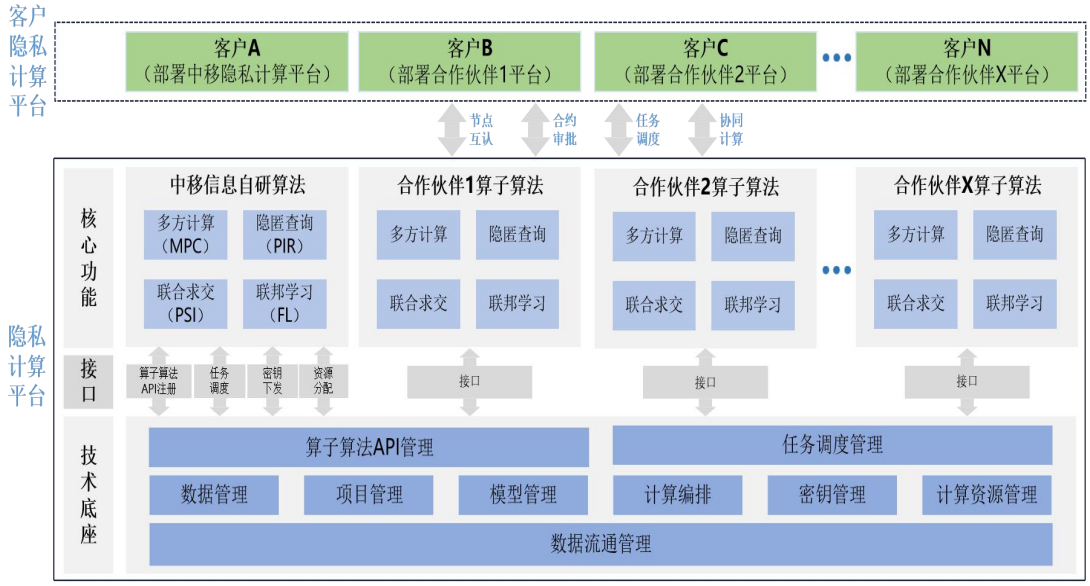
平台采用创新的云原生“1+X”隐私计算架构，打造高效、安全的技术基座：

“1”个技术底座：集成了统一的资源、数据、项目管理和 API 调度能力，保障平台稳定可靠。

“X”个算法模块：汇聚多种主流隐私计算算法与功能组件，支持异构算法

一键集成、灵活调用。

该架构成功实现了算法与算力解耦、数据与算法解耦。通过可视化编排界面，用户可像搭积木一样，通过拖拽快速组装定制化的隐私计算应用。系统具备卓越的开放性、灵活性与扩展性，精准适配各类复杂业务场景。



图四-23　基于隐私计算的数据流通方案架构图

- **主要功能**

平台集四大核心功能于一体，构建了完善的数据安全流通技术屏障：

多方安全计算能力，在无第三方环境下，保障多个参与方协同完成计算任务，各参与方仅获取自身结果，无法窥探他人原始数据。基于秘密分享、同态加密等密码学技术，真正做到“数据不搬家，价值可流动”。

联邦学习能力，在数据不出本地的前提下，通过加密机制实现多方联合建模。融合密码学与分布式优化，推动从“数据聚合”到“能力聚合”的新型协作模式。

安全求交能力，基于隐私保护集合求交（PSI）技术，实现多方数据的安全交集运算。在获取准确交集结果的同时，严格保障各方数据隐私，实现最小化信息披露。

隐匿查询能力，支持查询方从服务方获取数据，而服务方无法感知查询内容。具备百亿级数据处理能力，响应速度达秒级，完美支撑三要素验真、用户标签查询等高并发业务场景。

- **适用领域**

本方案广泛应用于对数据安全与隐私保护有高要求的领域：

（1）金融风控：助力银行、保险等机构在合规前提下联合构建反欺诈与信用评估模型。

（2）医疗健康：支持多家医院安全开展联合科研与疾病预测分析，保护患者隐私。

（3）政务共享：促进政府各部门数据互联互通，在保障公民隐私的同时提升服务效能。

（4）广泛适用：同样适用于运营商、互联网、能源等任何需进行安全数据协作的场景。

- **方案特点**

（1）架构领先，开放灵活：创新的“1+X”云原生架构，以统一底座集成各类可插拔算法模块，实现全面解耦。平台具备高度的开放性与扩展性，从容应对技术迭代与多样化的业务需求。

（2）安全合规，可信可靠：严格遵循国家安全标准，通信链路采用多重加密与认证保护，确保数据全流程“不出库”。支持无第三方架构，从底层构建坚实可信的安全防线。

（3）性能卓越，支撑业务：采用分布式密文计算架构，实现高性能、高并发、高可用的计算能力。百亿级数据查询可达秒级响应，满足实时业务对算力与效率的极致要求。

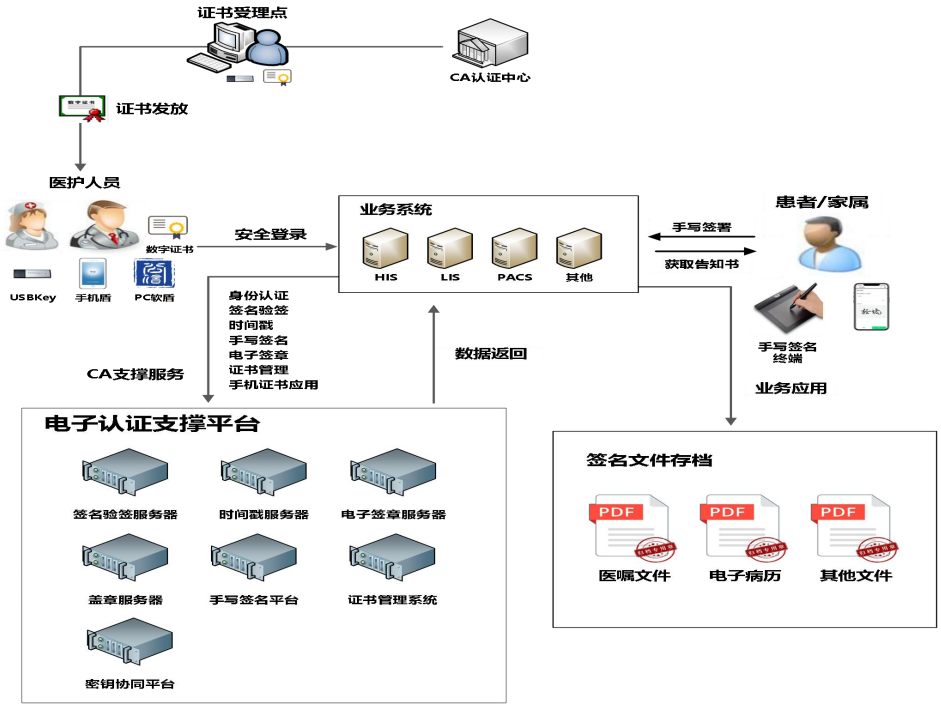
（4）操作便捷，易于使用：提供图形化 IDE 界面，支持拖拽式可视化编排。大幅降低技术使用门槛，使业务人员也能快速构建和部署计算任务，提升协作效率。

（5）部署灵活，按需适配：支持实体机、容器化、云端等多种部署模式，具备快速弹性扩容能力。并可灵活配置 CPU/GPU 算力资源，精准匹配从测试到生产的全周期需求，实现降本增效。

案例3. 医疗机构电子认证解决方案（辽宁公信）

- **案例意义**

随着医疗信息化建设的发展，全业务流程电子化成为必然趋势。一方面规范业务流程，提高工作效率，最大程度避免医疗风险，让诊疗过程更透明，也保证患者的合法权益。另一方面，医疗信息化面临着假冒身份、篡改信息、越权操作、否定责任等方面的安全问题。依据原卫生部《关于做好卫生系统电子认证服务体系建设工作的通知》、国家卫健委《医疗卫生机构网络安全管理办法》（国卫规划发〔2022〕29 号）的要求，需要在医疗信息系统建设过程中同步规划密码基础设施建设，构建电子认证服务支撑体系，从而保证诊疗过程中的身份可信、数据可信、行为可信、时间可信，可追溯、防抵赖，最大限度保障医患双方的合法权益。



图四-24　电子签名整体架构图

➢ **实现的主要功能**

医院内电子认证支撑平台包括签名验签服务器、时间戳服务器、证书管理系统、密钥协同平台（PC 软盾、手机盾）、手写签名平台、电子签章服务器、盖章服务器等密码安全产品，能够实现院内业务系统的电子认证服务功能如下：

统一的数字证书服务：

为医院构建统一的数字证书发放与服务机制，方便医院内数字证书发放和应用，同时为医院内证书用户提供高效、便捷的数字证书生命周期服务（新办、更新、变更、注销等）。

电子认证应用支撑平台包括功能：

（1）统一的身份认证服务：利用签名验签服务器实现基于数字证书的可信身份认证，为数字医疗信息系统解决行为人的身份凭证及凭证认证问题。

（2）医护人员电子签名服务：利用签名验签服务器提供的数字签名验证服务，实现医护人员在关键业务环节的电子签名和签名验证，实现医疗数据的完整性保护，以及责任认定等安全需求。

（3）可视化电子签章服务：通过电子印章服务器将数字证书与用户的章模或者手写笔迹进行绑定，实现数字医疗信息系统关键流程的可视化电子签章。电子签章系统符合国家密码局有关电子签章的规范，采用国家密码局规定的密码算法进行签名和加密。

（4）可信时间戳服务：为数字医疗信息系统建立可信时间戳服务。数字医疗信息系统通过调用时间戳服务对数据原文加盖时间戳，确保操作记录的时间可靠性。

（5）移动端电子签名服务：基于“密钥协同平台”实现用户在 PC 端扫码登录、扫码签名，也可以实现移动端登录及签名，满足 PC 端、移动端实现重要数据抗抵赖性安全需求。

（6）患者端手写签名服务：基于手写签名服务器与信息采集终端应用，可实现患者或患者家属对知情同意书的手写电子签名，确认患者端的责任归属，保障知情同意书在实现电子化后的合法可信。

（7）证书自助管理服务：移动证书通过密钥协同平台，实现医院内数字证书的自助管理。USBKey 证书通过证书管理系统，实现院内数字证书的自助管理。实现证书静默更新服务，减少人为更新证书造成的业务中断，减少不必要的业务风险。

（8）证据保全服务：基于数字签名技术，在电子数据生成时进行可信的固化处理，传输时进行可靠的加密封装，存储时进行长期的安全存储，通过电子数据固化时形成的时间戳和摘要数据，可以权威验证电子数据生成时间、数据内容的真实性与完整性，从而提高电子数据的证据效力。

- **方案优势**

（1）国内首创新功能

PC 软盾：PC 端安装证书助手，实现传统 USB-Key 证书功能，并能够做到“一张证书”在移动端、PC 端共用。解决手机证书、USB-Key 证书无法实现的功能，如手术室签名、传染病医院感染区等场景。

证书授权功能：证书具有授权他人使用功能，并能实现授权日志管理。解决主任医师证书多人同时共用问题，而且不需要颁发多个主任医师证书。

（2）集成便利化

中间件产品化：我公司的所有产品应用中间件已实现高度集成产品化，供应用系统嵌入、调用。能最大限度降低业务系统集成改造成本。

（3）服务效率高

“手机盾”产品无需在 PC 端安装证书解析工具，应用程序简便、易用，降低服务工作量；程序升级在服务端，保证容错效率更高效。“数字证书”颁发服务全部线上处理，支持多种身份核验功能，服务体验更完美。

案例4. 医疗领域密码应用方案（航天信息）

- **方案概述**

电子签名认证系统基于 PKI 安全体系的应用进行设计，方案主要以 PKI 基础设施为基础，以数字证书为媒介，以 CA 安全认证服务器为依托，通过服务器密码机、VPN 网关、协同签名系统、时间戳系统、PDF 电子签章系统、手写数字签名系统，将 PKI 安全体系与业务系统进行有效结合，以满足用户系统的应用层信息安全的要求。

实现为用户信息系统的电子认证集成和改造提供全方位服务支持，并且规范用户电子认证服务体系，建立响应快速的售后服务体系，并针对基于用户信息平台建设需求，实现高强度的应用安全保护，为用户应用提供统一的电子签名服务，内容包括：

数字证书服务：通过第三方 CA 证书对参与系统的人员进行数字认证。受理用户人员的数字证书申请、审核，并为其制作成数字证书并发放到使用人员手中；并在用户信息系统中实现以数字证书作为用户身份认证的唯一标识，取代传统的用户名+口令等安全级别较低的身份认证模式。

敏感数据机密性完整性保护：认证用户内部员工在参与业务系统的关键操作和关键数据进行签名或加密，来保障信息的保密性、完整性、可靠性。

时间有效性保护：通过可信时间戳的服务，来保障系统所处理的数据在某一时间（之前）的存在性。通过数字签名技术和基于公共标准时间源的时间服务系统紧密结合，对数据加上时间标记的技术。

可视化电子签名：电子签章服务主要采用使用签名和用户加盖印章方式来确保纸质文件有效性，而随着电子签名法的实施，数字签名和手写签名效力达到等同地位，用户也应该为使用用户信息管理系统的各级使用人员提供数字签名来实现电子文档的有效性验证。但数字签名是一串字符，不能像现实世界的手写签名一样直接展现给患者，因此，需要通过相关技术手段实现数字签名的可视化，而电子签章正是数字签名的图形化展示，在用户信息系统中集成电子签章系统能够有效直观地解决责任认定问题。

通信安全：采用 IPSEC/SSL 综合安全网关对通信信道采用国产密码算法如 SM2、SM3、SM4 等，进行机密性完整性保护。

法律法规支持：电子认证相关环节严格按照行业规定，数字认证技术严格遵照《电子签名法》《电子认证服务体系系列规范》《卫生系统电子认证服务管理办法（试行）》《电子病历基本规范（试行）》《电子病历应用管理规范（试行）》和互联网医院管理办法及互联网医院基本标准（试行）等相关法律法规的要求，为客户业务系统提供权威的法律保障。

- **需求分析**

（1）满足互联互通成熟度评级 4 级甲需求：根据《国家医疗健康信息区域卫生信息互联互通标准化成熟度测评方案（2017 年版）》对三级医院的信息互联互通标准化成熟度测评等级要求，以及国卫办医发〔2018〕20 号《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》，到 2020 年，三级医院要实现院内各诊疗环节信息互联互通，达到医院互联互通标准化成熟度 4 级水平。

电子病历系统需要达到互联互通标准化成熟度 4 级甲等或以上级别，其中涉

及无纸化归档，就要实现电子病历无纸化，首要核心是电子病历具备法律效力。病历作为医护人员在诊治患者全过程中行为是否合法的唯一能具有说服力的证据，电子病历与传统的手写纸张病历所反映的内容并无差别。

（2）满足电子病历评审五级需求：以电子病历为核心的医院信息化建设是医改重要内容之一，为保证我国以电子病历为核心的医院信息化建设工作顺利开展，逐步建立适合我国国情的电子病历系统应用水平评估和持续改进体系，2018年，国家卫生健康委员会制定了《电子病历系统应用水平分级评价管理办法（试行）》和《电子病历系统应用水平分级评价标准（试行）》，将电子病历划分为9个等级。

其中，要求地方各级卫生健康行政部门要组织辖区内二级以上医院按时参加电子病历系统功能应用水平分级评价。到2019年，所有三级医院要达到分级评价3级以上；到2020年，所有三级医院要达到分级评价4级以上，二级医院要达到分级评价3级以上。电子病历系统应用水平分级评价管理办法及评价标准，涉及电子签名有38分，可达5级或以上要求。

（3）权威合法CA数字证书认证需求：遵循国家卫健委制定的《卫生系统电子认证服务管理办法（试行）》，为医护工作人员、患者签发移动CA数字证书，用于移动端应用的身份认证、业务电子签名。

医护技端电子签名应用需求：在医院业务流程中，为医护人员实现对电子处方、电子病历、检验报告、电子健康档案等业务数据和文件电子签名。保障数据安全性、可靠性和责任可追溯，符合《电子病历基本规范（试行）》《卫生系统电子认证服务管理办法（试行）》和《中华人民共和国电子签名法》等法规和行业标准要求。

（4）患者端电子签名需求：使用可信的手写数字签名技术解决患者电子签名的问题，实现患者知情同意书无纸化，保障患者知情同意书的合法可信。病人或者家属知情文书的无纸化签署，采用手写数字签名模式，由患者手写签名系统手写签名笔迹数据，当前可靠时间信息，签署时权威采集指纹数据、录像视频数据、录音音频数据为患者及家属签发数字证书，完成对电子文档的数字签名。同时可使用有线签名屏、无线平板满足不同场景下，患者进行电子签名的需求。

（5）移动电子签名场景需求：能够结合微信这个已经成熟和广泛使用的APP终端工具，快速绑定实名身份和权限，与医院中的各个应用结合，实现安全、可靠的移动身份认证。实现移动登录认证、移动电子签名、手机扫一扫电子签名等应用。行为可追溯、抗抵赖和责任认定需求：建立可靠的责任认定机制，通过电子签名和时间戳技术，采用移动电子签名技术，实现任何操作和行为均可追溯，有效防止内容否认、时间否认和行为否认，以此约束各类用户的工作质量。

（6）数据安全保护需求：医疗数据是诊疗的基础，在国家医疗信息规划中，

未来要支持各医院卫生信息的共享，通过区域医疗需要实现信息共享协作，这就意味着电子健康档案和电子病历会在各医院平台和区域医疗平台之间流转。因此，医院医疗信息系统须建立医疗数据的完整性保护机制，利用可靠的电子签名技术保证数据在产生、传输、存储、再利用的整个生命周期过程真实、完整、准确，保证“数出有源”。

（7）电子病历归档管理需求：在医院的临床信息系统建设达到一定程度时，电子病历的无纸化存储，数字化病案管理成为紧迫需求。数字化病案管理的核心是建设独立的电子病案管理信息系统，将所有临床信息系统的数据进行整合，形成完整的电子病案内容，通过引入一种可靠的、通用的文件，将临床业务数据转化为版式文件，使得数据可脱离临床信息系统展示并供多方查阅。电子签名的建设，特别是患者文书实现无纸化，将对电子病历的归档，提供基础保障。

（8）电子病历归档管理需求：支撑医院信息系统通过第三方机构的商用密码应用安全性评估，顺利通过密评机构的评估。

5.电信与互联网领域

案例1. 国产密码算法的5G可信专网解决方案（辽宁移动）

- **案例背景**

当前国际、国内信息安全形势严峻复杂，网络攻击、黑客技术不断升级，数据泄露、失泄密事件危害严重。国家安全保密态势高压，一经发现泄露国家秘密，有关部门将对直接负责主管人员和相关负责人给予处分，对构成犯罪的将追究刑事责任。国家对工作秘密安全管控持续提速，已出台政策明确不允许在互联网未采取保护措施传递工作秘密。然而，机关单位保密手段欠缺，普遍缺少移动化安全保密解决方案，无法使用普通手机、平板等移动设备处理工作敏感信息。

在此背景下，中国移动践行央企政治责任，与互联网安全隔离的 5G 专用网络（5G 可信专网），可向党政机关、央国企、科研院所、涉密单位等提供高安全通信和移动办公服务。

- **方案架构**

中国移动 5G 可信专网是国内首个基于信创技术的全国产化专用网络；用户在中国移动 4G、5G 基站覆盖区域均可接入专网，实现了全国广域接入；专网与公众通信网络安全隔离、零暴露，业务端到端均采用 SM 系列国密算法加密传输、加密存储；专网实现了专建、专维、专用，专属团队为专网提供了更高等级服务，保障高品质网络服务。

图四-25　专用网络示意图

➢ **主要功能**

（1）终端双系统在线：定制双系统终端，生活系统接入互联网，畅享精彩；工作系统接入专网，安全办公。

（2）通话端到端加密：工作系统提供端到端加密通话，通话质量好、体验佳。

（3）专属定制应用：定制终端工作系统内预置视频会议、即时消息、企业邮箱等专网办公应用。视频会议应用基于 VPN 双栈隧道加密技术，支持工作秘密级视频通信，满足最大 300 人同时在线的 1080P 高清会议；即时消息应用基于 SM 系列国密算法，支持用户个人信息、聊天、文件、通讯录等全面安全防护；企业邮箱应用基于信创国产系统，提供反垃圾、防病毒功能，支持手机、平板、电脑等多种终端形态接入访问。

➢ **适用范围与场景**

中国移动 5G 可信专网可向党政机关、央国企、科研院所、涉密单位等提供高安全通信和移动办公服务。

曾为某国家机关 300 余名公务人员配发专网定制终端，与办公电脑协同，满足用户高安全移动办公需求。

案例2. 个人数据可信流通方案（辽宁移动）

➢ **案例背景**

数据已被国家顶层设计确立为新的生产要素，《关于构建数据基础制度更好发挥数据要素作用的意见》与《“数据要素 X”三年行动计划（2024- 2026）》提出数据产权、流通交易、收益分配、安全治理“四大制度”，并推动数据要素贯穿生产、分配、流通、消费和社会治理各环节，加快把数据资源优势转化为经济发展新动能。

然而，数据无形、可无限复制且权属复杂，尤其是个人在享受公共和商业服务时留下的大量关联数据，既蕴含价值又面临隐私泄露与滥用风险。如何解决个人数据开发利用中存在的授权难、监管难、安全保护难等问题，提高数据供给意愿，是数据要素流通的重要课题。

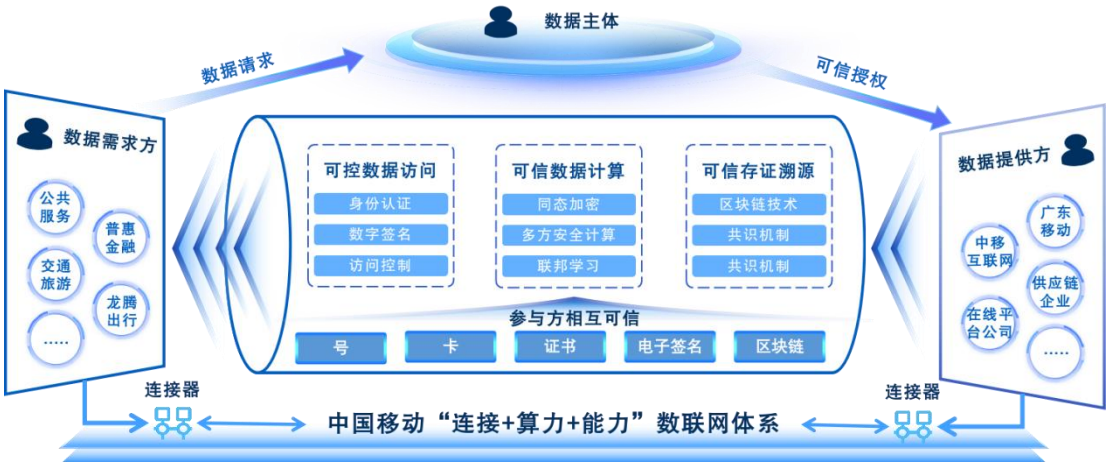
为此，中国移动基于移动认证规模、安全及 SIM 卡密钥管理能力等优势，打

造的数据可信流通解决方案，可实现数据主体、数据提供方、数据使用方等多方数据授权可信流通，解决数据要素流通合规困境、明确数据权属，有效推动多方数据融合应用，促进数据“供得出、流得动、用得好、保安全”。

本方案已获得广东省政数局主办的第二届“数据要素×”大赛广东分赛的数据创新应用奖、中国互联网协会主办的金灵光杯全国赛创新奖、中国信息协会主办的 2025“数字政府”成果与创新案例等多项荣誉。

- **方案架构**

以个人用户数据主权为核心，依托中国移动独特的“号-卡”体系和数联网（DSSN）基础设施，构建一个集“可信身份认证、自主授权管理、全程加密保护、链上存证溯源”于一体的个人数据安全可控流通解决方案，确保数据在产生、授权、流通、使用的全生命周期中，始终将控制权和知情权掌握在个人用户手中，平衡数据利用效率与隐私安全保护的关系，最终实现个人数据要素潜在价值的激活。



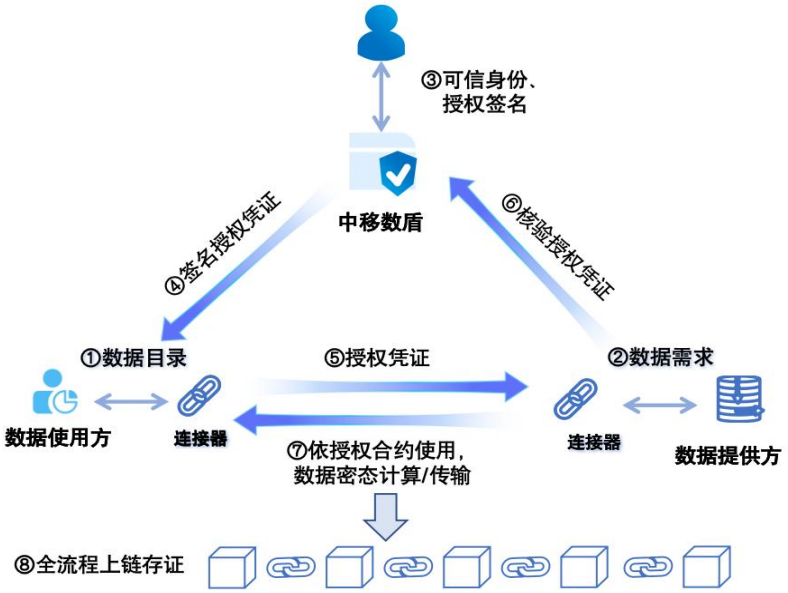
图四-26　个人数据可信流通架构图

本方案围绕“身份—授权—流通”三大环节展开。构建可信统一身份标识，以实名手机号码为核心，以承载国密安全芯片的超级 SIM 卡为硬件载体，通过号卡认证、三要素核验与人脸识别建立“人—机—卡”一致性，颁发可信身份证书并同步写入区块链与 SIM 卡；SIM 卡据此生成公私钥对，私钥仅存卡内，公钥上链存证，用户可凭借私钥完成数据加密与签名。并建立个人数据可信授权与存证机制。当数据使用方申请调用已上架数据时，系统向用户发起授权请求，经用户确认后自动生成授权凭证与策略，使用 SIM 卡私钥签名并上链存证；数据使用方持授权凭证向数据持有方请求数据，数据提供方核验凭证后返回加密数据，并将使用记录实时上链，用户可随时查看、更新或撤销授权。

- **主要功能**

本方案基于手机号构建统一的可信账号体系，结合 SIM 卡密钥管理和数字签名功能，完成对数据资产的授权；基于区块链可信存证能力，各参与方均可溯源查询，防止抵赖，确保数据利用全程合规。主要涉及数据资产上架、资产流通授

权、资产流通确权和授权凭证查询四大功能：



图四-27　区块链可信存证示意图

（1）数据资产上架功能。数据提供方在数据交易平台上架数据，平台向个人用户发送授权请求，个人用户自主决定是否允许其数据进行上架交易。

（2）资产流通授权功能。数据使用方向个人用户发起用数请求，个人用户同意后向其颁发具有个人签名的授权凭证，用以保障数据授权的透明化。

（3）资产流通确认功能。数据持有方与使用方，基于密钥交换技术构建使用方－持有方临时的对称会话密钥，保障数据流转的端到端安全。数据使用方携带凭证向数据持有方或者数据交易平台获取数据，数据提供方对凭证进行核验。

（4）授权凭证查询功能。将每一次数据流通操作通过智能合约上链存证，固化成可信、可追溯、不可否认的技术证据，为合规审计与监管审查提供决策支撑。数据流通各参与方均可查询授权凭证，凭证在区块链上存证，确保数据利用全程合规。

- **适用领域**

本方案以“手机号为身份，卡为安全硬件”，构筑身份可信、授权可信、通道可信的多方信任底座，结合中移数盾可信身份、授权确权、数据控制等能力，不仅适用于对数据交易中心、数商、大型国央企、数据需求方等有数据要素流通需求的客户，更有助于赋能构建跨区域、跨行业、跨机构的城市级可信数据空间建设。

- **方案特点**

本方案严格落实《个人信息保护法》《网络安全法》《数据安全法》等要求，遵循《信息安全技术 个人信息安全规范》《信息安全技术 个人信息处理中告知和同意的实施指南》等国家标准要求，推动知情同意模式的个人数据流通模式。

具备以下三大特点：

（1）全国首创以“号码即账户、SIM 卡即安全”的数据可信流转技术体系。本方案以实名制手机号码作为个人数据空间的统一身份标识，通过将安全能力下沉至超级 SIM 卡硬件层面，确保数据管理自主性、安全性和稳定性的统一。

（2）全面构建了以个人为中心的“泛中心化”数据流通新范式。个人数据空间业务模式以《个人信息保护法》为基石，巧妙融合中心化平台的撮合效率与分布式授权技术的可追溯性，打造了“数据可查、权限可追”的泛中心化数据流通生态，有效打通数据要素“确权－流通－变现”的全链路，更容易在现有市场环境下推广和被接受。

（3）首创性以“用户赋权”为支点，撬动一个多方共赢的数据要素流通新生态。本方案依托独特的“号-卡”生态和硬件级安全优势，重塑了个人在数据价值链中的核心地位与信任基础，不仅激发了个体参与数据共享的活力，也为构建一个权责清晰、多方互信、价值合理分配的可持续数据要素流通新生态奠定基础。

案例3. 云环境下省级集约化建设方案（航天信息）

- **案例概述**

由某运营商省分公司牵头、航天信息股份有限公司及西部 CA 联合打造的云环境下商用密码集约化服务体系，基于密码运算、密码设备及资源集中化管理手段，屏蔽后台密码设备多样性，实现密码服务集约化、合规化、共享化和云化，达成数据机密性、完整性、真实性、不可否认等安全目标。项目构建统一云密码服务平台，整合管理服务与密码服务能力，打造高效、可靠、易扩展、可统管的云密码基础设施，既为省公司移动通信网络（5G 核心网）、重点业务支撑系统（4A、调度中心）、数据中心（ODS 大数据平台）、云服务（内部云资源池）等内部系统提供服务，又具备向政务、卫健、交通等行业信息系统扩展的能力。截至申报时，平台已上线运行，4A 系统、5G 核心网、内部云资源池等 7 类系统密码应用方案通过专家评审，各项运行指标正常，有效提升省公司内部相关系统密码应用合规性与安全防护水平。

- **需求分析**

某运营商拥有众多移动通信网络、重点业务支撑系统、重要增值业务、数据中心和云服务，融合了大量跨部门、跨平台、跨行业的数据，易遭受网络攻击，存在用户假冒、数据篡改、信息泄露等安全风险。云平台技术架构极其复杂，融合了大量的软硬件资源，因云平台采用虚拟化技术，云平台的主机边界、存储边界和网络边界相对于传统数据中心来讲变得模糊，存在资源池节点数量多、安全数据隔离逻辑复杂等难点，同时云平台敏捷，提高效率，灵活性，也伴随着重大挑战安全性。云平台安全与其自身因素是相辅相成的关系，传统的安全控制通常

无法满足云的安全需求。云平台安全防护难度大，如何通过密码技术保障云平台自身密码安全防护，实现机密性、完整性、真实性、不可否认等安全目标，成为企业亟须解决的问题。需要研发设计出一套完整、体系化、可扩展的密码方案，解决云平台环境下密码应用合规问题。

（1）密码产品繁杂众多问题：由于某运营商 IT 应用系统众多，密码安全应用存在建设标准不一等问题。同时，云上密码应用涉及多种密码安全软硬件配套产品，密码服务能力不同，缺少建设统一标准、统一规范、功能全面的密码安全平台对各类密码安全产品进行统一接入、统一调用、统一管理手段。

（2）系统用户访问安全问题：结合当前某运营商实际情况，存在非授权人员访问应用系统的风险，系统中的重要数据存在被非法获取或篡改的风险，在用户的身份鉴别、重要数据防篡改和防泄漏、审批流程不可否认、新增密码设备或应用接入等方面仍需继续提高，缺少有效地对信息化系统中高并发用户可信认证等密码服务保障问题。

（3）密钥安全管理手段问题：某运营商在项目实施前缺少密钥安全管理手段，另加密密钥的安全性对其保护的数据的机密性至关重要，有权访问密钥的威胁参与者可以读取敏感数据，甚至可能为虚假或修改的记录生成有效签名，因此密钥管理需要提供强大冗余资源合理管理手段。

（4）密码安全决策分析问题：由于商用密码应用改造覆盖应用系统、密评信息、密码应用情况、行业、区域等多个信息维度，管理部门对密码安全类问题缺少体系化认知，难能对某运营商应用密改情况清晰把握，无法及时跟踪、管理决策，缺少决策分析有效支撑手段导致密码安全方面的管理效率较低。缺少体系化全周期密码应用过程的监督管理手段，难以高效合理保证密码安全问题事前、事中、事后的联动及响应机制。

（5）密码服务调度策略问题：云上信息化系统的密码应用安全改造涉及多类实体化密码产品及配套软件产品，通过信息化系统与密码产品直接对接、调用密码服务，存在大量资源冗余浪费问题，缺少对密码资源的合理统管分配方式，难能合理对密码产品的安全能力进行合理调配、高效使用。

- **设计方案**

（1）设计思路：鉴于某运营商存在信息系统多、承载业务重要、数据量大、敏感信息多，需要基于密码技术构建可信网络空间，服务新时代信息系统建设发展的特点，本方案按照“安全合规为基础、落地应用为重点、集约管理为要求、高效完备为特色”的原则，覆盖密码安全管理、安全技术、安全运营“三大体系”，构建某运营商一体化密码应用服务，并与系统整体网络安全等级保护相结合，综合考虑系统物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，形成体系化、分层次、合理可行的密码支撑保障体系。满足

《基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

本方案建设目标是建设某运营商核心云密码服务基础设施，赋能某运营商密码能力，为某运营商移动通信网络、重点业务支撑系统、重要增值业务、数据中心和云服务等领域提供标准、合规、高效、可扩展的商用密码服务，通过密码服务扩展能力具备为政务、卫健、交通等行业信息系统提供密码支撑和保障的能力。

（2）技术路线：随着信息化建设的不断深入发展，由于涉及大量敏感政务数据的处理和存储，信息安全问题成为需要重视解决的核心问题之一。密码技术是保障信息安全的关键技术之一。本次目标是建设合规、正确、有效的一站式密码服务，为某运营商在移动通信网络、重点业务支撑系统、重要增值业务、数据中心和云服务等领域提供密码运算服务，并与系统整体网络安全等级保护相结合，综合考虑系统物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，形成体系化、分层次、合理可行的密码支撑保障体系。满足《基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

- **主要功能**

本方案根据某运营商信息系统部署方式和业务功能，在满足总体性、完备性、经济性原则的基础上，设计一套科学合理、目标明确、措施完备的密码应用技术方案。通过部署 SSLVPN 安全网关、服务器密码机、签名验签服务器、国密浏览器、智能密码钥匙这些密码产品并正确配置，满足系统的密码应用需求，形成体系化、分层次、合理可行的密码支撑保障体系，为系统提供全方位的密码应用防护。

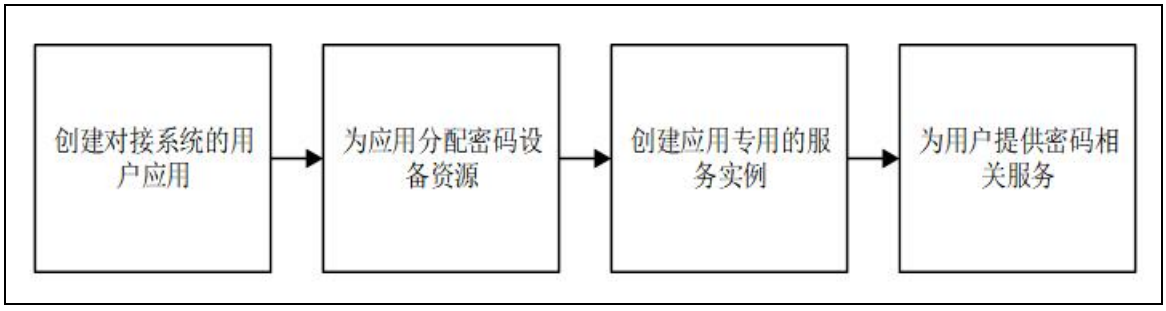
- **管理服务**

系统管理员具备系统管理、设备管理、应用管理、密钥管理、平台监控、态势感知功能权限。

（1）系统管理主要是对使用系统的机构人员进行管理，同时配置态势感知所监控的相关服务，包括机构管理、人员管理、角色管理、系统配置功能。

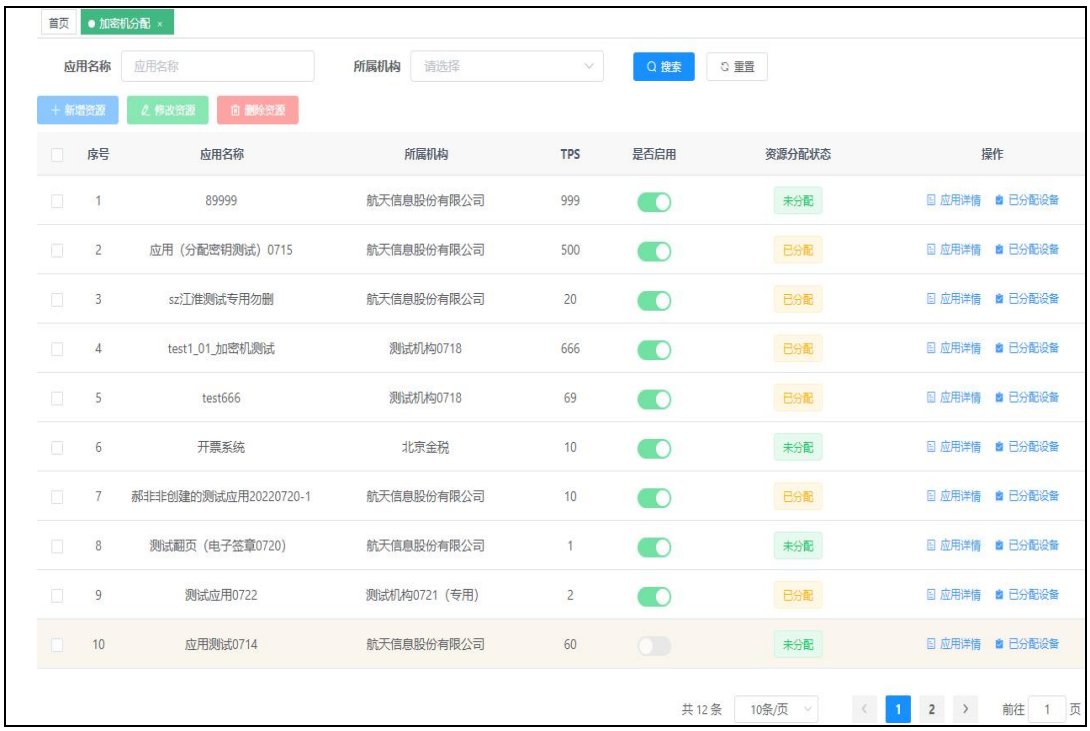
（2）设备管理主要是添加系统使用的相关密码设备，包括加密机管理、签名服务器管理、签章服务器管理、时间戳服务器管理、协同签名服务器管理功能。

（3）应用管理主要是管理对接系统的用户应用，为用户应用分配设备资源、创建应用专用的服务实例，主要的操作逻辑如图所示。



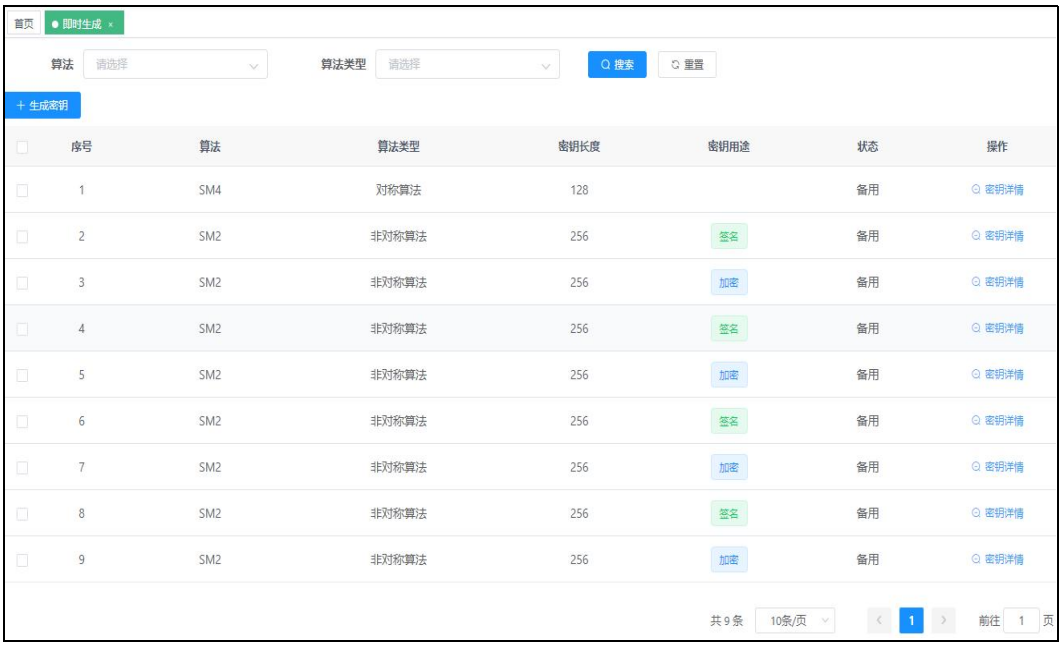
图四-28　操作逻辑图

（4）资源分配主要是为用户应用分配设备资源，包括：加密机分配、密钥分配、电子签章分配、签名服务器分配、协同签名服务器分配、时间戳服务器分配。当用户应用选择了加密机资源后，可以在此分配加密机设备资源，点击加密机分配进入页面，加密机分配的功能包括，查询、新增资源、修改资源、删除资源、应用详情、已分配设备信息功能，如图所示。



图四-29　资源分配图

（5）密钥管理是对密钥提供生成、存储、分发、注销、归档、恢复等全生命周期管理服务。



图四-30　密钥管理图

（6）平台监控主要是对平台的密码设备状态、应用服务器状态、服务实例

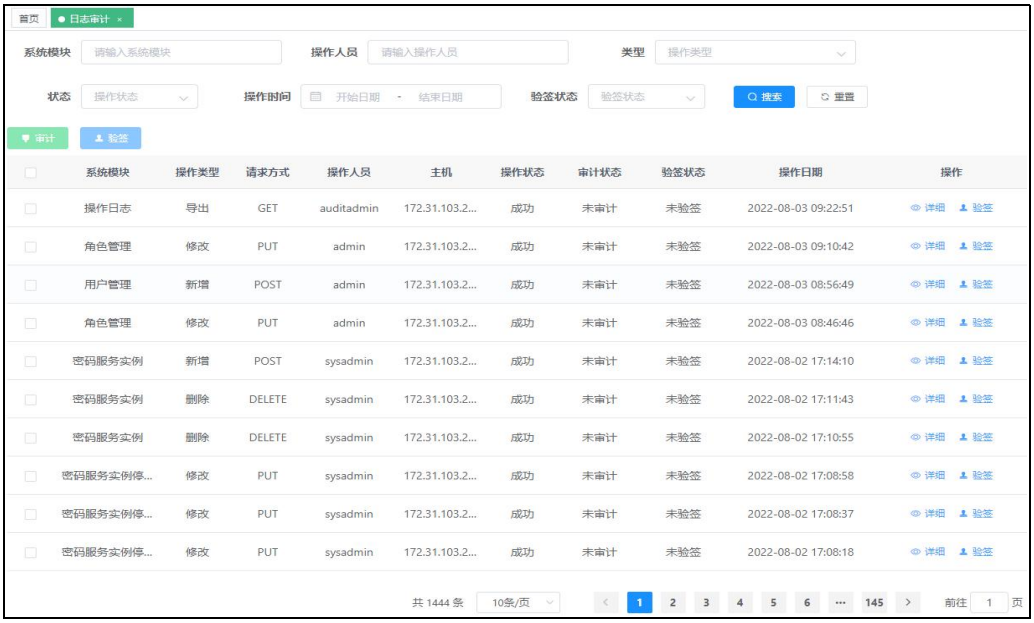
状态进行监控，主要包括设备监控、应用服务器监控、密码服务实例监控功能。

图四-31　平台监控图

（7）态势感知功能用于大屏展示统一密码服务平台设备服务态势，主要包括：设备数据、设备状态、系统运行数据、系统服务情况、每秒事务数、汇总数据，如下图所示。

图四-32　态势感知功能图

（8）审计管理主要是对系统的相关日志进行查看、管理、审计。主要用于完成对日志的验签与审计功能，如下图所示。



图四-33　审计管理图

- **密码服务**

（1）通道加解密服务：提供某运营商不同应用系统与用户之间交互数据使用的传输加密，为应用系统与用户之间建立加密通道。支持 SSL 或 IPSEC 协议接入服务，支持国密算法。

（2）个人数字证书服务：遵循国内相关标准颁发，用来证明个人数字身份。通过采用国产密码技术，采用 SM2 算法支撑客户端数字签名与签名认证等。

（3）设备数字证书服务：遵循国内相关标准颁发，用来证明密码设备的数字身份。

（4）数据加解密服务：为业务系统提供数据对称加密、非对称加密、对称解密、非对称解密等服务。

（5）数据签名服务：为业务系统提供基于国密算法的数据签名、签名验证服务。

（6）随机数服务：提供基于硬件的真随机数服务。

（7）数据完整性服务：提供 HMAC 等模式数据完整性服务。

6.工业领域

案例1. 某大型能源企业密码服务平台（北京数字认证）

- **案例背景**

某大型能源企业运营的业务系统属于国家关键基础设施，随着网络化，数字化发展，其业务系统的网络安全保障一直是工作之重，以前各级公司、分支机构自行建设密码服务体系，应用系统之间无法实现互通，造成信息孤岛，密码服务投入成本高昂，但是应用却极不便捷，存在密码应用管理难、密码服务效率低、

密码服务扩展难等问题。2018 年起，该企业以国产密码算法为基础、以提升业务系统密码应用安全为目标、以规范业务系统密码技术应用为宗旨，规划建设密码服务体系，推进国产密码的全方位应用，全面支撑业务安全合规应用。

➢ **建设目标**

密码服务平台作为某大型能源企业国产密码服务体系的关键组成部分，需依照“统一规划、统一建设、统一运维”的建设思路，利用分层抽象、功能隔离、标准化外部接口等技术手段，提供“安全合规、敏捷高效、广泛兼容、功能完备”的密码服务，从而实现密码服务标准化与组件化。

➢ **建设方案**

图四-34　能源企业密码服务平台架构图

密码服务平台依托于标准规范，基于国产密码算法，通过统一密码接入层、统一密码服务层、统一密码服务层三层支撑架构，面向集团内各类业务系统进行各类密码资源和密码业务的有效整合，提供统一的、标准的密码服务，从密码算法、密码技术、密码服务、密码协议到密码应用流程囊括密码应用的各个方面，提供全方位综合的密码服务。同时，为了保证密码服务平台的安全稳定运行，提供了配套的服务支撑系统，包括开放平台、运行系统、运维系统。

➢ **应用效果**

（1）以私有云模式建设，已完成 80 多个集团内业务系统集成，计划 2 年内接入 300 多个业务系统，覆盖集团所有二级单位。

（2）实现对 80 多台密码机和云密码机的统一管理、调度和监控。

（3）实现了千万级用户的隐私保护，支撑万级 TPS 数据签名服务；面向几十万集团内部用户提供统一的身份认证和电子签名服务；为费用报销系统的报销

单据提供 100 多万笔电子签章服务。

案例2. 某电力企业统一密码服务平台（北京数字认证）

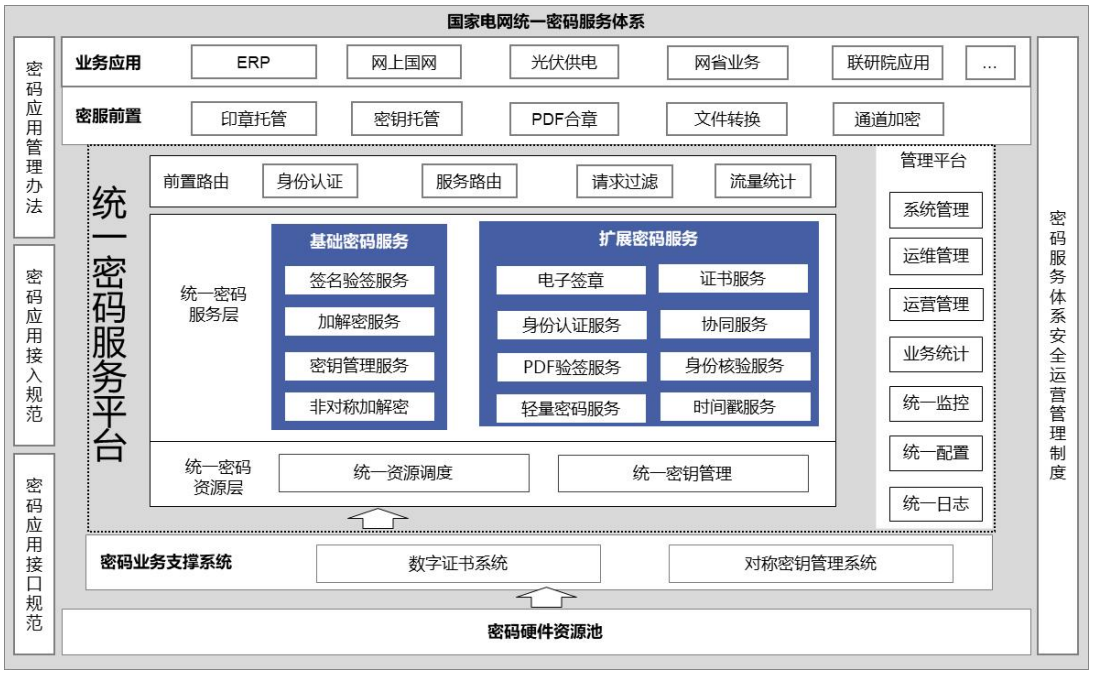
➢ 案例背景

某电力企业高度重视商用密码工作，在国家安全法律法规总体框架下，逐步完善公司商用密码应用责任体系、技术支撑体系、运营服务体系、制度标准体系、评估检测体系、风险管控体系，推进公司商用密码应用的新格局。2018 年起，开展“统一密码”基础设施建设、密码服务平台建设和密码体系管理运营，为公司提供高效、安全、合法的密码服务，保障电网生产运营和社会服务安全。

➢ 建设目标

密码服务体系建设内容包括：数字证书系统、统一密码服务平台、监控与灾备环境。数字证书系统为密码服务平台提供证书签发和密码运算等基础支撑，密码服务平台提供多样的密码服务，并为业务系统提供统一服务接口。监控与灾备环境解决密码服务平台数据同步和状态监控问题。

➢ 建设方案



图四-35　国家电网统一密码服务平台架构图

根据发展业务总体架构设计思路，统一密码服务平台主要包括前置路由模块、证书服务模块、密码服务模块、平台管理模块、扩展模块、数字证书系统和对称密钥管理系统，采用微服务的方式部署在云平台上，能够提供数据加解密、身份认证、密码运算、证书签发、证书验证、电子签章、签约服务、事件证书、协同证书等密码服务，满足业务常用密码应用需求，完善集团密码服务体系。

➢ 应用效果

（1）集中管理密码设备，统一提供密码资源，在其之上构建身份鉴别、电

子签名验签、数据加解密等密码功能服务，成为客户在物联网以及人机交互场景下最有效、最可靠、最经济的信息安全基础设施。

（2）实现了密码服务的统一化以及运维管理常态化机制，通过统一密码服务平台对集团内所有密码服务进行统一管理、统一调用、统一监控，解决了实现了传统密码服务互信难、管理难、运维难、监控难等问题。

（3）采用 3 地数据中心+27 省的两级系统部署架构，成功支撑公司“交易系统、营销 2.0、人资系统”等各专业业务系统共 400 余套接入。截至目前，已累计签发密钥 6 亿多个、数字证书 4000 万张、签名验签服务 1.1 亿次、电子印章 15 万个，各类应用场景日均提供证书服务 4500 万次。

案例3. 安全关键行业密码应用解决方案（沈阳自动化所）

随着智能制造、国防军工等安全关键行业数字化转型的深入，工业无线网络已成为关键生产设施不可或缺的神经脉络。然而，无线信道的开放性、传统通信协议与安全机制的对外依存度，使得网络空间安全风险日益凸显，严重威胁国家关键信息基础设施安全。

本方案旨在系统阐述，如何通过自研的工业无线技术（例如 WIA-FA）与国家商用密码算法的深度融合，构建高安全、高可靠、高性能的内生安全体系。结合在工业通信领域的技术积累与在国防军工等重点行业的成功实践，提出覆盖技术、产品、标准与应用的完整解决方案，为提升我国安全关键行业的本质安全能力提供路径方案。

- **问题与难题分析**

（1）通信协议可控程度低

当前工业现场广泛采用的无线局域网技术（如 Wi-Fi、ZigBee）其核心知识产权与芯片供应链受制于国外，底层协议存在不可控的安全隐患。虽已有 WAPI 等自主标准，但其在工业高实时、高可靠场景下，仍存在跨 AP 切换时间延长、管理帧无法加密等固有缺陷，难以满足智能制造对确定性与可靠性的严苛要求。

（2）传统安全机制存在结构性缺陷

空口传输脆弱：管理帧与控制帧明文传输，为信令欺骗、拒绝服务（DoS）等攻击提供了可乘之机。密码算法强度不足：沿用国际算法或非官方证书体系，其安全强度与合规性无法满足现有国家标准对商用密码算法的强制应用要求。

密钥管理不规范：密钥/证书的生成、存储、分发环节存在安全盲区，密钥泄漏风险高，缺乏集中化、标准化的全生命周期管理。

（3）在工业环境下面临严峻性能与集成挑战

实时性瓶颈：通用密码技术的软硬件开销与工业控制毫秒级时延要求形成矛盾，密钥频繁更新易导致通信中断。动态适应性弱：工业无线网络拓扑多变，静态密钥管理机制无法适应链路动态切换，影响业务连续性。互操作性差：不同厂

商的密码模块与工业设备在硬件接口、软件驱动上存在壁垒，导致“插不上、连不通”的集成困境，抬高部署与维护成本。

总体设计方案以“协议自主化、密码国产化、管理智能化”为核心原则，构建了端到端的内生安全体系。

- **体系架构**

构建以“一个中心、三重防护”为核心的纵深防御体系。

一个中心：以统一密码服务平台与无线安全管理系统为核心，实现集中化的密钥管理、策略下发与安全态势感知。

三重防护：安全通信防护：基于国密算法的设备双向认证与空口全报文加密。区域边界防护：通过协议转换、访问控制白名单实现网络隔离；计算环境防护：采用安全芯片保障密钥存储与运算的物理安全。

- **密码技术应用框架**

身份认证：基于 SM2 数字证书，实现“设备－网络－管理系统”间的双向身份认证，杜绝非法接入与“伪基站”攻击。

加密保护：采用 SM4 算法对业务数据及协议帧进行端到端加密，确保数据传输机密性；采用 SM3 杂凑算法保障数据完整性。

密钥管理：基于 SM2 协商机制动态生成会话密钥，由 KMS 实现密钥的全生命周期管理与多态轮转，确保前向安全与业务无损更新。

- **核心技术与创新**

（1）高可靠通信协议

基于国家标准 GB/T 26790（WIA-FA），对物理层与链路层进行深度定制与密码增强。全报文加密：实现对数据帧、管理帧与控制帧的全方位加密，杜绝空口信令泄露。高性能链路技术：采用频域轮询、帧聚合与高精度时间同步技术，将漫游切换时间控制在毫秒级（<1ms），满足 AGV、巡检机器人等移动场景的实时性要求。

（2）软硬协同的密码应用体系

标准化密码接口：定义统一的硬件抽象层与软件 API，打通密码设备与工业无线设备间的互操作壁垒。高性能密码计算：在无线网关、节点等设备中集成国产密码芯片，提供硬件级加速，在满足高性能计算需求的同时，保障密钥的物理安全。

（3）动态自适应的智能安全管理

多态密钥机制：引入“当前密钥”与“预置密钥”并存的多态模型，支持密钥的无感更新，保障业务零中断。智能访问控制：基于深度学习技术自学习网络行为特征，生成动态白名单，实现从“被动防御”到“主动免疫”的转变。

➢ **典型应用场景**

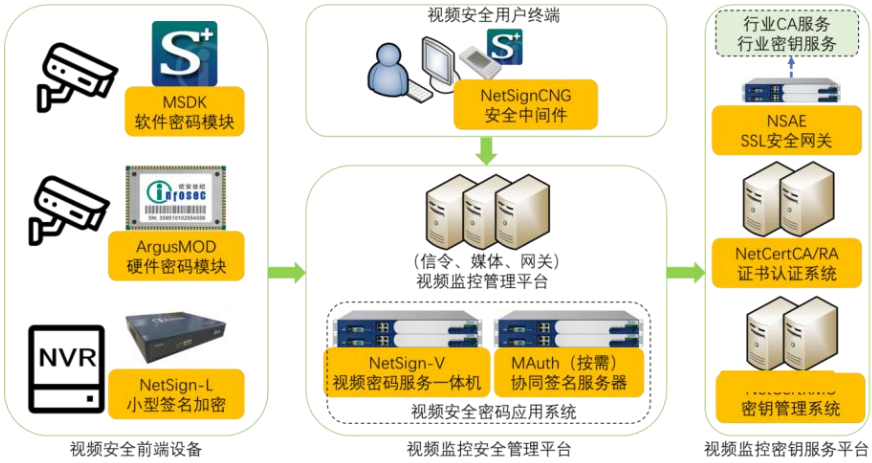
（1）高动态 AGV 集群协同作业；

（2）国防军工智能制造车间智能化终端设备；

（3）国防军工车间智能化量具设备。

7.新兴领域

案例1. 视频加密解决方案（信安世纪）



图四-36　视频加密解决方案示意图

➢ **主要技术**

数字证书、数字签名、统一密钥管理、视频码流加密、信令加密。

核心业务：视频监控安全管理平台、视频监控密钥服务平台、视频安全用户终端、视频安全前端设备。

➢ **涉及产品**

NetSign 签名验签服务器、NetSignCNG 安全中间件、Mauth 协同签名服务器、NSAE 应用安全网关、NetCert 证书认证系统。

用户安全需求：

（1）视频监控安全管理平台密码合规性建设；

（2）信令、媒体、数据安全防护管控。

➢ **解决方案优势**

（1）为视频安全前端设备提供各类适配环境，如软件密码模块、硬件密码模块、NVR 轻量级签名加密服务；

（2）通过签名安全中间件提供视频用户终端安全防护；

（3）为视频监控安全管理平台搭建专属密钥服务平台，提供相应对称密钥及非对称密钥管理服务。

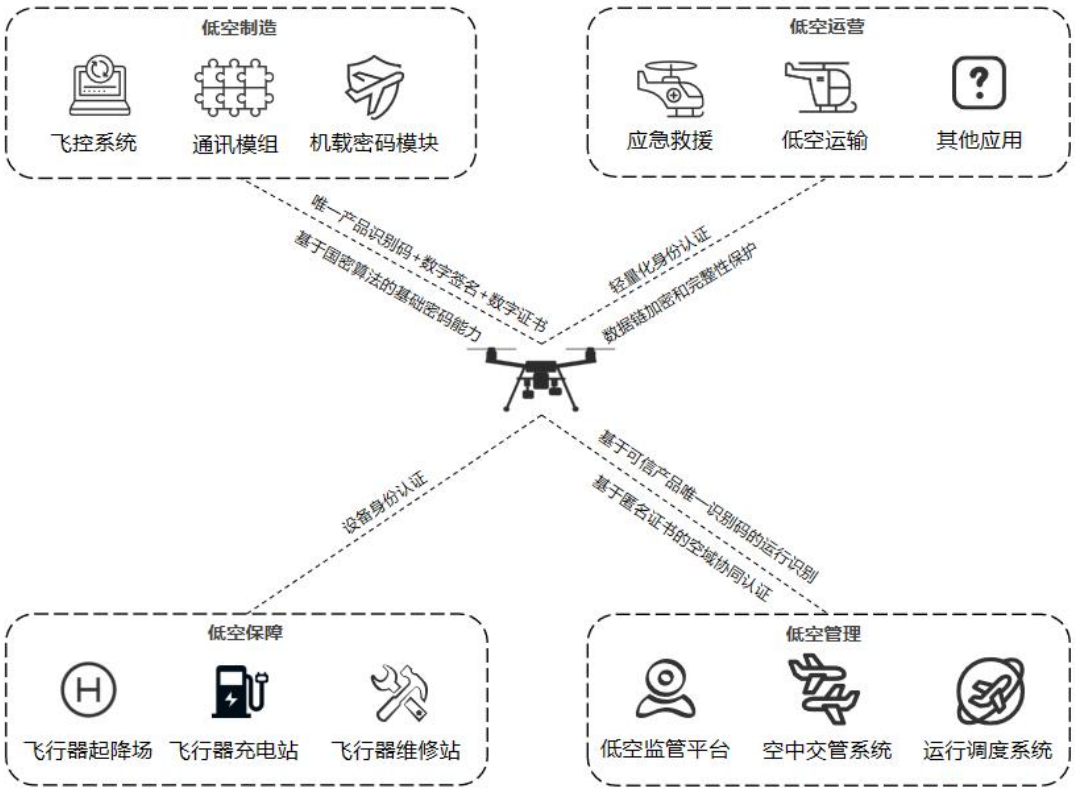
➢ **客户收益**

（1）视频监控安全管理平台作为视频业务核心系统，符合 GB/T 39786 密评

安全合规性建设需求；

（2）提供针对视频数据及业务系统数据独立的密钥管理体系，保证数据机密性、完整性。

案例2. 低空智能网联密码应用解决方案（吉大正元）



图四-37　低空智能网联密码应用示意图

- **低空制造**

唯一产品识别码：发放者数字签名+数字证书绑定，作为飞行器的唯一合法数字身份；

基于国密算法的软、硬件密码模块，为飞行器提供“安全芯”。

- **低空运营**

空地双向身份认证、空中组网认证，为低空运营的各业务场景提供身份真实性保障；

数据链加密，提供数据机密性和完整性保护，全方位保障低空运营服务网数据链安全。

- **低空管理**

运行识别——唯一识别码+数字签名，实现自动化监管和动态资源调度，保护低空管理航路网和空联网的数据链安全；

协同认证—匿名数字证书+数字签名，空联网空域信息交互。

➢ **低空保障**

空地双向设备身份认证－数字证书，为低空保障的各硬件基础设施、软件基础设施提供身份真实性保障。

案例3. S2i码与商用密码技术解决方案（沈阳安创科技）

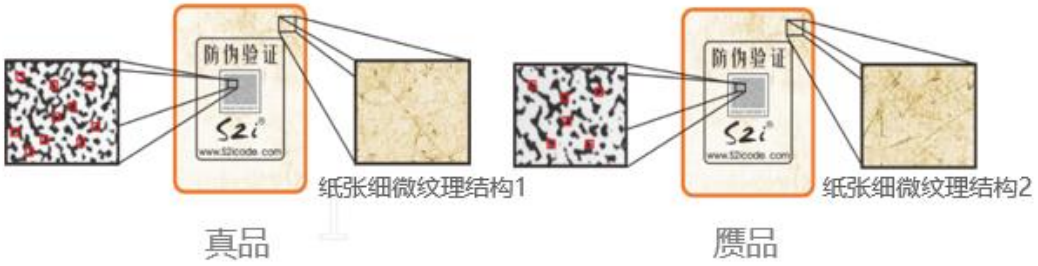
S2i 码不同于现在使用较为广泛的二维码编码技术（日本 QR 码），是一项具有国际发明专利的中国自主知识产权的底层基础科学研发新成果。不同于 QR 码的单极结构，S2i 码是一种多极特殊编码，利用多极编码技术和油墨、物理材质等在印刷或雕刻时的不同物理变化，使其成为在数学和物理上不可能被复制的新一代安全认证技术，具有难复制、易识别、零工艺、低成本等特性。

图四-38　多极特殊编码（S2i）结构示意图

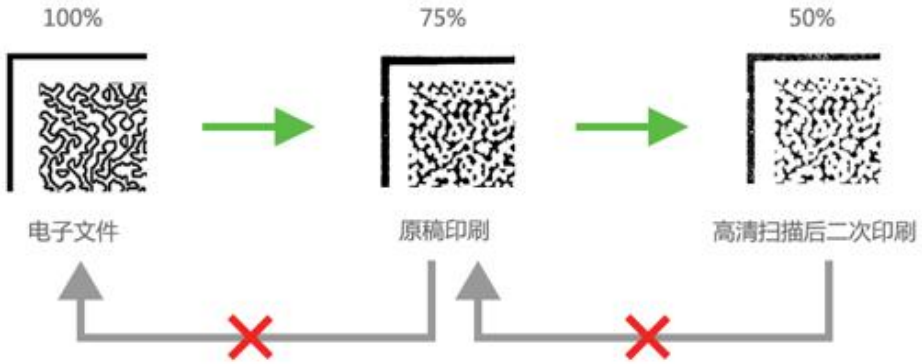
S2i 码与商用密码技术相结合能够解决二维码在生成、使用和监管追溯全生命周期中的一些安全问题：

（1）生成过程实现可信：利用国密算法（SM2/SM4）替换 S2i 码中的 RSA 算法，在用户侧，实现对二维码中敏感信息的加密保护；在服务侧，使用公钥基础设施体系（PKI 体系）和签名验签技术完成对用户信息真实性和完整性的校验。从而在物联网、供应链、工业互联网、数字化转型等场景中，提供自主研发、安全可信且具备合法的身份鉴别与防伪溯源等服务。同时在 S2i 码生成时，利用密码设备提供硬件级安全防护，杜绝谁都能生成二维码的问题。

（2）使用过程中实现防复制：利用 S2i 码与油墨、物理介质等结合产生不变纹理的特性，实现防复制、防篡改。同时与商密算法相结合，在明文加密的过程中也保证了唯一性，不仅延续了基础编码的唯一性保障，更通过密码学加密层实现了质的飞跃，尤其在防破解、防关联、防伪造方面表现突出，有效防止二维码被伪造或篡改，杜绝谁都能复制二维码的问题。



图四-39　S2i 码结合物理介质产生不变纹理区分真品/赝品



图四-40　S2i 码在印刷中油墨物理变化示意图

（3）事后监管实现可信追溯：通过对 S2i 码扫码数据的测量和分析，可以判断出使用信息渠道是原版、复印版或是精细修复的仿制品，甚至还能通过印刷过程中的物理特性确认 S2i 码的印刷品是否属于同一批次，以此来对扫码数据进行实时监控，分析判断扫描假码行为，可追溯至提供造假环境的制版厂、印刷厂或者假码扫码现场的定位信息，可作为法律溯源参考依据。

- **相关对策建议及拓展应用场景**

一是从构建安全技术体系入手，提升加密和认证技术在保障二维码安全中的应用。推广基于密码技术的二维码加密和认证方法，确保只有合法的用户和设备才能识别和解析二维码内容，防止信息泄露和篡改。二是从完善安全管理机制入手，建立二维码国家标准和规范。基于密码技术的二维码安全新标准、明确二维码的编码规则、生成与识别要求、安全等级等标准，规范二维码市场秩序，为监管提供依据，推动二维码产业的健康、可持续发展，使其更好地服务于我国的数字经济建设和社会发展。加大监管力度，建立健全跨部门的监管协调机制，明确各部门的监管职责，加强信息共享和协作，严厉打击利用二维码进行违法犯罪活动的行为。

经过多次对应用场景的探讨与研究，结合我省实际情况，能够形成了一些产业合作的新兴领域：

（1）政务服务领域：在信息获取、查询及服务窗口应用，将办事指南、政策文件、政务服务事项等制作成国密二维码，在提高便捷性的同时，杜绝被篡改、伪造、复制，确保了只有合法的用户才能扫到正确的码，同时也可对伪造者进行溯源。在文件流转中应用，将文件信息进行数字化，使用商密技术进行加密后置于 S2i 码中，确保电子文件在网络上安全传输，同时也可印刷至纸质文件上，以达到防复制、防篡改、防伪造的目的。

（2）市场监督管理领域。结合我省明星食品、农产品、药品，如本溪大米、丹东草莓、朝阳大枣、阜新小米、盘锦河蟹、东北制药厂等，在产品宣传、防止假冒伪劣及产品溯源中应用，可使用 S2i 码进行全流程监管，在实现一品一码、

一批一码、一物一码、查看生产批次、产品溯源等追溯信息的同时，使用商密技术将核心字段进行数字签名，在保障有码正品流入市场的同时，对伪造二维码、篡改二维码等行为进行溯源，主动预警并追踪造假窝点，有利于打造我省知名高端产品，形成热门可信 IP。

（3）工业企业数字化转型领域。我省制造业、军工产品众多，通过 S2i 码的技术应用落地，可助力我省工业企业、军工企业数字化转型，在工业数字化转型及军工等高端制造业中应用，在防伪的同时，可将工业互联网 128 位标识在 S2i 码中加密存储，离线认证，确保标识解析入口唯一、双向认证。也可将工业产品数字化，进行即时数据加密标签打印，为企业提供判断正品外流证据、伪造产品证据、产品信息认证等服务，实现防伪、存证的目的，保障制造和流通安全。

案例4. “车路云一体化”密码应用解决方案（吉大正元）

图四-41 “车路云一体化”密码应用架构示意图

- **身份管理**

为物联网业务各参与对象颁发数字证书，标识其在网络中的唯一身份（身份强标识，无法篡改）；提供基于数字证书开展安全业务过程中的身份有效性查询和校验。

- **通讯安全**

面向物联网各业务场景中的关键、敏感数据进行加密处理，实现数据的机密性和隐私保护。

- **车联网信息校验**

面向物联网业务平台端存储、下发或接收的信息，提供密码服务功能，保证数据的完整性和机密性。面向物联网业务交互双方，提供抗抵赖功能。

案例5. 量子加密通信解决方案（辽宁移动）

➢ 案例背景

传统加密技术面临着日益严峻的安全挑战，如量子计算技术发展可能对现有加密算法造成威胁。量子加密专线融合量子保密通信技术与国密算法，为专线提供了更高级别的安全保障，可有效抵御潜在的安全风险，确保数据传输的保密性、完整性和真实性。

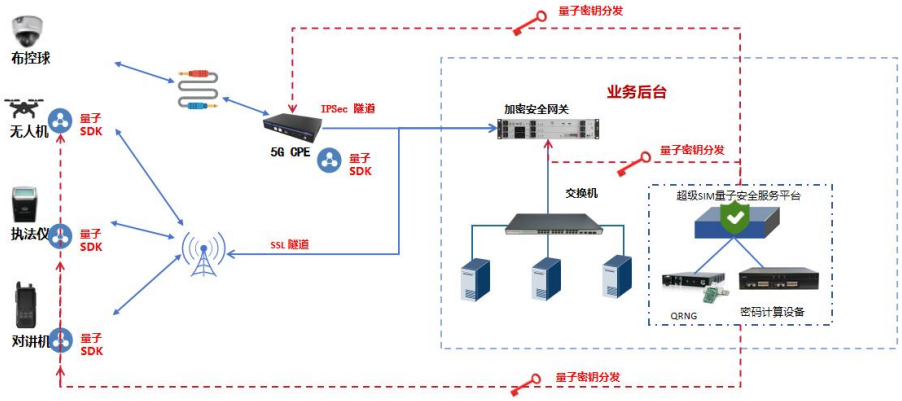
量子保密通信基于量子力学原理，利用量子态的不可克隆性和测量坍缩特性实现密钥分发。通过量子随机数发生器可生成具备无条件安全性的真随机密钥，结合量子密钥分发技术，任何对量子信道的窃听行为都会改变量子态，从而被通信双方察觉。这为数据加密提供了坚实的基础，确保加密密钥的安全性。

国密算法是我国自主研发并推广应用的一系列密码算法，如 SM2、SM3、SM4 等。这些算法在安全性、性能等方面具有良好表现，符合国家信息安全标准和监管要求。国密算法用于对数据进行加密、解密、签名和验证等操作，与量子密钥相结合，构建起双重安全防护体系。

➢ 方案架构

为应对量子技术对传统加密的破解风险，创新将量子密钥融合应用到 IPsec、SSL 协议中，建立通信节点间量子 VPN 通道，基于超级 SIM 量子能力建立高速量子加密专线，实现网络层量子加密保护，应用于数据中心间或局点间通道级保护。

本方案在业务后台机房部署 1 套量子加密网关、1 套量子安全服务资源池，针对各类型终端融合量子 SDK、5G CPE 设备，从而构建量子 IPSec、量子 SSL 加密隧道。在运营商专网专线的安全基础上，叠加量子加密，保障信息传输安全性。



图四-42　量子加密专线架构图

量子加密专线产品包含超级 SIM 量子密码资源池（超级 SIM 量子安全服务平台、量子 SDK、QRNG）、IPSec VPN 以及 5G CPE 设备。

超级 SIM 量子安全服务平台：提供接入认证、密钥协商、数据加解密等量子增强安全服务。量子安全服务平台从 QRNG 获得量子密钥，提供量子密钥 SAAS 服务，应用系统只需要调用 API 接口即可实现量子安全服务功能，无需参与复杂

的密钥管理。

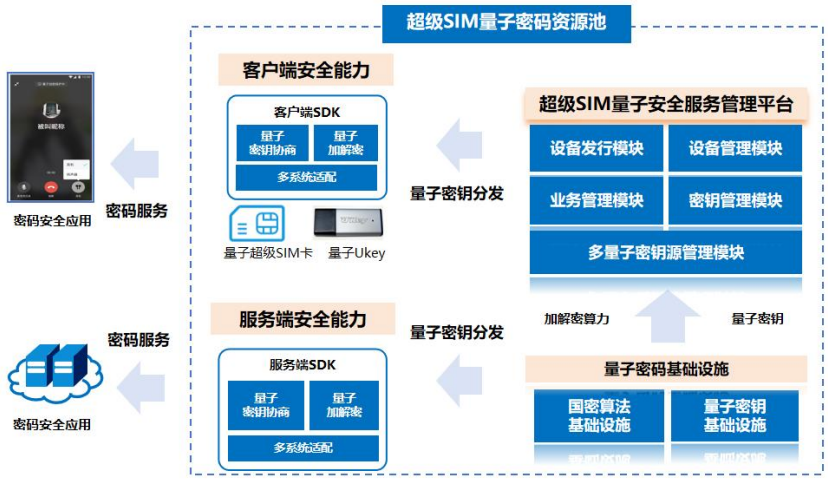
量子 SDK：量子 SDK 用于端侧使用，适用环境包括 Linux、Windows、Android 以及 IOS 等操作系统。量子 SDK 融合运用量子密钥，对经典密码算法进行密钥安全增强，向应用系统提供基于量子密钥融合增强的安全认证、密钥分发、加解密等服务。

QRNG：基于脉冲型相位涨落原理的真随机数发生器。采用脉冲光源相位涨落和延迟干涉生成的随机相位信号，作为量子随机熵源，结合信号探测和数据后处理，输出量子随机数序列。

IPSec VPN 及 5G CPE：基于 IPSec 协议与 SSL 协议，融合量子 SDK 密钥分发管理，构建量子+国密的双重加密隧道。

- **主要功能**

产品由超级 SIM 量子安全服务平台、量子超级 SIM 卡、量子 SDK、量子密码基础设施组成，通过量子超级 SIM 卡及量子 SDK 为应用系统提供量子密码能力，实现量子密钥的高效分发与运用，构建起强大的安全能力体系。



图四-43　超级 SIM 量子密码资源池功能图

（1）量子密钥全流程管理：支持离线/在线量子密钥充注，支持量子密钥、会话密钥等密钥管理，实现密钥从生成、销毁、分发到恢复的全生命周期管理，且可对业务密钥与量子密钥分库存储管理，还具备密钥策略配置与维护功能。

（2）设备与密钥状态监控：可监控设备状态、应用调用次数，能精准查询量子安全介质的充注密钥量、充注更新模式及状态等信息，支持设置并实时查询密钥及设备有效期；提供远程注销、紧急挂失、状态锁定等安全运维操作。

（3）端侧协同服务：向端侧提供量子软 KEY 和 SDK 协同服务，基于协同签名技术对端侧应用进行接入认证，支持量子密钥在线充注，提供安全的密钥充注及协商服务。

- **适用领域**

本方案适用于党政、公检法军等具有高安全保密通信需求的行业应用。

（1）构建量子+全生态合作场景，提供集成量子能力的量子 SDK，实现设备发行与量子密钥的灵活注入及全生命周期管理，助力合作伙伴共同探索量子应用场景创新，可打造量子专线、量子无人机、量子对讲、量子执法仪、量子印章等产品生态，助力国家量子科技的快速普及。

（2）创新融合国密算法和量子密码双重密码服务，设计了新型量子超级 SIM 卡应用，在提供纯量子加密、纯国密加密以及二者自适应切换的混合加密模式的同时，优化卡应用更新机制，提升机卡通道效率，全方位提升超级 SIM 卡安全能力。超级 SIM 量子安全服务平台还为应用系统量身打造基于量子密钥融合增强的全业务接入流程，涵盖密钥分发、加解密等关键环节，保障数据传输与存储的安全，为客户构建坚固的信息安全防线。

（3）无条件的安全性，采用了业界公认被证明为无条件安全的量子保密通信技术，通过利用量子态的独特物理属性，能够有效抵御任何形式的窃听与篡改，确保信息在传输路径上的绝对保密性。基于量子力学“量子不可分割”与“量子态不可克隆”的核心原理，以及“一次一密”加密策略，能够从根本上超越了传统公钥加密体系，实现了理论上的“无条件安全”通信。

第五章 密码应用合规要求与密评

密码应用合规是网络与数据安全的核心防线，更是落实《密码法》《商用密码管理条例》等法律法规的法定要求。无论是关键信息基础设施还是各类信息系统，规范的密码应用都是抵御安全风险、保障业务稳定的基础支撑。

本章聚焦密码应用合规核心要点，一方面明确通用安全的技术与管理要求，另一方面系统阐释商用密码应用安全性评估的法定职责、实施流程与标准依据，全面梳理 “三同步一评估” 等关键合规要求，为辽宁省各行业、各单位密码应用的合规性、正确性、有效性提供实操指引，筑牢数字安全发展的密码屏障。

（一）政务信息系统密码应用基本要求

政务信息系统作为国家政务运行的核心载体，其商用密码应用合规性直接关系到政务数据安全与国家治理效能。辽宁省政务信息系统密码应用严格遵循国家法律法规与标准规范，构建起“合规筑基、安全创新”的应用体系，为数字政务建设提供坚实保障。基于 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，结合当前密码技术、产品和服务的实际情况，给出了针对信息系统密码应用的措施建议。信息系统责任单位也可结合实际，自主选取适合的密码技术、产品和服务，以满足相关商用密码应用要求。

1. 通用要求

信息系统责任单位需从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面采用密码技术措施，建立安全的密钥管理方案，并采取有效的安全管理措施，对信息系统进行保护。

信息系统使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应遵循密码相关国家标准和行业标准，没有标准可遵循时可经由省级国家密码管理部门向国家密码管理部门提出申请，对相关算法、技术进行安全性审查。信息系统采用电子认证服务的，责任单位需选择具有电子认证服务资质的机构，若为政务信息系统，需选择具有电子政务电子认证服务资质的机构。

2. 物理和环境安全要求

对信息系统所在机房等重要区域的物理防护，应具备以下密码功能：

确认进入各重要区域的人员身份，防止无关和假冒人员进入；

保证门禁系统进出记录和视频监控音像记录的存储完整性，防止被非授权篡改。

3. 网络和通信安全要求

对信息系统与外部实体之间网络通信的安全防护，应具备以下密码功能：

确认通信实体的身份，防止与假冒实体进行通信；

保护通信过程中的数据，防止数据被非授权篡改，防止重要数据泄露。

4. 设备和计算安全要求

对信息系统中各类设备和计算环境的安全防护，应具备以下密码功能：

对设备的特权用户（含系统管理员、安全管理员、审计管理员等，以下简称管理员）和普通用户的身份进行识别和确认，防止假冒人员登录；

在远程管理时，对远程管理通道进行保护。在远程管理通信过程中，防止与假冒实体进行通信，防止数据被非授权篡改，防止重要数据泄露；

保护计算机、服务器等设备中的系统资源访问控制信息（如设备配置信息、安全策略、资源访问控制列表等）、重要信息资源安全标记（如数据标签等）、日志记录（如系统日志、数据库日志等）和重要可执行程序（如重要应用程序等），防止被非授权篡改；保护重要可执行程序的来源真实性，防止假冒程序文件的加载。

5. 应用和数据安全要求

对信息系统中应用及其数据的安全防护，应具备以下密码功能：

确认应用系统的管理员和普通用户的身份，防止假冒人员登录；

对应用系统的访问控制策略（如安全策略、资源访问控制列表等）、数据库访问控制信息（如用户身份信息、数据库安全策略、用户权限列表等）、重要信息资源安全标记（如数据标签）等进行保护，防止被非授权篡改；

保护客户端与服务端之间、应用系统之间在非安全网络信道中传输的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息等），防止数据泄露、非授权篡改；

保护存储的重要数据（包括但不限于鉴别数据、重要业务数据、重要用户信息、业务审计日志等），防止数据泄露、非授权篡改；

保护应用系统中可能涉及法律责任认定的数据发送和接收操作，确保发送方和接收方无法否认已经发生的操作行为。

6. 密钥管理要求

在信息系统密码应用方案中，需包含完整的密钥管理方案，明确采用的密钥种类及管理环节，并设计安全的技术实现方式，确保密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等生存周期的安全。

密钥管理方案的技术实现需由通过商用密码产品认证的密码产品提供，未采

用该方式的密钥管理方案技术实现可由省级密码管理部门提请国家密码管理部门组织开展安全性审查。

7. 安全管理要求

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，信息系统的安全管理措施包括管理制度、人员管理、建设运行和应急处置 4 个方面。

在管理制度方面，责任单位需建立相应的密码应用安全管理制度和操作规范，覆盖密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等相关内容。相关制度可针对商用密码保障系统单独制定，也可在已有的信息系统安全管理相关制度规范中体现。

在人员管理方面，责任单位需根据信息系统密码管理工作需要设立密码管理及操作相关岗位，制订人员岗位责任、人员考核、人员培训、人员保密和调离等相关规定，并按照规定进行人员的配备与管理。

在建设运行方面，责任单位需参照本指南要求制定信息系统密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，重点做好密码应用方案设计与评估、密码保障系统建设与密码应用测评、密评，以及相关闭环管理工作。

在应急处置方面，责任单位应制定密码应用应急处置方案，需在项目建设阶段和系统运行阶段，分别明确典型紧急事件及应急处理处置方案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置。

（二）商用密码安全性评估

1. 密评定义与核心价值

商用密码应用安全性评估（以下简称“密评”）是指按照法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。作为商用密码安全监管的核心手段，密评既是落实《密码法》强制要求的法定程序，也是防范密码应用安全风险的关键防线。

从行业发展视角看，密评的核心价值体现在三个维度：一是合规保障价值，通过标准化评估验证系统密码应用是否符合国家强制性要求，为系统合法合规运行提供权威依据；二是风险防控价值，精准识别密码算法滥用、密钥管理疏漏、产品配置不当等安全隐患，从源头遏制网络安全事件；三是产业驱动价值，倒逼企事业单位强化密码应用能力，拉动商用密码产品与服务需求，促进产业高质量发展。对辽宁省而言，密评更是保障关键信息基础设施安全、维护数字经济秩序的重要支撑。

密评更是规范商用密码应用的关键抓手，通过“以评促建”“以评促改”“以评促用”，为网络和信息系统安全提供科学评价方法，确保密码有效使用与管理，构建坚实的网络安全密码屏障。

2. 密评类型与核心评估内容

2.1 密评的类型

根据评估阶段与场景差异，商用密码安全性评估主要分为两类：一是规划阶段评估，针对商用密码应用方案开展评估，未通过评估的方案不得作为密码保障系统建设依据；二是运行阶段评估，对已建成运行的系统定期开展评估，未通过评估的需限期改造，改造期间不得投入运行。两类评估均遵循《信息系统密码应用基本要求》（GB/T 39786-2021）等国家标准，形成全生命周期的安全管控。

2.2 密评核心评估内容

密评工作的核心评估内容就是对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证。具体而言：

在合规性评估方面，主要判定信息系统使用的密码算法、协议、密钥管理是否符合法律法规及密码相关国标、行标要求；

在正确性评估方面，主要核查密码算法、协议、密钥管理及密码产品、服务的使用是否准确无误；

在有效性评估方面，主要评估信息系统中密码保障系统是否在实际运行中发挥作用，能否满足系统安全需求，密码应用相关的管理制度是否建立并有效落实，切实发挥作用。

在系统密评过程中，参照 GM/T 0116、GB/T 43206、《商用密码应用安全性评估 FAQ》，结合重要网络与信息系统主要保护对象确定各个层面的测评对象。

2.3 密评的测评对象

2.3.1 密码技术应用测评

2.3.1.1 物理和环境安全

测评对象：物理和环境安全层面的测评对象为重要网络与信息系统所在的物理机房，具体为机房的电子门禁系统、视频监控系统。

2.3.1.2 网络和通信安全

测评对象：根据重要网络与信息系统中的各典型业务及其商用密码应用实际现状，分析网络和通信安全层面涉及的测评对象，测评对象包括互联网与政务外网、浏览器与服务端、VPN 客户端与 SSL VPN 等各类相关通信信道。

2.3.1.3 设备和计算安全

测评对象：重要网络与信息系统在设备和计算安全层面涉及的测评对象包括通用设备、网络及安全设备、密码设备、各类虚拟设备的操作系统和数据库系统等。

2.3.1.4 应用和数据安全

测评对象：重要网络与信息系统在应用和数据安全层面涉及的测评对象包括

具体业务应用系统，以及提供身份鉴别功能的密码产品等。重要网络与信息系统涉及的应用用户包括系统管理员与业务用户。重要网络与信息系统涉及的关键数据包括鉴别数据、重要业务数据、重要审计数据、个人敏感信息、重要业务日志。

2.3.2 安全管理测评

安全管理测评包括管理制度、人员管理、建设运行和应急处置。

3. 密评流程

从工作实施流程来看，密评分为四个阶段，包括测评准备阶段、方案编制阶段、现场测评阶段和报告编制阶段。

3.1 测评准备阶段

测评项目启动：明确评估目标、范围及双方职责，组建匹配项目规模的专业评估团队；

信息收集与分析：收集系统建设文档、网络拓扑、安全策略、密码产品资质等资料，梳理数据资产及业务流程；

工具和表单准备：配备协议分析、算法合规性检测、漏洞扫描等专业检测工具，制定评估记录表单与核查清单。

3.2 方案编制阶段

测评对象和指标确定：依据 GB/T39786-2021 等标准，明确具体测评对象及对应的机密性、真实性、完整性等保护需求；

测评工具接入点确定：针对不同密码产品和功能，规划工具检测的关键节点与方法；

测评方案编制：形成包含测评依据、方法、步骤、人员分工的完整方案，明确现场测评重点。

3.3 现场测评阶段

实施准备：与被评估方对接现场环境，确认系统运行状态及配合事宜；

现场测评与记录：通过工具检测、配置核查、协议分析、人员访谈等方式开展评估，详细记录检测数据与发现问题；

结果确认和资料归还：与被评估方核对测评记录，确认无误后归还相关资料原件。

3.4 分析与报告编制阶段

测评结果判定：对照标准逐项判定结果，区分合规项与问题项；

结果风险分析：评估问题可能引发的安全风险，明确风险等级；报告编制：撰写包含评估概述、过程、结果、改进建议的正式报告，附检测记录、访谈纪要等附件。

4. 密评开展要求

根据《商用密码管理条例》《商用密码应用安全性评估管理办法》等规定，对依法需用商用密码保护的重要网络与信息系统，明确以下开展要求：

全生命周期同步：需同步规划、同步建设、同步运行商用密码保障系统，确保全生命周期落实密评要求；

定期评估频率：系统建成运行后，运营者需自行或委托商用密码检测机构，每年至少开展一次密评，保障密码保障系统正确有效运行；

问题整改要求：未通过密评的系统，运营者需及时改造，并在改造期间采取必要措施保证系统运行安全。

第六章 信创融合

信创产业是实现科技自立自强、保障数字安全的关键抓手，而商用密码作为信息安全的核心技术，二者的深度融合是筑牢辽宁数字经济发展安全底座的必然选择。本章节立足辽宁信创产业发展实际情况，系统梳理信创产业发展趋势与相关政策，详解鲲鹏、龙芯、海光等核心密码芯片技术优势，剖析华为在辽宁信创产业布局成果，结合信创领域标准规范与典型实践案例，全面勾勒信创与商用密码协同发展的辽宁路径。

（一）信创发展趋势

在新时代国家战略与政策法规的持续深化引领下，信创产业已跨越初步探索期，正迈向全面应用推广的纵深发展阶段，其发展路径与内涵呈现出系统性的深刻变革。

首先，信创覆盖范围正从“党政+央国企”向头部民营企业加速延伸，全面支撑国家数字化安全体系建设，随着信创产业技术成熟度提升及政策引导深化，头部民营企业凭借其在国民经济中的战略节点地位，正成为信创生态拓展的新焦点，这一转变体现了信创从“政策驱动”向“价值驱动”发展演进。

其次，应用场景也在不断拓宽，从早期的电子公文等非核心业务，全面转向政务云、数据中心等核心应用领域，实现了“场景延伸”，信创已成为支撑数字化转型的安全基座。

与此同时，金融领域信创实践从大型机构向中小金融机构延伸，在头部金融机构业务系统国产化改造的基础上，区域中小金融机构信创节奏显著加快。同时，信创产业发展的重心不仅仅是部署国产化硬件、操作系统及数据库，如今更侧重于应用软件的适配与重构。整体来看，信创产业正形成全行业覆盖、全链条深化的发展格局。

（二）密码技术与信创融合

在信创发展的进程中，密码安全的基础性与核心地位日益凸显，其重要性已不容任何置疑。在《通用服务器政府采购需求标准（2023 年版）》中，密码算法实现指标中，要求“CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T 37092 或 GM/T 0028 的相关规定。”使用说明中强调：“通过商用密码检测机构检测并经商用密码认证机构认证合格。”

可以看出，密码技术不再是信息系统中可选的“附加”安全组件，而是深度融入其底层架构、内生于其血脉的“信任基石”。它构建了从身份认证、数据加密到行为不可否认的完整信任链，是保障数据全生命周期安全、维护网络空间主权、支撑数字政府与数字经济健康发展的核心技术手段。

面对日益严峻复杂的网络威胁与数据安全挑战，构建以密码为核心的安全防护体系，已不再是技术选择，而是发展的必然要求和战略底线。强化密码在信创体系中的深度融合与合规、正确、有效应用，是筑牢国家网络安全防线、实现高水平科技自立自强的关键之举，关乎全局，影响深远。

1. 鲲鹏芯片技术介绍

鲲鹏芯片是华为公司推出的一款高性能计算芯片，采用自主设计处理器微架构和片上系统，拥有100%处理器核心源代码、掌握完整知识产权和核心技术，具备独立自主演进能力；鲲鹏处理器已获得国密芯片一级证书，商密证书，保障业务安全启动。鲲鹏芯片主要用于满足多样化的计算需求，尤其在安全性方面表现出色。华为坚持硬件开放策略，开放鲲鹏服务器主板给13家整机伙伴，当前已有150多款机型，覆盖多种场景，2024年伙伴发货占比超过95%，已建立起健康可持续的鲲鹏商业生态。

以下是关于鲲鹏芯片的一些关键技术和特点：

1.1 技术特点

- 高性能片内/片间互联能力；
- 芯片集成度高：多合一SoC（CPU/网卡/SAS/SATA控制器/桥片/加速器）；
- 数据加解密：支持算法SM2、SM3、SM4、MD5、RSA、AES；
- 数据压缩：支持ZLIB数据格式，支持GZIP数据格式；
- TrustZone套件：基于鲲鹏芯片的硬件形态，Trustzone套件通过较小的TCB（可信计算基）和较少的对外暴露面，提供了较高的安全性，特别适用于加密机和密钥管理等高安全场景；
- TEE套件：面向云原生、机密虚机/容器、大数据以及AI等通用场景，鲲鹏提供TEE套件，解决了生态易用性问题，支持传统应用的适配迁移，工作量少，易用性强；
- 国密加速特性：鲲鹏芯片支持国密硬件加速，通过KAE加速器和openEuler UADK框架，提供机密虚机内的国密加速性能提升，适用于数据库黑匣子和密态计算等场景。

1.2 价值优势

- 鲲鹏芯片在云计算、大数据、分布式存储等领域具备显著应用价值及优势。
- 在大数据处理方面，鲲鹏多核高并发架构能够有效匹配大数据负载应用特征，提高大数据应用任务并发度，获得更好的处理性能。
- 在分布式存储领域，鲲鹏多核高并发架构天然适配分布式存储软件，通过将软件管理面与数据面分别绑定至足够多的CPU核心上，能够避免相互干扰，使技术资源匹配更精准合理，提供高效的存算分离服务。

- 在数据库场景下，通过软硬件协同优化提升效率。比如应用 RoCE 和 NUMA 技术缩短 CPU 访问外部网络与内存的路径，多核调度算法管理高并发访问时 CPU 内核之间的协同问题，提升系统性能。
- 在云平台方面，结合鲲鹏多核结构特点，在虚拟化层面通过对多核调度进行优化，可大幅降低虚拟化软件的 CPU 访问时延，降低业务对 CPU 的占用率，从而提升云服务整体性能。

1.3 鲲鹏机密计算

随着大数据及人工智能应用的不断深化，各类数据获取和使用越来越频繁，数据和模型一旦泄露，将会带来严重的社会负面影响以及巨大的经济损失，对数据安全和数据隐私的保护愈来愈重要，同时，国家相继颁布实施网络安全及数据安全的法律法规，对于数据隐私的保护，实现数据“可用不可见”将成为刚需。

在数字经济快速发展的背景下，大数据与人工智能技术的深度应用推动着数据采集与流通规模的持续扩大。伴随而来的数据泄漏风险已演变为威胁社会治理和经济发展的关键隐患，一旦发生将造成不可逆的社会信任损伤与巨额经济损失。当前，我国正加速构建数据安全防护体系，通过颁布实施《网络安全法》《数据安全法》《个人信息保护法》等系列法规，确立了数据要素市场化进程中的安全治理框架。在此政策导向下，机密计算技术体系的建设需求日益凸显，数据“可用不可见”将成为刚需。

鲲鹏机密计算是指通过在基于鲲鹏芯片的可信执行环境（TEE）中执行计算来保护“使用中”数据的技术。其核心目标是解决数据在计算阶段的安全保护问题，弥补数据全生命周期安全链条的缺失。鲲鹏机密计算以下三个方面的核心特性：

（1）隔离：通过硬件级隔离机制，将通用计算环境与机密计算环境严格分离，非授权实体无法访问机密数据。

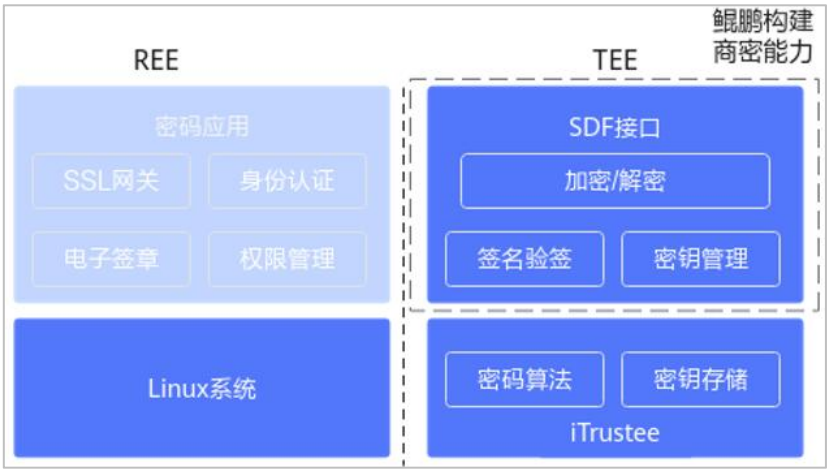
（2）加密：确保数据在内存计算过程中保持密文形态，有效防御特权软件或硬件层面的窥探攻击。

（3）可证明：利用远程证明机制向用户提供程序状态的度量证据，支持对运行环境的可信性验证。

1.4 鲲鹏商密应用

（1）鲲鹏商密应用模块定义

鲲鹏商密应用密码模块是基于鲲鹏 TrustZone 机密计算套件（iTrustee OS 的安全系统），通过对外提供 SDF 接口的加解密、签名验签以及密钥管理等能力，支持客户包括 SSL 网关、电子签章等密码应用，以支持客户完成等保、密评的相关要求。



图六-1　鲲鹏商业密码应用模块示意图

- 鲲鹏商密应用密码模块核心能力如下：
- 原生于鲲鹏服务器，每台主机可具备合规密码能力，天然“一机一密”；
- 软件定义密码服务，在产品快速部署、功能敏捷迭代等方面具备优势，比如升级支持后量子新算法；
- 基于 CPU 软件、CPU 指令集以及 KAE 硬件加速，覆盖小包/大包，多线程高并发的场景，性能好。

（2）鲲鹏 Boostkit TrustZone 机密计算套件

- 鲲鹏 Boostkit 机密计算是基于 TrustZone 技术的 TEE 方案，其核心是基于 iTrustee/CCOS 高安全操作系统构建的安全 TEE 能力，它的主要特点包括如下：
- 稳定可靠：基于华为自研的微内核安全OS，已在手机侧商用近10年，支持过亿级用户；
- 权威第三方认证：整体OS获得CC EAL 4+认证，内核部分获得CC EAL 6+认证；规格灵活：TEE侧安全内存支持按需配置。

（3）鲲鹏商密应用技术方案

商密应用密码模块基于华为自研 iTrustee 操作系统以及内置商密应用密码模块 TA，在系统启动时通过对 iTrustee+内置 TA 固件进行安全启动以满足完整性保护要求。同时，内置 TA 对外提供接口服务、鉴别服务，并基于 iTrustee

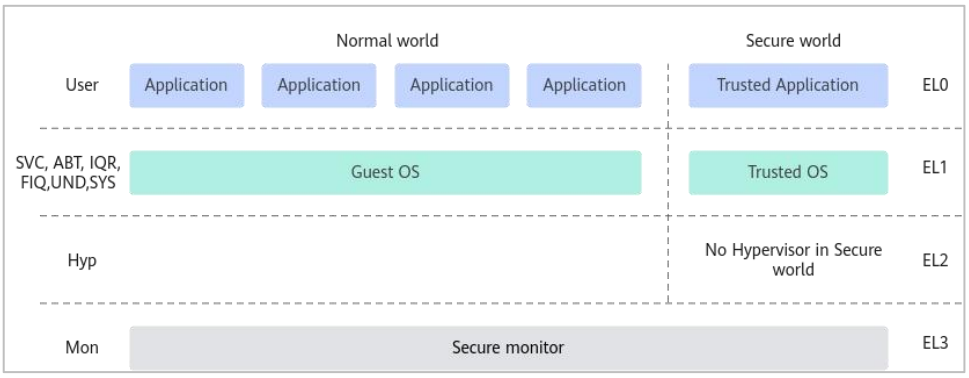
算法服务单元以及安全存储服务单元向外提供算法调用以及密钥管理的能力。

鲲鹏商密应用密码模块满足《GMT 0028-2014 密码模块安全技术要求》技术要求，其对外接口满足《GMT 0018 密码设备应用接口规范》的要求。

（4）鲲鹏 TrustZone 技术原理

鲲鹏机密计算基于鲲鹏处理器架构提供 TrustZone 技术。通过分时复用技术，区分 CPU 的运行状态，在同一套硬件系统上划分了两个独立的环境：

- Normal World：常规环境，即REE（Rich Execution Environment）；
- Secure World：安全环境，即TEE（Trusted Execution Environment）。



图六-2　TrustZone 技术架构原理图

这两个环境各自拥有自己的资源，包括内存和 Cache，根据 CPU 的设计不同，硬件设备也可被设计为 TEE 专用或在需要时可动态切换。只有 CPU 处于 TEE 安全状态时，才可以访问安全侧的资源和硬件。

在此被严格隔离的资源之上，TEE 和 REE 侧分别拥有自己的操作系统，用来执行用户的可信应用。

（5）鲲鹏商业密码方案价值

云化时代密码服务需求日益增长，应用场景多样，部署灵活可扩展，对商密应用能力需求日益强烈。基于鲲鹏商密应用解决方案将为政府及企业用户带来以下价值：

- 高安全隔离环境：密码服务、密钥管理等部署在 TEE 芯片级隔离环境中，保障密钥和数据安全。
- 高性能密码运算：利用鲲鹏 CPU 及加速器能力提供软硬协同的密码运算能力，可达中高端密码机性能。
- 高易用密码接口：具备软件定义密码能力，可实现密码产品快速部署、功能敏捷迭代。

2. 龙芯技术特点及应用

龙芯 SE 安全模块为内嵌式独立安全 IP 核，为基础软件、应用软件、应用系统提供安全、合规和标准化的密码支撑能力。龙芯 SE 安全模块为 CPU 芯片内部一个独立硬件 IP 核，独立于 CPU 计算资源，内部有独立的存储空间，进行密码存储。满足国家密码接口规范，用户可通过标准接口进行调用 SE 安全模块各项功能。龙芯安全模块 SE 拥有密码运算功能，可提供 SM2、SM3、SM4 等国密算法（并开放支持第三方联合拓展开发），属于硬件级密码运算，拥有安全存储、密钥管理和真随机数发生功能，符合国密相关标准要求。并支持虚拟化 SE 功能及可信度量功能，通过可信链进行硬件级逐级保护。同时龙芯 CPU 拥有两大安全机制，核内安全机制与片内安全机制。

核内安全机制：在处理器核之上对程序执行过程进行分析和保护，识别对核心数据或区域的攻击行为，保证计算机运行的安全性。

片内安全机制：在处理器核之外对程序的合法性进行监测和校验，对敏感数据和计算过程进行隔离和保护，通过密码算法保护杜绝数据被窃取的风险。同时采用启用了 SE 安全模块功能的服务器或存储等设备，可直接使用 SE 安全模块为云平台的重要数据加密、节点间传输安全、SE 虚拟化等功能提供密码支撑。

2.1终端磁盘加密应用

磁盘加解密解决方案采用龙芯 3A5000 终端设备，对接密码机，通过操作系统调用龙芯 3A5000 芯片 SE 安全模块中通过国密算法生成的密钥实现对磁盘分区安全加解密，保护敏感数据丢失与泄露。

操作系统安装时进行 DATA 分区，通过调用 cryptsetup 对指定/DATA 分区进行加密，加密密钥由密码机提供，包括非对称密钥（私钥 A 和公钥 B、CA 证书）和对称密钥 K。设备安装系统后，将私钥 A 和公钥 B、CA 证书烧录至龙芯 SE 芯片中。实现对磁盘需要加密分区进行数据保护。

2.2龙芯国密云应用

基于龙芯 3C5000 处理器+信创云平台，通过云平台管理龙芯 CPU 内置 SE 模块，为上层云主机提供灵活的顶层安全模块调度能力，进一步打通从底层硬件、云平台、密码服务的全栈场景，推动密评合规一体化解决方案的落地，有效解决党政、金融、央国企、关基等领域密码需求。

基础设施层：采用自主可控的龙芯 3C5000 服务器（内置 SE 安全模块）作为计算、存储、网络、密码服务的基础设施，为 信创云平台提供虚拟化功能的硬件支持。其中，龙芯 3C5000 CPU 的 SE 安全模块独立于龙芯处理器核工作，提供硬件密码引擎、密钥管理、安全存储与随机数发生等功能。安全模块支持国密算法 SM2/SM3/SM4，可以取代外置密码卡。

云平台服务层：信创云平台利用龙芯 SE 模块接口、密码管理服务平台的接口增加云平台国密功能，保障云平台内重要数据的存储机密性、存储完整性、传输机密性、传输完整性。

密码服务平台层：可部署第三方统一密码管理平台，ZStack 信创云平台将切分后的龙芯 SE 模块，透传给云主机，使得统一密码管理平台获得内生、合规的密码计算能力，构建新型密码资源池系统。

3. 海光技术特点及应用

曙光云在其云中心引入商用密码能力，结合海光 CPU 内嵌的密码模块，将商用密码能力云化，为业务系统提供了“泛在”的商密服务能力。鄂尔多斯信创警务云项目应用此方案，已通过国家信息技术安全研究中心完成了密码测评。相比于传统方式，该方案具有成本低、性能高、生态好等优点，具有推广价值。

基于 CPU 内生的密码方案有以下的优势：

就近加解密：都在本机上就近加解密，避免了数据在网络上的传输，减少了攻击面，更加安全；

加解密计算能力线性增长：有多少海光 CPU，就有多大的加解密计算能力；

降低成本：减少了密码机采购成本、减少了因增加密码机带来的运维复杂度、减少运维成本；

跟云结合之后，租户密码服务会更加安全：VPC 内的应用系统通过云平台内部网络调用基于 CPU 的密码服务，租户无需通过业务网络就能调用密码服务，极大提升了业务系统调用密码服务的安全性。

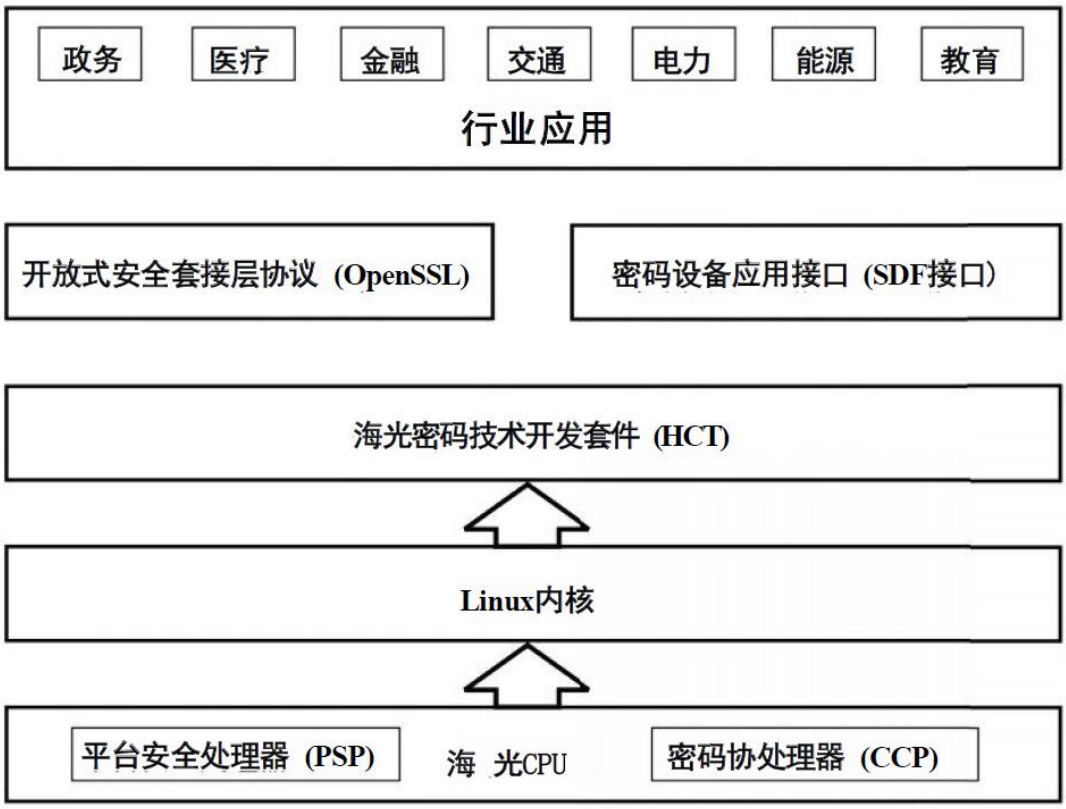
3.1内嵌密码CPU生态体系内生安全应用方案

信息安全是创新发展的重要保障，CPU 是构建网络信息系统安全防护体系的起点和根基。如果 CPU 存在漏洞或后门安全隐患，威胁将无法预估，甚至无从防御。网络安全风险源于图灵机原理和诺依曼结构无防护机理及部件的先天性缺陷，传统的“封堵查”老三样被动防御难以应对严峻的安全形势。安全可信是国家网络安全法律、战略和等保制度的明确要求。自主的不一定安全，但不自主一定不安全。正确的做法是在自主设计的基础上，加上从可信根开始的可信机制与安全保密机制。海光在 CPU 芯片内集成了国密算法、安全可信与访问控制机制，相当于把纪检组派到办公室，安全性进一步提高，性能也进一步提高，同时大幅度降低成本。通过内嵌密码协处理器的方式避免了加解密导致通用计算资源的开销，同时免去了密码卡与整机硬件和操作系统之间的适配工作，可以有效加快商用密码生态体系的建设和迭代。

海光 CPU 芯片中集成了安全模块，可以在硬件层面实现基于国密算法在存储、传输和计算全流程对数据进行密码保护，已经在数据库、云计算、人工智能、桌面电脑、VPN 以及工业控制等领域构建了丰富的解决方案，在各行业进行推广。

海光 CPU 密码生态体系海光 CPU 内嵌密码协处理器 CCP 与安全处理器 PSP，支持 SM2/SM3/SM4 算法的硬件加速、密钥管理、虚拟化等功能。海光可信密码模块符合 GM/T 0028《密码模块安全技术要求》第二级要求，已获得商用密码产品认证证书（证书编号：GM001212220220761）。

海光正积极构建海光 CPU 密码生态体系，与国产应用软件产品厂商建立广泛的合作，形成基于海光可信密码模块的数据库、云桌面管理、云备份、电子印章等内生安全产品及应用方案，通过直接调用海光 CPU 的密码能力，高效快速地实现信息系统机密性、完整性、不可否认性和真实性的保护，在满足合规性要求的同时，为密码应用的各方带来更高的价值，实现商用密码从“能用”到“好用”质的转变。目前，海光信息已正式对外发布完整的开发套件和指导手册（https://www.hieco.com.cn/hygonarch/7），任何单位和个人均可通过以上指导手册，快速完成海光密码技术验证环境的部署。海光 CPU 密码应用技术开发生态体系如下图所示：



图六-3　海光 CPU 密码应用技术开发生态体系示意图

（三）华为在辽宁信创产业布局与生态建设

1. 本地化布局

华为在辽宁本地持续深耕，在沈阳市浑南区成立华为辽宁区域总部，定位为华为在辽宁业务的生态中心、服务中心和创新中心。2024 年 10 月，辽宁省与华

为技术有限公司签署全面深化战略合作协议，双方将在新型基础设施建设、培育新质生产力、赋能新型工业化、数字辽宁建设、要素资源配置等 5 个领域 26 个具体方向上深化务实合作。华为依托鲲鹏芯片技术，支撑沈阳本地信创产业发展及“辽河信创”产线成立。此外，华为依托辽宁本地完善的鲲鹏技术服务团队，支撑全省各行业的信创部署实施及服务保障。

2. 华为构建信创生态

华为在辽宁建立鲲鹏生态创新中心，助力信息技术应用创新领域软硬件适配工作。构建鲲鹏技术路线自主化、智能化适配验证技术体系，形成高效、透明、可审查的适配验证流程；发布客观、公正、可信的适配验证报告；培养一批信息技术应用创新技术人才。

（1）洞察信创生态图谱

基于党政机关、事业单位、国资国企等数字化转型发展趋势，共同梳理各行业在综合办公、经营管理、生产运营等各个信息系统应用场景的解决方案生态图谱，支撑信息技术应用创新和数字化转型过程中明确的发展目标，科学规划技术储备。

（2）信息技术应用创新适配攻关

为党政机关、事业单位、国资国企等提供鲲鹏技术路线的软件适配验证服务，基于信创生态图谱和各用户单位应用系统技术栈情况，进行系统适配迁移评估和调优规划。

（3）信息技术应用创新人才培养

开展信息技术应用创新产业发展与技术能力相关培训，培养了解信息技术应用创新产业趋势、掌握信息技术应用创新能力的科技人才。

（4）信息技术应用创新适配服务保障

为党政机关、企事业单位、国资国企等提供信息技术应用创新咨询、成果展示等服务，做好鲲鹏技术路线的服务保障工作。

（四）信创标准体系、信创适配

1. 信创相关标准体系

1.1 国家政策标准

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

《信息安全技术网络安全等级保护安全设计技术要求》GB/T 25070-2019

《信息安全技术网络安全等级保护测评要求》GB/T 28448-2019

《信息系统密码应用基本要求》GB/T 39786-2021

1.2 采购需求标准

《一体式计算机政府采购需求标准（2023 年版）》

《通用服务器政府采购需求标准（2023 年版）》

《操作系统政府采购需求标准（2023 年版）》

《工作站政府采购需求标准（2023 年版）》

《数据库政府采购需求标准（2023 年版）》

《台式计算机政府采购需求标准（2023 年版）》

《台式计算机批量集中采购配置标准（2024 年版）》

《便携式计算机政府采购需求标准（2023 年版）》

《便携式计算机批量集中采购配置标准（2024 年版）》

2. 信创适配

在当前信创发展全面深化的背景下，信创适配已不再是简单的产品替换，而是一项涉及技术、生态、管理和安全的系统性工程。因此，为指导信创领域应用软件适配工作，辽宁省颁布如下 2 项地方标准：

- 《软件适配验证技术规范》DB21/T3891-2023
- 《信息技术应用创新软件适配性能调优技术指南》DB21/T 4172-2025

信创适配工程通常包括技术栈适配，应用与数据迁移、安全合规以及实施治理策略四个层面，具体描述如下：

2.1 技术栈适配：筑牢基础

这是适配的根本。需确保从底层芯片（ARM、C86 等架构）、操作系统，到上层的数据库、中间件等全栈软硬件的兼容性。应用软件需针对国产平台进行源码改造或重新编译，以保障稳定运行。

2.2 应用与数据迁移：保障连续

这是核心与高风险环节。重点在于业务应用改造与数据迁移。需将应用系统适配新的国产中间件和数据库连接，并将数据从原有库（如 Oracle）平滑迁移至国产库，涉及 SQL 脚本、存储过程等改造，必须进行充分一致性校验。

2.3 安全合规建设：刚性要求

安全是信创的内在要求。必须依据国家标准，集成国密算法（SM2/SM3/SM4），并确保其正确有效应用，以满足“信创测评”与“密评”的合规要求。

2.4 实施治理策略：控制风险

规范流程是成功保障。建议设立跨部门团队，遵循“评估－规划－测试－实施”流程。采用“双轨并行”或分阶段迁移策略，优先非核心业务，并通过充分的功能、性能及用户验收测试，最大限度降低对业务连续性的影响。

总而言之，成功的适配需要技术、管理、安全与生态的协同推进，从而实现

从“可用”到“好用”的跨越。

（五）信创行业解决方案（华为）

信创解决方案在不同行业属性上具有不同特点，不同行业的信创解决方案因其业务特性、系统架构和合规要求的不同而存在显著差异。虽各有差异，但都遵循“统筹规划、试点先行、平滑演进”的核心原则。其本质是以业务为牵引，以技术为支撑，以安全为底线，在保障现有业务连续性的前提下，稳步构建 IT 根基。以下是几个主要行业的解决方案核心要点梳理：

1. 党政机关

核心诉求：实现电子公文、办公业务系统安全能力，确保国家政务信息安全。

解决方案：

- 技术栈：优先完成服务器、台式机、笔记本、操作系统、办公软件的全面替换。
- 应用：重点聚焦电子公文系统、协同办公平台的适配改造，确保内外部公文流转的安全与可靠。
- 安全：严格执行等保测评和密评要求。

2. 金融行业

核心诉求：在满足极高业务连续性、数据一致性和严格金融监管的前提下，实现核心业务系统的平稳迁移。

解决方案：

- 路径：采取“由外到内、由易到难”的策略，从渠道类（如网银、手机银行）、经营管理系统等外围系统切入，逐步向核心交易系统（如账务核心、交易核心）深入。
- 技术：极度重视分布式架构和数据库兼容性。通过单元化、微服务改造，以及数据库和中间件的集群部署，来满足高并发、高可用的业务需求。
- 策略：广泛采用“双轨并行”和灰度发布策略，在业务无感的情况下实现平滑迁移，严控风险。

3. 医疗行业

核心诉求：保障 7x24 小时业务不中断，解决海量医疗数据（如 PACS 影像）的存储与性能瓶颈，并确保患者隐私安全。

解决方案：

- 路径：从医院信息平台（HIS）的后台数据库和实验室信息系统（LIS）等相对独立的系统开始试点，再逐步扩展到电子病历（EMR）、医学影像归档系

统（PACS）等核心临床系统。

- 技术：重点攻克海量非结构化数据（如医学影像）在信创存储架构下的存取性能问题。数据库改造是重中之重，常采用异构数据同步技术实现平滑过渡。

4. 能源与电力行业

核心诉求：满足工业控制系统的实时性、高可靠性要求，并保障国家关键基础设施安全。

解决方案：

- 路径：从管理信息系统（如 ERP、财务系统）向生产管理系统（MIS）、再到监控与数据采集系统（SCADA）、集散控制系统（DCS）等工控系统逐步推进。
- 技术：解决方案需与行业专用的硬件设备和实时操作系统（RTOS）进行深度适配。安全要求极高，需构建从网络边界、主机到控制终端的全方位防护体系。
- 合规：需同时满足能源行业网络安全规定和信创要求。

5. 教育与科研

核心诉求：支持大规模、高并发的在线教学与科研计算需求，实现教学软件的广泛兼容。

解决方案：

- 路径：从行政办公、教务管理系统入手，逐步扩展到智慧教室、在线学习平台，最后是科研计算集群（HPC）。
- 技术：解决方案需重点解决多媒体教学软件、特定科研应用软件在信创平台上的兼容性问题。对于 HPC 场景，需实现计算芯片、编译器等基础算力设施的自主化。
- 生态：推动教学应用软件的适配迁移，构建丰富的信创教育软件生态。

第七章 人才培养

人才是商用密码产业高质量发展的第一资源，更是辽宁抢占数字安全产业高地、筑牢区域安全屏障的核心支撑。当前，商用密码技术迭代加速、应用场景持续拓展，对专业化、复合型密码人才的需求愈发迫切。

本章聚焦密码人才建设核心议题，系统梳理行业人才发展格局，明确人才核心能力与分类标准，构建科学完善的人才建设体系与发展方向，并立足辽宁产业实际，探索具有区域特色的密码人才培养路径，为全省商用密码产业发展注入持久智力动能。

（一）密码人才发展宏观格局

1. 国家战略与产业发展驱动下的人才使命

在中华民族伟大复兴战略全局和世界百年未有之大变局交织激荡的时代背景下，密码人才的战略价值被提升到前所未有的高度。其肩负的核心使命，深刻体现了国家意志与时代需求的统一。

首先，密码人才是筑牢国家网络空间安全屏障的“守护者”。随着全球进入万物互联的时代，网络空间已成为继陆、海、空、天之后的“第五疆域”，其安全性直接关系到国家主权和政权安全。关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。密码技术通过提供身份认证、数据加密、信任传递等核心安全服务，构成了关键信息基础设施安全防护体系的基石。密码人才需要通过持续的技术创新与精准的应用部署，有效抵御网络攻击、防止数据泄露、打击网络犯罪，确保国家能源、交通、金融、电信等关键系统稳定运行，有力维护国家网络空间主权和安全。

其次，密码人才是驱动数字经济高质量发展的“赋能者”。数据作为新型生产要素，是发展新质生产力的核心引擎。数据的自由流动与共享利用，必须以安全可信为前提。密码技术通过在数据产生、传输、存储、使用、销毁的全生命周期提供安全保障，确保了数据的机密性、完整性和不可否认性，是释放数据价值、促进数据要素市场化流通的关键保障。在工业互联网领域，密码技术保障着生产控制指令的准确无误和生产数据的防窃取防篡改；在智慧城市领域，密码技术守护着海量市民隐私数据和城市运行数据的安全；在数字金融领域，密码技术是电子支付、数字货币等业务可信开展的基石。密码人才必须深入行业场景，将密码技术与业务需求深度融合，解决产业数字化转型中的安全痛点，为数字经济健康发展保驾护航。

最后，密码人才是引领密码技术自主创新的“开拓者”。当前，全球科技竞争日趋激烈，密码领域的技术制高点争夺尤为关键。一方面，量子计算等新兴技

术的发展对传统密码算法构成潜在威胁，研制能够抵御量子计算攻击的后量子密码算法迫在眉睫；另一方面，同态加密、安全多方计算等隐私计算技术为数据“可用不可见”提供了全新范式，成为数据要素化进程中的关键技术。面对技术变革的浪潮，密码人才必须勇立潮头，聚焦密码基础理论研究和前沿技术攻关，突破核心技术瓶颈，构建安全高效的密码技术体系和产业生态，不断提升在全球密码领域的话语权和竞争力。

2. 密码人才供需现状与结构特征

密码产业虽处于快速发展阶段，但人才队伍的供给侧与产业发展的需求侧之间存在严峻的结构性矛盾，具体表现为总量缺口巨大、层次结构失衡和区域分布不均。

2.1 人才需求总量持续攀升，供需缺口日益扩大

我国密码人才的现状还远远不能满足信息化和数字经济安全的迫切需要。据不完全统计，目前我国仅有少数军队院校及地方高校开设密码相关专业并培养专业人才，当前密码行业相关工作岗位的人才需求缺口约 20 万人，密码专业基础人才缺口巨大。据预测，在《密码法》全面落地、密评密改工作强制推进，以及各行业数字化转型加速的多重因素驱动下，这一缺口在未来三到五年内仍将持续扩大。特别是在密码应用安全性评估、密码合规咨询、工业互联网密码应用、数据安全密码防护等新兴岗位，人才需求呈现爆发式增长。

2.2 人才结构矛盾突出，高端与复合型人才极度紧缺

当前的人才供给不仅在数量上不足，在质量与结构上也无法满足产业升级的需求，呈现出“葫芦型”而非健康的“金字塔型”结构。

高端领军人才“一将难求”。在密码算法设计、量子密码、隐私计算等前沿技术领域，具备深厚理论功底、卓越创新能力和国际视野的战略科学家、顶尖专家数量稀少。同时，既懂技术又懂管理、能够统筹密码产业发展与安全治理的高端管理人才同样凤毛麟角，这直接影响了密码技术的原始创新能力和产业生态的顶层构建。

“密码+行业”复合型人才“千金难觅”。密码技术的价值在于应用，而应用的成功与否取决于对行业业务逻辑的深刻理解。当前，绝大多数密码从业人员来源于计算机、数学、通信等专业，虽然具备一定的技术基础，但对特定行业（如工业制造、电力能源、医疗健康、智能交通）的业务流程、系统架构、安全需求和监管政策缺乏深入了解。能够为特定行业设计定制化、体系化密码应用解决方案的复合型人才，成为制约密码技术在各行各业深度应用的瓶颈。

基础人才队伍“专业不精”。调研显示，超过 80%的现有密码从业人员未接受过系统的密码学学历教育，多通过短期培训或自学转型而来。这部分人才虽然

能够应对标准化的密码产品部署和基础运维工作，但在面对复杂系统的密码方案设计、深度安全风险评估、密码系统性能优化等任务时，往往显得力不从心，影响了密码保障的整体效能。

2.3 人才区域分布高度集中，区域协调发展面临挑战

密码人才的分布与数字经济发展水平高度相关，呈现出明显的“东强西弱、南密北疏”的空间格局。京津冀、长三角、珠三角三大经济圈凭借其完善的数字产业生态、密集的科研院所、优厚的薪酬待遇和发展机会，汇聚了全国绝大多数密码人才，形成了强大的“虹吸效应”。这些地区不仅拥有大量的密码产品供应商、服务商和测评机构，还通过与顶尖高校的紧密合作，形成了“产学研用”一体化的人才培养闭环。

相比之下，东北地区、中部部分省份和西部地区则面临着密码人才“引不来、留不住”的困境。这些地区密码产业基础相对薄弱，龙头企业较少，高能级的科研平台和具有竞争力的薪酬体系尚不完善，导致本地培养的人才外流，外地人才引入困难，形成了“人才短缺—产业落后—人才流失”的负向循环，加剧了全国密码人才发展的不平衡性，也对区域数字经济的安全均衡发展构成潜在风险。

3. 新时代密码人才发展核心趋势

面对新形势、新要求，密码人才发展呈现出三大核心趋势，深刻影响着未来人才培养的方向与模式。

3.1 技术深度融合催生能力要求升级与新型岗位涌现

密码技术正与人工智能、量子信息、物联网、区块链等前沿技术发生深刻的化学反应，这不仅拓展了密码的应用边界，也对人才的能力谱系提出了全新要求。

“AI+密码”领域：需要人才掌握机器学习技术，能够利用 AI 优化密码算法参数、实现智能化的异常流量检测和攻击识别，同时也要防范 AI 技术本身可能带来的模型窃取、数据投毒等新型安全风险。

“量子+密码”领域：要求人才不仅精通经典密码学，还须具备量子力学基础，能够从事量子密钥分发系统的研发、后量子密码算法的设计与分析等工作。

“物联网/工业互联网+密码”领域：需要人才熟悉受限环境的资源特性，掌握轻量级密码算法和高效密钥管理技术，能够为海量终端设备设计安全、低功耗的密码防护方案。

这些融合趋势要求密码人才从单一的“技术专家”向具备跨学科知识、能够解决复杂场景下安全问题的“跨界融合型”人才转变。同时，隐私计算工程师、后量子密码研究员、工业互联网安全密码架构师等一批新型岗位应运而生。

3.2 人才培养体系加速向专业化、标准化演进

为满足产业对高质量人才的渴求，国家正从学历教育和职业教育两端发力，

推动人才培养的规范化和体系化。

在学历教育方面，我国密码人才培养体系取得了里程碑式的进展。2021 年，教育部正式批准设立“密码科学与技术”本科专业（代码：080918TK），标志着密码学本科人才培养的规范化开端。紧随其后，2022 年国务院学位委员会和教育部在发布的《研究生教育学科专业目录》中，于交叉学科门类下新设“密码”硕士专业学位类别（代码：1452），为培养高层次应用型密码人才奠定了制度基础。截至 2025 年 4 月，全国开设“密码科学与技术”本科专业的高校已增至 22 所，包括南开大学、山东大学、武汉大学、西安电子科技大学、北京理工大学。在硕士层面，全国约有 18 所高校具备“密码”专业学位硕士点的招生资格。这些举措共同推动了密码人才正规化培养进入快车道。

在职业教育方面，2022 年版《中华人民共和国职业分类大典》首次增设“密码工程技术人员”和“密码技术应用员”职业，随后人社部会同相关部门迅速制定了国家职业技能标准，为社会化培训和职业技能等级认定提供了根本遵循。此举极大地推动了密码技能人才队伍的标准化建设和规模化培养。

3.3 产教融合成为培养实战型人才的核心路径

密码技术具有极强的实践性，闭门造车式的培养模式无法满足企业的实际需要。因此，深化产教融合、校企合作，已成为提升人才培养质量与效率的共识。

当前，全国范围内已形成多种协同育人模式：

共建产业学院与联合实验室：高校与企业共同投入资源，建设贴近实战的教学环境，将产业技术前沿和实践案例引入课堂。

“订单式”培养：企业根据未来岗位需求，与高校共同制定培养方案，学生毕业后直接进入企业工作，实现“毕业即上岗”。

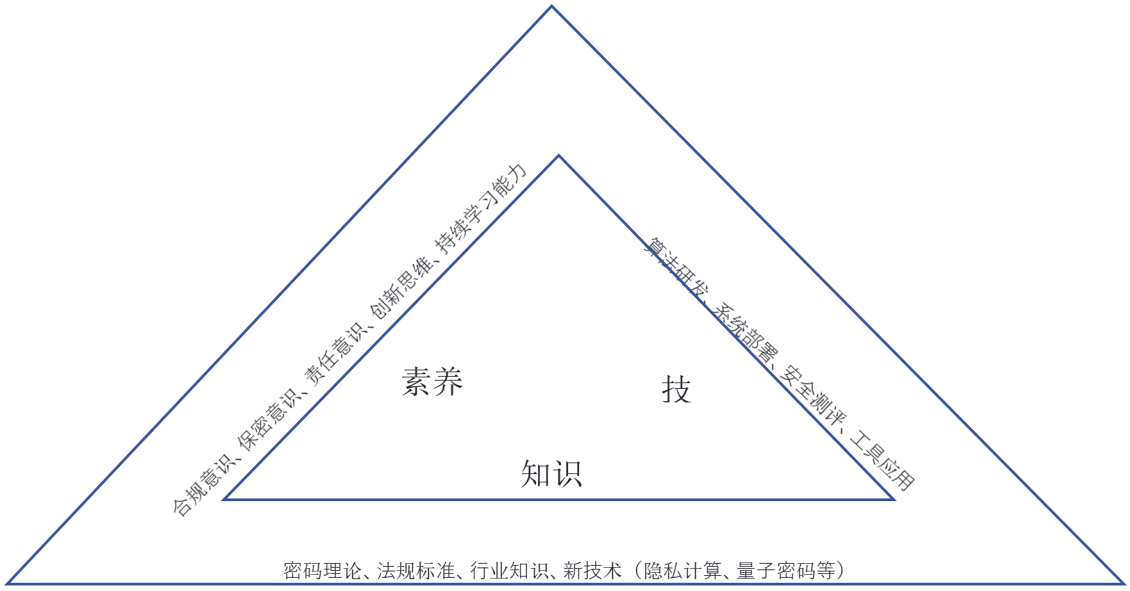
“双导师制”：为学生配备高校学术导师和企业实践导师，共同指导其理论学习和项目实践。

未来，产教融合将从“点对点”的合作，向构建“政产学研用金”多方参与的育人生态演进，通过共建实习实训基地、共享科研设施、共办技术竞赛、共同开展技术攻关等多种形式，全面提升人才的创新能力和实践能力。

（二）密码人才核心能力与分类标准

为科学地培养、评价和使用密码人才，必须建立清晰的人才能力模型和分类体系，为人才培养供给侧改革提供精准“导航”。

1. 人才核心能力三维模型



图七-1　人才核心能力三维模型图

1.1 知识维度：构建复合知识结构

坚实的理论基础：包括高等数学（特别是数论、近世代数）、信息论、计算复杂性理论，以及对称密码（如 SM4、AES）、非对称密码（如 SM2、RSA）、哈希函数（如 SM3）等核心密码算法的原理、安全性和应用场景。对国密算法的深入理解是中国特色密码人才培养的必然要求。

系统的法规标准知识：这是合规开展工作的前提。必须熟练掌握《密码法》《网络安全法》《数据安全法》《商用密码管理条例》等法律法规，以及 GM/T 系列行业标准、密码应用安全性评估规范等。从业人员需时刻以法规标准为准绳，确保密码应用的合法合规。

宽广的行业与关联领域知识：需了解目标行业（如金融、政务、工业）的业务流程、信息系统架构和安全需求。同时，需掌握计算机网络、操作系统、数据库、云计算、大数据等 IT 基础知识的网络安全相关知识，才能将密码技术无缝嵌入到业务系统中。

前沿的新技术知识：这是保持竞争力的关键。需持续跟踪学习隐私计算、量子密码、区块链、零信任等新兴技术的基本原理及其与密码技术的结合点，保持知识体系的时代性。

1.2 技能维度：锻造解决实际问题的实战能力

技术研发能力：面向研发类人才。包括密码算法设计与分析能力、密码协议形式化验证能力、密码芯片/软件/系统的设计与实现能力。要求能够运用编程语言（如 C/C++、Python、硬件描述语言）和开发工具，将理论算法转化为安全、高效的实体产品。

应用实施能力：面向应用类人才。包括密码需求分析、应用方案设计、密码产品选型与部署、系统集成与调试、日常运维与故障排查、密钥全生命周期管理等能力。要求能够根据业务场景，制定出最优的密码应用实施方案并确保其稳定运行。

安全测评能力：面向服务类人才。包括依据国家标准对密码产品进行检测认证的能力、对信息系统进行密码应用安全性评估的能力，以及进行渗透测试和风险分析的能力。要求能够熟练使用各类测评工具，准确识别安全风险并提出有效整改建议。

1.3 素养维度：培育支撑长远发展的职业品格

极强的合规意识与保密意识：密码工作事关国家安全和公共利益，必须将合规操作和保守秘密内化为职业本能，对任何违规行为和泄密风险保持“零容忍”。

高度的责任心与严谨细致的作风：密码系统无小事，任何一个微小的疏忽都可能引发重大安全事件。必须具备对工作极端负责的态度，追求精益求精。

持续的创新思维与学习能力：密码领域攻防对抗激烈，技术迭代迅速。必须保持开放心态，勇于探索新技术，善于自主学习，不断提升自我。

良好的团队协作与沟通能力：密码应用往往是系统性工程，需要与业务人员、开发人员、管理人员等多方协作，能够清晰、准确地沟通技术方案和安全价值至关重要。

2. 按产业价值链的人才分类

从密码产业生态构成的角度，可将人才分为四类，他们在产业链中扮演不同角色，共同推动产业发展。

类别	职责	核心能力
研发类	算法设计、产品开发、 前沿技术攻关	理论创新、编程能力、 技术洞察力
应用类	系统部署、运维、行业场景适配	实践能力、行业理解、问题解决
服务类	测评认证、咨询培训	标准掌握、沟通能力、服务意识
管理类	政策制定、产业规划、生态构建	战略视野、统筹协调、领导力

研发类人才：位于产业价值链的源头，是技术创新的引擎。主要包括算法研发人才（专注密码基础理论和新算法设计）、产品研发人才（负责密码芯片、板卡、软件、系统等产品的工程化实现）和前沿技术研发人才（攻关量子密码、同态加密等下一代技术）。他们是产业核心竞争力的体现。

应用类人才：位于价值链的中端，是技术落地的桥梁。他们分布在各行各业，负责将密码产品和技术应用到具体的业务系统中，确保安全目标的实现。可根据行业细分为政务密码应用人才、金融密码应用人才、工业互联网密码应用人才等。

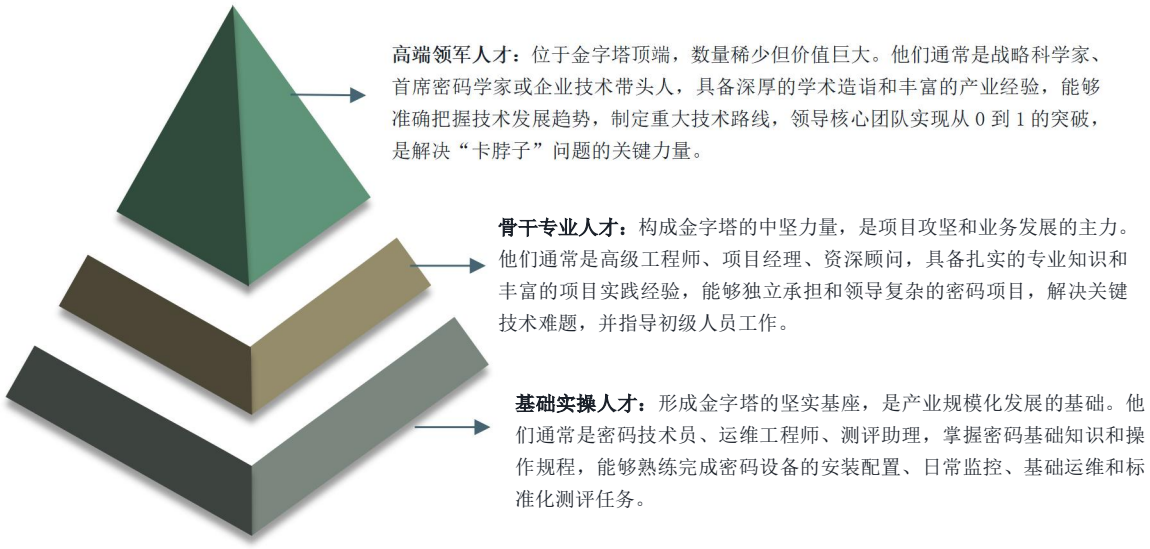
他们是密码价值实现的最终环节。

服务类人才：位于价值链的支撑端，是产业健康发展的保障。主要包括测评认证人才（负责密码产品及应用的安全性检测与评估）、咨询规划人才（为企业提供密码体系建设规划、合规咨询等服务）和教育培训人才（从事密码知识传播和技能培训）。他们为产业提供专业服务和人才供给。

管理类人才：位于价值链的顶层，是产业生态的构建者。包括政策制定与监管人才（在政府机构从事密码政策法规、发展规划制定和行业监管）、产业管理人才（负责密码产业园区建设、生态培育）和企业管理人才（密码企业的经营者、管理者）。他们决定着产业发展的方向和环境。

3. 按技术层级的人才分类

从人才能力和职责的维度，可以构建一个层次分明、梯队合理的人才金字塔结构。



图七-2　技术人才分类

这三类人才分工协作，共同构成一个完整的战斗力体系。培养策略上应“稳定基础、壮大骨干、突破高端”。

（三）密码人才培养体系建设现状与方向

经过近年来的努力，密码人才培养体系已初步建成，但仍在探索中前进，面临诸多挑战与机遇。

1. 产学研协同培养的实践格局

一个以学历教育为基础、以职业培训为补充、以产学研协同为核心的多层次、多渠道人才培养格局正在全国范围内形成。

1.1 学历教育体系不断完善，夯实人才供给主渠道

高等教育承担着为国家输送高层次密码人才的重任。在本科层次，20 所高校开设的“密码科学与技术”专业，普遍构建了以密码数学、密码学原理、国密算法、密码工程为核心的课程体系，并注重与计算机、网络安全等学科的交叉融合。在研究生层次，密码硕士专业学位的设立是一个重大转折，它强调应用导向，要求学生必须在密码产业相关部门进行为期不少于半年的实践，毕业论文选题要求来源于产业真实问题，有力推动了高层次人才培养与产业需求的对接。在职业教育层次，高职专科“密码技术应用”专业的设立，旨在培养面向密码设备运维、系统集成、基础测评等岗位的技能型人才，填补了实操层面学历教育的空白。

1.2 企业主体作用日益凸显，实践培养环节得到强化

越来越多的密码企业认识到，参与人才培养既是社会责任，也是获取优质人力资源的战略投资。

深度参与教学过程：企业通过共建产业学院、设立“订单班”、派遣企业专家担任产业导师、共同开发实训课程和教材等方式，将产业最新的技术、标准和案例带入校园。

提供真实实践平台：大型密码企业和测评机构纷纷建立内部实训基地或对外开放实习岗位，让学生接触真实的项目、产品和技术环境。例如，学生在企业的密评项目中担任助理，全程参与评估流程，其收获远非模拟实验可比。

推动在职人员提升：企业通过建立内部培训学院、组织技术分享会、支持员工考取专业认证等方式，构建学习型组织，持续提升现有员工的专业能力。

1.3 政策与行业组织协同发力，优化人才培养生态系统

政府和行业组织在营造环境、制定标准、搭建平台方面发挥着不可替代的作用。国家密码管理局、教育部、人社部等部委通过政策联动，为密码学科建设、产教融合项目、职业技能培训等提供指导和支持。中国密码学会、中国网络安全审查技术与认证中心、各地方密码行业协会等组织，则通过举办密码技术竞赛、学术会议、专业培训，开展人才能力评价和团体标准制定，促进了学术交流、技术普及和人才流动，为人才培养注入了持续活力。

2. 人才培养的关键瓶颈与优化路径

密码人才培养体系仍面临一些深层次的瓶颈问题，亟待破解。

2.1 当前面临的关键瓶颈

学科建设滞后于技术迭代与产业需求：部分高校课程内容更新缓慢，对后量子密码、隐私计算、工业互联网安全等前沿和热点领域覆盖不足。密码学与具体行业知识的交叉融合课程稀缺，导致培养的人才“懂密码不懂业务”。高水平、有产业经验的师资严重不足。

产教融合“校热企冷”，深度与广度不足：许多校企合作停留在协议层面，缺乏长期、稳定、深入的合作机制。企业出于知识产权保护、项目周期压力等原因，参与人才培养的内生动力不足，提供的实习岗位和项目资源有限。

高端人才引育困难，成为最大短板：在全球范围内争夺顶尖密码学者的竞争中，我们在薪酬待遇、科研环境等方面不具优势。本土培养的博士生和国际一流水平仍有差距，成长为领军人才需要更长周期和更多资源投入。

职业培训市场鱼龙混杂，认证公信力有待提升：社会培训机构质量参差不齐，培训内容与岗位实际需求脱节。部分职业认证考试内容陈旧，未能及时反映技术发展，导致证书的市场认可度不高。

区域发展失衡问题突出，马太效应明显：优质密码教育资源和高薪岗位过度集中于少数发达地区，东北、中西部等地区的人才培养能力弱，人才“孔雀东南飞”现象严重，制约了全国密码产业的均衡布局和协调发展。

2.2 系统性的优化路径

针对上述瓶颈，需采取多管齐下的系统治理方案：

路径一：深化密码学科综合改革。动态更新课程体系，大幅增加前沿技术和行业应用课程比重。实施“师资双千计划”，推动千名高校教师到企业挂职锻炼，聘请千名企业专家到高校兼职授课。鼓励高校与科研院所共建高水平密码实验室。

路径二：构建校企命运共同体。政府可通过“金融+财政+土地+信用”的组合式激励，对深度参与人才培养的企业给予实质性奖励。推广“产业教授”制度，赋予企业导师在研究生培养中更大话语权。探索建立“密码人才培养成本共担与收益共享机制”。

路径三：实施高端人才“引育破壁”行动。设立国家级密码引才专项，面向全球诚聘顶尖人才，提供具有国际竞争力的包干制科研经费和团队组建自主权。设立“密码青年英才基金”，重点支持 40 岁以下优秀青年学者开展高风险、高回报的原创性研究。

路径四：推动职业培训与认证体系提质增效。建立严格的密码培训机构白名单制度和退出机制。推动认证标准与岗位要求、技术发展实时联动，鼓励认证结果与薪酬、晋升挂钩。打通学历教育、职业培训与就业之间的壁垒。

路径五：促进区域间密码人才协同发展。实施“东密西送”人才支持计划，鼓励东部地区高校、企业对口中西部和东北地区联合培养人才。支持在有条件的地区建设密码特色产业集群，以产业集聚带动人才集聚。完善区域性人才公共服务体系，营造宜居宜业环境。

3. 政策引导下的人才培养标准化建设

标准化是规模化、高质量培养人才的前提。正通过自上而下的政策引导，快速推进密码人才培养的标准化进程。

国家层面：构建顶层制度框架。教育部制定的《密码科学与技术专业教学质量国家标准》和国务院学位委员会发布的《密码硕士专业学位研究生指导性培养方案》，为学历教育提供了统一的“施工蓝图”。人社部制定的《密码工程技术人员国家职业技能标准》等，则清晰地定义了职业活动内容、技能要求和相关知识，为职业教育与培训提供了权威依据。

地方层面：推动标准落地与特色化实施。各省（区、市）密码管理局、教育厅、人社厅等部门协同，结合本地产业规划，出台配套实施细则和扶持政策。例如，在制定本省的密码人才培养方案时，会重点考虑本地支柱产业（如辽宁的装备制造、广东的电子政务）对密码人才的特定需求，在标准框架内体现地方特色。

行业层面：细化标准与促进自律。中国密码学会等行业组织发挥其专业优势，制定更为细化的能力评价标准、培训课程规范等团体标准，作为国家标准的有效补充。同时，通过开展行业自律，对培训质量进行监督，维护健康的市场秩序。

通过“国家定框架、地方抓落实、行业补细节”的三级联动，一个覆盖人才培养全链条、全周期的标准化体系正在加速形成，为密码人才队伍的规范化、专业化建设奠定了坚实基础。

（四）辽宁省密码人才培养

辽宁省立足国家战略需求与自身资源禀赋，正积极探索一条以产业需求为导向、以场景实战为特色、以全链条保障为支撑的密码人才培养新路。

1. 辽宁密码人才培养的战略定位与基础条件

1.1 战略定位：服务全面振兴，打造东北密码人才新高地

辽宁省将密码人才培养深度融入“数字辽宁、智造强省”建设和全面振兴新突破三年行动的大局中。其核心战略定位是：建设成为立足辽宁、辐射东北、服务全国的工业互联网密码应用创新高地与密码人才集聚区。具体而言，就是要为辽宁省重点布局的 22 个产业集群和 4 个万亿级产业基地（先进装备制造、石化和精细化工、冶金新材料、优质特色消费品）的数字化、智能化转型，提供坚实可靠的密码安全人才保障和技术支撑。这不仅关乎本省数字经济的发展安全，更承担着引领东北地区密码产业协同发展、优化国家密码人才区域布局的重要使命。

1.2 基础条件：多维优势构筑人才培养坚实基座

辽宁在密码人才培养方面具备得天独厚的综合优势。

政策环境优越：辽宁省密码人才培养工作紧密衔接国家战略，以《密码法》和《商用密码管理条例》为根本遵循，结合本地实际出台了一系列支持政策。例如，《辽宁省实施加快数字人才培育支撑数字经济发展行动方案（2024—2026年）的若干措施》将密码技术列为重点培训领域，并提供资金保障。省密码管理局通过专项考核、政策解读等方式，确保政策落地见效。此外，辽宁省还将密码

人才培养纳入数字辽宁建设整体布局，与数字经济、网络安全等规划协同推进，形成政策合力。

区域优势明显：辽宁省作为东北地区密码产业创新高地，具有区位优势和政策倾斜，可吸引周边省份密码人才集聚。通过建设密码产业园、举办技术论坛、开展人才交流等活动，打造密码技术生态圈。同时，辽宁省通过借鉴优秀省份密码学科经验，建设本地密码人才培训中心，开展职业认证、技能竞赛等活动，提升人才专业水平。

产业场景丰富：作为共和国工业长子、老工业基地，辽宁拥有大量关键信息基础设施和工业互联网平台，为密码技术应用提供了丰富的实操场景。例如，在智能制造领域，密码技术可用于保障生产线数据安全；在能源电力领域，密码技术可保护电网控制系统免受网络攻击。这些场景为密码人才提供了真实的实战环境，学生可通过参与企业项目，掌握密码技术在实际业务中的集成、运维与优化技能。辽宁省依托这些优势，打造“密码+工业”特色人才培养模式，开设工业密码应用、工控系统安全等专项课程，培养既懂密码技术又熟悉工业业务的复合型人才。

科教资源集聚：辽宁省已初步构建覆盖本科、研究生、职业教育的密码学历教育体系。密码智能化产业学院作为省内首家密码本科学院，聚焦密码技术与产业融合，开设算法设计、工程应用等核心课程；研究生培养基地通过校企合作，培养高层次研发人才；在职业教育端积极申请密码相关专业，填补技能型人才培养空白。辽宁省通过借鉴积累多年的高校资源整合经验，支持沈阳工业大学、东北大学等高校加强密码学科建设，开设密码科学与技术专业，扩大人才培养规模。

实践平台多样：辽宁省通过校企合作、平台共建等方式，强化密码人才实践能力培养。例如，北方实验室与高校共建研究生培养基地，为学生提供密码测评、安全协议设计等实战机会；沈阳问天量子等企业在量子密码等前沿领域布局，为学生提供科研实践平台。辽宁省进一步拓展合作范围，鼓励密码企业与高校共建密码实训实验室，配备先进密码设备，模拟真实应用场景，提升学生动手能力。

2. 辽宁特色人才培养体系构建

辽宁摒弃“就教育谈教育”的狭隘思路，构建了一个将教育链、人才链与产业链、创新链深度融合的特色培养体系。

2.1 学科筑基：打通学历教育通道，夯实人才理论基础

本科教育突出“产教融合”：沈阳工业大学与北方实验室共建的密码智能化产业学院已经建立，聚焦密码技术与产业场景的深度融合。该学院依托辽宁省工业互联网、智能制造、能源电力等优势产业，开设密码算法设计、工业控制系统安全、密码应用测评等特色课程，强调理论与实操结合，为学生提供真实的工业场景实训机会。例如，结合辽宁鞍钢、沈鼓集团等企业的工业互联网平台，开展

密码技术在工控系统中的应用实践，培养学生解决实际安全问题的能力。

辽宁警察学院和大连秘阵股份有限公司共同申报的公共安全产业学院，是全国公安院校中首家挂牌密码学院的高校，也是辽宁省第二家密码学院。该校还与辽宁省国家密码管理局签署密码领域合作协议，聚焦密码技术与警务实践的结合，培养既懂密码技术又具备警务实践能力的复合型人才，适配公共安全领域的密码安全需求，属于特色化密码产教融合模式。

大连理工大学城市学院和曙光信息产业股份有限公司还共同申报了中科曙光信创产业学院。

研究生教育聚焦“高端创新”：辽宁省着力打造高层次人才培养平台。沈阳工业大学和北方实验室校企共建的省级研究生联合培养基地，形成了“实习实践—产业研发—学位研究”的递进式培养模式。企业多名高级职称专家受聘担任研究生导师，双方共同制定培养方案、组建混合型师资队伍，为研究生提供密码测评、信息安全等前沿实践环境。自 2022 年起每年为企业定制培养 10 名左右在职研究生，实现产学研用深度融合。

职业教育瞄准“技能实操”：辽宁省积极申请密码学相关专业，填补职业教育在密码领域的培养空白。在职业认证方面，“密码工程技术人员”“密码技术应用员”资质获批，推动密码实操型、技能型人才的系统化培养。这些基础为构建本地化、专业化的密码人才梯队提供了以实践为导向的技能培养平台。大连职业技术学院、大连枫叶职业技术学院获得密码技术应用专业专科（高职），面向密码技术应用、密码应用安全测评等领域，培养能从事国产密码产品部署管理、商用密码产品检测、商用密码应用测评等工作的高素质技术技能人才。同时，省内职业院校可依托《辽宁省实施加快数字人才培育支撑数字经济发展行动方案（2024—2026 年）的若干措施》中的政策支持，争取高技能人才培训基地补助资金，强化密码技能实训条件建设。

2.2 产业赋能：激活企业主体作用，实现供需精准对接

企业参与人才培养全过程：成立了由省内重点企业技术负责人组成的“密码专业教学指导委员会”，直接参与培养方案审定、课程大纲编写和毕业要求制定。

共建共享实践资源：联合培养过程中，学生可以接触到最新的测评设备和高度仿真系统，模拟真实工作场景，提升实战能力。

以真实项目驱动能力提升：将企业的实际需求转化为学生的课程设计、毕业设计和科研训练项目。这种“真刀真枪”的锻炼，极大地提升了学生的工程实践能力和综合素养。

3. 人才就业渠道多元

辽宁省密码技术人才的就业渠道多元，主要流向政府部门、关键信息基础设施运营单位、密码产品研发企业、测评机构及高校科研院所。随着“数字辽宁”

战略的推进，密码技术在政务、金融、医疗、能源、低空经济等领域的应用不断深化，密码人才就业岗位持续增加。据统计，辽宁省密码相关岗位年均增长率超过 20%，其中密码应用部署、密码测评、密码系统集成等实操型岗位需求最为旺盛。

为提升人才就业质量，辽宁省推动建立密码人才认证与就业衔接机制。例如，省密码管理局联合人社部门开展密码技术应用员、密码工程技术人员职业资格认证，持证人员可优先推荐到省内重点企业就业。同时，依托密码智能化产业学院、北方实验室等平台，开展定向培养，学生毕业后直接进入合作企业工作，实现“毕业即就业”。此外，辽宁省还鼓励密码人才在本地创业，为密码技术初创企业提供税收优惠、创业孵化等支持，进一步拓宽就业渠道。

4. 面临的挑战及应对建议

4.1 面临挑战

培养体系与产业需求脱节：高校专业课程设置更新滞后于密码技术迭代速度，对密改密评、量子密码等前沿领域的教学覆盖不足，实践教学环节与企业实际需求衔接不紧密，导致人才实践能力与岗位要求存在差距。辽宁省需进一步加深做强校企合作，将行业最新需求融入课程设计，例如开设工业密码应用、密码测评实务等实战课程。

高端人才集聚能力不足：相较于京津冀、长三角等密码产业发达地区，辽宁省在科研平台能级、薪酬激励机制、产业生态完善度等方面竞争力较弱，高端密码人才“引育留用”难度较大。需通过政策扶持、资金投入、平台建设等方式，提升人才吸引力。

跨行业协同机制不健全：密码人才在金融、医疗、低空经济等重点应用领域的行业适配性不强，尚未形成“一专多能”的行业适配型人才培养机制，人才流动与资源共享壁垒尚未完全打破。辽宁省将凭借密码人才分类经验，按研究型、工程型、应用型、管理型四类人才需求，构建差异化培养路径，提升人才与产业的匹配度。

4.2 应对建议

面对挑战，辽宁正把握机遇，构建“引育留用”闭环人才生态。为确保人才“引得来、育得强、留得住、用得好”，辽宁省需着力构建一套覆盖人才发展全生命周期的保障机制。

“引才”端：实施精准化、多元化引才策略。通过“兴辽英才计划”“项目+团队”打包引进、“柔性引智”广纳贤才等多元化方式，吸引高端人才入辽、驻辽。

“育才”端：构建终身化、实战化、产业化培育体系。设立专项资金支持开

展密码应用场景化教学、推动职业认证与就业衔接并实施补贴制度、深化产学研用合作、开展密码技术竞赛与交流等多种方式培育具备复合能力的实战型技能人才。

“留才”端：营造宜居宜业的发展软环境。开展“辽聚英才”安居工程，对密码人才提供住房、子女教育、医疗保障等优惠，吸引外地人才扎根辽宁；鼓励密码人才在本地创业，提供创业孵化支持；评选表彰先进密码领域先进事迹，给予精神和物质双重激励，提升人才的职业自豪感和归属感。

“用才”端：搭建人尽其才的发展硬平台。“揭榜挂帅”给机会、“创新工作室”给舞台、“成果转化激励”给实惠，充分激发密码人才工作热情。

第八章 参编单位简介

辽宁省商用密码产业发展报告是由辽宁省工业和信息化厅、辽宁省国家密码管理局、辽宁省商用密码协会主编，协会会员单位共同编撰。本次报告的编撰过程得到了测评机构：北方实验室（沈阳）股份有限公司、沈阳赛宝科技服务有限公司；电子认证机构：辽宁数字证书认证管理有限公司、辽宁广烁科技有限公司；运营商：联通（辽宁）产业互联网有限公司、中国移动通信集团辽宁有限公司；密码生产研发企业北京数字认证股份有限公司、北京信安世纪科技股份有限公司、中国科学院沈阳计算技术研究所有限公司、中国科学院沈阳自动化研究所、大连秘阵科技有限公司、辽宁公信安全信息科技有限公司、沈阳安创信息科技有限公司 、长春吉大正元股份有限公司、辽宁航天信息有限公司、沈阳问天量子科技有限公司；密码与信创企业华为技术有限公司、龙芯中科技术股份有限公司 、曙光信息产业股份有限公司 19 家会员单位的鼎力支持与深度参与，形成了跨领域、多层次的协同编撰，为辽宁省商用密码产业发展报告提供了坚实的技术保障与数据支撑。

辽宁省商用密码协会，成立于 2021 年 9 月，会员单位由在省内从事商用密码生产研发企业、测评机构、科研院所、高校、运营商、集成商构成，协会现有会员单位 127 家。

根据《辽宁省社会组织评估实施办法》，经 2025 年全省性社会组织评估委员会决议、厅党组会审议，辽宁省商用密码协会获得“2025 年全省性社会团体和基金会的评估”4A 等级，这一荣誉的取得，不仅是对协会自身规范化建设、专业化服务能力的高度认可，更体现了协会会员单位凝心聚力、携手共进的坚实力量，也彰显了业务主管单位在统筹规划我省商用密码产业布局、指导协会夯实产业根基、赋能行业合规化建设过程中起到了关键作用。

协会秉持开放包容、合作共赢的理念，致力于为会员单位搭建优质高效的交流服务平台；积极宣传贯彻党和国家相关方针政策、法律法规，推动全省密码行业规范健康发展，维护公平有序的行业市场秩序；充分发挥桥梁纽带作用，做好业务主管单位的得力助手，为辽宁省密码产业高质量发展注入强劲动力、贡献坚实力量。

（一）测评机构

1. 北方实验室（沈阳）股份有限公司

1.1 单位基本情况

北方实验室（沈阳）股份有限公司是一家以网络安全服务和信息技术咨询服务为主营业务的信息技术服务提供商，是国家级专精特新“小巨人”企业、国家中小企业公共服务示范平台，依托自主研发的智能渗透攻击、主机攻击监测预警等关键核心技术，主要从事网络安全检测评估、网络安全咨询、网络安全运营、信息系统工程监理和信息系统咨询设计等业务。公司聚焦政务、水利、通信、教育、医疗、金融、能源、国防、交通等关键信息基础设施行业领域，致力于为客户提供覆盖信息系统全生命周期的综合性、跨阶段、一体化的第三方网络安全服务以及信息技术全过程服务。公司以“第三方”视角，秉承“保障数字安全，护航数字中国”的企业使命，坚持“创新驱动发展”的经营理念，持续为高质量推进网络强国建设贡献力量。目前在北京、安徽、广东等多个地区成立了 14 家分公司、13 家子公司，于 2024 年 10 月 23 日在新三板挂牌。

公司是国家 CNAS 认可实验室，国家高新技术企业，拥有省级工程实验室、省级技术创新中心、省级企业技术中心、省级新型研发机构、市级新型研发机构、辽宁省网络与信息安全信息通报中心北方分中心。同时，公司是国内首批网络安全等级保护测评机构、商用密码检测评估机构，是密码行业标准化技术委员会成员、全国信息安全标准化委员会成员、辽宁省商用密码协会会长单位、工业信息安全检测应急支撑单位、国家信息安全漏洞库（CNNVD）一级技术支撑单位（最高等级），是多家权威机构认可的网络安全百强企业之一，曾入选数世咨询《中国数字安全 100 强》中坚力量名单，也曾入选中国计算机学会抗恶劣环境计算机专委会、信息产业信息安全测评中心、安全牛联合发布的第十一版《中国网络安全企业 100 强》名单。

1.2 商用密码产品（服务）解决方案情况

公司是国家第一批密评机构，聚焦“密码能力可信评估与全生命周期应用支撑”，构建起贯穿前期咨询规划、中期检测评估、适配部署到后期持续运营的一体化服务链条。

1.3 行业成功案例

近五年来，公司密评业务已在全国范围内落地生根，累计完成 2000 余个系统的商用密码应用安全性评估项目，案例全面覆盖政务、能源、金融、公安、医疗、工业、教育、税务等关键行业领域，凭借专业的技术能力、完备的资质保障与丰富的实践经验，赢得了各行业客户的广泛认可，形成了一批具有行业标杆意义的典型案例。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203104801004487L8
生成时间：2025年12月03日 10:48:01

扫一扫
核验码

公共信用信息概览

北方实验室(沈阳)股份有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210112752774519B	法定代表人/负责人/执行事务合伙人	杨丽春
企业类型	股份有限公司(非上市、自然人投资或控股)	成立日期	2003-08-04
住所	辽宁省沈阳市浑南区智慧三街199-1号（101）		

信用信息概要

行政管理	19条	诚实守信	8条
严重失信	0条	经营异常	0条
信用承诺	8条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

2. 沈阳赛宝科技服务有限公司

2.1 单位基本情况

沈阳赛宝科技服务有限公司成立于2011年，注册地址沈阳市浑南新区高歌路2-1号B座225室，现办公地址辽宁省沈阳市和平区市府大路55号，单位性质全资国有单位，原辽宁省电子信息产品监督检验院（辽宁省信息安全与软件测评认证中心）成立的独资公司。目前，公司纳入省国资委统一监管，辽宁利盟国有资产经营有限公司作为公司唯一股东，持股100%。注册资本1100万元。员工总数110人，研发及技术团队占比超74%（82人）。核心资质荣誉包括高新技术企业、辽宁省专精特新“小巨人”企业，拥有商用密码评估相关专业技术团队支撑。累计获得多项软件著作权，技术实力雄厚。

2.2 商用密码产品（服务）解决方案情况

公司作为商用密码检测机构，核心服务涵盖信息系统商用密码应用安全性评估、密码应用方案商用密码应用安全性评估以及相关咨询业务等多维度赋能服务，并针对省内政务领域政务云系统密码应用方案给予合理化建议，确保密码资源应用建设和使用的合规性、正确性、有效性。

2.3 行业成功案例

在政务领域完成多个密码应用安全性评估项目，助力系统合规达标；在金融、医疗、交通等领域也积累了丰富项目经验，为多家单位提供密码应用测评服务，形成成熟服务模式，获客户广泛认可。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203100856630568B21
生成时间：2025年12月03日 10:08:56

扫一扫
核验码

公共信用信息概览

沈阳赛宝科技服务有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210112569408617G	法定代表人/负责人/执行事务合伙人	金鑫
企业类型	有限责任公司（非自然人投资或控股的法人独资）	成立日期	2011-03-03
住所	沈阳市浑南新区高歌路2-1号B座225室		

信用信息概要

行政管理	0条	诚实守信	7条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

（二）电子认证机构

1. 辽宁数字证书认证管理有限公司

1.1 单位基本情况

辽宁数字证书认证管理有限公司成立于 2004 年 3 月 16 日，注册资本 3,000 万元，办公地址位于沈阳市和平区和平南大街 28 号甲 3，属于民营企业，员工总数 33 人，研发团队占比 21%。

已获资质有国家密码管理局《电子认证服务使用密码许可证》《电子政务电子认证服务机构》资质，工业和信息化部《电子认证服务许可证》资质、卫生部《医疗卫生电子认证服务机构》资质，国家信息中心《国家电子政务外网辽宁省电子认证服务分中心（LRA）》资质，软件著作权 6 项。

1.2 商用密码产品（服务）解决方案情况

辽宁数字证书认证管理有限公司主要面向省内政企、医疗领域客户群体提供安全合规的数字证书服务，包括国密企业和个人证书、国密 SSL 证书、国际 SSL 证书等服务类型。

解决方案：区别传统 PC 端使用数字证书应用场景，通过数字证书服务和协同签名系统集成部署，可实现数字证书自助申请、自动审核、下发等功能，简化数字证书申请流程，提升数字证书使用便捷性，全面支持业务系统身份认证和数据加解密的需求，实现密码技术深度融合应用。

1.3 行业成功案例

省内某政务类 APP 通过对接数字证书服务和协同签名系统，实现数字证书自助申请、自动审核和下发等功能，公务人员使用数字证书完成身份认证。目前在该 APP 下使用数字证书人数已达到 1 万多人。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203115107972487C6
生成时间：2025年12月03日 11:51:07

扫一扫
核验码

公共信用信息概览

辽宁数字证书认证管理有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210000759117482Q	法定代表人/负责人/执行事务合伙人	李东海
企业类型	其他有限责任公司	成立日期	2004-03-16
住所	沈阳市和平区和平南大街28号甲3		

信用信息概要

行政管理	0条	诚实守信	4条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

2. 辽宁广烁科技有限公司

2.1 单位基本情况

公司成立于 2015 年，注册资金 3000 万元，注册于辽宁大连市，办公地址位于辽宁省大连市中山区，员工总数 35，研发人员占比 86%，是民营企业。是国家级高新技术企业、雏鹰企业、科技创新型企业、国家 ISO9001 质量管理体系认证企业，是辽宁省商用密码协会监事单位，省内首个通过商用密码产品认证的企业。获得商用密码产品认证证书、国家保密科技测评中心检测及进入国家信创名录的产品。累计获得 52 项软件著作权。

2.2 商用密码产品（服务）解决方案情况

公司自主研发的电子印章系列产品涵盖统一电子印章平台、统一身份认证平台、统一电子证照平台等核心系统，解决方案支持信创云、政务云、私有云等多场景部署，提供公安备案、全国互认的电子印章制作与应用服务，可通过辽事通、辽宁政务服务网等渠道实现便捷申领，满足政务与商务领域电子文件签署的安全可信需求。

2.3 行业成功案例

公司承建多个省级、地市级印章管理系统，作为公安部第三研究所电子印章应用试点单位，实现与全国电子印章管理与服务平台的备案互认。目前，为全国各级政府及企事业单位提供电子合同签署、电子档案管理等服务，支撑政务事项办理与商务合作中的电子文件可信签署，形成政务与商务领域电子印章互信互认的典型应用案例。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203102302577655X1
生成时间：2025年12月03日 10:23:02

扫一扫
核验码

公共信用信息概览

辽宁广烁科技有限公司

存续

登记注册基本信息

基础信息

统一社会信用代码	91210204341167191F	法定代表人/负责人/执行事务合伙人	李秀春
企业类型	有限责任公司(自然人投资或控股)	成立日期	2015-09-09
住所	辽宁省大连市沙河口区富华街10号1-5号		

信用信息概要

行政管理	1条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

（三）运营商

1. 联通（辽宁）产业互联网有限公司

1.1 单位基本情况

成立于 2018 年 3 月 28 日，注册于沈阳经济技术开发区，办公地址位于沈阳市大东区。公司为国有企业，注册资本 1 亿元，现有员工 482 人，其中研发团队 102 人，占比 21%。公司为高新技术企业、专精特新企业、瞪羚企业，并担任辽宁省商用密码协会理事单位。技术实力方面，拥有专利 24 项（发明专利 7 项，外观专利 17 项），软件著作权 126 项。

1.2 商用密码产品（服务）解决方案情况

公司遵循《密码法》及国家政务信息化项目管理要求，面向辽宁省各委办厅局业务系统，提供“密码服务平台+云服务器密码机”SaaS 化模式及“服务器密码机+签名验签服务器”硬件堆叠模式，结合 VPN 与数字证书等产品，满足密评国家标准三级系统要求，实现安全合规。

1.3 行业成功案例

作为辽宁省政务云建设的主要服务商，公司为政务云平台提供密码服务，保障其通过密评。在互联网区与公共服务区云平台中，采用签名验签服务器和服务器密码机，分别提供签名验签与加解密服务，结合个人数字证书、SSL VPN 网关、国密浏览器及堡垒机管控，实现身份认证、链路加密与访问控制，确保平台安全合规。

面向云租户，公司构建了云上密码服务平台及底层云服务器密码机资源，提供统一密码安全能力与集中化管控，支持租户隔离、资源计费、弹性扩容。该平台独立于政务云的计算与存储资源，可按需为租户分配加解密、签名验签、身份认证及密钥管理等密码服务，满足业务系统密码应用需求。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203103556844 3D555
生成时间：2025年12月03日 10:35:56

扫一扫
核验码

公共信用信息概览

联通(辽宁)产业互联网有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210100MA0XMJTP81	法定代表人/负责人/执行事务合伙人	吕生亮
企业类型	有限责任公司（非自然人投资或控股的法人独资）	成立日期	2018-03-28
住所	辽宁省沈阳市沈阳经济技术开发区花海路36-3号		

信用信息概要

行政管理	0条	诚实守信	2条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

2. 移动中国移动通信集团辽宁有限公司

2.1 单位基本情况

中国移动通信集团辽宁有限公司隶属于中国移动通信集团，负责中国移动在辽宁的网络建设和业务经营，为地方社会提供全方位的数字化服务。公司成立于 2000 年，注册和办公地址为沈阳市浑南新区新隆街 6 号，单位性质为国有，注册资本 514012.7 万元。公司目前认定网信人才共 538 人，其中高级专家 37 人。

资质荣誉奖项：信息安全管理体系认证（ISO27001）；质量管理体系认证（ISO9001）；信息安全服务资质认证 CCRC（三级）；网络安全应急服务支撑单位（国家计算机网络应急技术处理协调中心 CNCERT）；网络安全技术保障支撑单位（辽宁省通信管理局）。

近三年以来，在安全风险识别、安全防御、安全检测、数据安全管控等方面孵化专利 20 余项。

2.2 商用密码产品（服务）解决方案情况

超级 SIM 智能密码钥匙、号码认证等 5 项商用密码产品。

政务系统密码应用解决方案：通过建设政务云密码资源池，采用“三同步一评估”的建设原则，为政务系统提供合规的密码服务能力。

数据要素流通基础设施方案：基于数联网、主体授权等能力优势，打造可信数据流通基础设施，解决数据要素流通合规困境、明确数据权属，有效推动多方数据融合应用。

2.3 行业成功案例

政务：政务系统密码应用解决方案；

可信通信：基于国产密码算法的 5G 可信专网解决方案、量子加密通信解决方案、高校 5G 专网国密二次鉴权解决方案；

数据要素流通：数据要素流通基础设施主体授权方案、基于隐私计算的数据流通利用基础设施方案、个人数据可信流通方案、基于可信数据流通的医疗保险快速核保方案。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251205095111065812 9D
生成时间：2025年12月05日 09:51:11

扫一扫
核验码

公共信用信息概览

中国移动通信集团辽宁有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210000719646152 9	法定代表人/负责人/执行事务合伙人	刘宏志
企业类型	有限责任公司(外商投资企业法人独资)	成立日期	2000-12-27
住所	辽宁省沈阳市浑南区新隆街6号		

信用信息概要

行政管理	18条	诚实守信	10条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月05日	报告出具单位	国家公共信用和地理空间信息中心

（四）密码生产研发企业

1. 北京数字认证股份有限公司

1.1 单位基本情况

北京数字认证股份有限公司成立于2001年，2016年在深交所上市（股票代码：300579），被誉为“中国电子认证第一股”。公司注册地址为北京市海淀区北四环西路68号1501号，辽宁省内办公地址位于沈阳市和平区文化路77号华航大厦803。单位性质为国有控股，注册资本2.7亿元，员工总数超1500人，研发团队占比超30%。核心资质涵盖电子认证服务许可证、电子政务牌照、WebTrust国际认证等，持有近50个商用密码资质；先后荣获国家科技进步奖二等奖、密码科技进步奖等重要荣誉，是高新技术企业与网络安全产业中坚力量。技术实力雄厚，累计拥有200余项商用密码产品资质及180余项软件著作权。

1.2 商用密码产品（服务）解决方案情况

代表性商用密码产品涵盖密码服务管理平台、云服务器密码机、签名验签服务器、服务器密码机、时间戳服务器、手写信息数字签名系统、协同签名系统、电子签章、安全认证网关、数据库加密与访问控制系统等20余种。

政务领域：推出数字政府密码保障解决方案，解决政务数据安全防护与身份可信认证问题，应用于政务服务、财税等场景；

医疗领域：提供医疗卫生全流程密码保障方案，保障医疗数据共享与电子病历安全，适用于医院无纸化办公、医保支付等场景。

1.3 行业成功案例

在政务领域，业务覆盖全国30多个省份及自治区、服务20+国家部委及500+客户，参与数十个省市级密码保障体系规划建设，为数字政府建设筑牢安全底座，支撑政务信息化安全运行；

医疗领域，服务全国2000余家医疗机构，构建智慧医院密码保障体系；教育领域，为全国300多所高校提供密码服务，助力教育数字化转型；在金融、企业数字化转型、车联网等行业拥有成熟项目经验，具备全场景密码应用服务优势。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251229174440095688W22
生成时间：2025年12月29日 17:44:40

扫一扫
核验码

公共信用信息概览

北京数字认证股份有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91110108722619411A	法定代表人/负责人/执行事务合伙人	林雪焰
企业类型	其他股份有限公司(上市)	成立日期	2001-02-28
住所	北京市海淀区北四环西路68号1501号		

海关注册登记信息

所在地海关	京中关村	备案日期	2019-07-17
经营类别	——	海关注销标志	正常

信用信息概要

行政管理	2条	诚实守信	9条
严重失信	0条	经营异常	0条
信用承诺	4条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月29日	报告出具单位	国家公共信用和地理空间信息中心

2. 北京信安世纪科技股份有限公司

2.1 单位基本情况

公司成立于 2001 年 8 月，注册地址位于北京市海淀区，辽宁省分公司办公地址为沈阳市和平区三好街同方广场。作为民营上市公司，注册资本约 3.17 亿元，员工总数 900 人，其中研发团队超过 400 人，技术团队 200 余人。公司是国家高新技术企业，曾获省部级科技进步奖，并担任多省商用密码协会副会长单位等职务。技术实力方面，累计拥有专利 188 项、软件著作权 219 项，掌握 16 项重大核心技术，已取得商用密码产品认证证书 45 个。

2.2 商用密码产品（服务）解决方案情况

公司以密码技术为核心，结合网络安全技术，围绕身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列，为各类网络环境提供基础安全支撑。针对政务业务上云需求，提供密码资源池解决方案，支持云租户集约化、多样化密码应用，按需分配服务资源，保障云上业务系统的身份、网络与数据安全。

公司积极响应国家密码应用政策，提供覆盖多领域、多场景的商用密码改造方案，从设计、对接到实施提供全流程一站式服务，助力客户通过密评合规要求。

2.3 行业成功案例

公司产品与服务广泛应用于多个行业：

金融：网上银行、手机银行、二代征信、数字人民币系统等；

交通：ETC 密钥系统、联网收费、智慧停车、港口管理系统等；

烟草：资金管理、营销系统、物流可视化平台等；

集团企业：司库系统、财企互联、办公系统等；

运营商：CBSS、BOSS 系统、IT 云平台等；

工控：车联网认证、水库监测数据采集等；

其他：包括政务云密码资源池等重要案例。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203112157113B7K62
生成时间：2025年12月03日 11:21:57

扫一扫
核验码

公共信用信息概览

北京信安世纪科技股份有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	911101086003810384	法定代表人/负责人/执行事务合伙人	李伟
企业类型	股份有限公司(上市、自然人投资或控股)	成立日期	2001-08-31
住所	北京市海淀区建枫路(南延)6号院2号楼1层101		

海关注册登记信息

所在地海关	京中关村	备案日期	2009-08-21
经营类别	——	海关注销标志	正常

信用信息概要

行政管理	2条	诚实守信	4条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

3. 中国科学院沈阳计算技术研究所有限公司

3.1 单位基本情况

中国科学院沈阳计算技术研究所有限公司（简称沈阳计算）始建于1958年，原为中国科学院沈阳计算技术研究所，2001年整体转制为高新技术企业。公司以数字化、信息化和智能化技术为主要研发方向，以技术、产品和服务创新及规模产业化为发展目标，重点面向能源行业、智能制造产业和特种业务领域，提供综合解决方案及专业化服务，助力信息化和工业化的两化深度融合，推动行业技术进步和产业升级，赋能未来。

沈阳计算所拥有多个国家级和省级技术创新平台。紧密围绕国家重大战略与产业升级需求，先后承担01、04、07国家科技重大专项，国家重点研发计划等国家级重大科研项目50余项，突破多项制约产业发展的关键技术，形成一系列国内领先的技术产品。先后获得国家、中国科学院、部委及地方奖励100余项，包括国家科学技术进步奖二等奖、中国标准创新贡献奖一等奖等。取得专利200余项，获得计算机软件著作权130余项，编制国际和国家标准40余项。

3.2 商用密码产品（服务）解决方案情况

中国科学院沈阳计算在通信领域，面向工业互联网、移动通信网络等场景，提供密码应用方案，涵盖身份认证、数据传输加密与密钥管理等服务，保障通信安全合规，已在多个行业专网中成功部署应用。

3.3 行业成功案例

通信领域：面向工业互联网、移动通信网络等场景下，提供传输过程中密码应用方案。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203100344726646GW
生成时间：2025年12月03日 10:03:44

扫一扫
核验码

公共信用信息概览

中国科学院沈阳计算技术研究所有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210112817787266M	法定代表人/负责人/执行事务合伙人	聂林
企业类型	其他有限责任公司	成立日期	2001-06-25
住所	沈阳市东陵区南屏东路16号		

海关注册登记信息

所在地海关	浑南海关	备案日期	2003-07-02
经营类别	——	海关注销标志	正常

信用信息概要

行政管理	3条	诚实守信	4条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

4. 中国科学院沈阳自动化研究所

4.1 单位基本情况

中国科学院沈阳自动化研究所成立于 1958 年，注册地址南塔所区位于辽宁省沈阳市沈河区南塔街 114 号，浑南所区位于辽宁省沈阳市浑南区创新路 135 号，是中国科学院直属事业单位，开办资金 11170 万元人民币。研究所拥有正式员工 1400 余人，其中中国工程院院士 3 人，具有高级职称的技术人员 600 多人。

牵头制定工业无线网络国家推荐标准（如 GB/T 26790）。

技术实力，累计获得 60 项相关专利及 6 项软件著作权，技术成果应用于国防、航空等关键领域。

4.2 商用密码产品（服务）解决方案情况

工业无线国密安全解决方案

主要解决工业无线网络数据传输机密性（防窃听）与完整性（防篡改），设备非法接入与伪基站攻击和传统国际算法依赖导致的供应链安全风险。采用 SM2 数字证书双向认证、SM4 空口加密、SM3 完整性校验，支持 AGV 小车、量具、工具类设备在高动态场景下的毫秒级漫游切换。

应用场景：智能制造车间、军工生产设施（如航天、核工业领域）。

4.3 行业成功案例

为省内某军工单位部署高安全工业无线网络，解决 AGV 搬运车、量具量仪等移动设备的安全接入问题。通过国密算法实现设备与控制系统的双向认证与数据加密传输，保障生产指令与参数配置的机密性、完整性。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203112621446991U2
生成时间：2025年12月03日 11:26:21

扫一扫
核验码

公共信用信息概览

中国科学院沈阳自动化研究所

登记注册基本信息

基础信息

统一社会信用代码	12100000400012449R	法定代表人	史泽林
举办单位	中国科学院	审批机关	国家事业单位登记管理局
地址	辽宁省沈阳市沈河区南塔街114号		

信用信息概要

行政管理	32条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

报告说明

5. 大连秘阵科技有限公司

5.1 单位基本情况

公司成立于2015年11月，位于大连高新技术产业园区，为民营企业，注册资本555万元。现有员工17人，其中研发人员15人。公司为高新技术企业，技术成果包括3项国家发明专利、4项国际发明专利、2项外观设计专利及40余项软件著作权。

5.2 商用密码产品（服务）解决方案情况

（1）秘盾密码安全令牌：采用图形化掩码技术对OTP动态口令进行二次保护，避免明文口令被窃取或盗用，提升身份鉴别安全性。产品包含嵌入式软件端与管理系统端，可与堡垒机、VPN等密码设备对接。

（2）秘阵认证管理系统：面向政务等领域B/S架构业务系统，依托国密浏览器实现客户端身份鉴别，无需外接硬件介质，满足密评合规要求。该系统部署便捷，有效降低采购成本与改造难度。

5.3 行业成功案例

1. 市和区县级大数据中心：信创政务云密码资源池建设方案
2. 金融行业：股份制银行，城商行，农商银行
3. 政务信息系统（B/S架构）合规性改造
4. 与堡垒机，SSL-VPN等密码设备的对接使用
5. 与IAM统一身份认证平台的对接使用，实现“等保&密评”双合规的密码级双因子认证。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203105101863324F97
生成时间：2025年12月03日 10:51:01

扫一扫
核验码

公共信用信息概览

大连秘阵科技有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210231MA0QC9B86L	法定代表人/负责人/执行事务合伙人	孙冠桦
企业类型	有限责任公司(自然人投资或控股)	成立日期	2015-11-03
住所	辽宁省大连高新技术产业园区火炬路1号创业园A座3-8、9室		

海关注册登记信息

所在地海关	七贤岭海关	备案日期	2022-05-13
经营类别	——	海关注销标志	正常

信用信息概要

行政管理	11条	诚实守信	1条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

6. 辽宁公信安全信息科技有限公司

6.1 单位基本情况

辽宁公信安全信息科技有限公司成立于2019年6月，注册及办公地址在辽宁省沈阳市浑南区，单位性质为民营企业，注册资本500万元，公司员工总数22人，研发团队占比45%。

公司是国家级高新技术企业、辽宁省商密协会理事单位、沈阳市高企协会理事单位。已通过“ISO9001质量体系认证”及“ISO27001信息安全体系认证”。

公司拥有商用密码产品认证证书5项，软件著作权25项。

6.2 商用密码产品（服务）解决方案情况

公司自主研发：签名验签服务器、时间戳服务器、密钥协同平台、电子签章服务器、手写签名服务平台在内的多款商用密码产品。

公司的主要业务方向在医疗领域，其中《医疗机构电子签名服务解决方案》为医疗机构构建了统一的数字证书发放与服务机制，方便医疗机构内数字证书发放和应用；同时为医疗机构证书用户提供了高效、便捷的数字证书全生命周期服务，实现了医护人员统一的身份认证服务、电子签名服务、可视化电子签章服务、可信时间戳服务、移动端电子签名服务、患者端手写签名服务、证书自助管理服务、证据保全服务。保证诊疗过程中的身份可信、数据可信、行为可信、时间可信；可追溯、防抵赖，最大限度的保障医患双方的合法权益。实现医疗机构业务全程数字化，提高工作效率，最大程度避免医疗风险。

6.3 行业成功案例

辽宁省卫健委直属三甲级医疗机构2家，医科大学系三甲级医疗机构2家及各级卫健委平台项目3个。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203101127500042 9H
生成时间：2025年12月03日 10:11:27

扫一扫
核验码

公共信用信息概览

辽宁公信安全信息科技有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210112MA0YQUK84L	法定代表人/负责人/执行事务合伙人	许耸石
企业类型	其他有限责任公司	成立日期	2019-06-24
住所	辽宁省沈阳市浑南区天赐街7-3号1104-1109		

信用信息概要

行政管理	1条	诚实守信	3条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

7. 沈阳安创信息科技有限公司

7.1 单位基本情况

公司成立于 2011 年，注册及办公地址：辽宁省沈阳市皇姑区怒江街 91 号(沈阳数创工场 6 楼 601),民营企业,注册资本为:494.4852 万元人民币，员工总数为 12 人，研发团队占比 67%。单位属于国家高新技术企业，截至目前拥有 1 项发明专利，3 项实用新型专利，65 项软件著作权。

7.2 商用密码产品（服务）解决方案情况

跨境电商平台通过防伪技术实现商品全流程透明化，既是应对假货问题的必要手段，也是提升消费者信任、优化供应链管理的战略选择。通过 S2i 码技术与国密算法的有效融合可有效解决商用防伪和溯源问题：

1. 安全性分析:S2i 独有的编码技术在加密层结合国密算法 SM4，实现了“双重安全+真实性+完整性”三位一体，在确保商品标识本身全球唯一性的同时，也保证了该唯一标识的生成过程安全、传输存储可靠和使用验证可信。

2. 经济性考虑:在制作成本方面,S2i 码利用现有印刷设备即可，无需增加其他工艺和材料；在品牌声誉方面，可有效防止买真退假、真假混卖，减少假货投诉；平台商家也无需投入更多资源来应对知识产权保护与打假问题，降低了运营成本。

3. 便利性分析：用户无需专业设备，通过国密认证 App 扫码即可验货，提升了商品安全性。同时也有助于监管部门维护营商环境和市场秩序。

7.3 行业成功案例

优势行业：跨境电商、母婴行业、食品、医药保健品、农产品和文档证件等。

已完成项目：韩国化妆品跨境电商防伪溯源监管系统、ABC 卫生巾防伪打假解决方案、医疗保健品 IP 授权系统、政府部门工作人员证件、GA/CSP 统一认证标识等。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203112520203I0Q50
生成时间：2025年12月03日 11:25:20

扫一扫
核验码

公共信用信息概览

沈阳安创信息科技有限公司

存续

登记注册基本信息

基础信息

统一社会信用代码	912101055783626492	法定代表人/负责人/执行事务合伙人	孙宏宇
企业类型	其他有限责任公司	成立日期	2011-07-14
住所	辽宁省沈阳市皇姑区怒江街91号（沈阳数创工场6楼601）		

信用信息概要

行政管理	2条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	1条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

8. 长春吉大正元股份有限公司

8.1 单位基本情况

长春吉大正元信息技术股份有限公司、成立于 1999 年 2 月、省内办公地址（辽宁省、沈阳市皇姑区北陵大街平安财富中心 21 层）、注册资本 1.93 亿元、现有员工 800 余人，研发团队占比 32%。

公司为国家 863 计划成果产业化基地、国家火炬计划软件产业基地骨干企业、中国密码学会理事单位等，曾获国家科技进步奖二等奖、密码科学技术进步奖一等奖等多项荣誉。累计获得 300+项相关专利及 410+项软件著作权，参与编写国家及行业标准 50+，国家级重点项目 25 个。

8.2 商用密码产品（服务）解决方案情况

公司产品涵盖数字签名类产品 10 余款，身份鉴别产品 30 余款，密码基础产品 10 余款、数据安全类产品 3 款、通信及网络安全 3 款、物联网安全 7 款，满足金融、工业、政府、医疗、教育、电信、能源、军队、军工等行业应用。典型案例包括：

（1）政务云密码资源池：解决政务云的集约化建设需求，满足密评的合规性要求，实现密码资源的统一管理和统一标准。

（2）“车路云一体化”安全方案：基于国产密码技术，保障车、路、云三者间的身份认证与通信安全，防范车辆控制破解、数据篡改等风险。

8.3 行业成功案例

（1）某省政务云平台：对政务云平台租户构建统一密码服务管理平台满足本省全网应用接入总数:499 个、全网服务总量:17047993、全网密码设备管理总数：295 台、日均提供密码服务次数：日均 26 万，实现全省的政务应用成功通过商用密码测评。

（2）某汽车企业车联网平台：实现车辆、云端与路侧设备间的安全认证与通信，每日满足下线车辆 11000 余台签证，云端日均访问鉴别量 230000 多次。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203120319076998 7Y
生成时间：2025年12月03日 12:03:19

扫一扫
核验码

公共信用信息概览

长春吉大正元信息技术股份有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91220000702580185D	法定代表人/负责人/执行事务合伙人	于逢良
企业类型	其他股份有限公司(上市)	成立日期	1999-02-12
住所	长春市高新区光谷大街1300号19层-22层		

信用信息概要

行政管理	20条	诚实守信	9条
严重失信	0条	经营异常	0条
信用承诺	10条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

9. 辽宁航天信息有限公司

9.1 单位基本情况

由中国航天科工集团发起设立的高新技术企业，成立于 2004 年，注册办公地址：沈阳市和平区。国有企业。注册资本：1000 万元，公司员工总数：468 人，研发团队占比 43%。

基于密码技术研究成果，已获得发明授权专利 200 余项，软件作权百余项，参与多项国家、行业及团体标准编制。

9.2 商用密码产品解决方案情况

自主研发电子签章、签名验签服务器、服务器密码机、协同签名、数字证书、密钥管理、数据库透明加密等。

政务：为政府部门提供政务系统密码改造方案、政务云平台安全建设方案，具备多级政务云平台安全建设能力。

税务：为税务部门提供密码安全解决方案，包括自助办税终端建设方案，电子税务局、征收管理系统等金税三期密码改造方案。

医疗：提供医用签电子认证服务方案、电子病历应用安全解决方案，提供便捷的电子签署服务。

9.3 行业成功案例

（1）省级一体化数据平台密码解决方案

截至 2025 年上半年，平台已经为某省内 30 余家单位近 200 多个业务应用提供服务，累计提供各类密码服务 30 亿次。

（2）医疗领域密码应用方案

电子医疗文档通过数字证书、电子签章、时间戳固化，可溯源，防止事后换页、篡改条款。无纸化办公，降低院感风险；符合“互联网+医疗健康”政策，保障医疗信息系统通过密码应用安全性评估。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203101233378670Q69
生成时间：2025年12月03日 10:12:33

扫一扫
核验码

公共信用信息概览

辽宁航天信息有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	91210100760093684 8	法定代表人/负责人/执行事务合伙人	王涛
企业类型	其他有限责任公司	成立日期	2004-06-25
住所	辽宁省沈阳市和平区市府大路200号14层		

信用信息概要

行政管理	7条	诚实守信	10条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

10. 沈阳问天量子科技有限公司

10.1 单位基本情况

沈阳问天量子科技有限公司是安徽问天量子股份有限公司的全资子公司，成立于2019年7月，注册资本1000万元，公司地址为：沈阳市大东区滂江街22号，民营企业，现有员工25人，其中研发人员20人，比例为80%。

公司现已建成沈阳市量子产业技术研究院（有限公司）、院士工作站、辽宁大学量子信息前沿技术创新研究院等。拥有点对点量子密码通信技术、 量子密码通信组网技术、量子密码通信核心器件等多项国际和国内专利，获得专利10余项，软件著作权9项。2022年获批“沈阳市科普基地”、2023年获批辽宁省高等学校研究生校外教育基地、2024年获批“沈阳市量子信息产业联盟”。

10.2 商用密码产品解决方案情况

量子政府专网方案：

2019年在沈阳建设了东北地区首条量子安全政务外网测试线路。目前正在开展“一网、一中心、一平台、多场景”的量子信息安全体系。即：量子QKD通讯网、量子CA中心、量子云控平台；多量子应用场景。

量子工业区块链方案：

通过引入量子联盟链、大数据、知识图谱、安全联动机制及自主研发的核心安全技术，构建一套实时监控、智能预测、安全协同的工业互联网企业级安全监测与态势感知平台。

10.3 行业成功案例

公司为边防、金融、工业、电力、军工等行业提供量子通信安全专网建设、量子密钥分发服务及抗量子计算技术解决方案，并进一步提供 5G+PQC 融合技术支撑。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251205134722913SP683
生成时间：2025年12月05日 13:47:22

扫一扫
核验码

公共信用信息概览

沈阳问天量子科技有限公司

存续

登记注册基本信息

基础信息

统一社会信用代码	91210114MA0YTJCM4M	法定代表人/负责人/执行事务合伙人	殷海峰
企业类型	其他有限责任公司	成立日期	2019-07-29
住所	辽宁省沈阳市大东区滂江街22号45-91室		

信用信息概要

行政管理	3条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	2条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月05日	报告出具单位	国家公共信用和地理空间信息中心

（五）密码与信创企业

1. 华为技术有限公司

1.1 单位基本情况

华为技术有限公司成立于 1987 年，是全球领先的 ICT 基础设施和智能终端提供商，为民营企业，注册资本约 410 亿元。截至 2024 年底，公司拥有员工 20.8 万人，其中研发人员占比 54%，业务覆盖 170 多个国家和地区。华为坚持高强度研发投入，2024 年研发投入达 1797 亿元，近十年累计投入超 1.24 万亿元。公司在全球持有有效授权专利超过 15 万件。华为辽宁区域总部位于沈阳市浑南区，全面服务辽宁各行业数字化转型。

华为具有高新技术企业、国家技术创新示范企业、国家知识产权示范企业、国家科学技术进步奖、国家技术发明奖等企业资质；同时具有信息安全管理体系认证、网络安全框架管理体系认证、隐私信息管理体系认证等安全及隐私相关认证资质。

1.2 商用密码产品（服务）解决方案情况

华为在商用密码领域聚焦基础设施层，提供基于自研鲲鹏系列 CPU 芯片的信创服务器及解决方案。鲲鹏 920 处理器获国密芯片一级证书，具备完整自主知识产权，支持国密算法硬件加速。核心方案包括：

（1）鲲鹏商密应用密码模块：基于 TrustZone 机密计算套件，提供标准 SDF 接口，支持加解密、签名验签及密钥管理功能，适用于 SSL 网关、电子签章等场景，助力客户满足等保、密评要求。具备原生集成、软件定义、高性能并发等优势。

（2）Boostkit TrustZone 机密计算套件：基于高安全微内核操作系统构建 TEE 环境，通过 CC EAL 4+整体认证及 EAL 6+内核认证，支持云原生、密态计算等场景，具备灵活配置、稳定可靠的特点。

1.3 行业成功案例

（1）政企行业案例：面向政务电子印章场景，基于鲲鹏技术构建内生密码模块，满足政务场景下的电子印章安全管理和行政审批无纸化需求；面向隐私计算与数据安全场景，鲲鹏硬件结合 BoostKit 机密计算套件，为隐私计算、数据保全等场景提供高性能密码算力。

（2）金融行业案例：基于鲲鹏 TEE 的内生国密方案，商用对接人脸识别、云平台等业务应用，实现海量金融互联网应用的敏捷上线，降低传统密码设备对接的工作量；在银行用户实名身份认证场景下，通过鲲鹏内生密码模块支撑合规二级密码模块，实现安全高效的实名认证。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203110453584022Q2
生成时间：2025年12月03日 11:04:53

扫一扫
核验码

公共信用信息概览

华为技术有限公司

存续　守信激励对象

登记注册基本信息

基础信息

统一社会信用代码	914403001922038216	法定代表人/负责人/执行事务合伙人	赵明路
企业类型	有限责任公司(自然人投资或控股的法人独资)	成立日期	1987-09-15
住所	深圳市龙岗区坂田华为总部办公楼		

海关注册登记信息

所在地海关	沿中海关	备案日期	2008-04-11
经营类别	——	海关注销标志	正常

信用信息概要

行政管理	1,442条	诚实守信	10条
严重失信	0条	经营异常	0条
信用承诺	29条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

2. 龙芯中科技术股份有限公司

2.1 单位基本情况

龙芯中科面向国家信息化建设需求，面向国际信息技术前沿，以创新发展为主题、以产业发展为主线、以体系建设为目标，坚持自主创新，全面掌握 CPU 指令系统、处理器 IP 核、操作系统等计算机核心技术，打造自主开放的软硬件生态和信息产业体系，为国家战略需求提供自主、安全、可靠的处理器，为信息产业的创新发展提供高性能、低成本的处理器和基础软硬件解决方案。

龙芯中科主营业务为处理器及配套芯片的研制、销售及服务，主要产品与服务包括处理器及配套芯片产品与基础软硬件解决方案业务。目前，龙芯中科基于信息系统和工控系统两条主线开展产业生态建设，面向网络安全、办公与业务信息化、工控及物联网等领域与合作伙伴保持全面的市场合作，系列产品在电子政务、能源、交通、金融、电信、教育等行业领域已获得广泛应用。

2001 年，中国科学院计算技术研究所开始研制龙芯处理器，得到了中国科学院知识创新工程、863、973、核高基等项目大力支持，完成了十年的技术积累。2010 年，在中科算源和北京市政府共同牵头出资支持下，龙芯开始市场化运作，对龙芯处理器研发成果进行产业化。

2.2 商用密码产品（服务）解决方案情况

依托处理器内置的安全 SE 模块，提供的可信计算能力，可保障产品自身的安全可信。融合通用计算技术、密码运算和可信计算技术，广泛应用于电子政务、金融、能源、交通、通信等重要领域，赋能关键信息基础设施和新基建网络安全保障能力建设。

2.3 行业成功案例

在党的二十大报告中提及的十大科技成果中，多项成果采用了龙芯 CPU。2020 年 1 月—2023 年 12 月底，采用龙芯 CPU 技术路线的整机产品（含桌面端和服务器）数量在各 CPU 技术路线中排名前两位。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203100938944471 7M
生成时间：2025年12月03日 10:09:38

扫一扫
核验码

公共信用信息概览

龙芯中科(辽宁)技术有限公司

存续

登记注册基本信息

基础信息

统一社会信用代码	91211500MA7BQPHWXD	法定代表人/负责人/执行事务合伙人	张戈
企业类型	有限责任公司（非自然人投资或控股的法人独资）	成立日期	2021-11-10
住所	辽宁省沈抚示范区金枫街75-1号0306		

信用信息概要

行政管理	2条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

3. 曙光信息产业股份有限公司

3.1 单位基本情况

曙光信息产业股份有限公司（中科曙光）是在中国科学院推动下，基于国家“863”计划成果组建的国家高新技术企业，于 2014 年在上海证券交易所上市。公司主营高效能计算机、服务器、存储产品及系统集成服务。2009 年在辽宁盘锦设立全资子公司，具备年产 20 万台信创高效能计算机及安全产品能力，拥有服务器密码安全相关专利 32 项。公司为商用密码产品生产定点单位，持有相关产销及密评资质，其天津政务云平台已通过商用密码应用安全性评估三级认证。

3.2 商用密码产品（服务）解决方案情况

中科曙光商用密码产品全面支持国密算法（SM2/SM3/SM4 等），通过自研处理器实现 CPU 指令集级国密加速，性能较软件方案提升约 3 倍。产品具备身份鉴别、数据传输加密、链路保护、密钥管理等完整密码功能，满足高安全场景需求，已在政务云、工业控制等领域实现规模化应用。

3.3 行业成功案例

（1）政务云平台：天津政务云平台通过密评三级认证，为云上系统提供身份认证、数据传输与存储加密等全流程密码服务。

（2）工业控制领域：全系列工控产品内置国密算法自研处理器，支持网络隐匿、零信任认证与数据加密，保障工业系统全域安全。

（3）其他领域：产品亦服务于金融、通信、能源等行业，为用户提供合规、可靠的密码应用支撑。

信用中国
WWW.CREDITCHINA.GOV.CN

报告编号：20251203104031276A6943
生成时间：2025年12月03日 10:40:31

扫一扫
核验码

公共信用信息概览

中科曙光信息产业(北京)有限公司

存续

登记注册基本信息

基础信息

统一社会信用代码	91110302MA01RP6W3G	法定代表人/负责人/执行事务合伙人	白俊雪
企业类型	有限责任公司(自然人投资或控股的法人独资)	成立日期	2020-06-03
住所	北京市北京经济技术开发区科谷一街10号院11号楼1702		

信用信息概要

行政管理	2条	诚实守信	0条
严重失信	0条	经营异常	0条
信用承诺	0条	信用评价	0条
司法判决	0条	其他	0条

报告生成日期	2025年12月03日	报告出具单位	国家公共信用和地理空间信息中心

第九章 附录 密码基础知识

（一）商用密码技术基础

1. 商用密码定义与概述

1.1 商用密码的定义

依据《密码法》，商用密码是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。它是保障公民、法人和其他组织在经济社会活动中信息安全的重要工具，通过加密算法、密钥管理、密码协议等多种技术手段，将原始信息转化为密文形式，使得未经授权者难以获取信息内容，同时在需要验证信息来源和完整性时，提供可靠的安全认证机制。例如在电子商务交易中，商用密码技术可对用户的账号密码、交易金额、商品信息等进行加密传输和存储，确保交易数据不被窃取、篡改，保障交易双方的合法权益。

1.2 商用密码的作用与意义

在当今数字化时代，商用密码的作用举足轻重。从保障信息安全层面来看，它能有效防止信息泄露、篡改与伪造，为各类信息系统筑牢安全防线。在金融行业，客户的账户资金信息、交易记录等通过商用密码加密保护，确保了金融交易的安全可靠，维护了金融秩序的稳定。在政务领域，商用密码助力政府部门实现公文传输、政务数据共享，提升政务工作的保密性和公信力。

从促进数字经济发展角度而言，商用密码是数字经济运行的安全基石，它增强了企业和用户对数字业务的信任度，推动了电子商务、电子支付、数字政务等新兴业态的蓬勃发展。以电子合同签署为例，商用密码的数字签名技术确保了合同的法律效力和不可抵赖性，使得线上商业合作更加便捷高效，降低了交易成本，激发了市场活力。

此外，商用密码在维护国家安全和社会公共利益方面也发挥着重要作用，它提升了国家关键信息基础设施的安全防护能力，有效抵御外部网络攻击和信息窃取，为国家经济社会的稳定发展提供了坚实保障。

1.3 商用密码与其他密码的区别

根据《密码法》，我国密码分为核心密码、普通密码和商用密码三类，它们在应用领域和管理方式上存在显著差异。

核心密码用于保护国家秘密信息，所保护信息的最高密级为绝密级，其设计、生产、使用等环节均由国家密码管理部门实行最严格的监督管理。主要应用于国防、外交、情报等涉及国家安全的关键领域，旨在维护国家核心利益不受威胁，如军事指挥系统、国家情报通信网络等。

普通密码用于保护不属于国家秘密但又需要较高安全性的信息，保护信息的

最高密级为机密级，通常应用于政府机关内部通信、敏感业务数据传输等场景，由国家密码管理部门进行统一管理，在保障信息安全的同时，兼顾一定的业务便利性和信息共享需求。

而商用密码主要用于保护公民、法人和其他组织的非涉密信息，广泛应用于金融、通信、电商、医疗、教育等市场经济活动领域，以满足各类商业主体和个人对信息安全的需求。在管理方式上，商用密码实行产品自主检测认证制度，鼓励市场主体依法开展商用密码相关业务，在遵循国家相关标准和规范的前提下，市场调节作用更为明显，旨在激发市场活力，促进商用密码产业的创新发展。

2. 商用密码核心技术解析

2.1 密码算法基础

（1）SM1：对称密码算法（硬件专用，算法不公开）

核心结论：我国设计的硬件专属对称加密算法，算法细节不对外公开，仅通过芯片等硬件实现，安全性依赖硬件防护。

核心功能：与 SM4 类似，用于数据加密和解密，采用分组密码体制。

技术特点：密钥长度 128 位，安全性高，算法不公开可避免软件层面的攻击，仅能通过指定硬件芯片（如国密安全芯片）调用。

典型应用：金融 IC 卡、社保卡、身份证芯片、加密狗、硬件加密模块（HSM）等需要高安全级别的硬件设备。

核心区别：与 SM4（算法公开、软硬件均可实现）不同，SM1 完全依赖硬件，无法通过软件独立实现，适合对安全性要求极高的场景。

（2）SM2：椭圆曲线公钥密码算法（非对称）

核心结论：替代 RSA 的国密非对称算法，基于椭圆曲线原理，密钥短、效率高，是身份认证、数字签名的核心标准。

核心功能：支持数据加密、数字签名、密钥协商三大核心能力。

技术优势：256 位密钥安全性等价于 RSA 2048 位，计算速度更快，存储和传输成本更低。

典型应用：电子合同签署、国密 SSL 证书、政务系统身份认证、金融交易密钥协商。

替代对象：国际算法 RSA、ECC，是我国非对称加密的主流选择。

（3）SM3：密码杂凑算法（哈希摘要）

核心结论：替代 SHA-256 的国密哈希算法，生成固定长度摘要，不可逆、抗篡改，是数据完整性验证的基础。

核心功能：将任意长度数据转化为 256 位（32 字节）固定摘要，无法从摘要反推原数据。

技术优势：抗碰撞性强，运算效率高，适配各类数据校验场景。

典型应用：用户密码存储（存储摘要而非明文）、文件完整性校验、SM2 数字签名的摘要生成。

替代对象：国际算法 SHA-256、MD5（MD5 已淘汰），是国密体系中哈希摘要的强制标准。

（4）SM4：分组密码算法（通用对称加密）

核心结论：替代 AES 的国密通用对称算法，加密解密用同一密钥，速度快、适配广，适合海量数据加密。

核心功能：对 128 位数据块加密，支持 ECB、CBC 等多种工作模式，软硬件均可实现。

技术优势：128 位密钥安全性等价于 AES-128，运算效率与 AES 相当，适配各类通用场景。

典型应用：VPN 加密、Wi-Fi 国密认证（WPA3-CCMP-256）、硬盘存储加密、数据库敏感字段加密。

替代对象：国际算法 AES，是国密体系中通用对称加密的核心算法。

（5）SM7：对称密码算法（RFID 标签专用）

核心结论：针对 RFID/NFC 等低功耗标签设计的对称算法，适配小容量存储、低算力硬件场景。

核心功能：用于标签与读写器的短距离通信加密，实现标签身份认证和数据防篡改。

技术优势：128 位密钥，算法结构简洁，运算量小，适合低功耗设备。

典型应用：门禁卡、支付 NFC 卡、物流追溯标签、工业物联网传感器标签。

适用场景：专门针对“低功耗、小存储”硬件，区别于 SM4 的通用海量数据加密场景。

（6）SM9：标识密码算法（无证书非对称加密）

核心结论：无需提前交换公钥的国密标识算法，用户标识（手机号、邮箱）作为“公钥”，适配物联网、分布式场景。

核心功能：基于身份的加密（IBE）和签名，省去公钥证书（PKI）的管理成本。

技术优势：密钥分发简单，适配海量设备接入，降低系统部署复杂度。

典型应用：物联网设备通信加密、邮件加密（用邮箱作为标识）、政务大数据平台身份认证。

替代对象：传统 PKI 体系（RSA+证书），解决公钥管理繁琐的问题。

核心算法对比表

算法	类型	核心特点	核心应用场景
SM1	对称加密（硬件专用）	算法不公开、依赖硬件	金融 IC 卡、身份证芯片、加密狗
SM2	非对称加密（椭圆曲线）	密钥短、效率高	电子签名、身份认证、密钥协商
SM3	哈希摘要	不可逆、抗篡改	密码存储、数据完整性校验
SM4	对称加密（通用）	速度快、软硬件适配广	VPN、存储加密、数据库加密
SM7	对称加密（标签专用）	低功耗、小算力	RFID/NFC 标签、门禁卡
SM9	非对称加密（标识）	无证书、易管理	物联网、分布式身份认证

这些算法覆盖了从硬件安全、通用加密到物联网专用的全场景，是我国商用密码的核心支撑。

2.2 密钥管理技术

密钥管理涵盖密钥生成、存储、分发、更新和销毁等多个关键环节。

密钥生成：需采用安全的随机数生成器和特定的算法，确保生成的密钥具有足够的随机性和不可预测性，以增强加密的安全性，例如使用伪随机数发生器结合密码学算法生成高强度的密钥。

密钥存储：至关重要，通常采用硬件安全模块（HSM）、加密文件系统等方式，将密钥安全地保存起来，防止被非法获取，在银行的密钥管理系统中，通过 HSM 来存储核心密钥，利用其物理防护和加密机制，保障密钥的安全。

密钥分发：将密钥安全地传送给合法的使用者，可采用安全的通信协议（如 SSL/TLS）、密钥分发中心（KDC）等技术手段，确保分发过程不被窃听和篡改，在企业网络中，通过 KDC 为不同部门的用户分发加密通信所需的会话密钥。

密钥更新：随着时间推移或安全事件发生，需要对密钥进行更新，以降低密钥被破解的风险，定期更换密钥，或者在检测到密钥可能泄露时及时更新。

密钥销毁：当密钥不再使用时，要进行彻底的销毁，防止密钥被恶意利用，通过多次覆盖、擦除等方式确保密钥无法恢复。

完善的密钥管理技术是保障商用密码安全性和有效性的核心，直接关系到信息系统的整体安全。

2.3 密码协议与机制

身份认证机制：是密码协议的重要组成部分，通过多种方式确认用户或设备的真实身份。常见的有基于密码的认证方式，用户输入预先设置的密码进行身份验证，但这种方式安全性相对较低。多因素身份认证则结合多种因素，如用户名密码、数字证书、短信验证码、生物特征识别（指纹、人脸识别等）等，极大地增强了身份认证的安全性，在网上银行登录时，除了密码，还需通过手机短信验证码或指纹识别进行二次认证，有效防止账号被盗用。

数据加密协议：用于将明文数据转换为密文，以确保数据在传输和存储过程中的保密性。在网络通信中，采用 SSL/TLS 协议，通过协商加密算法和密钥，对传输的数据进行加密，防止数据被第三方窃取。

数字签名机制：利用非对称加密算法，实现对消息来源和完整性的验证。发送方使用私钥对消息摘要进行签名，接收方使用发送方的公钥验证签名，如果验证通过，则可确认消息未被篡改且确实来自发送方，在电子合同签署中，数字签名确保了合同内容的真实性和不可抵赖性，保障了合同双方的合法权益。

这些密码协议和机制相互协作，为信息系统提供了身份识别、数据保密、完整性验证等全方位的安全服务。

（二）重点场景领域的商用密码技术应用

1. 工业企业的商用密码应用

1.1 工业网络与数据安全需求

当前，工业企业面临着日益严峻的网络和数据安全威胁。随着工业互联网的发展，工业企业的生产系统与外部网络的连接更加紧密，勒索软件攻击、数据泄露等安全事件频发。根据 Zscaler 安全威胁实验室发布的《2023 年全球勒索软件报告》，截至 2023 年 10 月，全球勒索软件攻击的数量同比增长了 37.75%，我国工业企业同样面临着巨大的安全风险。

工业企业的生产数据，如工艺流程数据、设备运行参数等，一旦被窃取或篡改，可能导致生产中断、产品质量下降，甚至引发安全事故。某汽车制造企业曾遭受勒索软件攻击，导致生产线被迫停产数天，造成了巨大的经济损失。

在这种背景下，工业企业对商用密码技术的需求极为迫切，希望通过商用密

码保障网络通信的安全，防止数据在传输过程中被窃听、篡改；对重要数据进行加密存储，确保数据的机密性和完整性，提升工业控制系统的整体安全性。

1.2 智慧工厂场景下的密码应用方案

以智慧工厂为例，在用户身份鉴别方面，通过身份认证网关与各应用系统集成，实现内部人员访问时的身份鉴定与权限管理。覆盖工厂中的各个服务、车间中的各个节点，并与密码服务平台的用户身份认证集成，对访问用户的身份进行严格鉴定和权限控制，只有经过身份认证的人员才能访问相应的内部资源。同时，提供证书自助服务，允许用户、终端等实体在线自助进行数字证书的申请、更新、解锁等操作，方便用户管理自身身份凭证。

在数据传输环节，采用 SSL/TLS 协议结合商用密码算法，对生产数据在车间内部网络、企业内部网络以及与外部合作伙伴网络之间的传输进行加密，确保数据在传输过程中的安全性。

在数据存储方面，利用 SM4 等加密算法对重要生产数据进行加密存储，无论是存储在本地服务器还是云端存储平台，都能有效防止数据泄露。

对于设备之间的通信，也通过商用密码技术建立安全通道，确保设备控制指令和运行状态数据的安全传输，保障智慧工厂生产系统的稳定运行。

1.3 应用成效与未来发展方向

商用密码在工业企业的应用取得了显著成效，有效提升了工业企业网络和数据的安全性，降低了安全事件发生的概率。通过身份认证和权限管理，减少了内部人员违规操作和外部非法入侵的风险；数据加密保障了生产数据的机密性和完整性，确保了生产的连续性和稳定性，提高了企业的生产效率和经济效益。

未来，随着工业互联网的进一步发展，工业企业对商用密码的需求将不断增长，应用场景也将更加丰富。一方面，将加强对工业物联网终端设备的密码应用，实现设备的身份认证和数据加密，保障海量物联网设备的安全接入和数据交互。另一方面，探索在工业大数据分析、供应链协同等场景中的商用密码应用，解决数据共享和隐私保护的难题，促进工业企业数字化转型和产业生态的协同发展，推动工业领域的数据安全治理水平不断提升。

2. 智慧城市中的商用密码应用

2.1 物联网场景通信安全保障

在智慧城市中，大量设备需要接入网络进行数据交互，商用密码在设备接入认证和通信传输加密方面发挥着关键作用。在智能交通领域，交通摄像头、智能路灯、车载终端等设备接入城市物联网时，通过数字证书和身份认证技术，利用商用密码算法对设备身份进行验证，确保只有合法设备能够接入网络，防止非法设备接入导致的安全隐患。

在通信传输过程中，采用国密 SSL/TLS 协议结合 SM2、SM4 等商用密码算法，对设备与设备之间、设备与管理平台之间的数据传输进行加密，保障交通数据，如车辆行驶轨迹、交通流量信息等在传输过程中的保密性和完整性，防止数据被窃取或篡改，确保智能交通系统的稳定运行。

在城市政务网络中，各部门之间的数据通信同样依赖商用密码保障安全，实现政务信息的安全传输和共享，提升政务工作的协同效率。

2.2 数据全生命周期安全防护

智慧城市中汇聚了海量的数据，包括居民个人信息、城市运行数据等，商用密码贯穿数据全生命周期，保障数据安全。在数据存储阶段，对数据库中的敏感数据，如居民身份证号码、医疗记录等，使用 SM4 等加密算法进行加密存储，防止数据存储介质丢失或被盗时的数据泄漏风险。

在数据使用过程中，通过数字签名和身份认证技术，确保数据使用者的身份合法，并对数据操作进行记录和审计，保证数据使用的合规性和可追溯性。

当城市不同部门或机构之间进行数据共享时，利用商用密码技术对共享数据进行加密和授权管理，只有获得授权的接收方才能解密和使用数据，保障数据共享的安全可控。

同时，在数据完整性保障方面，采用哈希算法（如 SM3）计算数据的哈希值，并与原始哈希值比对，实时监测数据是否被篡改，确保智慧城市数据的真实性和可靠性。

2.3 核心应用场景的密码赋能

在智慧政务场景中，商用密码用于电子公文传输、网上行政审批等业务。电子公文在传输过程中经过数字签名和加密处理，确保公文的真实性、完整性和保密性，接收方通过验证数字签名可以确认公文来源和内容未被篡改，保障政务办公的安全高效。在网上行政审批中，企业和居民通过数字证书进行身份认证，提交的申请材料被加密传输和存储，保护了用户隐私和政务数据安全，提升了政务服务的便捷性和公信力。

在智慧交通中，除了上述网络通信安全保障外，商用密码还应用于电子支付场景，如停车缴费、公交卡充值等。通过加密技术保障支付数据的安全，利用数字签名确保支付交易的不可抵赖性，为城市居民提供安全、便捷的出行支付服务。

在智慧医疗领域，商用密码保障患者病历信息的安全共享和医疗设备之间的数据交互安全，医生通过身份认证访问患者病历，不同医疗机构之间在授权下安全共享患者的检验检查结果等信息，提高医疗服务的质量和效率，保护患者的隐私权益。

（三）基于数据生命周期的商用密码技术场景

数据在全生命周期中面临着诸多安全威胁，商用密码技术贯穿数据采集、传输、存储、使用与共享等各个阶段，为数据提供全方位的安全保障，确保数据的机密性、完整性、可用性、真实性和不可否认性。

1. 数据采集阶段的密码应用

1.1 设备身份认证与数据加密

在物联网环境中，商用密码技术对于设备身份认证和数据加密至关重要。大量的物联网设备如传感器、摄像头等接入网络，面临着设备身份被冒用、数据被窃取或篡改的风险。通过基于 SM2 或 SM9 算法的数字证书机制，为每个物联网设备颁发唯一的数字证书，在设备接入网络时，利用证书进行身份认证，只有通过认证的设备才能与网络进行通信，有效防止非法设备接入。

在数据采集过程中，对采集的数据进行加密处理，采用 SM4 等对称加密算法，对设备采集的原始数据进行加密，确保数据在传输前就处于密文状态，即使数据在传输过程中被截获，没有正确的密钥也无法获取数据内容，保障了数据采集的安全性和可靠性。

1.2 工业数据采集安全场景

以某大型汽车制造企业为例，其生产线上部署了大量的传感器，用于采集设备运行状态、产品生产参数等数据。在未采用商用密码技术之前，数据采集过程中存在较大安全隐患，曾发生过竞争对手通过非法接入设备获取生产数据，试图窃取生产工艺的事件。

为解决这一问题，该企业引入商用密码技术，为每个传感器设备配备基于 SM2 算法的数字证书，实现设备接入认证，只有通过认证的传感器才能将采集的数据上传至生产管理系统。同时，利用 SM4 算法对采集的数据进行加密，在数据传输过程中，即使数据被第三方截取，也无法获取有效信息。

采用商用密码技术后，该企业数据采集的安全性得到显著提升，再未发生过数据被窃取或篡改的事件，保障了企业生产的正常运行和核心生产数据的安全，避免了因数据安全问题导致的生产延误和经济损失，维护了企业的核心竞争力。

2. 数据传输阶段的密码应用

2.1 通信加密与安全通道建立

在数据传输过程中，建立安全通道和进行通信加密是保障数据安全的关键。通过 VPN（虚拟专用网络）技术，利用 IPsec 协议结合商用密码算法，如 SM2、SM4 等，在不同网络节点之间建立加密隧道，实现数据的安全传输。

在企业分支机构与总部之间的数据传输中，通过 IPsec VPN 建立安全通道，

对传输的数据进行加密和完整性校验，防止数据在传输过程中被窃听、篡改或伪造。

在云服务场景中，用户与云平台之间的数据传输，采用 SSL/TLS 协议结合商用密码算法，保障数据传输的机密性和完整性，确保用户数据在传输过程中的安全性。这些技术通过加密通信内容，验证通信双方身份，确保数据在传输过程中的安全性，防止数据泄露和被恶意篡改。

2.2 不同网络环境下的应用策略

在有线网络环境中，虽然网络相对封闭，但仍面临内部人员非法获取数据、网络攻击等风险。可以采用链路加密技术，对网络链路中的数据进行加密，利用 SM4 算法对传输的数据进行逐包加密，保障数据在有线网络传输中的机密性。同时，结合访问控制技术，对网络设备的访问进行身份认证和权限管理，防止非法人员接入网络获取数据。

在无线网络环境下，由于信号易被窃取和干扰，安全风险更高。除了采用 WPA2/WPA3 等无线加密协议结合商用密码算法进行加密外，还可以利用身份认证技术，如 802.1X 协议结合数字证书，对无线接入设备进行身份认证，确保只有合法设备能够接入无线网络。

对于移动设备的数据传输，采用端到端加密技术，利用 SM2 算法进行密钥协商，SM4 算法对数据进行加密，保障移动设备与服务器之间数据传输的安全，适应不同网络环境的特点，采取针对性的商用密码应用策略，有效提升数据传输的安全性。

3. 数据存储阶段的密码应用

3.1 数据库与文件存储加密

在数据库存储方面，商用密码技术发挥着重要作用。对于关系型数据库，可以采用数据库字段加密技术，利用 SM4 算法对数据库中敏感字段，如用户身份证号、银行卡号、密码等进行加密存储，只有授权用户通过解密操作才能查看明文数据，防止数据库被非法访问时敏感数据泄露。也可进行全库加密，对整个数据库文件进行加密，确保数据库文件在存储介质上以密文形式存在，即使存储介质丢失或被盗，没有密钥也无法读取数据内容。

在文件存储加密方面，对于企业重要的文档、设计图纸等文件，利用 SM4 算法进行加密存储，将文件加密后存储在本地硬盘或云存储平台，同时结合密钥管理技术，确保密钥的安全存储和使用，保障文件存储的安全性，防止文件被非法复制和传播。

3.2 数据备份与恢复中的密码保护

在数据备份过程中，商用密码技术用于保障备份数据的安全。采用加密备份

技术，利用 SM4 算法对需要备份的数据进行加密，然后将加密后的备份数据存储在异地备份中心或云端备份平台，防止备份数据在存储过程中被窃取或篡改。

在数据恢复时，只有拥有正确密钥的授权人员才能对备份数据进行解密恢复，确保数据恢复的安全性和准确性。

通过密钥管理系统对备份数据的加密密钥进行安全管理，定期更新密钥，防止密钥泄露导致备份数据安全风险，保障数据备份与恢复过程中的数据安全，确保在数据丢失或损坏时能够安全、可靠地恢复数据。

4. 数据使用与共享阶段的密码应用

4.1 访问控制与权限管理

在数据使用过程中，商用密码技术通过访问控制和权限管理确保数据安全。基于数字证书和身份认证技术，利用 SM2 算法对用户身份进行验证，只有通过身份认证的用户才能访问数据系统。

结合权限管理系统，根据用户的角色和业务需求，为用户分配不同的数据访问权限，如只读、读写、修改等权限。在企业财务系统中，财务人员拥有数据读写权限，而普通员工只有只读权限，防止未经授权的用户访问敏感数据。

同时对用户的数据操作进行记录和审计，通过数字签名技术确保操作记录的不可篡改和可追溯性，保障数据使用的安全性和合规性。

4.2 隐私计算与数据脱敏

在数据共享和隐私保护方面，商用密码技术与隐私计算、数据脱敏等技术相结合。在多方数据合作场景中，利用同态加密、安全多方计算等隐私计算技术，结合商用密码算法，实现数据“可用不可见”。在联合数据分析中，各方数据在加密状态下进行计算，无需共享原始数据，即可得到计算结果，保护了数据所有者的隐私。

在数据脱敏过程中，利用商用密码技术对敏感数据进行加密脱敏处理，将敏感数据转换为脱敏后的数据，如将身份证号中的部分数字替换为星号，同时确保脱敏后的数据在业务应用中仍具有可用性，在保障数据隐私的前提下，实现数据的安全共享和利用，满足不同场景下的数据共享和隐私保护需求。

（四）商用密码应用的技术趋势

1. 与新兴技术的融合发展

1.1 量子计算与抗量子密码

量子计算技术的飞速发展对现有密码体系构成了严峻挑战。传统密码算法，如 RSA、ECC 等，其安全性基于数学问题的难解性，而量子计算机凭借其强大的计算能力，能够运行 Shor 算法，在多项式时间内分解大整数，从而破解基于 RSA、

ECC 等公钥加密体系的密钥。这意味着一旦量子计算机达到实用化，目前广泛应用的基于传统密码算法的信息系统将面临巨大的安全风险，数据的保密性和完整性将受到严重威胁。

为应对量子计算带来的威胁，抗量子密码的研究和应用成为当前密码领域的重要方向。抗量子密码算法基于格理论、哈希函数、编码理论等数学难题，具有抵御量子计算机攻击的能力。我国积极参与抗量子密码的研究，在国际上取得了一系列重要成果。西交利物浦大学丁津泰教授领衔的研究团队在国际公开 Darmstadt 格最短向量（SVP）挑战赛中“破译 200 维难题”，刷新全球纪录，为抗量子密码标准设计提供了实证基础。2025 年 2 月 5 日，商用密码标准研究院发布公告，在全球范围内公开征集新一代商用密码算法，明确要求算法需同时抵抗经典计算攻击和量子计算攻击，标志着我国商用密码算法正式向抗量子技术迈进。目前，抗量子密码在金融、政务等领域的试点应用也在逐步展开，为未来大规模应用奠定基础。

1.2 人工智能与密码技术的结合

人工智能与密码技术的结合为信息安全带来了新的发展机遇。在密码算法优化方面，人工智能技术能够对密码算法进行分析和改进，提高算法的效率和安全性。通过机器学习算法，可以自动寻找密码算法中的最优参数配置，提升加密和解密的速度，同时增强算法抵御攻击的能力。

在密钥管理中，利用人工智能技术分析用户行为和数据特征，实现智能密钥生成和管理，根据用户的使用习惯和安全需求，动态生成高强度的密钥，并优化密钥的存储和分发方式，降低密钥泄露的风险。

人工智能还可用于安全检测与预警，通过对网络流量、系统日志等数据的实时分析，利用深度学习算法快速准确地识别异常行为和潜在的安全威胁，及时发出预警并采取相应的防护措施，提升信息系统的安全防护能力。

1.3 区块链与密码技术的协同创新

区块链技术与密码技术在多个方面实现了协同创新应用。在身份认证方面，区块链利用密码技术构建去中心化的身份认证体系，通过数字证书和数字签名，确保用户身份的真实性和不可篡改，实现用户在不同应用场景下的身份互认和统一管理。

在数据共享场景中，结合同态加密、零知识证明等密码技术，区块链能够实现数据的安全共享，各方在不泄露原始数据的前提下进行数据的协同计算和分析，保护了数据所有者的隐私。以医疗数据共享为例，患者的医疗数据存储在区块链上，利用密码技术进行加密，医疗机构在需要使用数据时，通过区块链智能合约和密码协议，在满足特定条件下对加密数据进行计算和分析，而无需获取原始数据，既保障了医疗数据的安全，又促进了医疗研究和医疗服务的提升。

区块链与密码技术的协同创新，为解决数据安全和信任问题提供了新的思路和方法，推动了数字经济的发展。

2. 密码技术的国密算法

2.1 国产密码算法与产品的发展现状

我国在商用密码算法和产品研发方面取得了显著进展。自主研发的 SM2、SM3、SM4、SM9 等商用密码算法，已广泛应用于金融、政务、通信等多个领域。SM2 椭圆曲线公钥密码算法，在电子政务的身份认证和电子签名中发挥着重要作用，保障了政务业务的安全开展。SM3 密码杂凑算法用于数据完整性校验，在软件代码签名、文件完整性验证等场景中确保数据未被篡改。SM4 分组对称加密算法在物联网设备通信加密、云存储数据加密等方面得到大量应用，保障了数据的机密性。

在密码产品方面，国内企业不断创新，推出了一系列高性能、高安全性的商用密码产品，如密码机、加密芯片、数字证书认证系统等。这些产品不仅满足了国内市场的需求，还在国际市场上逐渐崭露头角，提升了我国商用密码产业的国际竞争力。

2.2 推动国产化的政策支持与产业举措

国家出台了一系列政策支持商用密码国密算法支持措施。《密码法》的颁布实施，为商用密码产业的发展提供了法律保障，明确了商用密码的地位和作用，规范了商用密码的应用和管理。中办 2018 年 36 号文件《金融和重要领域密码应用与创新发展工作规划（2018—2022 年）》要求，在金融银行、电子政务等关键领域全面推进信创密码技术的应用，推动了国产密码算法和产品在重要行业的广泛应用。

产业界也积极采取举措，加强产学研合作，促进技术创新和成果转化。国内高校和科研机构在商用密码领域开展了深入研究，为产业发展提供了技术支持。企业加大研发投入，不断提升产品性能和质量，完善产业生态。众多密码企业与上下游企业紧密合作，形成了从芯片、设备到系统集成的完整产业链，共同推动商用密码国产化进程。

2.3 面临的挑战与应对措施

在商用密码国产化过程中，面临着诸多挑战。技术层面，部分国产密码算法和产品在性能和兼容性方面与国际先进水平仍存在一定差距，在处理大规模数据加密和复杂业务场景时，可能出现效率不高、与现有系统适配困难等问题。市场层面，由于国外密码算法和产品长期占据市场，用户对国产密码的认知度和接受度有待提高，国产密码产品在市场推广中面临一定阻力。人才层面，商用密码领域专业人才相对匮乏，人才培养体系有待完善，难以满足产业快速发展的需求。

针对这些挑战，需采取一系列应对措施。加大技术研发投入，鼓励高校、科研机构和企业开展联合攻关，突破关键技术瓶颈，提升国产密码算法和产品的性能和兼容性。加强市场培育和推广，通过政策引导、宣传培训等方式，提高用户对国产密码的认知度和信任度，营造良好的市场环境。完善人才培养体系，在高校设置相关专业和课程，开展职业培训和技能认证，加强人才储备，为商用密码国产化提供坚实的人才支撑。

3. 密码服务的云化与平台化

3.1 密码云服务的优势与应用模式

密码云服务具有诸多优势，能够有效降低企业的密码应用成本。企业无需自行搭建复杂的密码基础设施，只需通过云平台按需租用密码服务，减少了硬件采购、运维管理等方面的投入。密码云服务具有灵活便捷的特点，企业可以根据业务需求随时调整密码服务的规模和类型，实现资源的高效利用。

在应用模式上，密码云服务主要采用按需使用的方式，企业根据自身业务量和安全需求，向云服务提供商购买相应的密码服务套餐，如加密服务、签名服务、密钥管理服务等。一些云服务提供商还提供定制化的密码解决方案，根据企业的特殊业务场景和安全要求，量身定制密码服务，满足企业个性化的需求。

3.2 密码服务平台的架构与功能

密码服务平台通常采用分布式架构，由密钥管理中心、密码运算节点、安全认证模块、审计模块等多个部分组成。密钥管理中心负责密钥的生成、存储、分发和更新，采用安全可靠的密钥管理技术，确保密钥的安全性和可用性。密码运算节点承担加密、解密、签名、验签等密码运算任务，通过集群部署和负载均衡技术，实现高效的密码运算处理。安全认证模块对使用密码服务的用户和设备进行身份认证和权限管理，确保只有合法的用户和设备能够访问和使用密码服务。审计模块对密码服务的使用情况进行实时监控和记录，便于进行安全审计和合规性检查。

密码服务平台还具备与其他系统的集成能力，能够与企业的业务系统、云计算平台等进行无缝对接，为企业提供一体化的密码服务解决方案。

3.3 发展前景与潜在风险

密码服务云化、平台化具有广阔的发展前景。随着云计算、大数据、物联网等技术的广泛应用，各行业对密码服务的需求不断增长，密码云服务和平台能够更好地满足这些新兴技术场景下的密码应用需求，市场规模将持续扩大。

然而，密码服务云化、平台化也存在一些潜在风险。安全风险方面，云服务提供商的安全防护能力直接关系到密码服务的安全性，如果云平台遭受攻击，可能导致密钥泄露、密码服务中断等严重后果。合规风险方面，不同国家和地区对

密码服务的监管政策存在差异，云服务提供商需要确保自身的服务符合各地的法律法规和监管要求，否则可能面临法律风险。

为应对这些风险，云服务提供商需加强安全技术研发，提高云平台的安全防护能力，建立完善的安全管理体系；同时，要密切关注各地的监管政策，及时调整服务策略，确保合规运营。