中国工业互联网研究院
China Academy of Industrial Internet

全国商用密码应用优秀案例汇编

工业和信息化部密码应用研究中心

2022 年 9 月制

序　言

党的十八大以来，在以习近平同志为核心的党中央坚强领导下，密码事业取得历史性成就、实现历史性变革。2019 年 10 月 26 日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，于 2020 年 1 月 1 日起正式施行。密码法的颁布施行，是促进密码事业发展，保障网络与信息安全，提升密码事业科学化、规范化、法治化水平的重要保障。

在以网络化、数字化、智能化为主要特征的新一轮技术革命浪潮下，工业互联网、车联网、5G 通信、物联网、云计算、区块链等新技术新业态迅猛发展，同时也面临严重的网络安全威胁。密码技术通过加密保护和安全认证两大核心功能，实现防假冒、防泄密、防篡改、抗抵赖等安全需求，是保障网络与信息安全最有效、最可靠、最经济的关键核心技术和基础支撑。

本案例集对重点行业典型场景的商用密码应用优秀实践进行了总结，可为商用密码从业单位、商用密码检测机构以及信息系统运营单位了解重点行业商用密码建设情况，更好开展密码应用推进工作提供参考。本案例集的发布，是增强密码安全意识、畅通商用密码产业供需对接、共建密码应用工作良好生态的重要举措，对推动商用密码在重要领域实现更快速、更深入、更广泛的应用具有重要意义。

在党的二十大召开之际，让我们以习近平新时代中国特色社会主义思想为指导，坚定不移推进《中华人民共和国密码法》的贯彻实施，深入践行“密码安全为人民”的理念，进一步筑牢密码安全防线，为实现中华民族伟大复兴的中国梦保驾护航！

中国科学院院士

2022 年 7 月 1 日

编 制 说 明

深入推进商用密码在金融和重要领域的应用，是落实党中央密码工作的战略部署，是落实国家法律法规的必然要求。工业和信息化领域重要网络和信息系统数量繁多、密码应用需求大、密码应用推进任务重，亟需加快推进工业和信息化行业密码应用与创新发展。

首届全国商用密码应用优秀案例遴选活动是在工业和信息化部、国家密码管理局的指导下，由工业和信息化部密码应用研究中心（以下简称“中心”）主办，以产业促进为目标，是共建密码应用工作良好生态的重要举措。本次遴选活动本着广泛参与的原则，面向全社会公开征集密码应用优秀案例，受到社会各界企事业单位、社会团体的积极响应，征集到涵盖了工业互联网、车联网、电子政务、信息通信等重点行业领域案例共计 102 项。为保证案例遴选活动的公正、严谨，中心组织开展两轮案例评审。其中，第一轮重点针对申报材料的专业性、编写质量、与密码应用的相关性等方面开展评价，共选出25项案例进入次轮评审。第二轮评审，成立了以中国科学院院士冯登国为组长、以密码行业产、学、研、政等领域专家为评委的评审组，通过集中评审，现场质询、材料查阅等环节，最终评选出 15 项优秀案例。

为持续发挥案例遴选工作产业促进效用，进一步凝聚智慧、形成合力，中心牵头组织将 15 项优秀案例提炼形成《全国商用密码应用优秀案例汇编》（以下简称“《汇编》”），冯登国院士亲自作序，集中体现《密码法》实施以来工业和信息化领域密码应用的突出成果。希望通过《汇编》，将商用密码应用的经验分享给从事、关心商用密码应用工作的各界人士，持续推动商用密码在重要领域和典型场景的融合应用、合规应用，着力引导技术创新和实践推广，为密码事业发展积极贡献力量。

牵头编写单位：

中国工业互联网研究院（工业和信息化部密码应用研究中心）

参与编写单位：（按名称笔画排序）

卫士通信息产业股份有限公司

中国电信股份有限公司北京分公司

中国信息通信研究院

中国移动通信集团山东有限公司

中国移动通信集团有限公司信息安全管理与运行中心

北京炼石网络技术有限公司

北京数字认证股份有限公司

杭州安恒信息技术股份有限公司

国汽（北京）智能网联汽车研究院有限公司

国家广播电视总局广播电视卫星直播管理中心

视联动力信息技术股份有限公司

蚂蚁科技集团股份有限公司

深圳奥联信息安全技术有限公司

鼎链数字科技（深圳）有限公司

腾讯云计算（北京）有限责任公司

《全国商用密码应用优秀案例汇编》编写组

主　　编：鲁春丛

副 主 编：张晓彤

编审人员：

王　聪	查奇文	焦智灏	闫　飞
关志刚	唐明环	张　峰	于　乐
张弘扬	姬生利	何　畅	刘建行
张　聪	谢家贵	陈　剑	赵光亮
覃才俊	李　莎	万　涛	刘红梅
王　晟	刘　伟	庄威先	张远云
林俊燕	刘桂海	徐淑卿	卫振强
李　超	徐江斌	冯　勇	辛　文
任家萍	盛　诚	张新强	白小勇
王晓春			

目　录

基础软硬件

广播电视网

（一）移动云国产商用密码规模化应用

牵头申报单位：中国移动通信集团有限公司信息安全管理与运行中心

联合申报单位：中移（苏州）软件技术有限公司

中国移动通信集团广东有限公司

北京邮电大学

路云天网络安全研究院

一、案例综述

（一）案例背景

过去十年是云计算突飞猛进的十年，全球云计算市场规模增长数倍，我国云计算市场从最初的十几亿增长到现在的千亿规模，云计算政策环境日趋完善，云计算技术不断发展成熟，云计算安全愈发受到重视。

（二）案例简介

本案例根据《密码法》、《网络安全法》、《个人信息保护法》等法律法规要求，结合云平台自身特色，对商用密码产品在信息系统、云计算平台方面应用的安全性、合规性，以及云计算平台类的关键信息基础设施和租户关键应用系统等开展商用密码应用对标，并针对性提出安全解决方案。通过商用密码的应用，保证了云平台密码算法、

密码设备、密码协议、密钥管理等方面的合规性，确保了云计算平台网络安全服务的自主可控性和安全性。

本案例分两方面建设：一是通过对标 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等相关标准，积极完善平台自身的密码防护管理手段和技术手段，尤其是对于重要业务系统开展商用密码替换国际算法的改造工作。二是在上述对标、改造工作基础上，统筹规划密码服务建设，向云平台业务应用系统提供快速、合规、安全的密码应用服务。

目前本案例成果已为 POS 收单、互联网支付、预付费卡支付、P2P，电子病历、电子发票、电子合同、电子保单等业务及应用提供密码安全服务。

本案例立足强化自身密码能力、长远布局密码服务，不断推进安全、合规的云平台密码服务，努力践行央企责任与使命。

二、行业挑战

尽管云计算有着降低成本、提高生产力、加快中小企业创新和产品进入市场的速度、给用户带来更高的业务灵活性等诸多优势，但云计算的安全性问题也相伴随行。根据 IDC 等研究机构的调研显示，在阻碍中国行业用户上云、用云的因素中，缺乏安全的信任度是其中的重要原因之一。用户信息滥用、隐私泄露等潜在安全风险是政府部门、企业和各类组织机构在选择云计算服务和应用部署云平台的主要阻力。

云计算安全的核心目标是数据安全和隐私保护，密码与密钥管理技术是实现云计算安全的基础技术和核心机制，合理运用密码技术是提高云计算应用安全、增强云计算使用者使用信息的重要手段。

三、项目实施情况

（一）总体技术架构图及介绍

总体架构参考 OSI 七层网络模型思想，自下而上，传递密码基础服务能力的基础上，结合云平台自身特点及密码应用基本要求，使平台基础业务模块能够高效、集约化地调用密码功能。总体架构既体现出密码服务的技术特点，又兼顾了相应的密钥管理和安全管理规范。

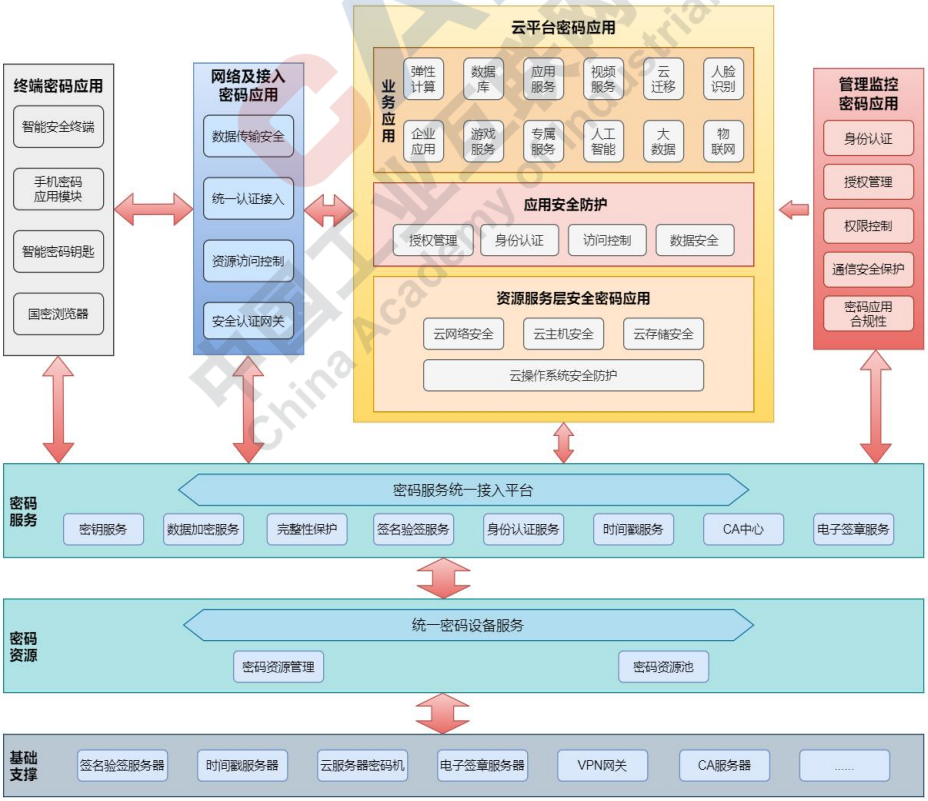

图 1.1 总体技术架构图

（1）基础支撑层

基础支撑层主要包含云服务器密码机资源池、CA 证书认证中心等密码基础设施。其中，云服务器密码机资源池是平台最基础、最关键的资源服务，承担了密码安全重中之重的部分就是密钥的管理和使用，CA 认证中心能够安全地解决身份认证、信任管理的问题，安全认证网关可满足通信过程中的信道加密需求。另外，还部署和应用了包括密码芯片、密码模块、密码整机和密码系统类相关产品，集成了密码资源层所需的各类型密码设备，提供电子认证、密钥管理、密码应用等基础功能，由密码资源层统一管理和分配使用。

（2）密码资源层

包含密码资源池和密码资源管理，提供统一的密码设备服务，为云平台租户提供虚拟密码设备和产品的租用服务。

（3）密码服务层

将基础支撑层和密码资源层设备和服务抽象化，通过统一接入平台向云平台、终端、网络接入、监控管理等提供各类型密码安全服务，包含通用密码服务、密钥服务、典型密码应用服务等，承载了业务需要，向云平台用户按需提供弹性的密码服务。以密码服务统一接入平台的中间件形式提供服务，提高各业务应用资源调用密码服务的便捷，也易于进行管理。

（二）应用场景架构图及讲解

密码服务应用场景中使用虚拟密码机密码运算能力，通过标准 API 接口为业务应用提供加密/解密、签名/验签、杂凑运算、消息鉴

别码的产生和验证等通用密码服务。

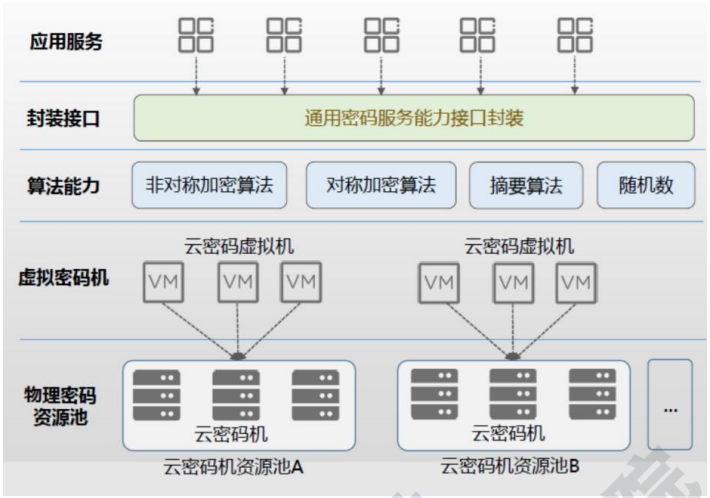

图 1.2 应用场景架构图

将密码服务器资源池化，通过虚拟化技术虚拟密码机，实现集中化、透明化、集约化的管理；虚拟密码机提供弹性、按需的服务能力，实现统一密码资源池组内的高可用；通过虚拟机实现算力服务，通过接口封装，提供统一接口能力，实现与物理密码服务器相同接口能力。譬如 POS 收单、互联网支付、预付费卡支付、P2P 等各类第三方支付业务在强监管要求范围内必须采取密码设备保证系统安全性，满足监管合规要求；支付数据在传输、存储过程中需保证完整性、保密性、支付身份的认证、支付过程的不可否认性等，保障业务安全。

对此移动云提供以下服务:

密钥管理： 生成和管理支付渠道等的密钥

身份认证： 提供支付介质或用户身份认证

验证服务： 提供 PIN 等的加密传输和验证

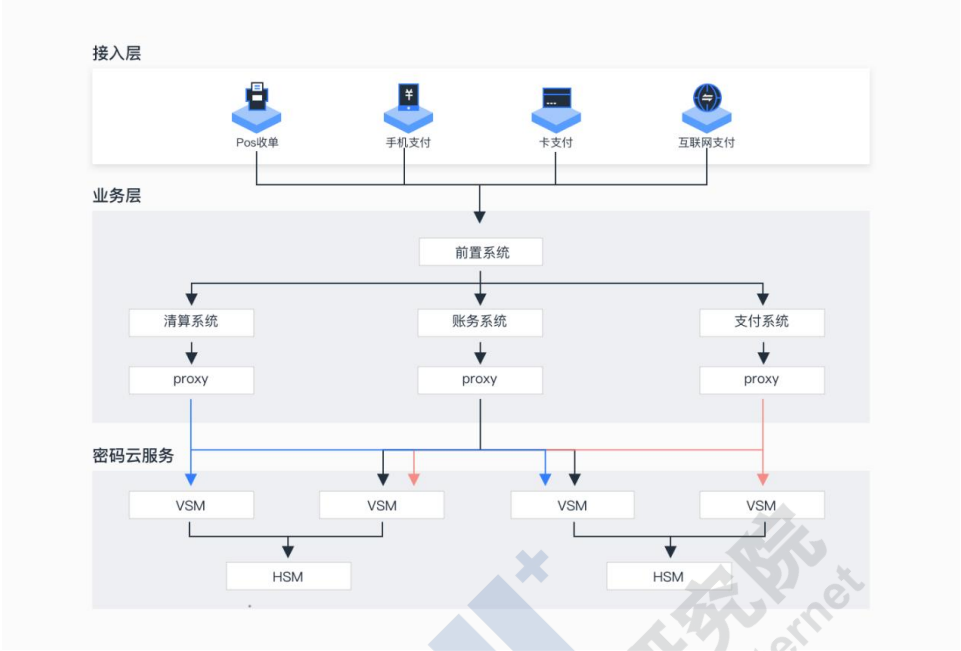

图 1.3 金融支付应用场景

四、实施效果

（一）核心技术自主可控，助力新基建

1、云平台由众多分布式服务器和其上运行的应用构成，面临资源隔离、数据存储、数据共享、多租户、虚拟化等带来的安全问题。

2、运用商用密码算法和技术建立用户资源隔离机制、数据加密存储和传输机制、统一身份认证机制和虚拟化安全机制，助力国家数字基础设施建设。

（二）创造良好云计算生态，维护云原生安全

在做好顶层设计基础上，由政府主导、企业参与，制定云计算相关法律及标准；优化、规范基础设施架构；支持数据开放，构造开源的生态环境；建设优质服务体系，提升用户体验。

（三）发挥云计算规模化优势，降低用户商密改造成本

1、商密在云计算平台的规模化应用，将充分发挥云平台计算资源管理和技术优势。

2、协助政府和企业用户快速搭建基于商密基础设施的安全计算环境，快速集成密码计算资源，减少企业投入，降低用户技术门槛和使用成本。

（四）实践效果显著，方案可用可推广

1、整合改造密码支撑资源，建设合规云上密码服务系统，相关方法和技术高可用、易推广。

2、通过专业商用密码测评机构的测评，《移动云密钥管理系统》已符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第三等级要求，获测评单位的高度评价。

（二）基于商用密码的腾讯云数据安全中台保护方案

牵头申报单位：腾讯云计算（北京）有限责任公司

联合申报单位：财付通支付科技有限公司

一、案例综述

（一）案例背景

2022 年 1 月 12 日，由国务院发布的《“十四五”数字经济发展规划》指出：提升网络安全应急处置能力，加强金融、能源、交通运输等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。加快发展网络安全产业体系，促进数据加密等网络安全技术应用。

腾讯云作为我国主流的云计算厂商，已在金融、政务、零售、教育等各个领域，为传统行业的数字化转型提供接口。由于云上商用密码及数据安全保护方案仍缺乏成熟的应用实践，腾讯云致力于基于云数据安全中台打造云架构中商用密码技术应用的最佳范例，并与主管单位、生态合作伙伴联合输出一套成熟的安全云数据商用密码保护技术方案标准。

（二）案例简介

腾讯云数据安全中台保护方案通过基于商用密码的数据加密软

硬件服务（HSM/SEM）、密钥与凭据管理系统（KMS/SSM）、云访问安全代理（CASB）三大核心能力，打造端到端的云数据全生命周期安全体系，保障数据在识别、使用、消费过程中的安全。借助云数据安全中台提供的极简化加密 API 和 SDK 服务，微信付款码和微黄金系统完成腾讯金融支付全系统全链路的密码国产化改造，该应用场景为金融行业的商用密码改造带来具有技术创新价值的借鉴。

二、行业挑战

伴随云计算时代的快速发展，数据爆炸式增长让数据安全和隐私保护问题变得复杂，也让各行业陷入了大数据安全防护的迷思之中。比如，金融行业对数据访问控制、处理算法等方面提出高安全要求；政务行业需要隐私保护的安全监管等。虽然行业以及具体的防护需求都不尽相同，但归根结底都是要保证数据本源的安全。

例如早期微信支付的密码安全体系均基于国际密码算法，依赖于 OpenSSL 等国外开源基金会运营的开源项目；同时，国际密码算法的安全性、是否有后门尚有争议，以及可能会遭受制裁等威胁。密码安全与自主可控关系到系统安全。在该项目实施后，微信支付业务有序地开展国产商用密码改造，对现有密码算法进行升级替换，腾讯金融已完成商用密码在微信付款码和微黄金业务的应用，微信付款码用户量达亿级，微黄金用户量也突破百万级。

三、项目实施情况

（一）总体技术架构图及讲解

图 2.1 项目总体架构图

腾讯云数据安全中台保护方案通过基于商用密码的数据加密软硬件服务（HSM/SEM）、密钥与凭据管理系统（KMS/SSM）、云访问安全代理（CASB）三大核心能力，打造端到端的云数据全生命周期安全体系，保障数据在识别、使用、消费过程中的安全。借助腾讯云数据安全平台，企业用户可以轻松构建基于商用密码的极简数据安全解决方案，提供从数据获取、处理、分析与服务方面的数据安全保护能力支持。

（二）应用场景架构图及讲解

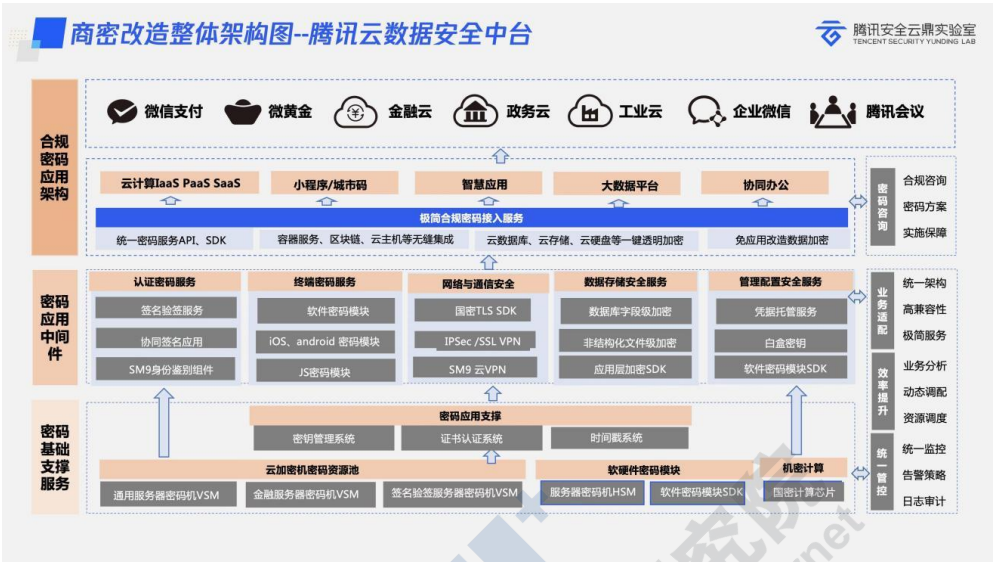

图 2.2 案例应用场景架构图

腾讯云数据安全平台在云端围绕数据生命周期，形成了一套极简完整的云数据安全解决方案。腾讯云数据安全解决方案将数据加密技术以服务化、组件化的方式融合到架构中，实现云核心运算环境、数据存储、密钥等关键数据的隔离保护，并提供认证、终端安全、数据存储等密码服务，打通商用密码服务产业链上下游环节，在云架构中实现基于密码服务的数据全生命周期的云数据安全解决方案。

财付通作为微信支付的技术支撑组织，为落实好年国产密码应用工作，选择了单日请求量过亿的付款码支付系统以及与工商银行合作的重点创新项目微黄金结算系统作为试点项目。基于开源代码 GmSSL 实现财付通国密自研库，并对算法性能进行优化来完成两个系统的国密改造工作，切实推进建立以 SM 算法为主要支撑的金融信息安全保障体系，实现财付通内部的安全核心产品及系统自主可控。

项目创新点主要体现在:

1、云架构的数据安全技术创新: 腾讯云安全能力平台基于云架构创新密码技术应用，通过数据加密软硬件服务、密钥与凭据管理系统以及云访问安全代理，根据用户需求弹性、按需配置、安全共享等高度灵活的云数据加密服务。

2、创新云密码应用解决方案: 基于融合架构体系及密码应用中间件，实现云计算架构中的核心运算环境、数据存储、数据库以及密钥等关键数据的隔离保护，并提供认证、终端安全、网络与通信安全、数据存储安全、管理配置、方案咨询等商用密码服务。

3、算法安全及兼容: 完全自主研发商用密码模块，彻底摆脱了对国外开源密码算法库（如 OpenSSL、BoringSSL 等）的依赖，实现了密码的自主可控。

4、性能优化: 密码模块在性能优化上取得突破性进展，SM2 签名单核性能可达 5 万次/秒，SM4 单核性能可达 4Gbps; 解决了信创 CPU 环境中商用密码算法性能低下的问题。

四、实施效果

（一）社会经济效益

腾讯云数据安全平台从架构及商业化设计上，基于行业生态，打通密码行业上下游产业链，适配云及多元化的应用场景，帮助用户极简化的实施云数据安全保护及数据加密方案，降低企业的商用密码应用成本，将有力推动数据安全与密码应用产业的创新发展，创造可观

的经济效益。

（二）优化性能，推动密码国产化，保障信创等相关产业安全

腾讯孵化了基于商用密码的自研算法模块，实现了核心代码的完全自主可控。目前自研商用密码算法性能已经优于国际密码算法性能，尤其在国产 CPU 的高性能兼容支持上，为国产商用密码算法的应用落地扫除了一大技术障碍，助力国产化信创生态的完善。

（三）保障金融安全

在该项目开展以前，微信支付的密码安全体系均基于国际密码算法，依赖于 OpenSSL 等国外开源基金会运营的开源项目，存在境外制裁风险。而密码安全与自主可控关系到系统安全，从而影响支付业务的安全保障能力。在该项目的推进实施后，微信支付业务稳步有序地开展国产商用密码改造工作，对现有密码算法进行升级替换，目前，微信付款码与微黄金已完成首批试点工作并通过验收。

（四）推动商用密码技术与云基础设施融合

越来越多的企业通过大规模部署云计算在推动战略性变革，腾讯云数据安全中台构建一套完整的云数据安全治理解决方案，加速云计算产业优化升级步伐，保证云上核心数据安全性。基于云数据安全中台原生嵌入国产密码技术，借助强大的辐射效应，有力推动在金融、政务以及国家关键行业中的基于国产密码的数据安全保护应用落地。

（三）基于商用密码的 V2X 通信安全认证防护系统 SCMS

申报单位：国汽（北京）智能网联汽车研究院有限公司

一、案例综述

（一）案例背景

2021 年 7 月工信部起草《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》强调车联网安全能力建设，针对 V2X 通信，推进基于 PKI 的安全认证与审计技术。2021 年 9 月，工信部发布《关于加强车联网网络安全和数据安全工作的通知》中提到要加强车联网网络安全防护，保障车联网通信安全，要求企业建立车联网身份认证和安全信任机制，强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施，防范通信信息伪造、数据篡改、重放攻击等安全风险，保障车与车、车与路、车与云、车与设备等场景通信安全。鼓励相关企业、机构接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通。

（二）案例简介

基于商用密码的 V2X 通信安全认证防护系统 SCMS 最早实现了与 IEEE、ETSI 等国际标准的接轨，通过此平台实现 C-V2X 安全认

证体系方案设计、建设，建立 PKI 信任体系，实现基于 V2X 技术的通信单元交互安全，实现身份认证、安全传输、数据完整性、有效性等安全特性，解决当前车与车、车与路边单元等 V2X 体系内攻击漏洞以及安全隐患，建立一个安全的网络运行环境。目前已为 C-V2X“新四跨”先导应用示范活动、北京高级别自动驾驶示范区等持续提供服务，可支持大量的 V2X 直连通信应用场景，全面适配多种 V2X 终端设备，同时本系统可实现终端跨信任域的互联互通，提高通信的安全及效率。

二、行业挑战

（一）《V2X 车辆管理白皮书》指出，V2X 通信具有跨行业的特点，目前产业所关注的焦点是如何打通行业内的信任。工业和信息化部车联网安全信任根管理平台 TRCLA 提供了这样的平台，但 TRCLA 长期离线，降低 TRCL 更新频率，减少离线 TRCLA 的操作，提高安全性，不接受企业直接向 TRCLA 申请接入。为保护 TRCLA 的安全性，国汽智联的 V2X 通信安全认证防护系统 SCMS 中包含了 ROOT CA 模块，直接接入 TRCLA，车企、示范区等接入 ROOT CA 模块，最终实现跨信任域的身份认证，保障多品牌车辆的安全互联互通，构建车车通信安全保障能力。

（二）终端设备的第一张身份证书的认证授权至关重要，因为它需要为后续假名证书及应用证书申请提供签名。本系统对认证授权机构创新设计，开发出了设备配置管理系统（DCM），可根据认证设

备的序列号或 X.509 证书的方式对终端的身份确认，保障了注册证书签发的安全性。

（三）车辆终端在道路行驶中，使用假名证书签发主动安全消息，攻击者会根据假名证书模拟车主的行驶路线，追踪车主的位置。为了防止车主隐私泄露，本系统设计了每周为车主颁发 20 张假名证书，假名证书每 5 分钟随意变换使用。同时，本系统采用了密钥衍生、链接值及密钥重构技术，极大地保护了车辆隐私并减少了假名证书申请和下载的交互次数。

三、项目实施情况

（一）总体技术架构图及讲解；

基于商用密码的 V2X 通信安全认证防护系统 SCMS 将以 YD/T 3957-2020《基于 LTE 的车联网通信技术 安全证书管理系统技术要求》为标准开发，实现 V2X 通信过程中信息的完整性、不可否认性以及车辆的隐私保护等安全特性。解决当前车与车、车与路边单元、车与人通信的安全隐患。

系统将采用微服务架构设计思路，遵循模块化原则，设置相对独立的功能模块，这些功能模块包含了根 CA 机构（Root CA）、中间证书机构（ICA）、注册证书签发机构（ECA）、认证授权机构（AAA）、假名证书签发机构（PCA）、假名证书注册机构（PRA）、链接值签发机构（LA）、应用证书签发机构（ACA）、应用证书注册机构（ARA）、异常行为管理机构（MA)、可信证书列表管理机构（TCMF）等。构

建不同需求的车联网安全证书管理系统，在系统中各模块之间采用安全连接实现各项功能。各模块使用的密码设备采用统一的调用接口，所有密码运算均在密码设备中完成。

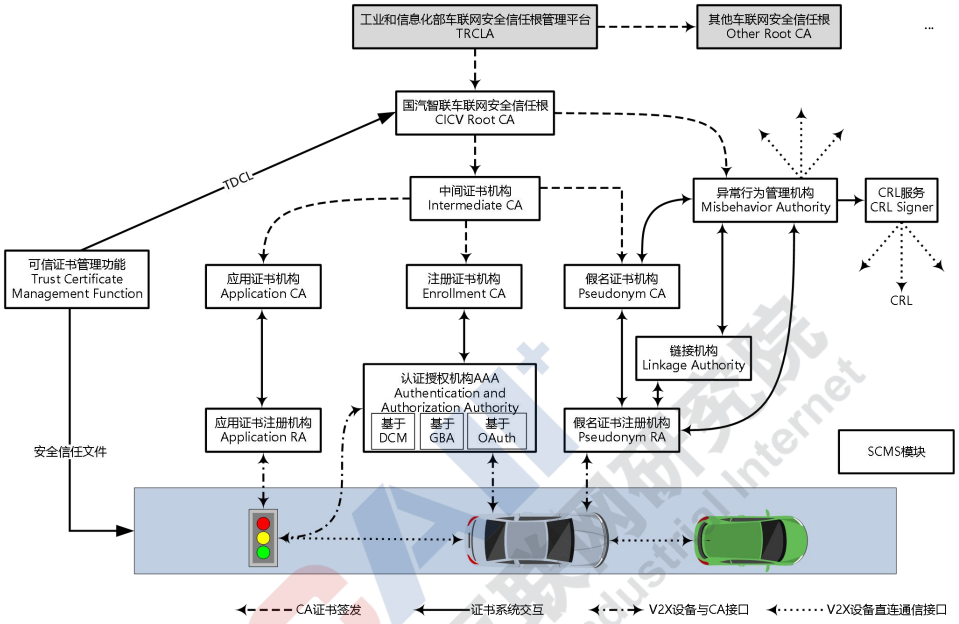

图 3.1 SCMS 系统架构图

此 SCMS 系统可以实现 V2X 设备向 ECA 申请注册证书、向 PCA 申请假名证书、向 ACA 申请应用证书，同时支持将异常终端的注册证书放入黑名单，将证书撤销列表提供给 CRL 服务实体，V2X 设备或其他证书管理实体通过此接口从 CRL 服务实体下载或检查证书撤销列表等服务。

（二）应用场景架构图及讲解

V2X 一期应用有安全、效率、信息服务 3 大类，分为前向碰撞预警、交叉路口碰撞预警、左转辅助、盲区预警/变道辅助、逆向超车预警、紧急制动预警、异常车辆提醒、车辆失控预警、道路危险状

况提示、限速预警、闯红灯预警、弱势交通参与者碰撞预警、绿波车速引导、车内标牌、前方拥堵提醒、紧急车辆提醒、汽车近场支付17个场景。这些应用场景的通信都是基于PC5的一对多广播的方式直连通信，这种通信方式使得消息容易受到消息的伪造、消息的篡改、终端的伪造等外界攻击。

攻击场景案例1：一个非官方的路侧设备伪造红绿灯发送错误的交通信号消息，车辆收到假消息后采取错误行动导致交通混乱。

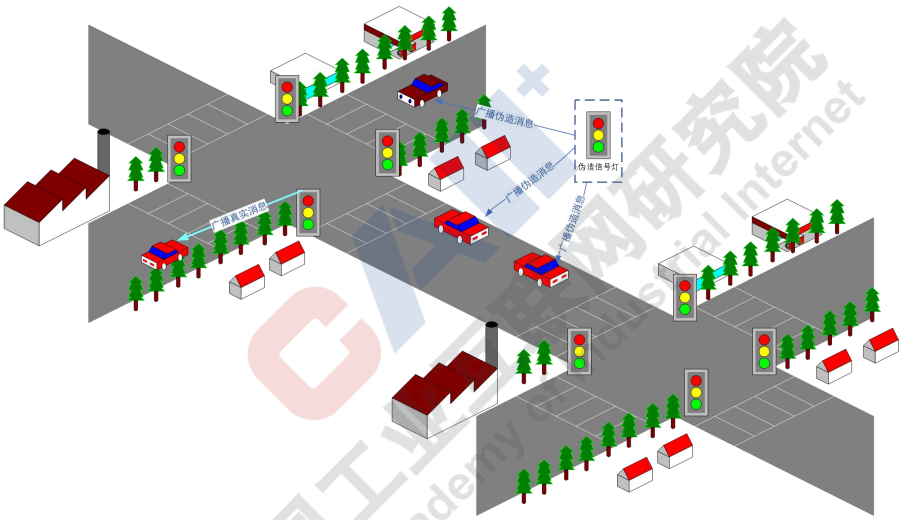

图3.2 伪造红绿灯的交通示意

攻击场景案例2：一个普通车辆伪造救护车或警车等特种车辆，向红绿灯发送绿灯保持消息，导致交通效率降低。

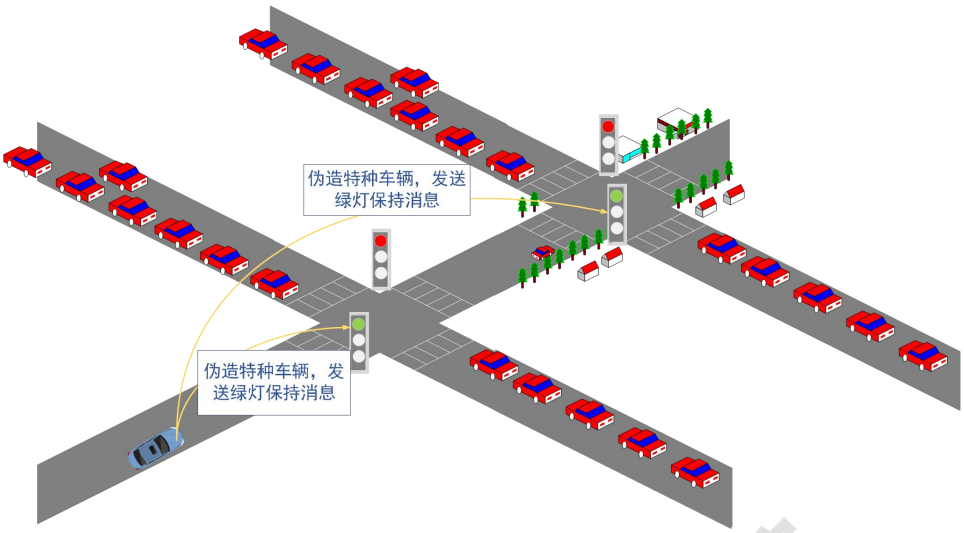

图 3.3 伪造特种车辆的交通示意

为解决以上问题，车辆及路侧设备在终端生成密钥对并向本案例 SCMS 系统申请证书，可为车辆及路侧设备签发证书并通过 ROOTCA 下发安全信任文件，从而车辆及路测设备发出的消息使用证书公钥对应的私钥签名，保障了信息的完整性、不可否认性。整体架构如下图所示。

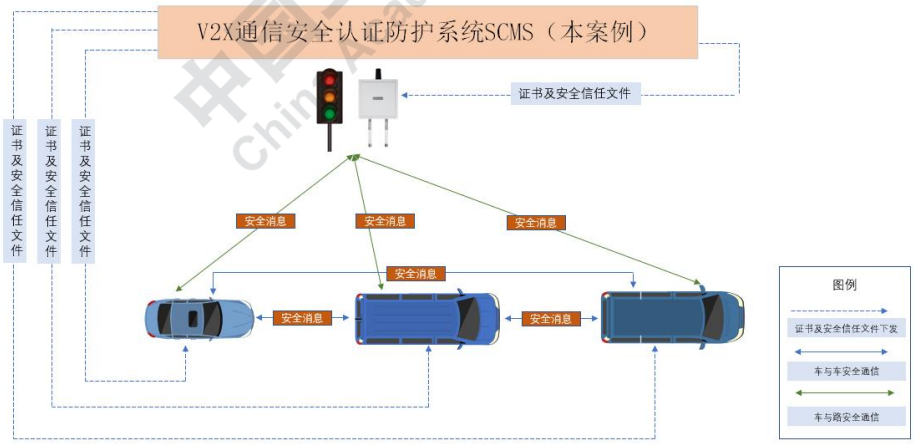

图 3.4 SCMS 系统应用架构图

商用密码技术在本案例中发挥的作用主要体现在保障数据传输真实性、完整性及行为抗抵赖保障方案。

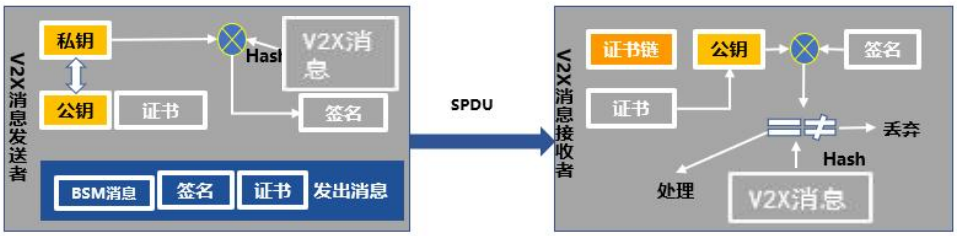

图 3.5 商用密码应用情况图

本案例 SCMS 系统解决了 V2X 消息的真实性、完整性及行为抗抵赖，具体流程如下:

1、V2X 消息发送者在终端本地生成国密公私钥对，并构造身份证书的申请请求，用私钥签名，发送到 SCMS 系统。

2、SCMS 系统审核身份证书请求的合法性，若判断为合法请求，将用 SCMS 系统中的 ECA 模块签发 EC 证书并返回给终端。

3、终端生成密钥扩展因子，构造假名证书申请请求并用 EC 证书对应的私钥签名发送到 SCMS 系统。

4、SCMS 确认假名证书请求的合法性后，经过一系列操作得到假名证书完整公钥和私钥因子，SCMS 系统中的 PCA 模块使用完整公钥签发假名证书，加密扩展公钥加密假名证书及私钥因子得到加密文件，并用 SCMS 系统中的 PCA 模块对加密文件签名得到 PC-Zip。终端请求按照规定时间下载假名证书，在本地重构私钥得到完整私钥。

5、当终端要发送 BSM 消息时，首先对 BSM 消息进行哈希运算

得到哈希值，使用假名证书公钥对应的私钥对哈希值签名，将 BSM 消息、哈希值、假名证书组成 SPDU 消息一同广播出去。

6、消息接收者接收到 BSM 消息后，用本地的证书链验证证书的有效性，确认证书有效后，用证书的公钥验签 SPDU 签名，验签通过后证明了消息发送者的完整性、真实性和不可否认性。

四、实施效果

（一）经过大规模验证，SCMS 系统可保障 V2X 通信的数据安全传输，具备极高的推广意义

国汽智联的基于商用密码的 V2X 通信安全认证防护体系 SCMS 案例已在工信部身份认证和安全信任试点项目中得到充分的应用，同时也将此案例应用到了北京市高级别自动驾驶示范区，通过大规模的测试，从实践中验证了本系统可解决 V2X 通信中数据传输的真实性、完整性、不可否认性要求。国汽智联的基于商用密码的 V2X 通信安全认证防护体系 SCMS 也验证了 CCSA 标准 YD/T 3957-2021《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》，为其他 CA 厂商在车联网通信安全系统开发工作提供极高的示范参考价值。

（二）开发异常行为管理功能，具备极高的行业领先性及示范意义

国汽智联的基于商用密码的 V2X 通信安全认证防护体系 SCMS 案例，具备异常行为管理的功能。其中异常行为管理模块主要负责接收来自车辆上报的异常行为报告，通过分析、识别车联网系统中的异

常行为者并通过撤销其通信证书的方式将异常行为者从系统中删除。当前，国汽智联的 SCMS 案例的异常行为管理模块在国内处于领先地位，为其他厂家开发类似功能可提供技术支持。

（三）实现跨行业跨品牌的互联互通

国汽智联的基于商用密码的 V2X 通信安全认证防护体系 SCMS 案例的 ROOTCA 模块加入了工信部 TRCLA 身份认证平台，同时实现了多个车企、示范区的 ICA 接入 ROOTCA，保障了多品牌车辆的安全通信，构建 PC5 通信安全。目前已接入约 17 家企业接入，解决国内 73% V2X 相关业务的跨行业跨品牌互联互通问题。

（四）互联网域名体系商用密码技术研究及应用

申报单位：中国信息通信研究院

一、案例综述

（一）案例背景

互联网域名体系是最关键的网络基础设施，是支撑全球网络设备互联互通和信息数据共享的主要手段。由于历史原因当前我国域名体系中使用的加密算法都是国际通用的密码算法，不具备自主知识产权且易被利用攻击，存在较大的安全风险。

近年来国家高度重视网络空间安全，相继出台了《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《信息安全等级保护管理办法》等多个安全法规来规范和保障网络空间的安全性。商用密码算法具备自主知识产权，符合国家网络空间安全战略，实现互联网域名领域的密码算法技术的国产化替换、大力推广商用密码算法是防止后门漏洞的最有效方法，是保障网络安全的主要举措。

（二）案例简介

本案例首先进行了域名系统中相关技术协议标准和各系统实施应用现状的调研，综合分析域名注册、域名数据存储、域名解析等各个环节商密算法替换对整个域名体系软件系统和生态的影响。形成商

密在域名注册通信、本地数据存储、解析区数据同步三大典型应用场景的具体解决方案，完成两家域名注册管理机构，两家域名注册服务机构，三家基础电信企业的现网环境试点和应用。域名相关业务系统商密升级改造后，各项指标符合管理机构要求，系统可用性未受影响，切实保障了域名注册环节用户敏感数据的安全。

本案例可有效解决域名服务领域中目前面临的密码非自主可控的问题，形成各个应用场景下的示范应用及确立各应用场景下的密码使用规范，并将相关应用在域名行业内推广，形成行业示范带动作用。

二、行业挑战

域名体系作为重要的互联网关键基础设施之一，当前商用密码防护情况不容乐观。**一是**各环节的数据加解密流程风险不可控，互联网起源于美国，目前域名体系中绝大部分数据存储及传输环节均使用国际标准的密码加密，受境外相关管制机制的控制，存在巨大风险；**二是**全流程替换商密的改造难度较大，域名体系涉及标准协议、软件系统、基础工具库等众多环节，目前基本不支持商密算法，全面改造替换的难度大；**三是**国内域名运营机构全面推广并覆盖商密难度高，要提高域名行业整体安全水平，需要在国内域名注册管理机构、域名注册服务机构、基础电信企业等众多域名机构中实现商密覆盖，且尚无相关国际、国内标准，需要通过政策引导等方式推动相关机构实施商密替换，全面推广难度高。

三、项目实施情况

（一）总体技术架构图及讲解

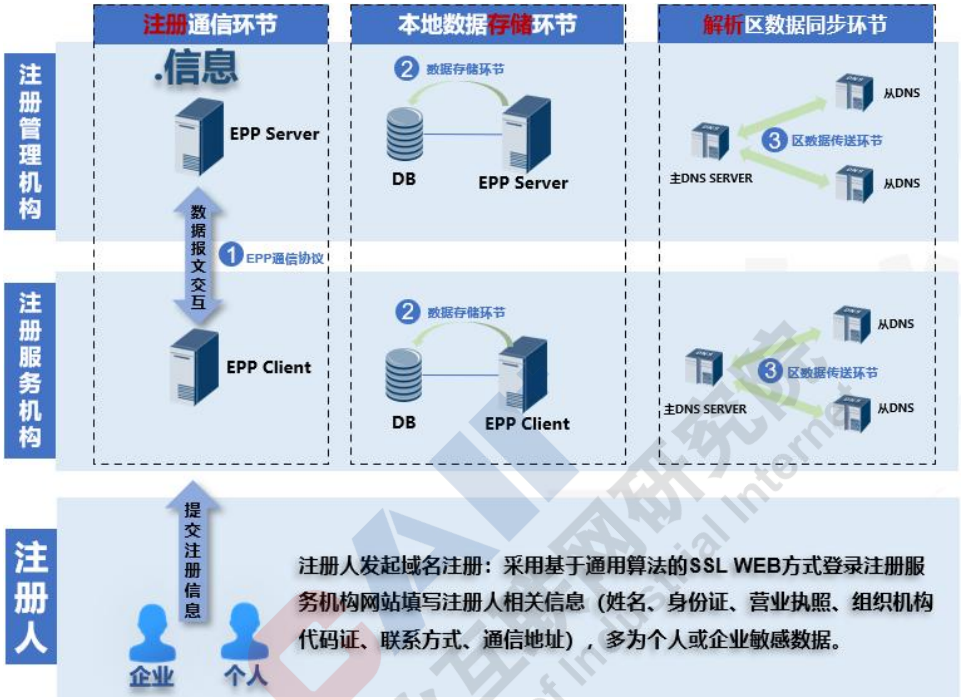

图 4.1 域名体系商用密码总体技术架构图

互联网域名体系商用密码技术研究及试点应用案例中，主要选取域名体系中域名注册通信、本地数据存储、解析区数据同步三大重点环节进行了商用密码的技术研究，形成完整技术方案在现网进行试点，并推动形成三项域名商密相关行业标准立项，可有效提升域名行业数据采集、数据存储、数据分发过程中的数据安全性，为域名这一关键网络基础设施保驾护航。

（二）应用场景架构图及讲解

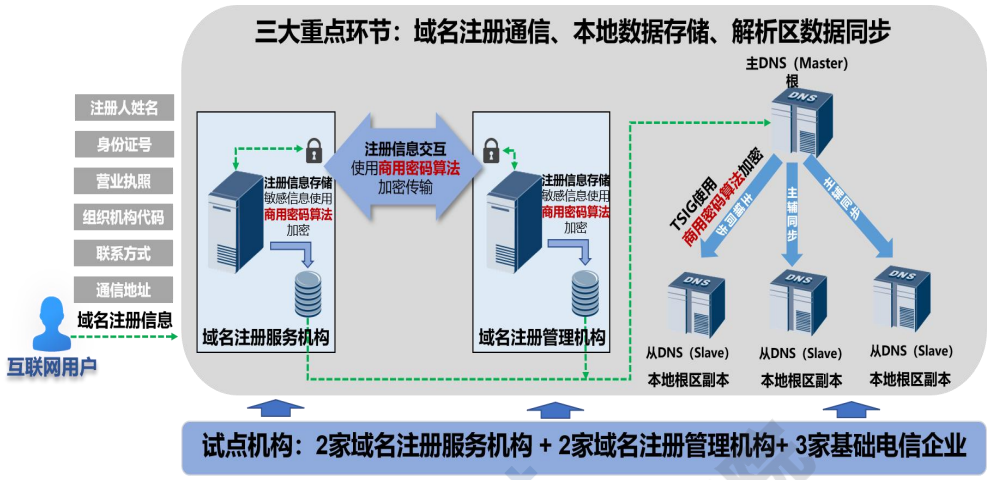

图 4.2 域名体系商用密码技术应用场景图

2020 年在 2 家域名注册管理机构，2 家域名注册服务机构，3 家基础电信企业的现网环境中，完成了域名注册通信、本地数据存储、解析区数据同步三大重点环节中商用密码的试点应用工作，经功能、性能、稳定性、兼容性等综合测试评估，相关系统在使用商用密码算法之后系统可用性未受影响，且系统技术指标符合管理机构要求，可在域名行业内大范围推广。

域名注册通信环节：注册服务机构与注册管理机构通过大量的 EPP 协议报文，传输用户注册的敏感信息，如姓名、身份证、营业执照、组织机构代码证、联系方式、通信地址等。EPP 通信协议是域名注册服务机构与域名注册管理机构之间的数据报文交换协议，主要是完成互联网注册人发起的域名注册请求，其安全保障基于 TLS（Transport Layer Security，传输层安全性协议）。本环节主要是对 TLS 协议进行商用密码改造。采用商密算法替换目前 TLS 中的国际

算法，HASH 算法由 SHA-1,SHA-256 等替换为商密算法 SM3，数据加密通信将 AES,DES 等算法替换为商密算法 SM4，RSA/DSA 等算法替换为商密算法 SM2。同时考虑到域名注册机构的实际业务需求，提出了“双算法并存”的解决方案，即服务端可同时支持国际密码和国产商用密码客户端的连接。

本环节试点工作选取 ZDNS、纳网科技两家域名注册管理机构和泰尔英福、ZDNS 两家域名注册服务机构，针对其业务系统数据报文交互中的证书颁发、密钥交换、通信数据交换等环节进行商密改造。在使用商用密码后，系统 TLS 握手耗时、平均响应时间、并发用户数等主要指标层面均无明显影响，业务系统长时间运行完全正常，可确保域名注册通信过程中的数据安全。同时基于该环节的研究及试点工作，推动完成了域名商密相关行业标准《互联网域名注册服务加密技术要求》的立项工作。

本地数据存储环节：注册人的注册请求中携带大量的个人或企业的敏感数据信息，如姓名、身份证、营业执照、通信地址、系统密码等，系统将对这些数据进行加密存储。该环节商密算法应用需要业务系统进行敏感信息摘要算法替换、数据存储加密逻辑调整、对称加密数据的先解密再采用商密算法加密等，系统调用的算法由国际通用的 DES、AES、SHA、MD5 统一修改为商密的 SM4、SM3 算法。

本环节试点工作选取 ZDNS、纳网科技两家域名注册管理机构和泰尔英福、ZDNS 两家域名注册服务机构。商密算法应用后各项业务功能正常，且性能无明显影响，可确保域名数据存储过程中的数据安

全。同时基于该环节的研究及试点工作，推动完成了域名商密相关行业标准《互联网域名数据存储加密技术要求》的立项工作。

解析区数据同步环节：DNS 区传送为现有互联网域名服务领域应用最为广泛的技术，广泛应用于根区副本数据下发、权威 DNS 的主辅区文件同步等场景中。区数据传送时，会使用 TSIG 校验数据的一致性，其原理是对区传送的所有数据进行 HMAC（哈希消息认证）运算，生成消息摘要，并用该摘要生成 TSIG 记录，校验数据一致性。TSIG 需要客户端和服务端有相同的对称密钥。本环节主要实现 TSIG 的生成和校验可以支持商密算法，在 HAMC 框架内追加商密 SM3 消息摘要算法，在区传送中 TSIG 配置时可选商密 SM3 消息摘要算法，从而实现商密算法的应用。

目前现网根区文件分发系统中副本分发环节正逐步替换为商用密码，涉及三大基础电信企业以及众多公共递归服务商，目前商用密码使用率已超过 70%，覆盖全国每日约 36.3 万亿次域名解析查询。同时基于该环节的研究及试点工作，推动完成了域名商密相关行业标准《互联网域名区文件传送数字签名技术要求》的立项工作。

基于上述试点技术方案及应用成果，工信部统一协调部署，扩大试点相关环节在现网域名体系中的应用范围。**在域名注册通信、本地数据存储环节、解析区数据同步环节**，已有十余家域名运营机构启动在现网系统的相关环节中支持商用密码，预计 2023 年中完成现网系统升级，公共递归服务商用密码使用率将提升至 90%，进一步提高域名体系总体安全性。

四、实施效果

（一）摸排行业现状并形成域名体系各环节商密改造方案

开展域名行业密码技术调研，全面摸排域名国际国内技术协议标准和系统实施应用现状，综合分析域名服务各个环节商密算法替换对整个域名体系软件系统和生态的影响。结合调研结果和国家密码相关政策法规，给出未来 2 到 3 年的商密应用行动计划和推进策略建议，并形成商密在域名领域应用的具体实施方案。

（二）攻克技术难点并完成域名典型场景的现网试点

依据调研成果，选取域名注册通信、本地数据存储、解析区数据同步三大典型环节首先验证实施商密算法的替换，完成技术开发、实现实验室环境的技术落地。同时完成在两家域名注册管理机构、两家域名注册服务机构、三大基础电信企业等机构的现网试点技术验证，系统功能、性能、安全性、兼容性等方面均可达到生产应用的要求。

（三）沉淀技术成果并可应用于域名产业国产化替换

通过在域名领域设立商密应用的相关技术要求和标准，不断推动国产化替换进程，目前已形成一套商密替换功效评估方法、一篇商密应用试点效果研究评估报告、一套商密 SDK 软件开发工具包、一套商密应用评测工具，同时课题组申请的三个域名行业商密标准已通过中国标准化协会相关工作组评审，同意立项，正在有序推进。

（五）融合商用密码技术的 SecureV2V 自主安全协议

申报单位：视联动力信息技术股份有限公司

一、案例综述

（一）案例背景

电子政务视联网，是基于自主研发的 V2V 通信协议及相关技术，不依赖西方主导的 IP 协议，为我国各级政府、事业单位、医疗机构等搭建的一种专用视频通信网络。目前，已实现覆盖全国 31 个省，累计接入 22 万台视联网终端设备，接入各类视频监控超过 500 万路。电子政务视联网主要包括政法综治、雪亮工程、电子政务、远程医疗、互联网+监管、应急指挥等领业务，在浙江、新疆、海南、广东等省均已实现规模覆盖。

然而，面对技术的发展和算力的进步，电子政务的网络安全还需要国产密码技术来保障。密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。《密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循。《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

（二）案例简介

视联动力在清华大学、成都卫士通等单位的技术支持下，与国产

密码技术深度融合，打造了新型视频通信网络协议——安全视频通信协议（Secure V2V）。相关技术和方案的创新性和安全性得到了周仲义、倪光南、王小云三位院士和多位相关领域权威专家的肯定。随后SecureV2V 协议及其系统在新疆等地实现试点和应用。

二、行业挑战

目前视频通信行业安全环节十分薄弱，缺少密码技术应用。在视频通讯领域面临诸多挑战，容易受到黑客、病毒和木马等网络安全方面的攻击；此次采用视联网技术+国产加密技术，进行加密数据传输，实现视频内容不泄露、组网设备可管控的目标。随着网络安全风险日益凸显，亟待开展基于国产密码技术的电子政务视联网安全技术研究。采用国密算法对视联网通信协议进行加密融合，实现信息安全的自主可控。

此外，当前我国关键信息系统的技术严重依赖国外，如操作系统和网络基础设备等，由于关键技术受制于人，这使得我国的相关信息设施容易被敌对势力攻击和控制。随着信息安全技术的进步，特别是国产密码技术的发展为相关安全问题提供了解决方案。

三、项目实施情况

（一）总体技术架构图及讲解

1.总体技术框架

基于 SecureV2V 的电子政务视联网依据《GM/T 0054-2018 信息

系统密码应用基本要求》和《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》进行项目建设，从技术层面构建电子政务视联网密码保障体系，实现电子政务视联网的安全防护，综合保障电子政务视联网及其业务应用的安全。其总体框架如下所示。

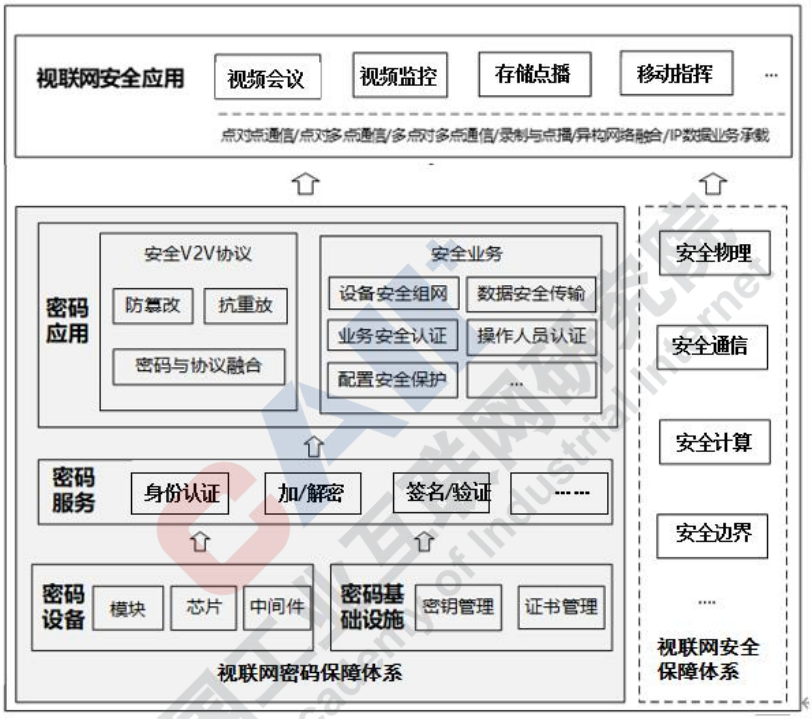

图 5.1 电子政务视联网密码应用总体框架

2.电子政务视联网密码保障系统

基于 SecureV2V 的电子政务视联网的密码保障体系，主要在以下方面对视联网进行密码保障。其中，在网络通信层面，从核心交换节点组网认证、业务管理类服务器接入认证、终端类设备接入认证、链路传输加密等方面进行真实性、机密性保护；在业务服务层面，从业务数据加密、控制信令完整性、管理指令完整性、业务认证等方面进

行业务和数据保护。同时，加强对视联网用户的安全管理，确保合法用户访问权限内的系统和资源，满足相关信息系统密码应用测评要求。

（1）密码设备

本方案以密码算法、密码协议、密码接口为密码基础，使用密钥管理服务系统、证书管理服务系统、服务器密码机、PCIE 加密卡和 USBKey 等软硬件密码设备为视联网提供密码服务支撑。

（2）密码基础设施

本方案设计密码技术与视联网相结合，实现在电子政务视联网环境中部署密钥管理和证书管理等密码基础设施。由密钥管理提供生成、存储、使用、分发、导入与导出、备份与恢复密钥等服务；由证书管理提供签发、存储、查询证书信息等服务。

（3）密码服务

基于密码设备和密码基础设施共同构建的密码服务，实现对上层视联网核心业务应用提供数据加密/解密、签名/验证、身份鉴别等密码服务。

（4）密码应用

基于密码技术实现设备组网和设备入网进行身份认证；基于密码技术实现各业务系统与终端进行业务安全认证，确保参与业务的设备身份合法；基于密码技术在协议中融入密码安全设计，抵御重放、篡改、破坏等攻击行为，实现音视频业务数据的安全传输；基于密码技术对关键性配置信息读取和存储过程，进行完整性校验，防止恶意篡

改。

（二）应用场景架构图及讲解

IP 协议在设计之初没有考虑安全性，而 SecureV2V 协议是一种采用主动安全理论的非 IP 网络通信协议。本方案通过在 SecureV2V 消息格式中融入了基于国产密码技术的各项安全防护机制，具有内生安全机制，实现了视联网通信的机密性、完整性、真实性、不可否认性保护。

本方案使用国家密码管理行政机构批准的非对称密码算法、对称密码算法、密码杂凑算法和随机数生成算法，算法采用获得国家密码管理行政机构批准的安全密码产品实现。终端类设备内置安全芯片，服务器类设备内置 PCIe 加密卡，系统用户配备 USBKey，以实现通信传输过程中数据加密，达到数据完整性和保密性的要求。

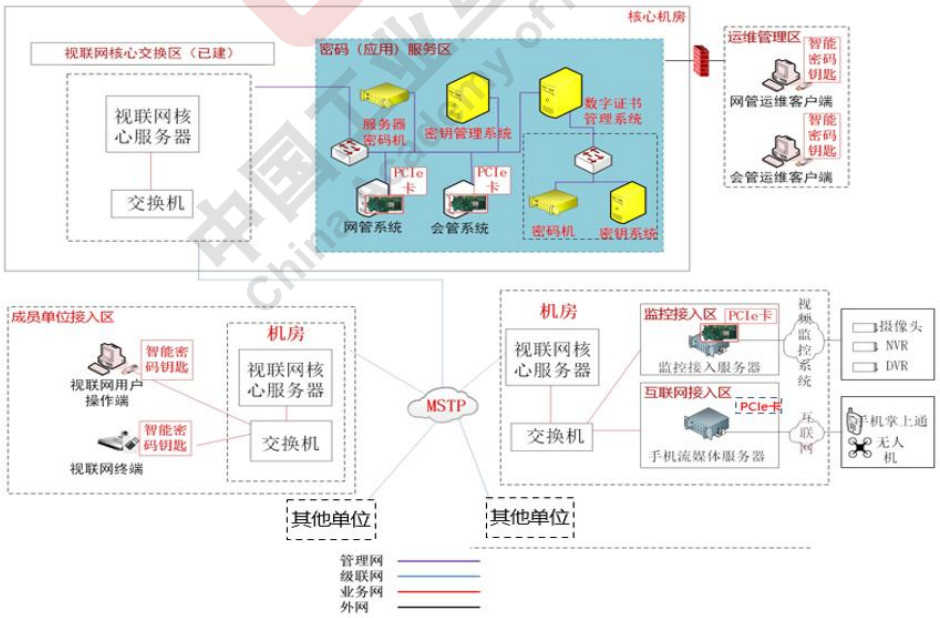

图 5.2 某省国密升级改造设备部署图

四、实施效果

（一）支撑地方政府的数字建设

2019 年，SecureV2V 自主安全协议及其系统在新疆完成试点建设，搭建了数十个点位的安全视频通信网络，并通过了三位院士主持的评审会，其安全性和创新性得到了肯定。

2020 年，海南省社管平台二期项目启动“一网两线”建设，涉及点位上千个。该项目基于国密算法加密的 SecureV2V 协议，是“一网两线、异构灾备”的新型网络安全防御体系。2020 年 5 月，启明星辰、绿盟科技、奇安信、神州希望对 “一网两线”系统进行攻防测试，测试结论良好，符合建设要求。

（二）推动技术融合与创新

网络安全信息安全的研究目标不断扩展，包括网络通信协议、网络体系结构等研究不断深化。本项目通过研究解决典型应用场景下的各种问题，积极申请相关专利和参与制定相关标准，不仅促进了国产密码技术在的深度应用，还能够为后续国产密码技术的应用推广提供参考

（三）促进视联网安全应用及视联网产业健康发展

SecureV2V 协议目前已成功实现在部分地区的试点应用，国产密码在视联网中的科学化、创新性应用有效地提升了系统整体安全性，可彻底改变传统体系中安全与业务分离的叠加设计理念，能够促进密

码技术在视联网安全应用中的健康发展，指导视频通信产业的安全应用推广和示范，为视联网在综合治理、电子政务、医疗教育等各行各业安全应用保驾护航。

（六）面向重要数据与个人信息保护的商用密码解决方案

牵头申报单位：北京炼石网络技术有限公司

联合申报单位：中国移动通信集团陕西有限公司

一、案例综述

（一）案例背景

电信运营商作为国内基础通信网络的提供者，业务支撑系统掌握海量的用户身份信息、位置信息、消费账单、通信使用状况、手机终端型号等数据。这些数据在流转过程中，因其蕴含的重要价值成为网络攻击的重点对象。因此，重要数据和个人信息的安全保护不仅是电信运营商的建设刚需，更是重要的社会责任。

而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，是安全的第一道防线，发挥保底作用。《密码法》《数据安全法》《个人信息保护法》《电信和互联网用户个人信息保护规定》等法律政策均要求采用商用密码等技术措施保障数据安全。为满足实战防护和合规要求，运营商亟需为应用系统叠加密码能力，构建安全可控的密码支撑体系，提升网络和数据安全保障水平。

（二）案例简介

本案例结合电信行业具体业务和需求，为电信运营商打造面向重

要数据与个人信息保护的商用密码解决方案。方案坚持“以数据为中心”的安全新思路，基于免改造商用密码技术，构建高覆盖率的安全增强点组合，融合识别、加密、去标识化、检测/响应、追溯等能力，有效保护结构化与非结构化数据，实现主体到应用内用户、客体到字段级的防护。

本方案可将安全更快更好的内建到电信业务系统中，全面应用于电信运营商业务支撑系统敏感数据保护场景、与上级数据同步解密场景、数据交互解密场景、大数据量表全量加密场景等，对重要敏感字段实现免改造加密保护，保障数据源头安全。

一、行业挑战

目前，电信运营商行业安全防护的功能性需求不足，导致其通过商用密码技术提升业务运行环节中各安全控制点的防护能力时，面临诸多挑战。一是通过大规模开发改造各类电信业务应用补充和增强安全能力，不仅周期长、难度高，而且风险大，一旦出现失误直接影响整个业务链正常运行；二是电信应用系统涉及的数据库版本和开发语言种类繁多，需统筹考虑解耦适配问题；三是电信业务支撑系统持续运转，通过加密保护敏感数据，必须保证不影响数据的高速读写和传输，且短时间实现快速切割上线；四是需充分考虑多层级信息系统加密功能的统一管理和可扩展性。

二、项目实施情况

（一）总体技术架构图及讲解

本方案结合国家法律法规及电信行业监管要求，以“敏感数据”为中心，以“电信业务应用”为抓手，基于免开发改造应用的密码技术、高性能国产密码和去标识化技术，结合部署在电信应用系统主路的AOE-Plugin、AOE-Proxy、高性能国密 SDK，以及 TDE 透明数据加密、TFE 文件安全、FDE 全磁盘加密等模块，形成高覆盖的数据控制点，横向覆盖营销与服务、业务开发与运营、资源与基础功能以及合作伙伴关系管理等应用，纵向叠加发现识别、加密等安全能力，实现集中式管控、分布式保护。本方案可在不影响电信运营商业务的前提下敏捷实施上线，实现敏感字段的有效保护。

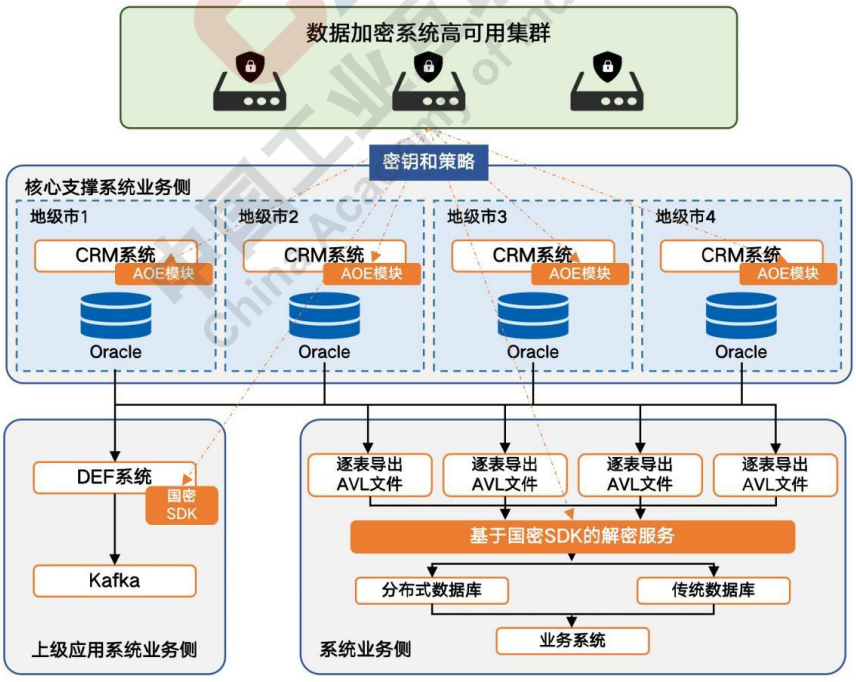

图 6.1 总体技术架构图

（二）应用场景架构图及讲解

业务支撑系统作为运营商核心系统，业务交错、数据量大、交流密集，包含众多敏感个人信息，且与外部多层级系统存在紧密联系。因此，本方案侧重以商用密码技术为核心，针对以下重点场景补足和增强密码能力，保障电信业务安全发展。

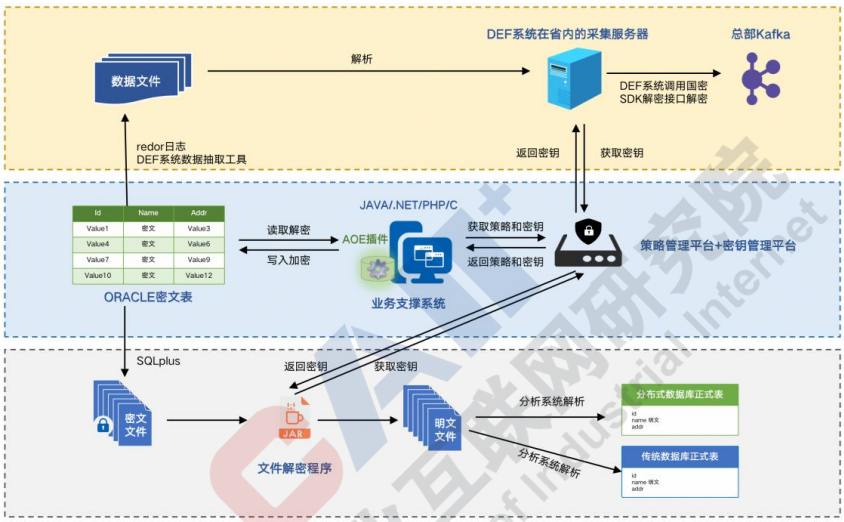

图 6.2 业务场景架构图

1、敏感数据免改造应用加密保护

电信业务支撑系统积累海量的敏感个人信息，在系统存储层、应用层、数据分发、访问控制、上云等环节均存在数据泄露威胁。本方案通过免改造商用密码技术，将数据加密模块以插件形式植入应用，可在不改造系统的情况下，针对上百个应用服务节点中的数十个字段进行策略设置，实现敏感字段的细粒度保护，并融合数据脱敏、密钥管理和策略管理等功能，提升电信系统数据安全防护能力。

2、各级应用系统数据同步解密

电信运营商业务支撑系统包含多个层级，如一级系统支撑总部全

网业务管理和业务运营，二级系统保障各省公司省内业务管理和业务运营。因此，该系统具有传输数据量大、实时性要求高、密文无法共享、存在传输风险等特点。本方案聚焦承载上报各省数据功能的 DEF 系统，通过集成高性能国密 SDK，支持国密 SM 系列算法，保障加解密不影响业务系统运行效率；同时按需加解密的实现，也可有效防止外部黑客拖库，内部越权访问，保障传输安全。

3、数据交互解密

电信运营商大量数据会传输到各级分析系统中，为保障后续数据使用正常，需要在传输过程中对数据解密处理。经过国密改造后的分析系统，解密程序采用多线程多任务处理方式，达到半小时解密几亿乃至几十亿条海量数据，实现高性能解密处理；且解密过程不改变原有业务流程、支持 AVL 文件类型、具备高可用、可配置等优势。

4、大数据量表全量加密

对数据库中现有历史明文数据进行全量加密处理，必然会影响到业务支撑系统的正常运行，如何将系统的割接影响降到最小，需考虑大数据量表全量加密。本方案解耦运营商系统使用的各类数据库品牌及版本，如 Oracle、SQL Server、MySQL、人大金仓、达梦等数据库，以及 JAVA、.Net、PHP、C 等语言；同时，支持多并发、多线程数据加密，适用于单表数亿条级别的数据加密、历史数据全量加密分批操作等，实现系统影响最小化。

三、实施效果

（一）打造电信密码应用新模式

本方案基于免改造应用的商用密码技术，为电信各类业务系统增强安全保护能力，保障海量重要数据和个人信息安全。同时，本方案优化算法实现，打造高性能加解密技术，对电信业务运行效率的影响降到更低。此外，在业务支撑系统等应用层以数据为抓手实现商用密码安全保护，使用加解密技术给数据重构“新边界”，为电信运营商打造防绕过的数据保护体系。

（二）理清统一安全管控新思路

本方案支持批量应用系统的分布式加密与集中式管控，通过统一的管理平台，实时掌握运营商总部与分支异地的多个应用运行状况，对应用中所有数据加解密状态、访问控制授权以及审计日志情况实现管理和监控，降低维护和运维成本。

（三）满足法律政策合规新要求

本方案可保障电信运营商核心数据资产不被攻击和泄露，满足国家和电信行业关于数据保护、信息系统商用密码应用规范要求，增强电信运营商对数据资产的安全控制权，提升个人信息在收集、存储、传输、处理等环节的安全性。

（四）走出各级复制推广新路径

本方案满足多项电信行业政策合规和实战防护要求，可快速在电信运营商内部开展平台建设、试点应用，实现一次建设、多重合规，避免重复投资建设，帮助电信运营商构建数据安全纵深防护体系。

（七）“5G+智能制造”商用密码解决方案

牵头申报单位：中国电信股份有限公司北京分公司

联合申报单位：三未信安科技股份有限公司

一、案例综述

（一）案例背景

5G 是新一轮科技革命和产业变革的代表性技术，是支撑数字经济社会发展的重要动力，是助力数字经济社会转型升级的关键网络基础设施，是“十四五”规划的重中之重，为构建现代化经济体系、实现经济高质量发展提供有力支撑。随着国家 5G 新基建战略的深入，数字化转型升级已进入高潮期，为了全面适应数字经济快速发展的新形势，积极应对全球国际竞争新格局，进一步增强我国在 5G 网络安全方面的主动权，加强自主可控的密码算法和密码产品的研发应用是保障 5G 作为国家重要信息基础设施安全的必要抓手。

近年来工业互联网安全事件层出不穷，国内外安全对抗也在不断升级，像台积电病毒入侵、海德鲁铝业网络攻击、委内瑞拉电网停电、伊朗电力系统瘫痪、以及最近的美国油气管网遭遇攻击等。

密码作为“保护信息、识别身份”的核心技术，将国密算法、技术和产品全面融入工业互联网中，一定能为智能制造行业出现的各种安全问题提供可靠的解决方案。

2021 年 12 月 28 日，工业和信息化部等八部门联合印发了《“十

四五”智能制造发展规划》，明确要求：“加强安全保障。加强智能制造安全风险研判，同步推进网络安全、数据安全和功能安全，推动密码技术深入应用。”

（二）案例简介

中国电信股份有限公司北京分公司联合三未信安科技股份有限公司开展 5G+智能制造国密应用创新项目，充分利用国产密码的优势，从增强的移动通信网安全需求、新技术驱动的安全需求和垂直行业驱动的安全需求出发，提升网络信息安全的自主可控和安全管理水平，全力支撑首都智能制造行业和工业互联网发展，助力智能制造和工业信息化安全建设。通过国产商用密码与 5G、智能制造的结合应用，逐步推进智能工厂协同创新平台的网络安全和数据安全的转型升级，促进智能制造自主、可控发展和升级。

二、行业挑战

智能制造行业具有高复杂性、开放性，连接平台的系统设备具有异构性，这些特征加剧其面临的安全风险。智能制造一旦遭到入侵或攻击将可能造成工业生产停滞，波及范围不仅是单个企业，更可能延伸至整个产业生态，重创国民经济，影响社会稳定，甚至威胁国家安全。

智能制造系统中接入设备异构，种类类型众多，海量异构工业设备接入智能制造平台时，连接条件和连接方式多样，存在大量不安全的接口。

同时终端设备资源受限。工业终端设备通常采用轻量化设计，存在计算、存储和网络资源等限制，且基于硬件的可信执行环境在工业边缘计算场景并未被大规模采用，这使得远离平台中心的终端设备容易遭受恶意入侵。因此需要提供轻量化的身份认证、可信验证、数据加密、隐私保护等高安全等级防护手段，增强终端设备的安全防护能力。

三、项目实施情况

（一）总体技术架构图及讲解；

5G+智能制造行业国产商用应用方案基于 5G+智能制造行业的基础架构，围绕 5G 专网通信、智能制造行业信息平台、终端的密码应用需求，将密码嵌入智能制造行业业务流程中，构建涵盖网络、智能终端行业平台、终端等层面的密码安全应用体系。

5G+智能制造行业，国产密码应用方案整体技术架构如下图所示：

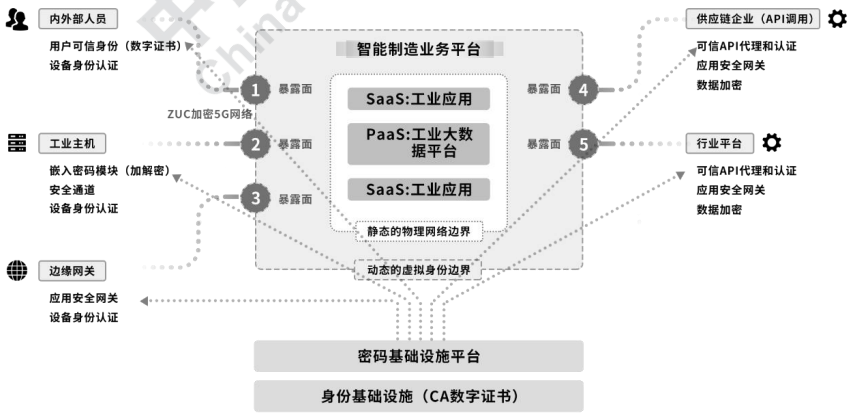

图 7.1 总体技术架构图

通过搭建的身份基础设施、密码基础设施平台，采用密码安全资源池/安全组件/服务等形式，为工业设备、控制系统、工业互联网平台、操作人员等提供 API 化的密码应用组件，将密码贯穿于智能制造行业的各个环节、场景，形成覆盖“端、边、云”的立体安全防护体系。

（二）应用场景架构图及讲解

本方案，主要涉及两个应用场景:

1、5G 网络接入采用 ZUC 密码算法

5G 网络接入阶段，满足数字化应用的大带宽、低延迟、高可靠优势下，解决安全性不足问题，形成安全通信解决方案，对基站和终端通信采用 ZUC-128 商用密码算法进行机密性和完整性保护。

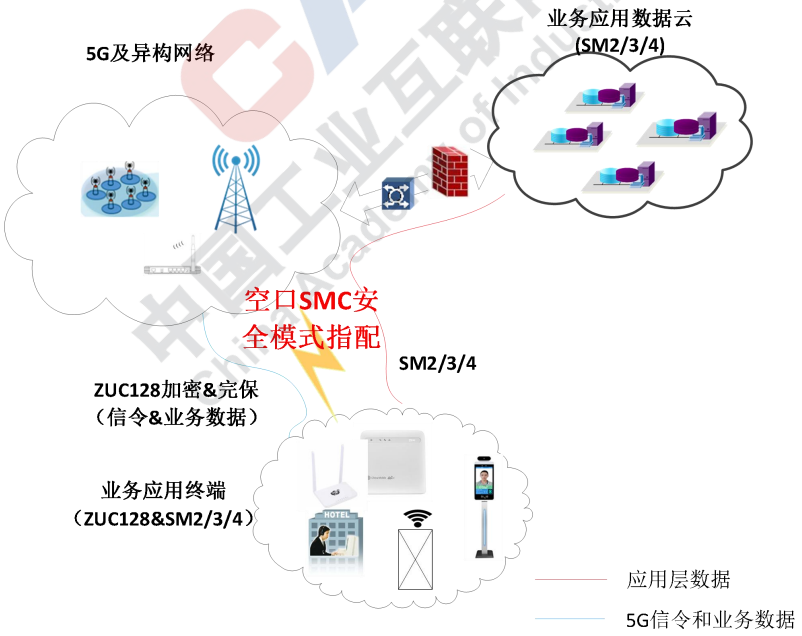

图 7.2 5G 网络接入场景

5G 终端和基站的空口、终端和核心网的 NAS 接口采用 ZUC-128 的机密性和完整性安全保护。业务应用层数据采用 SM2、SM3、SM4

的机密性和完整性安全保护。

2、智能制造业务重要数据保护

在 5G 接入网采用 ZUC 密码算法的基础上，在智能制造业务应用层如 5G+AGV、工业视觉、视觉监控、数据采集等采用 SM2、SM3、SM4 等国密算法，保障控制指令完整性、视频监控完整性、设备身份认证、企业敏感数据保护等。对于所有远程接入的通信过程都需要进行加密保护，防止窃听、篡改、伪造、重放等行为，同时从应用和内容层面防止机密数据的泄露。

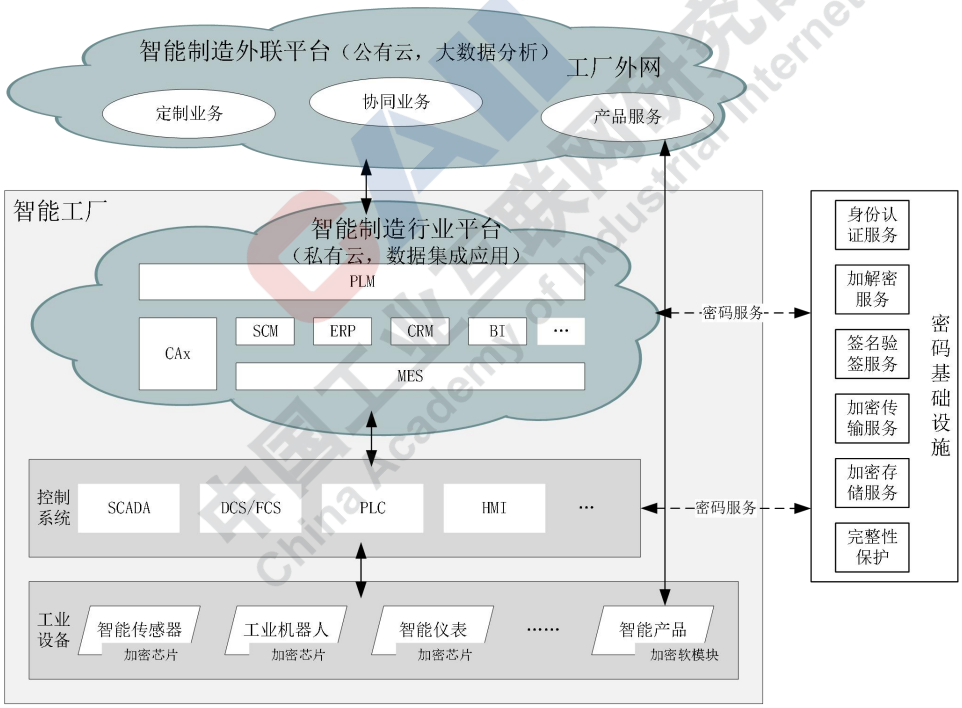

图 7.3 智能制造业务应用层密码应用场景

通过在各种智能制造终端上植入密码软模块/密码芯片，实现设备层的密码应用能力；密码基础设施实现了各种密码服务能力，如身份认证服务、加解密服务、签名验签服务、加密传输服务、加密存储

服务、完整性保护服务等，以组件化的密码服务 API 模式提供统一的密码服务，便于智能制造业务应用平台集成和快速改造，实现端到端的密码安全加持和赋能，密码融入和贯穿于智能制造的各个应用场景、环节中，内生于智能制造。

密码基础设施通过统一配置管理提供先进的、实时的、自动化、智能化的密码运营管理能力，支持密码服务创建、发布、上线、下线、销毁等环节的全流程全自动部署，在不影响业务实时运转的情况下，实现灰度部署，密码服务快速发布上线，自动回滚、自动备份。本方案能够有效保障智能制造企业应用的安全，且达到网络安全等级保护制度三级要求，符合商用密码应用安全性检查要求。

本方案在三一重工智能制造工厂得到了大力应用，覆盖了南口桩机、回龙观园区两张专网，涉及 5G+AGV、工业视觉、视觉监控、数据采集四大类业务，在 1000 多台设备（包括 5G 摄像头、控制柜、AGV、工业 Pad、控制 PC 等）上增加密码能力，推动国密在 5G+垂直行业中的融合发展，提高国产商用密码算法在工业信息化中的应用广度和深度。

四、实施效果

（一）推动了国密算法在智能制造行业的应用，降低智能制造行业应用密码门槛，成果易推广、可大规模复制

密码是国之重器，关乎党和国家安全，是我们党和国家的“命门”、“命脉”，习近平总书记高度重视密码工作。密码关系国家政治安全、

经济安全、国防安全和网络安全，关系社会组织和公民个人的合法权益。商用密码工作是密码工作的重要组成部分，在维护国家安全、促进经济发展、保护人民群众利益中发挥着不可替代的重要作用。在智慧制造行业中大力推广国产商用密码算法，有利于消除国外密码算法带来的算法风险。

（二）自主可控，掌握核心技术

构建从密码到网络全面自主的新型基础网络，是我国信息化发展、掌握核心技术的新方向。这种全新的技术路线，能够改变网络通信技术领域的被动叠加式安全防护理念，开创出在基础网络层面解决安全问题的全新技术体系，在国家信息化建设、新型互联网应用、传统产业升级、打破信息流通结构性障碍等方面发挥重要作用。

网络安全就是国家安全。摆脱西方 IP 技术体系的制约，实现从密码到网络的全面自主可控，是维护我国网络空间自主控制权的必经之路。只有在网络协议与密码应用的深度融合方面持续进行自主创新，才能够真正构建“中国人自己的网络”，牢牢把控网络空间安全的自主控制权。

（三）促进商用密码和智能制造行业深度融合，统一规划，集约和集中化建设

构建全方位的智能制造行业的密码应用安全体系，统一规划密码能力建设，充分考虑满足智能制造业务对轻量级、低时延加密认证的需求，实现一体化、集约化建设，提供从芯片级、到整机、到系统级、以及平台级的国密产品和服务，实现业务深度融合。采用顶层设计、

一体化建设、多点服务的集约化建设和服务模式，实现统一管理、按需服务、深度融合、快速部署、端到端的密码服务体系，避免重复投资、分散建设、重复建设等问题，有效减少智能制造企业的密码应用建设资金投入。

（四）保障智能制造业务安全，促进智能制造自主可控发展

构建全方位的智能制造行业的密码应用安全体系，提供从芯片级、到整机、到系统级、以及平台级的国密产品和服务，实现业务深度融合，解决了智能制造业务面临的网络窃取、企业核心商业数据篡改和窃取等各种网络和信息安全风险。

构建从密码到网络全面自主的新型基础网络，是我国数字转型、掌握核心技术的新方向，实现从密码到网络的全面自主可控，是维护我国网络空间自主控制权的必经之路。基于智能制造密码应用项目，突破多种密码技术，在智能制造行业与密码应用的深度融合基础上，丰富商用密码产品的应用场景和形态，推动我国商用密码产业发展，持续进行自主创新和可控发展，安全有序引导制造业向数字化转型，推动“中国制造 2025”安全健康发展。

（八）面向 5G 电力专网的双 CII 域国密应用实践

牵头申报单位：中国移动通信集团山东有限公司

联合申报单位：中国移动通信集团有限公司信息安全管理与运行中心

中移（杭州）信息技术有限公司

一、案例综述

（一）案例背景

随着国家首次对密码工作进行立法，推动信息安全产品/系统实现自主可控，支持国密算法是大势所趋。同时国外密码算法风险增加、传统证书存储模式弊端显露，基于硬件的国密算法是行业刚性需求。

《关键信息基础设施安全保护条例》出台明确关键信息基础设施，电力行业的业务形态和终端形态均向多样化发展，原有的电力专网平台体系结构已难以满足电力业务需求的发展。由于 5G 的 MEC 节点部署在靠近用户的网络边缘，受运营商的控制力减弱，因此更易被实施攻击行为。

（二）案例简介

面向的 5G+电力双关键信息基础设施（Critical Information Infrastructure，简称 CII）场景，以商用密码技术应用为核心，设计并实现了 5G 智能电网“端、网、边”三位一体的纵深防护体系，对 5G 网络和电力系统两大关键信息基础设施起到关键性的防护，形成三项

创新。

1、以“SIM 盾”为载体的分层共治接入认证：以 EAL4+安全芯片为载体，实现基于国密的多层密钥离管理机制。基于多层密钥管理机制，实现分层共治接入认证。

2、基于 SIM 卡的一机一密组件的数据保护：实现密钥分区隔离和基于业务的密钥派生，基于安全 SDK 实现对业务数据、控制信令加密传输保护。

3、基于 SM9 的轻量化边缘计算应用安全认证：基于 SM9 实现轻量化认证，并实现轻量化身份验签流程、多维度身份认证能力。

二、行业挑战

5G 电力专网通过网络切片、核心网下沉、边缘计算等技术实现了低时延接入和个性化管理，同时新技术、新场景带来新的安全需求，特别是设备接入安全、生产数据安全和边缘计算安全。

在 5G 终端接入安全方面存在安全挑战，如非授权的 SIM 卡接入网络、冒用正常 SIM 卡接入网络、未经授权接入生产专网或者接入特定系统，造成非法/恶意访问。

在 5G 电网数据安全方面存在如下安全挑战：终端侧的数据被窃取、数据在传输过程中被截获以及位于边缘侧的数据被非法访问。

在 5G 边缘计算的安全方面存在着如下安全挑战：恶意边缘计算 APP 访问内部系统导致业务数据泄露、未授权的边缘计算 APP 调用 MEP 的能力以及边缘计算 APP 间的未授权访问。

三、项目实施情况

（一）总体技术架构图及讲解

本方案重点关注解决基于运营商 5G 通信网 CII 和电力行业 CII 的业务安全需求，通过在 5G 通信网使用国密 SM9 系统，为 APP 提供便捷的认证服务，杜绝非法用户接入，保障 UPF 的安全。通过基于 SIM 卡的二次认证，实现合法用户安全接入电力 IDC 业务，保障系统安全，从而全面保障双 CII 的 5G 终端接入、5G 电网数据安全和 5G 边缘计算的安全。

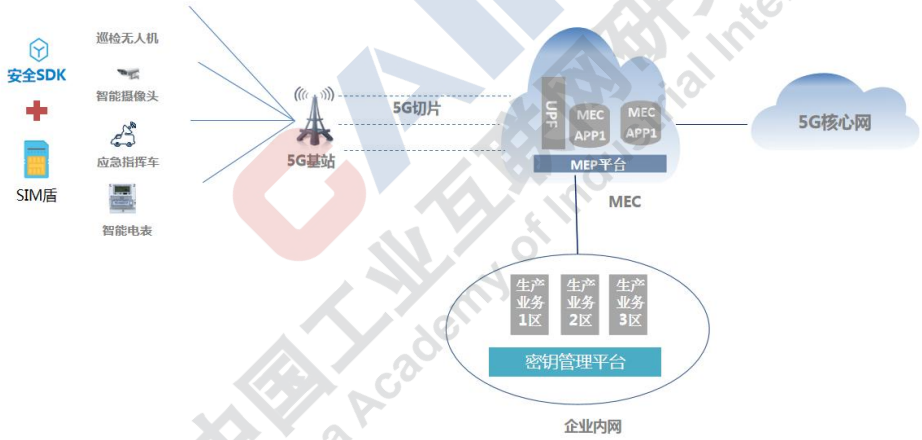

图 8.1 总体技术架构图

（二）应用场景架构图及讲解

1、以“SIM 盾”为载体的多层共治接入认证

以 SIM 盾为核心构建面向 5G 电力专网的多层共治接入认证机制，实现入网、 入区、入系统的分层级、高安全认证，同时实现网络运营商与电力运营商对接入认证的协同治理，满足分层、分域、细

粒度的访问授权，支撑电力专网零信任体系。

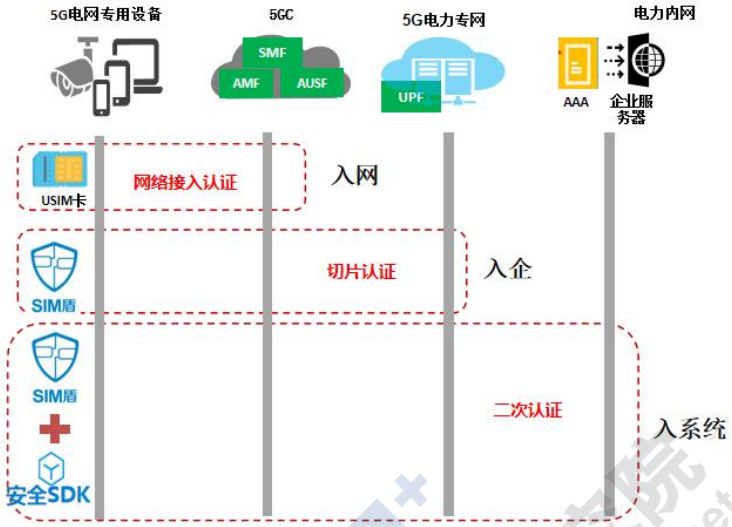

图 8.2 SIM 盾认证机制

以 SIM 盾为核心构建面向 5G 电力专网的多层共治接入认证的创新点如下：

- ✓ 入网：基于 USIM 5G AKA 机制实现 5G 网络接入，由运营商管理。
- ✓ 入企：基于 SIM 盾和基带芯片配合，利用 SIM 盾预置的切片认证密钥，通过 EAP-AKA 实现企业专用切片接入认证；运营商与电力企业协同管理。
- ✓ 入系统：基于 SIM 盾实现电力企业内网访问控制，电力企业管理。

图 8.3　SIM 盾创新升级

2、基于 SIM 卡的一机一密端到端数据加密保护

依据“安全分区、网络专用、横向隔离、纵向认证”电力监控系统防护原则，基于具备国密型号的 SIM 卡一机一密安全加密能力实现 5G 电力数据的安全加密、安全计算、安全传输。

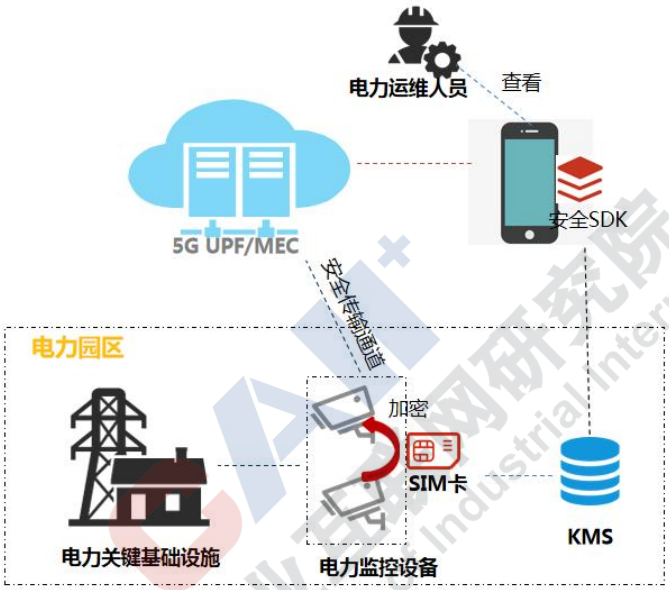

图 8.4 电力行业应用场景

基于 SIM 卡的一机一密端到端数据加密保护的安全方案的创新点如下:

- ✓ 基于业务唯一性的密钥派生机制，由根密钥、卡序列号、业务类别派生密钥，可以根据一个会话产生一个密钥、一个卡号产生多个密钥;
- ✓ 密钥分区隔离安全存储，保证每个密钥安全管理，防止密钥信息被非法访问;
- ✓ SIM 卡 SE 保障核心数据安全，5G 电力核心数据计算在 SIM

卡 SE 中完成；

- ✓ 视频数据关键帧加密，对 5G 监控设备视频数据关键帧进行加密，满足低功耗设备上 4K 视频加密需求。

四、实施效果

（一）账号统一管控，提升安全性

为 5G 电力专网统一并简化系统账号管理，方便系统互联互通，使用 SIM 盾解决账号众多、身份验证繁琐、权限分配复杂等身份认证领域问题，减少冗余账号、错漏账号发生的可能性，凸显手机号码对电力业务系统的价值。

（二）多种国密算法助力关基安全

支持如 SM2、SM4、SM9 等多种加密算法，利用 SIM 卡 EAL4+安全载体实现密钥安全管理和运算，可调用 API 接口可实现数据本身的加密，实现自身和对外的数据安全防护能力，预估效率提升 30%。

（三）系统易用，部署难度降低

采用 SM9 标识密码算法，在同一套密码系统中将身份认证与基于策略的数据加密有机结合在一起，节约服务器资源 20%，降低系统部署复杂度，降低用户使用门槛。

（九）基于轻量级国密算法的物联网安全解决方案

申报单位：深圳奥联信息安全技术有限公司

一、案例综述

（一）案例背景

随着国办印发的《金融和重要领域密码应用与创新发展工作规划（2018—2022 年）》、《网络安全法》《密码法》《数据安全法》《关键信息基础设施安全保护条例》《物联网新型基础设施建设三年行动计划（2021-2023 年）》等法律法规的相继发布，对石油行业及其物联网系统采用密码技术实现数据的安全保护和应用水平提出明确的要求。

石油行业是我国重要的关键基础设施，石油工业设备终端多架设在偏远地区，依赖互联网或者 TCP/IP 网络对工业设备及终端进行管控。由于设备工业控制系统使用的 RFID、传感器等芯片不同于传统的台式机和高性能计算机，网络环境存在计算能力、存储资源、功率消耗、带宽等受限。轻量级密码算法对比传统密码技术在物联网大并发、海量数据、低延时等要求下具有明显优势，可有效降低成本、提升效率、节省能耗，让密码技术真正在石油工控系统的全生命周期数据安全保护中发挥作用。

（二）案例简介

本案例按照油田控制系统中网络传输、认证、存储安全需求，以轻量级密码算法 SM9 为核心，综合部署轻量级密码产品体系，为油田工控系统提供“轻量、高效、安全”的整体安全解决方案，在人员办公协助系统、工业控制操作系统、视频监控系统、终端设备数据采集方面，实现身份认证、传输加密、存储加密、防泄密、防篡改、抗抵赖等功能，避免了越权访问、横向控制等多种安全问题，达到密码测评三级要求。

二、行业挑战

油田控制系统以往依赖于互联网或者 TCP/IP 网络对工业设备及终端进行管控，工控系统从硬件层到软件应用层均可能存在安全隐患，且随着信息化系统的复杂程度越来越高，系统脆弱点和漏洞越来越多，传统的网络安全技术已不能保障工控系统的安全性。

在该案例中，项目的油田信息化系统建设初期规划已不能满足现代安全需求，各办公设备、业务系统、密码使用相对独立和分散，缺少统一管理。一是当前在用的办公设备主要包括：云桌面、交换机、监管系统等，这些设备目前数据传输均采用明文方式，且接入服务端系统的认证仍使用传统方式；二是在工控网络、视频监控网络中的设备缺少统一认证、统一管理及数据安全存储；三是针对现有工作人员，以往口令式的身份认证系统已不能满足现有业务发展需要。亟需建设一套安全轻量的密码服务设施，为办公系统、工业控制系统、视频监

控系统等提供数据全生命周期安全保护。

三、项目实施情况

（一）总体技术架构图及讲解；

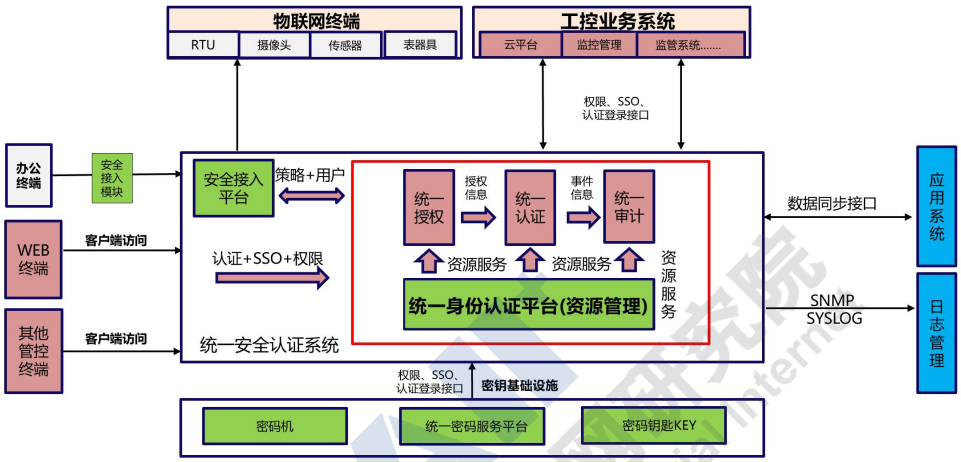

图 9.1 总体技术架构图

密码基础设施。包含服务器密码机（硬件）、统一密码服务平台（软件），提供数据加解密、密钥生成及密钥管理；密码钥匙 KEY，用于超级管理员、操作人员的身份认证。

统一身份认证平台。业务系统中的安全管理、交换机、云平台等通过接口与统一身份认证系统进行集成，实现统一的认证、用户管理、SSO、策略管理等功能。并由管理员统一管理维护各系统的用户账号、权限信息等。登录各系统时，均到用户统一认证系统进行认证，认证方式支持口令、USBkey、短信、SM9 挑战应答等多种方式，认证通过后并根据所属权限访问对应的系统。

安全接入平台。基于 IP 网络进行数据传输的应用，通过采用密码技术解决人员及设备认证安全和数据传输安全问题。通过在终端前

增加安全接入网关/模块的方式，与服务端安全接入平台进行认证并建立安全传输信道。办公终端的用户账号和访问策略信息由统一认证系统进行统一管理，办公业务终端接入时，安全接入平台到统一认证系统获取用户和策略信息

（二）应用场景架构图及讲解

在某油田项目中，分为二期工程实施:

一是改造办公区业务系统，实现密码安全能力集成。在不改变原业务系统情况下，通过部署密钥基础设施及统一身份认证平台实现增强级的人员身份认证、安全接入、以及数据加密传输、存储保护，覆盖办公类桌面系统、云平台、监控系统、监管系统等，经过授权机制实现单点登录，即授权工作人员一次安全认证即可登录多个系统，目前已为该油田项目 4 万多工作人员提供安全服务。

二是建设工控系统安全接入平台，为操作系统、视频监控系统及物联网设备终端采集系统提供数据全生命周期安全保护。项目上涉及种类多样的操作业务系统、摄像头、RTU、TTU 等终端设备或软件程序，需要对采集的数据进行加密处理。本案例核心应用 SM9 算法，具有标识加密、无证书、速度快、低带宽占用等优势，非常适合海量物场景下的数据加密及认证，在项目上已为 8000+终端设提供安全保障，为业务系统数据采集、传输、存储、共享进行全方位

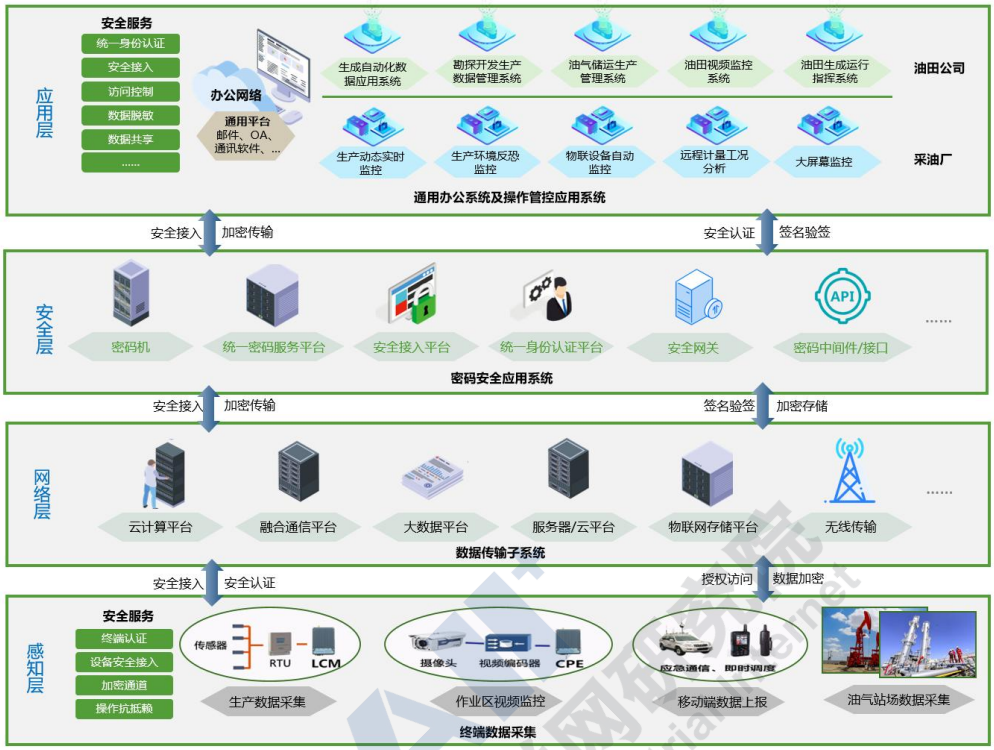

图 9.2 石油工控系统密码应用架构

案例基于四个层面（应用层-安全层-网络层-感知层）实现数据流转的整体安全，从感知层终端数据采集开始，在磕头机、RTU、TTU、LoRa 网关、无线通信、摄像头等终端设备前端部署安全网关/模块，提供安全认证及安全接入，与网络层间构建安全传输通道，在数据流转过程中保证数据的完整性、真实性、可用性及防篡改。安全层为密码产品应用层，通过构建密码基础设施及密码安全平台，以标准接口对接石油工控系统各个平台及业务系统。在应用层通过人员强身份认证及授权访问机制进入业务系统获取并使用数据图表。针对敏感信息，结合数据脱敏技术，保障数据不被非法窃取和泄露，实现“数据可信，安全可控”的防护目标。

四、实施效果

（一）安全合规，符合等保及密评要求

方案所采用安全产品已通过国家密码管理局及公安部认证，获得商用密码型号证书及安全检测证书，实现国产化自主可控，符合等保、测评等政策标准要求。

（二）为石油行业提供轻量级密码应用示范

案例以轻量级密码算法 SM9 为核心，具备高效、短签名、低延时、低消耗等特点，能够为超大量数据提供高效率的加解密、传输、存储、交换等安全功能。通过部署统一密码服务平台，提供密码综合治理能力，全方位保障数据隐私，方便客户自我管理和维护，降低人工及维护成本，并支持后期业务拓展需求，为客户提供一次建设，多级使用的密码安全服务。项目完成后，已服务 4 万+用户，采集端设备覆盖 8000+个，为产业形成示范效益。

（三）降低系统损耗，减少部署成本

在案例实践中，传统 PKI/CA 证书费用较高，而且面临一个主要挑战“物联网场景下由于传输带宽不足导致的网络延时问题”。项目通过应用轻量级算法 SM9，由于算法的无证书特性，在安全可靠的同时节省了大量的证书费用。在带宽方面，通过软件密码模块结合无线通讯方式，每个信道占用带宽只有几十 K，不容易受到同频干扰，误码率极低，保证了工业数据传输的稳定和准确性，且在上位机易控组态软件完成通讯，在 PLC 端无需编写任何程序，使用简单，大大降低了设备的维修费用、备件费用和人工费用，创造了良好的经济效益。

（十）数字政府（政务云）平台密码应用

申报单位：卫士通信息产业股份有限公司

一、案例综述

（一）案例背景

数字政府政务云平台汇集处理整个地区的电子政务业务，海量数据资源高度集中形成价值高地，大量的政府公共敏感数据、个人隐私数据等安全亟需防护，开放的互联网访问方式加剧了平台信息泄露的风险。

数字政府政务云平台属于国家关键信息基础设施，依据《国家政务信息化项目建设管理办法》（国办发〔2019〕57号文）要求，需要根据《信息安全技术 信息系统密码应用基本要求》（GBT 39786-2021）采取相关密码应用防护措施。

（二）案例简介

本案例设计了政务云商用密码应用体系，为政务云安全提供全方位密码保障支撑，实现政务云环境下各业务系统的数据全生命周期过程的机密性、真实性、完整性，达到业务处理过程的安全性、数据信息的可管可控，并可对政务云上运行的各种内部信息、行政事务信息、经济信息等进行加密保护，为各政务单位在处理政务云业务上提供统一认证、访问控制、单点登录、数据加解密、电子印章等密码应用的密码服务。

本案例可用于指导政务云密码应用建设，建设范围主要包括对政务云数据中心、委办厅局、异地灾备中心等的区域或单位信息系统的密码应用建设。

二、行业挑战

数字政府加快推进“互联网+政务服务”，建设统一的政务云平台，为政府及其部门提供协同、共享的基础信息平台服务。密码是数字政府网络安全建设的基石，在数字政府建设中，商用密码在云和大数据环境下主要面临以下主要挑战：

（一）云和大数据计算环境下对密码的“高性能”挑战

云和大数据环境下，大资源的密码运算，需要高效规模化的密码运算技术、高安全的多租户密码保护隔离技术、高可靠的密码智能集群聚合技术的大量应用。

（二）业务上云对密码的“服务化”、“虚拟化”挑战

商用密码应用开发和集成方面积累较少，商用密码的应用集成能力较少。密码产品形态、部署方式以及商业模式面临云计算中的服务化、以及云环境中虚拟化应用的需求挑战。

（三）业务应用对密码的“易用性”挑战

当前，缺乏统一、完善的密码应用技术对接标准和应用指南性标准，密码服务接口不统一。密码服务不同的接入方式和接口方式在运营、维护、服务等方面存在差异化的要求，导致密码难用、不好用。

（四）服务化对密码“运营管理”挑战

为满足政务信息系统密码应用需求，云密码服务的服务质量标准如何制定、提供哪些标准化密码服务等都对如何进行密码运营管理提出了挑战。

三、项目实施情况

以我公司实际承接并承担建设的“某省数字政府政务云密码应用试点任务”一期为例进行介绍，数字某省已经对接完成 62 个，正在对接 20 多个厅局 100 多个业务系统，其中正在对接的移动办公服务于 100 多万公务员。

（一）总体技术架构图及讲解

数字政府政务云密码应用方案，基于政务云平台的基础架构，围绕云平台、网络、云上业务的密码应用需求，以密码安全合规使用为核心目标，构建涵盖云平台、业务系统、终端、网络边界及通信等层面的密码应用保障体系，实现密码技术的有效使用和密码资源的合理分配。

政务云平台密码应用保障体系包括密码服务及管理支撑、云平台及业务系统密码应用、云平台管理安全密码应用、网络与接入安全密码应用、异地灾备中心密码应用、委办厅局用户终端安全密码应用、移动端安全密码应用，以及密码安全管理和密码安全运维。政务云平台密码应用体系架构如下图所示。

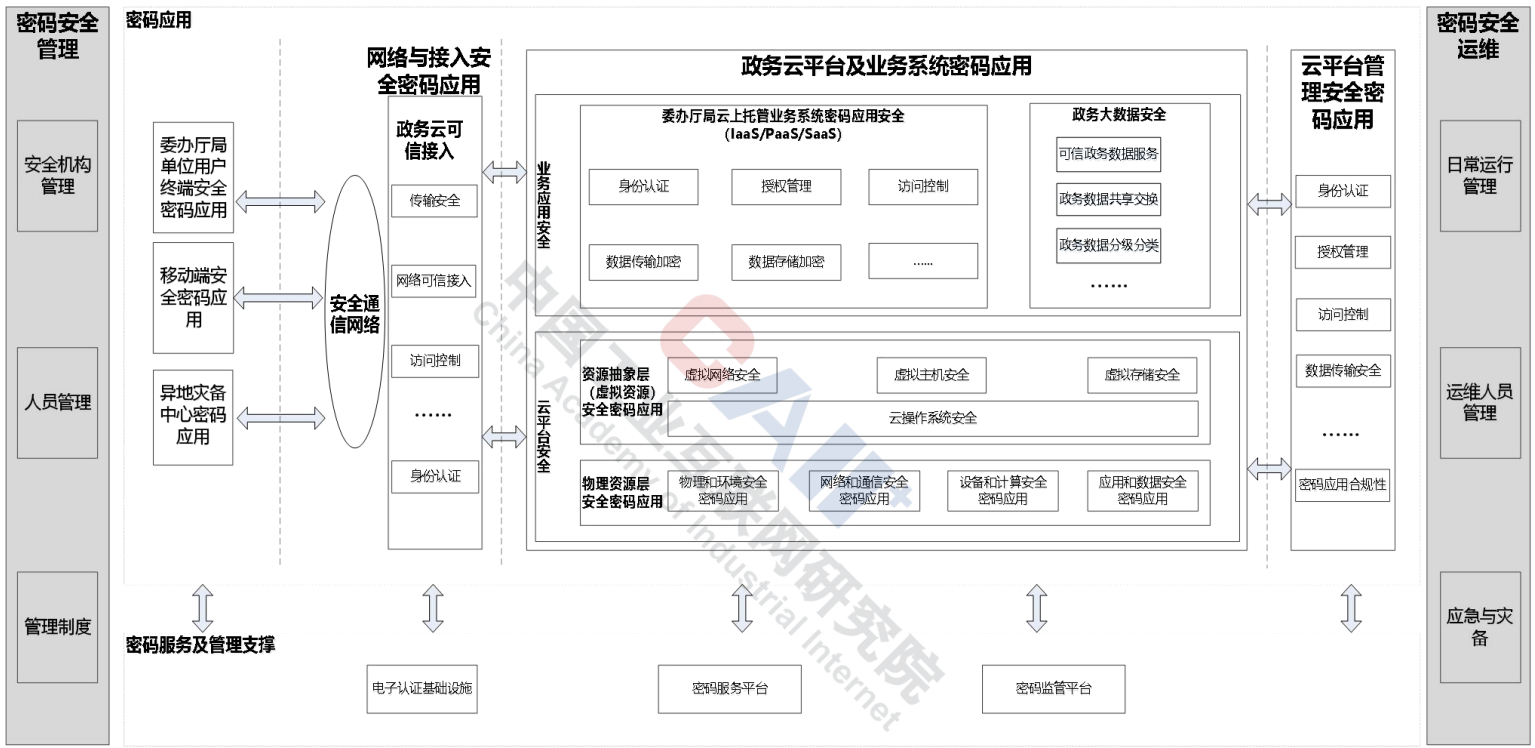

图 10.1 数字政府（政务云）密码应用总体框架

密码服务及管理支撑主要包括电子认证基础设施、密码服务平台和密码监管平台。电子认证基础设施为政务云平台的用户提供数字证书服务。密码服务平台为业务应用提供证书管理服务、密码计算服务、密钥管理服务、身份认证服务、时间戳服务、电子印章服务等。密码监管平台面向密码监管需求，对密码资源、密码产品的状态进行汇集采集，结合密码合规性标准，形成多维度呈现能力。

云平台及业务系统密码应用包括云平台密码应用和业务应用密码应用。云平台密码应用包括了物理资源层安全密码应用和资源抽象层安全密码应用，需满足等级保护三级的相关要求。物理资源层安全密码应用以密码作为基础支撑，从物理层面采用技术措施保证物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全。资源抽象层安全密码应用包括云操作系统安全、虚拟网络安全、虚拟主机安全、虚拟存储安全，为政务云平台提供虚拟资源安全保障。

业务应用安全密码应用主要包括委办厅局托管业务系统密码应用安全和政务大数据安全。托管业务密码应用安全包括对政务云平台访问人员的身份认证、访问控制、数据安全等。政务大数据安全包括政务数据分级分类、数据共享交换、数据可信等。

云平台管理安全密码应用包括身份认证、授权管理、权限控制、数据远程传输安全等实现基于对云管理的业务系统、数据、传输安全，同时还需要对密码合规性进行管理。

网络与接入安全密码应用主要包括对网络通信过程中数据传输加密、对接入用户的身份认证和访问控制并保障接入设备、系统的安全可信。

异地灾备中心密码应用主要包括对灾备中心的数据存储加密、管理人员的身份认证及访问控制。

委办厅局用户终端安全密码应用主要包括对省直单位终端自身的安全防护、终端用户的身份认证以及终端存储和处理数据的安全保护。

移动端安全密码应用主要包括对移动终端人员的身份认证、移动终端数据的存储加密、移动终端的密钥管理等。

密码安全管理从密码应用的安全制度、密码应用的人员以及密码应用组织机构等方面进行安全管理。

密码安全运维从密码使用的日常运行、运维人员以及应急与灾备等方面对密码应用进行运行保障。

（二）应用场景架构图及讲解

政务云密码服务平台为政务业务提供终端密码能力（支持移动终端本地数据加密保护）、身份认证服务、传输加密保护、重要业务数据保护、数据库和文件存储加密等安全防护，应用场景如下图所示。

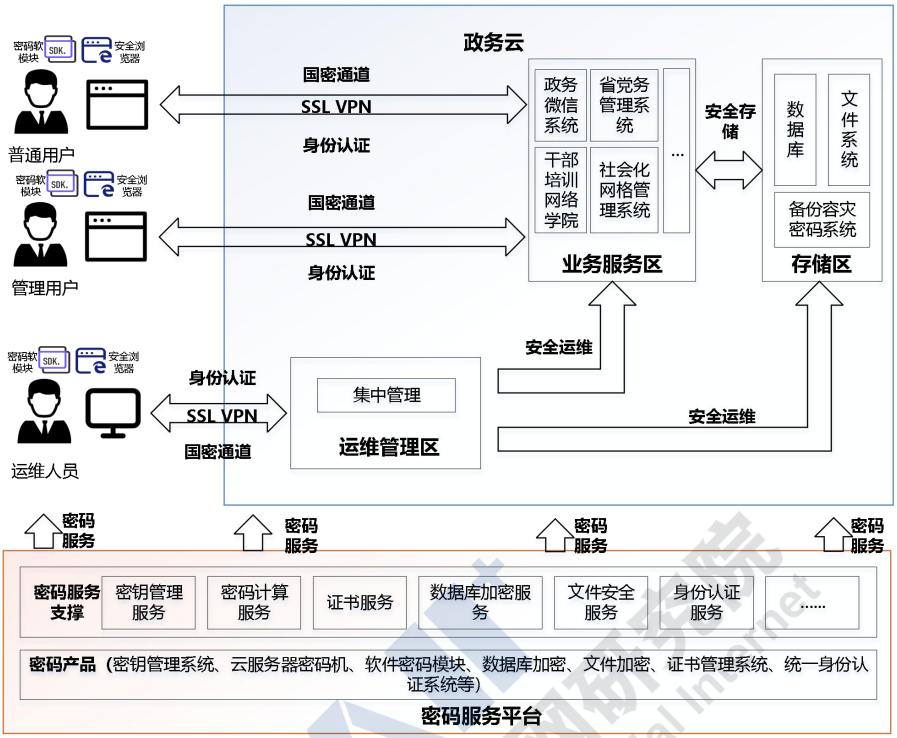

图 10.2 政务信息系统应用场景

密码服务平台：为满足政务云上各应用系统的数据签名/验证，数据加密/解密等密码服务需求，密码服务平台采用了适用于政务云、大数据环境下的云密码资源池系统。云密码资源池系统相关组成部分采用了一系列关键、核心技术，创新提出并打造政务云平台一体化密码应用保障体系；突破了多项在复杂云和大数据环境下密码应用的关键技术基，成功应用与某省政务云并拓展至全国多省市政务云，为密码产业注入新活力。

政务微信系统：将密码服务SDK套件部署于手机端，嵌入政务微信，提供商用密码算法实现、对政务单位工作人员的认证与鉴权、政务微信业务的加解密服务和本地密钥维护及在线密钥获取等功能，可实现跨政务单位的加解密能力。

备份容灾密码系统：在政务云两地三中心备份架构中，采用商用密码算法对政务云平台数据进行加密存储，保障存储系统内部数据安全，同时提供用户身份认证、权限管理等多种保护措施，构建可靠的数据存储系统和数据保护体系，已经陆续接入 12 个厅局单位，58 套业务系统，涉及业务主机 206 台，备份作业 242 个。

四、实施效果

（一）解决了密码应用在政务云及云上业务应用的难题，使密码变得可用、易用，成果可推广、可复制。

推动密码应用在云和大数据环境下的大规模、多场景、移动化、智能化应用。解决方案在党政领域多个省市进行应用推广，并成功进行签单和产品部署，主要包括海南省、宁夏、浙江、广东等多个省部级政务云，成都、中山等3个市级政务云，共涉及80多家政务部门。成果可以复制到金融、电力、军工、保险等行业。其中，数字广东正在对接20多个厅局100多个业务系统，对接的移动办公服务于100多万公务员。浙江政务云完成20多个业务系统对接，后续计划接入上百个业务系统。2021年产品填补了SM9算法空白，实现了鲲鹏、UOS互认，同时系统并发、响应、批量短报文加密性能分别提升10倍、20倍、400倍，部署时间从5-7天缩短到1-2天，应用适配从6周缩短到0.4-2周，应用快速适配模式初步建立。

（二）促进密码与数字政府建设深度融合，节约建设资金，保障政务云上数据安全。

基于方案的落地性项目实施完成，可以实现密码应用一体化、集约化，避免各省部级政务部门重复投资、分散建设、重复建设；解决了政务云密码的落地使用、密码同业务应用深度结合、密码保障数据安全等问题，通过项目试点应用，实现对身份认证、授权管理、数据传输、数据存储加密，有效降低系统遭受黑客攻击、入侵和数据泄露，提高了数字政府建设的安全水平，保障了数据安全，有效减少数字政府因网络攻击和数据泄露造成的资金损失。通过构建集约化、轻量化、服务化、标准化的密码服务新模式，避免各政务部门重复投资、分散建设、重复建设等问题，节约建设资金。

（三）保障国家网络安全主权，推动密码产业发展。

解决方案所推进的密码应用经济易用、平台适应性强，促进了密码与国家重大战略、新技术新应用、数字政府改革的深度融合发展，可进一步推动密码应用与创新发展。基于解决方案在全国各省市推进的数字政府密码应用项目，形成密码服务平台产品 1 套（含有商密认证证书的密码产品 6 种），实现政务应用系统基于云密码资源池的身份认证、签名验签及数据加解密等功能，保障政务云平台运行安全。

通过在政务领域关键信息基础设施进行密码应用保护，推广到金融、电力、能源等其他行业关键信息基础设施保护，维护了国家网络安全主权，促进了数字经济发展，保护了人民群众利益。基于落地性项目，突破多种密码技术，打造多种密码产品，丰富商用密码产品的种类和形态，推动了国家密码产业发展，提升了国家网络安全保障水平。

（十一）杭州市数据资源管理局密码服务平台建设

牵头申报单位：杭州安恒信息技术股份有限公司

联合申报单位：杭州弗兰科信息安全科技有限公司

一、案例综述

（一）案例背景

自 2020 年 1 月 1 日起《中华人民共和国密码法》正式施行，标志着我国在密码的应用和管理等方面有了专门性的法律保障。《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》自 2021 年 10 月 1 日起的正式施行，规定了信息系统第一级到第四级的密码应用的基本要求，适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

杭州市作为中国互联网之都，致力于数据资源的开放、共享和基于大数据技术的开发与利用。然而大数据技术引发的数据利用的新模式与保护数据安全之间存在着天然的冲突，数据的高共享和高利用势必会加大数据泄露的风险，形成了数据利用与保护国家重要数据资源和数据利用与保护个人隐私等多方面的矛盾。为有效促进该市大数据产业的健康发展，加强对政务数据资源的安全保障能力，需要建立全

市数据安全国产密码保障体系。

（二）案例简介

杭州市数据资源管理局密码服务平台建设项目（简称“本项目”）具备多业务场景下的密码安全综合性服务保障能力，构建了形成以“大数据+国密”为驱动的国产密码防护体系，为各个用户单位的信息系统顺利通过密码应用安全性评估奠定坚实基础。

本项目中的密码服务平台以商用密码资源池为基础，通过集成基础密码应用、终端密码应用等能力，为云上信息系统提供密钥管理服务、密码运算服务、移动终端密码服务等，保证政务用户可信、政务数据可靠。

云上信息系统可根据自身现状与密码应用需求，向密码服务平台申请密码资源并完成相应的密码应用改造，即可满足密码应用安全性评估要求。

二、行业挑战

密码是网络安全的核心支撑，是解决政务信息化安全问题最经济、最直接、最有效的手段。利用密码在安全认证、加密保护、信任传递等方面的重要作用，可以有效满足信息化时代政务信息化发展需求。

对于政务信息化来说，网络、数据、计算和平台四个方面，都存在不可忽视的安全风险，密码在四个层面发挥安全保障作用。首先，密码支撑政务信息化网络安全互联。通过合规、正确使用密码，能够

有效解决政务网络安全架构“鉴别、访问控制、机密性、完整性、抗抵赖”的基本安全需求问题；其次，密码助力政务数据安全防护。密码在政务大数据产生到传输、存储、共享等环节，可有效保证数据真实性、完整性、机密性、可追溯性。最后，密码推动政务信息化平台安全运行，保障各类上云业务的安全。

三、项目实施情况

（一）总体技术架构图及讲解

密码服务平台由密码资源层、密码支撑层、密码服务层、密码管理体系组成，其中三层密码服务构成从低到高的层级关系，低层可为上层提供密码能力支撑。网络边界设备建立安全通信链路，并保证通信实体身份的真实性。

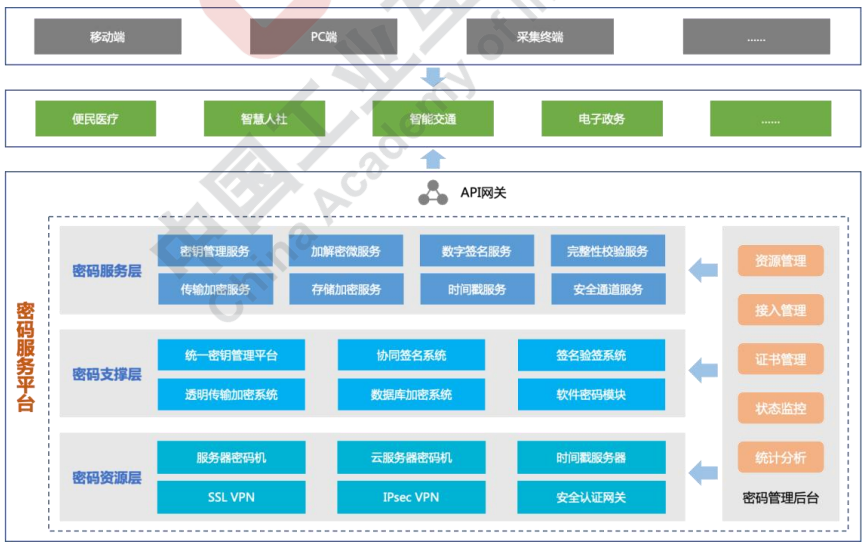

图 11.1 密码服务平台技术架构图

密码服务层：密码服务层是经过功能封装的密码功能服务，直面各个信息系统提供多种密码服务。密码服务层主要由密码服务 API

组成，符合商用密码行业标准。

密码支撑层：密码支撑层基于密码资源层中的密码基础设施，把面向应用场景的密码功能集合在一起，打包成易部署、易使用的虚拟机模板、微服务模板软件，在云中以虚拟机实例、微服务实例、软件中间件的形态提供服务。

密码管理后台：作为密码服务的支撑与运维平台，具备密码资源管理、资源状态监控、资源统计分析等功能。

（二）应用场景架构图及讲解

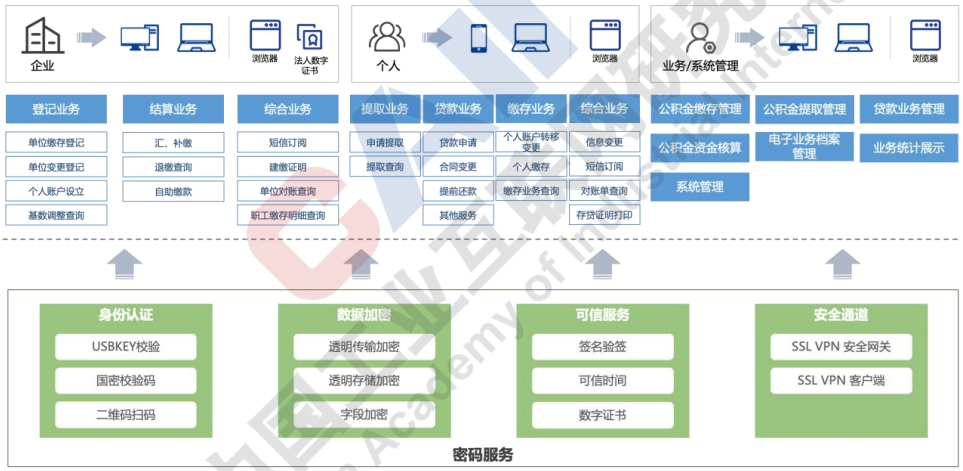

图 12.2 应用场景架构图

根据政务系统密码应用需求，方案通过部署在政务云的密码服务平台，向公积金系统提供对应密码服务，并开展系统的集成改造工作，分别面向企业、个人、业务/系统运维管理人员提供多设备终端、多业务场景的身份认证服务、数据加密服务、可信服务、安全通道服务等。

1、 企业通过浏览器登录系统办理登记、结算、综合业务

通过调用身份认证服务，采用具备国密数字证书的 USBKEY 登录系统办理业务，实现身份真实性保护；

通过调用传输加密服务（透明），无需公积金系统二次集成改造，实现业务数据在传输过程中的机密性与完整性保护；

通过调用数字签名服务、时间戳服务，实现可信服务保障，确保企业办理人在进行单位缴存登记、汇、补缴业务等业务时的行为抗抵赖，保障缴费数据完整可信、生成时间可信。

2、个人通过浏览器登录系统办理提取、贷款、缴存、综合业务

通过调用身份认证服务，采用国密校验码的方式，无需公众配备 USBKEY/更换浏览器，在浏览器登录界面输入特定国密校验码，实现个人用户的身份真实性保护；

通过调用传输加密服务（透明），实现业务数据在浏览器端即加密，到系统服务端解密，保障数据在传输过程中的机密性与完整性；

通过调用数字签名服务、时间戳服务，实现可信服务保障，确保个人用户在进行单位贷款还款、个人缴存等业务时的行为抗抵赖，保障还款数据完整可信、生成时间可信

3、业务人员登录系统开展公积金缴存管理、公积金提取管理、贷款业务管理、公积金资金核算等工作；系统管理人员进行系统运维管理

通过调用身份认证服务，采用具备国密数字证书的 USBKEY 登录系统办理业务，实现身份真实性保护；

通过调用传输加密服务（透明），实现业务数据在传输过程中的机密性与完整性保护；

通过调用安全通道服务，实现运维人员在远程运维时身份真实性保护，运维通道的数据机密性、完整性保护

4、公积金系统重要数据存储（企业基本信息、个人信息、受托银行信息、开发商与楼盘信息等）

通过调用存储加密服务（透明），无需公积金系统二次集成改造，实现重要数据的表级别加密存储，保障数据的机密性与完整性保护。

四、实施效果

（一）贯彻“集约化”理念

密码服务平台的建设，减少各单位为满足密码应用安全性评估的需要而重复投资密码基础设施，避免了安全系统的重复建设，节省密码应用领域的建设成本，节省支出。

（二）适用于多云、多机房、多租户，实现密码资源统一管理

面向多云、多机房、多租户的场景，通过多套密码资源池的搭建，减少基础设施重复投资，避免密码系统重复建设，实现各类密码资源的统一管理与调度，降低开发、运营和运维成本。

（三）轻量化改造，尽可能避免业务系统改造

密码服务平台提供多类型的密码服务，包括无需信息系统集成改造的透明传输加密、透明存储加密、加解密微服务等，能够应对云平台上多样化的信息系统，减少系统二次改造的成本。

（四）安全服务弹性扩容

密码服务平台的支持弹性扩容的特点，能满足功能不断扩展以及系统容量和用户数量不断增长的要求，使系统不会因将来内容和功能上的扩充而导致数据安全需求无法满足的情况。同时，对于业务系统可能会出现的需加密的数据激增、并发访问量过载等情况，平台对此

提供全面的扩容方案，从服务、数据、硬件三个维度保障密码服务的循环使用、动态分配。

（十二）智慧医院密码应用安全体系建设

申报单位：北京数字认证股份有限公司

一、案例综述

（一）案例背景

目前北京协和医院、北京宣武医院信息系统大多以电子化的途径收集、存储了大量患者个人基本信息、健康状况、医疗应用、医疗支付等数据，然而，医院现有信息系统缺乏安全措施，如何保证医疗电子数据的合法性、完整性成了医院信息系统建设中必须解决的重点问题。

为满足卫生行业政策要求，协和医院、宣武医院依托于本医院现有资源条件，以满足医院的实际电子认证服务建设需求出发，完善医院院内商用密码应用，实现医院医疗数据在身份真实性、数据完整性、数据机密性、责任认定等方面的信息安全体系建设。应用范围将覆盖门诊、住院、检查检验、病历归档、互联网诊疗等各个重要环节，将切实解决医院信息系统中的对身份认证、电子签名、可信时间戳、患者手写签名、可信病案归档等安全需求。

（二）案例简介

协和医院、宣武医院智慧医院密码应用安全体系建设的技术路线是采用公钥密码基础设施提供数字证书服务，并基于证书和商用密码

设备构建密码应用支撑系统为医院信息系统实现身份鉴别、数字签名、时间戳、电子签章等可靠电子签名应用。

协和医院、宣武医院信息系统安全系统建设密码应用场景主要包括医务人员的身份认证、医疗文书数字签名、患者知情文书数字签名、电子病案可信归档、互联网诊疗数字签名等各个环节。

二、行业挑战

近年来，医疗机构信息化建设的重点明显向临床业务领域倾斜，“建设以电子病历为核心的医院信息系统”成了业界通行的口号。减少医疗差错、保障医疗安全是临床信息化的主要诉求，而国家卫健委颁布的《三级综合医院评审标准》和《电子病历系统功能应用水平分级评价方法及标准（试行）》已成为系统建设的重要参照。

随着医院信息化建设的日益深入以及区域卫生信息化建设的逐步普及，数据泄露事件渐呈蔓延态势。从医疗机构内部人员监守自盗到 IT 黑客入侵窃取，手法多样，给医疗机构和病人带来了困扰，在社会上造成了不良影响。可以预见信息安全问题仍将是信息化建设进程中的重要制约因素，灾难恢复体系建设和入侵防护及数据库审计技术等依旧会受到医疗机构的高度重视。

三、项目实施情况

（一）总体技术架构图及讲解

图 12.1 密码应用支撑体系

密码应用支撑体系的设计是以国家及卫生健康行业密码应用推进政策和技术标准来规范指导，以密码应用基础设施、密码产品、密码技术、密码服务等作为密码应用基础支撑，以满足医院临床业务安全和提高医疗服务质量为目标，形成的适合于医院各类业务各应用场景的密码应用技术支撑，以保障医疗服务在身份可靠、数据可靠的环境下顺利开展。

商用密码算法体系包括非对称密码算法 SM2，哈希算法 SM3，对称分组算法 SM4，满足国密算法应用要求。

密码服务包括身份认证服务、数字签名/签章服务、时间戳服务、数据传输加密服务、数据脱敏服务、数据加密服务、数字证书服务、手写签名服务、数据访问控制服务。

满足信息安全四项基本属性，包括真实性、不可否认性、机密性、完整性。

基于 CA 服务，为医疗机构、互联网医院中的临床医护、患者、行政、后勤用户提供安全可信的密码服务，应用于病历书写、电子报告、患者签署、移动医疗、临床科研等多业务场景，保障了医疗数据的真实性、完整性、合法性。

（二）应用场景架构图及讲解

图 12.2 应用场景架构图

根据医院密码应用需求，本方案设计在医院部署密码软硬件设备，并与临床业务系统开展集成实施工作，分别面向医技护及患者提供支持多终端、支持多应用、支持多场景的可信身份服务、可信时间服务、可信行为服务、可信数据服务，应用于门诊看诊电子处方与病历记录、病房治疗电子病历应用、临床科研、电子病案归档、共享传输等众多应用场景。

1、医务人员通过 PC 端书写电子病历、处方、医嘱、检验检查报告、护理单等

涉及密码应用功能：医务人员书写完成电子病历进行提交或三级

审签时，执行医务人员个人数字签名、电子签章，并加盖时间戳，确保行为责任，保障电子病历完整可信、生成时间可信。

2、医务人员为患者或其家属生成住院须知、手术知情同意书等各类涉及患者知情确认的电子病历，患者或其家属阅读后签章确认

涉及密码应用功能：患者或其家属完成知情同意书阅读后，采集患者手写笔迹以及生物特征后，进行手写数字签名、电子签章，并加盖时间戳，确保知情确认行为责任后，再由医生进行个人数字签名、电子签章、时间戳，从而保障知情同意书完整可信、知情确认时间可信。

3、护士使用移动 PAD 到病房执行医嘱，填写并生成医嘱执行单等各类记录

涉及密码应用功能：护士在移动 PAD 端书写完成护理记录单进行提交时，在 APP 中点击提交或签名即可执行护士个人数字签名、电子签章，并加盖时间戳，确保行为责任，保障护理记录单的完整可信、生成时间可信。

4、电子病案归档与利用

涉及密码应用功能：电子病历入库前，业务系统调用数据加密服务接口，使用加密密钥对患者身份证号、手机号、住址等敏感信息进行加密，再入库存储。在需要使用敏感数据时，由业务系统调用数据解密服务将数据还原为明文。在需要对敏感数据检索时，由业务系统对检索字段进行 hash、加密处理后进行密文检索。

5、电子病历共享

涉及密码应用功能：医院共享电子病历前，对数据进行数字签名，确保数据传输过程中完整性和来源可追溯性，再通过安全传输通道实现数据加密传输。在平台或其他机构接收电子病历时，验证数字签名有效性后再入库保存。

四、实施效果

（一）为医院降本增效

在电子病历中应用密码技术，使医院电子病历满足《中华人民共和国电子签名法》对可信数据电文的书要求。实施电子签名后，电子病历数据可以作为有效的法律证据存在。通过在各业务流程加入电子签名、签章，优化了原有电子病历的流程，规范了医护人员的工作流程，提高了医护人员病历的书写质量和规范性，减少了医疗差错现象的发生。同时又为医院节省了大量的纸张印刷、耗材打印、库房管理等成本，为医院的自动化、信息化、智能化奠定了安全基础。

（二）助力智慧医院建设

医院密码技术的应用，进一步完善了医院信息化安全建设，在合法的电子化诊疗流程基础上，医生准确的诊断，方便、快捷、安全的信息传输，以及提供的真实、有效、合法的电子病历数据使得病人有了一个良好的就诊体验，真正营造“以患者为中心”的医院智慧服务体系建设环境，实现患者、医务人员、医疗机构、医疗设备的四方联动。助力医疗服务逐渐从被动、应对性的就诊向主动、常态性的预防保健进行转变，使得整个医疗生态圈中的每一个群体均可从中受益。

（三）满意于医院评级要求

医院密码应用体系建设符合《电子病历基本规范（试行）》、《卫生部办公厅关于做好卫生系统电子认证服务体系建设工作的通知》、《互联网诊疗管理办法》等国家卫健委的相关政策要求，符合《电子病历应用等级测评》、《医院智慧服务分级评估标准体系（试行）》等电子签名技术要求。已经有几十家使用密码技术的医疗机构通过电子病历系统应用水平五级及以上评级。

（十三）融合区块链特色的智慧城市统一密码支撑平台

申报单位：鼎链数字科技（深圳）有限公司

一、案例综述

（一）案例背景

2018 年全国网络安全和信息化工作会议，习近平总书记明确指出：没有网络安全就没有国家安全。2019 年 10 月 24 日的中央政治局第十八次集体学习时，习近平总书记强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展。探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

2021 年 3 月，深圳市坪山区密码管理局、坪山区发展和改革局、坪山区财政局、坪山区政务服务数据管理局联合分布《关于进一步加强政务信息系统密码应用与安全性评估工作的通知》，通知指出“为贯彻落实《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号）要求，依据《中华人民共和国密码法》和商用密码管理有关规定，现就进一步加强我区非涉密政务信息系统密码应用与安全性评估工作通知”，坪山区智慧城市中包括智慧水务、移动互联网、政务服务等信息系统建设，应当同步规划、同

步建设、同步运行密码保障系统，满足《信息安全技术 信息系统密码应用基本要求》，加强政府公共敏感数据、个人隐私数据等安全防护。

（二）案例简介

目前深圳市坪山的融合区块链特色的智慧城市统一密码支撑平台已顺利上线，为政数局、税务局、应急管理局等委办局提供一站式密码及区块链服务支撑。坪山密码及区块链的应用先行试点，探索出了密码及区块链应用落地切实可行的实施路径，提供一套较为完整的政务数据安全防护架构，有效助力持续优化营商环境、提升政务服务体验的政务创新目标，为下一步在深圳市乃至全国范围内推广密码及区块链应用奠定了坚实的基础。

二、行业挑战

目前智慧城市信息系统种类庞杂、数量众多、重要性强，密码应用改造需求迫切，密码应用建设主要存在以下问题:

（一）密码应用不合规，无法满足密评要求

现有信息系统普遍在算法使用、网络通信、身份鉴别、数据完整性保护等诸多方面存在不合规和不正确的问题。同时区块链底层平台建设方面，大量采用密码算法软件模块实现，密钥管理安全性不够，导致区块链应用本身存在安全风险。

（二）缺乏顶层规划，随信息系统分散建设，成本高

信息系统分散建设各自采购密码设备和服务，密码建设投入高、

利用率低，采购花费和部署时间成本高企，但密码设备的综合利用率却很低无法形成统一密码服务能力，密码设备的使用和管理也不规范，存在管理漏洞和安全隐患，容易形成“烟囱林立”的状况，与政务云协同性差，密码系统间无法互认互通，密码设备复用性不强，综合计算整体费用更高。

（三）密码服务与应用融合不够，成效差

传统密码应用建设大多通过堆叠密码设备，导致密码是密码、应用是应用，密码产品能够提供基本的密码功能，但与应用融合不够，无法提供应用级安全，同时系统单点部署，容易被攻击，出现故障时整个网络瘫痪。建设完成后，密码服务在运营、维护等方面未跟上，服务质量没有保障，导致密码用不上、体验差。

三、项目实施情况

（一）总体技术架构图及讲解

以集约化建设和管理为目标，构建融合区块链特色的智慧城市统一密码支撑平台，作为整体密码应用和服务的提供者，为智慧城市各业务应用系统提供融合区块链的密码服务和密码安全保障能力。依托具备自主知识产权的区块链底层技术，保证智慧城市系统数据全生命周期整体自主、可控、高效，如下图所示：

图 13.1 总体架构设计图

融合区块链的智慧城市统一密码支撑平台集成大部分主流厂商密码设备提供弹性可扩展的密码资源池模式，屏蔽差异化接口，兼容适配国产芯片、操作系统等国产化软硬件环境，采用微服务、容器化等技术支持灵活可靠的云环境部署，以标准化密码服务接口方式提供可调配、高性能、高可靠的密码服务能力，形成了一套密码安全管理制度，规范的密码安全管理体系与机制，打造多元化国产密码服务，在满足密评要求的同时，避免各业务系统密码应用在密码软硬件体系上的重复建设，缩减建设成本和周期。

（二）应用场景架构图及讲解

坪山区创新性地将政务区块链基础平台作为智慧城市建设的基础支撑系统进行上线，与大数据平台、政务云平台等基础平台一样，

为上层政务服务应用、城市治理应用提供底层平台支撑，有效地支撑政务信息化，并且实现与现有系统无缝衔接、集成友好。解决了坪山区政府信息系统数据共享难、业务跨部门协作难问题。如下图所示：

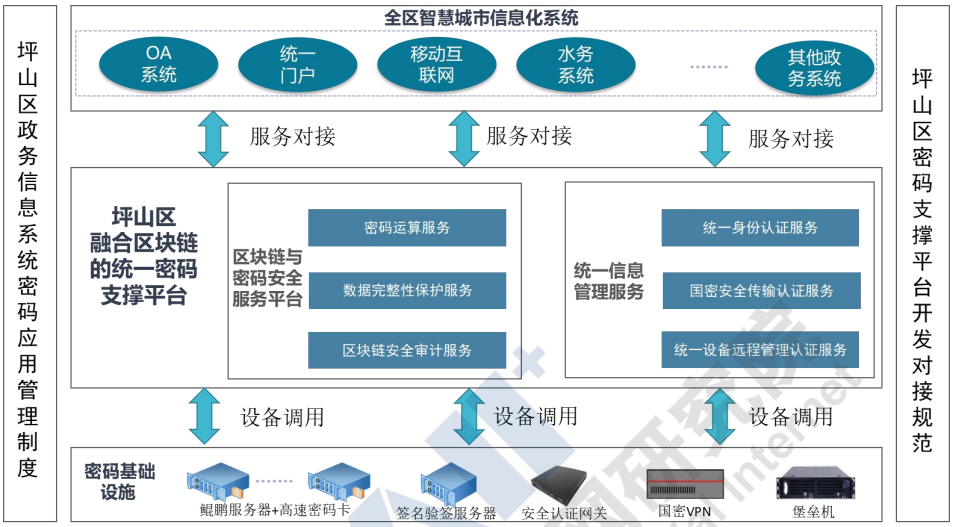

图 13.2 坪山区政务区块链平台

同时，基于一条主链构建不同应用子链，对接各部门节点的架构，有助于区块链系统的统一管理、统一运维，同时对区块链技术的应用，实现对数据跨部门流通的全流程监管，有效地保护了数据的隐私性和安全性。为各类政务信息系统提供统一的用户行为和操作日志的审计服务，能够保证日志信息的完整性和不可否认型，实现日志的不可篡改和不可删除，主要提供操作日志上链存储、操作日志可视化监管等功能。

区块链安全审计服务依托密码节点机硬件，面向业务系统提供日志上链、日志查询等服务，如下图所示：

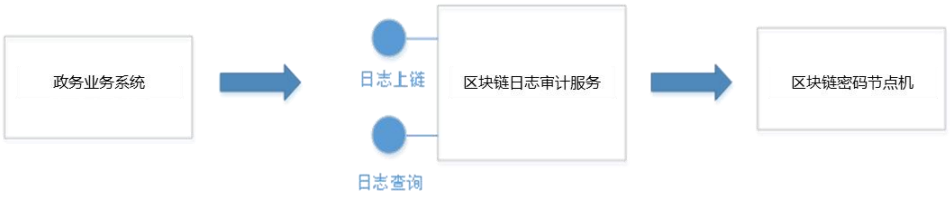

图 13.3 日志上链存证场景示意图

四、实施效果

（一）集约化密码服务平台，密码应用“统建统管”

面向全区的密码应用顶层设计，构建符合新型密码应用整体框架，通过集约化建设和统一密码服务支撑，有效降低建设和运维成本，避免密码资源重复建设，可视可控的密码应用态势感知，以区块链为底层信任基础设施赋能各个政府部门和行业，有力推动数字政府建设进入全新阶段，极大提高系统建设的经济效益。

（二）兼容适配多厂家密码设备，密码服务“灵活标准”

兼容适配各厂家密码设备，集成多种类型的密码软硬件产品，实现原有密码资源的利旧和密码设备的灵活更换，采用组件化密码服务提供弹性可扩展的能力，通过统一的区块链应用和密码服务接口，为业务系统提供可灵活配置的中台密码服务，减少业务系统密码应用改造工作量。

（三）密码+区块链“双融合”，构建新型信息安全服务

构建一个硬件密码资源池，通过密码+区块链“双融合”，支撑“两套平台”：统一密码基础支撑平台、国密联盟区块链基础设施，构建基于区块链的新型信息安全服务，提供高安全的国密区块链服务，具

备不可篡改、可追溯、高可靠、抗单点失效等优势，并赋能日志记录完整性、重要数据存储完整性、重要可执行程序来源真实性及不可否认性。

（十四）蚂蚁科技集团商用密码自研软硬件解决方案在云原生安全领域的全栈可信实践

申报单位：蚂蚁科技集团股份有限公司

一、案例综述

（一）案例背景

2020 年 1 月 1 日实施的《中华人民共和国密码法》明确提出：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 。同年 4 月，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，明确将“数据”同“土地、劳动力、资本、技术”等传统生产要素并列，成为一种新型生产要素参与分配。2021 年 8 月 17 日，国务院发布《关键信息基础设施安全保护条例》，并于 9 月 1 日起施行。

大型金融支付平台属于国家关键信息基础设施，真实、准确、完整、精准的海量金融数据直接关系到广大消费者的财产安全与人身安全。蚂蚁集团以合规经营及业务需求为牵引，持续多年投入，完成了商用密码体系的基础设施关键硬件、关键软件的自研和迭代升级，并基于商用密码在蚂蚁云原生技术中的应用，逐步推进全栈可信业务改造。

（二）案例简介

商用密码在蚂蚁云原生全栈可信中的应用，实现了以自研商密软硬件产品为基础设施，综合中间件、系统、安全业务以及可信产品等能力，凭借自研软硬件的高性能特性，兼具高级别安全资质，可满足金融级云原生基础设施全栈加密的需求，在海量高并发支付场景实现身份核验和每笔交易加密，解决了金融行业针对密码服务载体的合规要求以及性能需求。

本案例所涉及的商用密码应用场景包括支付宝交易抗抵赖等重要技术的实施与应用环节。

二、行业挑战

（一）海量金融交易中面临商用密码支持不足的挑战

目前大型金融机构、金融科技集团的业务处理，面临着大数量级金融交易中针对商用密码协议加速性能支持不足，多协议、多算法交叉使用支持存在缺陷等问题。此前同类产品主要针对低吞吐，低并发的传统应用场景，同时相关产品缺乏分散式密钥管理集群支持，金融领域高安全性要求以及商用密码合规应用下的要求。

（二）云原生场景中缺乏密码服务接口标准化的挑战

云原生技术需要支持多种应用层协议的接入，同时由于国内业务和国际业务长期并存，存在多算法类型、多协议交叉快速支持的需求，传统密码协议及密码设备无法有效支持。

（三）平台差异性对密码基础设施通用性的挑战

不同业务场景下，用户的硬件平台差异大，对密钥管理和商用密码算法的支撑能力弱，端上用户缺少海量用户场景下成本低、可快速部署、可支持商用密码算法和密钥管理的解决方案。

三、项目实施情况

（一）总体技术架构图及讲解

可信云原生商用密码应用以国家对大型金融行业密码应用推进政策和技术标准来规范指引，充分利用自研商密软硬件的底层优化和功能定制，围绕算力平台、网络优化、协议加速和可信密码服务等关键技术，以解决企业实际金融交易中的性能效率、安全合规、用户隐私数据安全以及降本增效等问题为目标的商用密码应用实践探索。云原生商用密码全栈可信应用架构如下图所示。

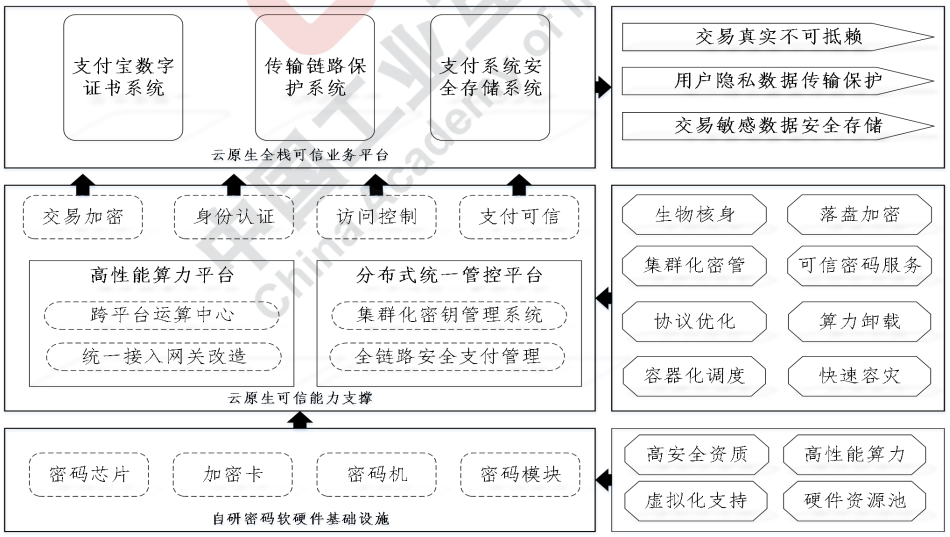

图 14.1 云原生商用密码全栈可信总体框架

云原生商用密码全栈可信的资源底座包括以具备高性能、高安全性的密码芯片、密码板卡等密码模块为代表的自研商密软硬件基础设

施。针对性地提供了数据流驱动弹性计算架构技术，大幅提升了金融级基础设施全栈加密的性能和丰富的密码体制支持。基于物理安全和逻辑安全等设计宗旨，结合硬件虚拟化技术，满足了针对大数量级金融支付业务所需要的高性能安全节点、集群以及计算安全等需求。密码硬件资源池化将各类密码硬件资源进行抽象，为北向应用提供各种分布式服务，在提供统一设备管控的同时满足等保三级及以上的相关要求。

云原生商用密码全栈可信的能力支撑是以软硬件密码资源为底座构造得到的各项服务能力。高性能算力平台包括跨平台运算中心以及统一接入网关改造，前者依赖自研高性能密码硬件的能力，通过算力统一、业务隔离、快速切换等技术，实现了国内、国际业务长期并存下密码算法多协议、多算法的高效交叉使用；而后者针对传统TLS/SSL 协议进行深度优化和升级，并通过硬件算法引擎实现应用负载转移，极大地提升了服务部署效率。而分布式统一管控平台包括集群化密钥管理系统以及全链路安全支付管理，前者利用密码卡、密码机集群化及虚拟容器支持，结合多级密钥体系实现不同业务、不同用户、不同密钥分类的安全存储和保护；后者通过预埋签名证书保证每笔交易的真实性，创新链路层商密协议升级确保了支付中用户隐私数据传输合规高效。

（二）应用场景架构图及讲解

1、支付宝交易抗抵赖

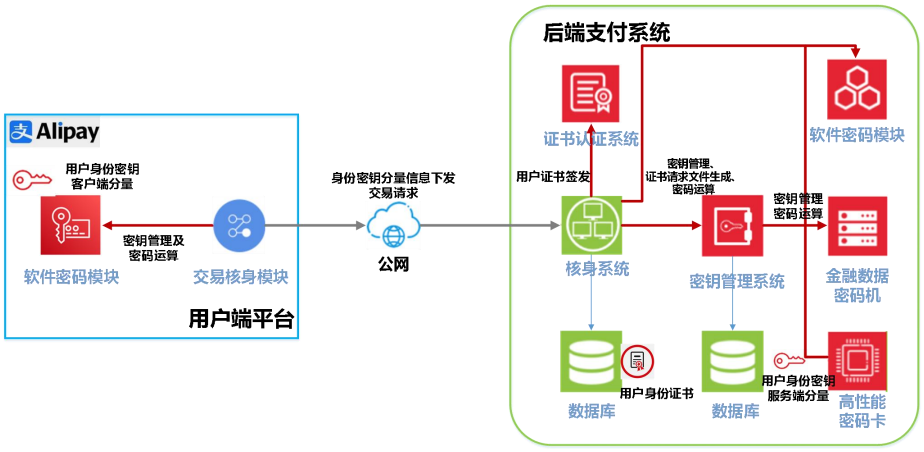

图 14.2 支付宝交易抗抵赖

通过支付宝客户端内嵌的软件密码模块保护移动用户的数据安全，为每一个用户创建单独的用户证书和用户协同签名密钥，对用户交易进行基于数字证书的抗抵赖认证，确保交易的真实性。采用自研软件密码模块，可以屏蔽不同类型用户硬件平台差异，便于在不同型号、不同厂商、不同平台上快速实现海量用户的抗抵赖能力部署。

2、支付宝用户隐私数据保护

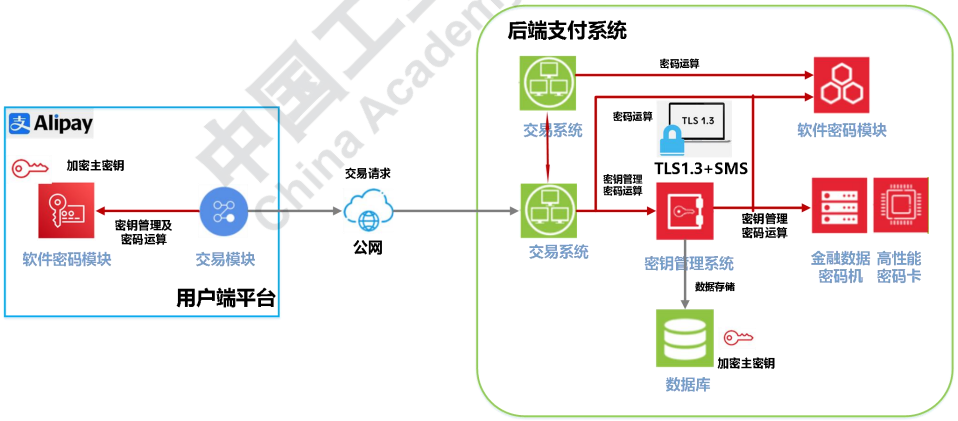

图 14.3 支付宝用户隐私数据保护

客户端到后台支付系统链路所涉及的用户隐私数据需要得到妥善保护，蚂蚁集团主导并推进了国际标准化组织 IETF 在 TLS1.3 中对

商密算法的支持，并在传输通道层面使用 TLS1.3+商密套件的方式保护数据的机密性和完整性。利用自研开源商密算法库对协议进行压缩优化，使用与自研高性能密码卡适配的加速 Engine，极大提升网络层密码运算效率。

四、实施效果

（一）解决密码技术在云原生场景下的应用难题，建设海量数据下密码易用性典范

在云原生场景下，以自研商密基础软硬件设施为底座，结合网络层协议优化、业务卸载、虚拟化硬件资源池等技术，凭借单卡分组加密 25Gbps、签名 28 万次/秒的性能，有效提升交易速度 30%、降低共识延迟 40%、加速密码运算 5-10 倍。实现了同海光、鲲鹏、中科等平台的国产化适配，同时部署时间缩短 50%以上，在线上支付、生物核身等业务场景性能提升 8-10 倍，满足了日常 80000 QPS、平均 rt<3ms 的性能要求，实现跨平台、跨业务的快速适配。

（二）密码应用在金融支付业务中的合规化和高等级安全能力升级

金融支付业务需要严守合规性要求，按照商密最高安全等级设计并研发的自研商密软硬件产品作为云原生密码软硬件基础设施，可保证金融交易中云上用户信息受到严格且完善的保护。利用统一身份认证平台和业务网关数据加密，可以有效地防御物理入侵、网络攻击，降低交易信息和用户敏感数据泄露风险。

（三）推动密码产业国产化高安全、高水平建设

在硬件层面，整套平台拥有商密认证安全三级资质的板卡以及安全二级资质的芯片等多个全国产化密码模块；在软件层面，自研商密算法库开源有利于密码生态国产化建设。基于以上自研商密软硬件设施，将统一身份识别、权限管控、签名验签、数据加密等商用密码服务应用于大规模金融支付交易业务中，可以有效提升支付系统整体安全水位、提高复杂场景下支付业务效率、降低企业生产运维成本，最大程度保障消费者个人隐私数据安全。基于商用密码在云原生技术中的应用，推动密码产业为代表的数据安全技术国产化高质量发展，有助于促进国家和企业在数字技术、数字金融等重大国计民生领域上的合作和创新，更有利于密码产业国产化朝向高安全、高水平方向建设。

（十五）基于国产商用密码的广播电视卫星直播端到端技术应用与实践

牵头申报单位：国家广播电视总局广播电视卫星直播管理中心

联合申报单位：国家广播电视总局广播电视科学研究院

北京数码视讯科技股份有限公司

北京永新视博数字电视技术有限公司

湖南国科微电子股份有限公司

北京数字认证股份有限公司

一、案例综述

（一）案例背景

广播电视卫星直播管理中心（简称卫星直播中心）是2011年10月经中央编办批准设立的国家广播电视总局直属事业单位。负责卫星直播节目平台和用户管理系统的建设、运行、管理，组织卫星直播新技术应用研究，开展卫星直播广播电视公共服务，服务全国卫星直播广播电视用户等。目前，卫星直播中心已发展超过1.49亿直播卫星用户，平台已成为全球用户数量最多的直播卫星平台，通过广播电视直播卫星集成传输了共计百余套高清电视节目、标清电视节目和广播电视节目。

为全面贯彻实施《密码法》，维护国家安全和社会公共利益，国务院明确要求要尽快完成数字电视条件接收系统（简称CAS系统）

国产密码应用安全体系建设。为保证广播电视公共服务高质量安全可靠发展，经广电总局批准，卫星直播中心于 2018 年组织相关科研院所和高新技术企业开展技术攻坚，实施基于广播电视卫星直播的新一代国产商用密码可下载条件接收系统（简称 DCAS 系统）和国产商用密码身份认证系统的技术研发和应用，2019 年完成系统建设。

（二）案例简介

项目依托支持国产密码算法的《GY/T 255-2012 可下载条件接收系统规范》和《GY/T 308-2017 单向可下载条件接收系统技术规范》，在保证兼容传统条件接收系统的同时，通过根密钥派生、用户端软件安全下载等机制，支持国产密码算法替代国外密码算法，解除了终端与条件接收系统的绑定，防御了传统条件接收系统加扰控制字共享所导致的安全威胁，实现卫星电视运营商不受单一条件接收厂商技术垄断的目标。

二、行业挑战

我国广播电视行业目前部署的 CAS 系统普遍采用国外算法，且与用户接收终端在芯片层面形成强绑定关系，一旦 CAS 系统被破解，将产生非法盗播、插播等严重影响社会稳定的安全问题。如 CAS 厂商倒闭，已部署的终端将无法被替换，后续业务运行和运营存在安全风险，并无法开展新业务。卫星直播节目平台仅采用一家基于国外密码算法的 CAS 系统，承担着超过 1.49 亿用户的节目加密和授权，安全风险程度更高，安全形势更加严峻。基于上述原因，国务院相关文

件明确提出要完成数字电视 CAS 系统国产密码应用安全体系建设。本项目基于直播卫星传输特点，部署基于国产密码的新一代 DCAS 系统及身份认证系统，对智能终端硬件安全芯片和安全模块进行技术攻关和产品研制，从而提升端到端整体安全防护能力。

三、项目实施情况

（一）总体技术架构图及讲解

基于国产商用密码的广播电视卫星直播端到端技术包含可下载条件接收系统和国密身份认证系统。

1. 可下载条件接收系统（简称 DCAS 系统）

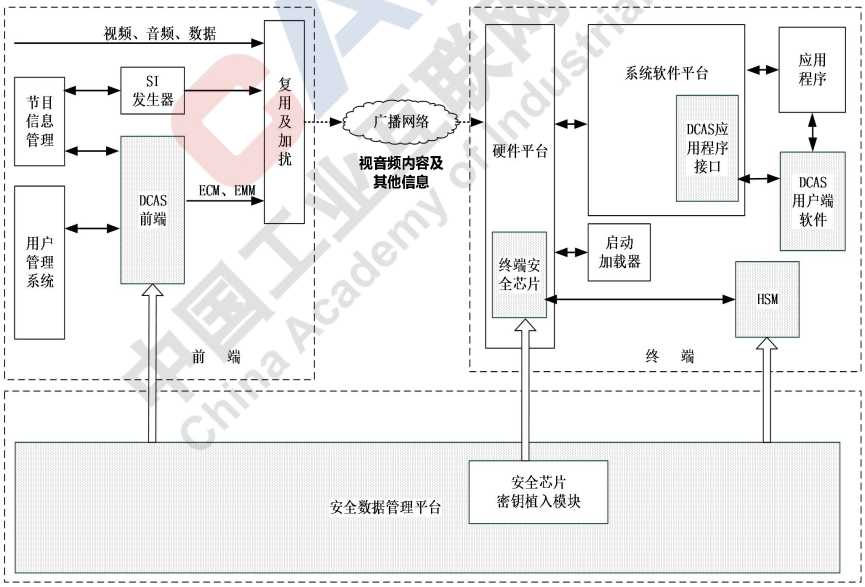

图 15.1 DCAS 系统架构图

DCAS 前端：对输入的音视频流进行加扰，通过广播信道发送授权等信息，完成业务的加密保护传送和合法授权控制管理。

DCAS 终端：对用户授权进行合法性验证，解扰数字电视业务，

实现业务的条件接收。终端软件平台可以安全地下载、更新和替换DCAS用户端软件。DCAS终端主要涉及终端安全芯片、DCAS用户端软件和DCAS应用程序接口和HSM。

DCAS安全数据管理平台：生成并管理DCAS相关密钥，向DCAS前端提供SCKv和Vendor_SysID等必要信息；通过密钥植入模块向终端安全芯片提供ChipID、ESCK、BL_KEY0等必要信息。

2. 国密身份认证系统

证书管理模块为卫星直播平台关键业务系统提供数字证书发放、更新、吊销等证书全生命周期管理功能。身份认证模块实现卫星直播业务系统的用户身份鉴别和认证功能，对关键业务系统配备双因素认证机制。用户个人信息保护模块将与业务系统对接、交互，对业务系统中存储的个人敏感数据进行加密存储。

（二）应用场景架构图及讲解

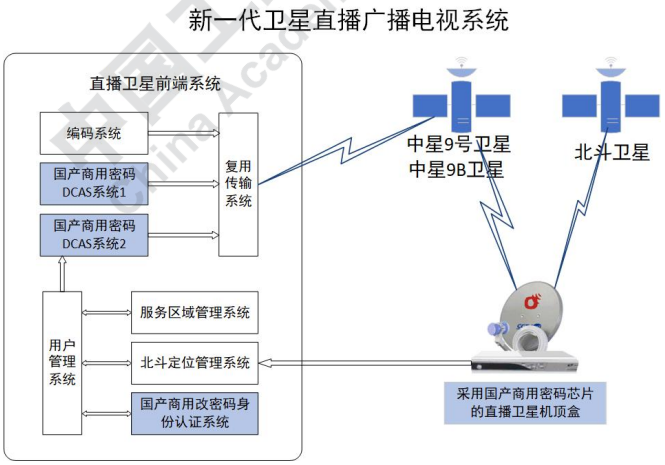

图 15.2 新一代卫星直播广播电视系统整体业务示意图

如上图所示，通过在DCAS系统、用户管理系统、直播卫星接

收终端中实现国产商用密码应用，形成了一个端到端、完整的新一代卫星直播广播电视系统国产商用密码技术解决方案。

1. 基于国产商用密码的 DCAS 系统建设，实现了我国广播电视卫星直播业务采用国产商用密码进行加密保护传送和授权控制管理，极大降低了卫星直播中心 CAS 系统被破解后严重影响社会稳定等方面的安全风险，同时解除了运营单位与 CAS 厂商的强绑定关系，减少了制约。这是国产商用密码在我国广播电视领域内 CAS 系统的首次应用，为我国广播电视领域商用密码的国产化提供了方法路径和借鉴指导。

2. 基于国产商用密码芯片的卫星直播智能终端的研发和生产，涉及直播卫星产业链相关高校、科研机构和生产企业三十余家，涵盖芯片、操作系统、终端等各方面，现已发展用户近 300 万户，为广大农村地区人民群众提供了优质丰富的高清电视节目和其他信息服务。直播卫星产业已形成“产学研用”良性循环的运营机制，为国产商用密码在广播电视领域的应用起到了积极的示范效应，将进一步促进国产商用密码技术与广播电视技术的融合应用。

3. 基于国产商用密码身份认证系统在卫星直播节目平台的部署应用，满足了国家关键信息基础设施保护和网络安全等级保护要求，强化了对卫星直播中心业务系统的安全访问、数据安全保护和用户信息保护，有效提高了中心网络安全保护能力，进一步保障了系统安全和数据安全。

四、实施效果

（一）为我国广播电视卫星直播公共服务安全提供了有力保障

针对我国广播电视直播系统在运行中出现的非法盗播、插播等问题，本案例在前端侧采用基于国产商用密码的 DCAS 系统，在终端侧采用基于国产商用密码的安全启动、DCAS 层级密钥和 DCAS CA 加解密等技术机制，从物理底层实现了数据传输的可靠性和安全性，有力保证了广播电视卫星直播系统运行安全，有效保障了农村地区人民群众听好广播、看好电视，极大巩固了党在农村地区的意识形态安全。

（二）有力扩大了国产商用密码的推广应用覆盖面

从应用面上看，我国广播电视卫星直播系统中的国产商用密码应用，得到了国内卫星直播全产业链包括主流运营商、条件接收系统厂商、芯片厂商、终端厂商、密钥管理平台等多方在产品层面、业务层面、实施层面的大力支持和积极参与，不仅加深了产业内厂商对国产商用密码的理解和支持，也有利于国产商用密码后续在整个广播电视领域的深度开发和应用。

（三）已实现较大经济效益，后续市场规模巨大

截至目前，本案例中支持国密的卫星直播高清智能终端已累计在国内销售并开通超过两百万台，实现国密算法在我国广播电视卫星直播领域的积极应用示范，后续将逐步替换现有超过 1.4 亿台用户接收终端，将产生巨大的经济效益。