中数国科密码服务平台
产品白皮书

中数国科集团

2025 年 5 月

■ 版权声明

目 录

1. 概述

1.1. 产品背景

(一) 数字经济快速发展，数据安全形势严峻

在新一轮科技革命和产业变革浪潮中，基于数据发展的数字经济已成为不可逆转的时代潮流。我国正处于从工业经济迈向数字经济的攻坚阶段，政府、企业正在着力推进数字化转型，数据价值愈发重要。

当前，云计算、大数据、人工智能、物联网、移动互联网等多种技术融合应用，网络安全的脆弱性凸显，数字经济发展伴随风险，面临数据泄露、恶意篡改、网络勒索病毒、非法入侵等新型安全问题。

(二) 密码是网络与信息安全的基石

《中华人民共和国密码法》中提出，密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。商用密码用于保护不属于国家秘密的信息。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

密码作为网络空间安全体系的重要组成部分，是网络空间安全和信任机制的“基因”和关

键技术，是信息保护和网络信息体系建设的基础。

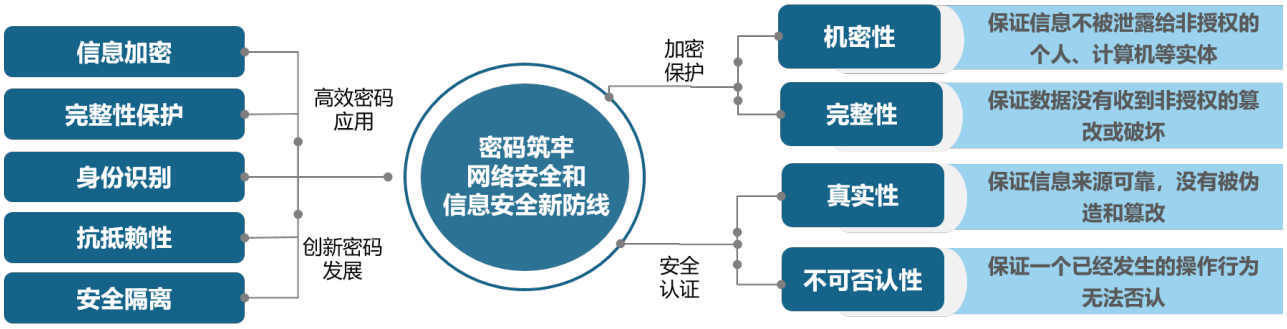

图 概述-1密码：网络安全和信息安全的基石

(三) 数据安全合规要求

数字经济发展面临着数据风险，数据安全上升至国家战略高度。国家在法律层面、国家数据安全标准、行业数据安全标准等方面不断推动提高数据安全防护、数据安全治理水平。先后颁布并实施的《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》，“三驾马车”相继落地，奠定了数据安全的法治基础；在国家数据安全标准层面，《大数据服务安全能力要求》、《大数据安全管理指南》、《个人信息安全规范》等各项标准正式发布；金融、工业领域、电信、车联网等行业也陆续出台和发布了行业数据安全标准，如《个人金融信息保护技术规范》、《工业互联网数据安全保护要求》等。

(四) 密码应用合规要求

国家高度重视密码工作，密集出台法律法规及相关政策，明确要求应发挥密码在网络

安全的核心保障和基础支撑作用。近几年先后颁布并实施了《中华人民共和国网络安全法》、《中华人民共和国密码法》、国家标准《信息安全技术 信息系统密码应用基本要求》等。法律法规的颁布将密码工作上升至依法规范的层面，政策文件的发布强调了加快推进密码应用工作的重点，标准规范体系的建立和完善为商用密码的应用提供了指导和参照。

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）明确规定应采用密码技术保证通信过程中数据的完整性、保密性；应采用密码技术保证重要数据在传输过程、存储过程中数据的完整性、保密性；应采用两种及以上鉴别技术对用户进行身份鉴别，其中一种鉴别技术至少应用密码技术实现。

《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）规定，信息系统应使用合规的密码算法、技术、产品、服务；不同安全等级的信息系统应采用相应的密码技术来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；信息系统应保证密钥全生命周期安全。

(五) 采用传统密码应用建设模式存在诸多问题

根据等级保护、密码测评等相关要求，各级政务部门、企事业单位在应用系统规划建

设时，需编制密码应用的建设方案。但对于建设模式的选择，往往采用传统的密码应用模式，引入不同类型、数量众多的密码设备、密码产品，对接各种密码应用业务。

这些密码产品分散部署，各自使用，面临着诸多问题和挑战：

- 部署环境新要求：云计算环境改变了密码应用模式，传统密码部署架构不适应云环境建设和要求。
- 合规要求：整体使用情况缺乏统计，密码服务缺乏量化，密码应用缺乏监管，难以满足合规建设的要求。
- 建设与运营难度大：传统密码应用模式，用户各自自行建设，重复开发，运维和升级困难。
- 管理复杂度高：密码设备分散、密钥分散；系统各自独立，管理方式和工具各异。
- 易用性低：产品种类繁多、厂商众多，各密码产品系统服务模式各异，密码应用复杂度高，专业性强，密码应用对接集成复杂。
- 资源利用率低：各单位密码服务建设不均衡，密码资源利用效能不足。

1.2. 产品定义

密码服务平台，是一套综合性服务平台软件系统，聚合集成多种密码设备、安全产品通过服务聚合能力，为用户提供统一管理、使用便捷的服务。

相较于传统密码应用建设模式，密码服务平台具备以下产品特性。

合规性：设计和建设合规，符合等保 2.0 和密评要求。

先进性：采用较新的架构设计，适应传统部署、云环境部署。

平台化：集约化设计、一体化管理。

服务化：适应云端、移动端、物联网端等新型场景。提供标准化、组件化服务，功能性能弹性扩展。

运维统一：统一的密码资源管理，统一的运维管理。

接口统一：各类服务接口统一，便于应用集成对接。

2. 产品简介

中数国科密码服务平台（以下简称密码服务平台）是中数国科集团严格遵照国家技术标准规范，基于国产密码算法，聚合密码设备和系统、数据安全防护产品，以数据为防护核心，以业务为防护对象，以密码为技术措施，以运营为体系保障，通过统一、标准化的

服务接口，为用户提供涵盖密码基础服务、密码通用服务、数据安全服务等，构建的密码与数据安全运营服务平台。

密码服务平台可将分散的各类密码资源和密码业务应用进行有效整合，降低用户密码应用管理的难度，为用户提供简单、便捷的密码服务；平台可提高密码设施资源的复用率，极大地降低用户的建设和投资成本。密码服务平台提供的体系化、标准化、可监控、可计量的服务模式，降低了用户集成使用密码服务的难度，缩短项目建设周期，提高了密码应用和安全服务效率。

密码服务平台能满足云计算环境下对密码和数据安全的服务需求，助力用户政务上云企业上云和数字化转型之路，满足用户项目建设安全、合规的要求。

对比项	传统密码设备部署方式	密码服务平台
监管与合规	密码服务整体使用情况缺乏统计； 各自建设带来合规性风险； 服务和运行缺乏监管。	**【合规】** 以通过商密测评的基础密码产品为基础，平台设计**符合等保2.0和密评**标准体系。 提供统一的服务与运行监管。
云计算环境适应	云环境改变了密码应用模式， 传统密码部署架构不适应云环境建设和要求。	**【部署灵活】**支持云环境部署； 满足密码能力上云，云上密码服务的模式。 以平台化、服务化为单位租户提供密码服务。
建设与运营	各自建设，重复开发，运维和升级困难	**【平台交付、服务交付、省心】** 采用平台建设与运营模式，直接为用户交付能力。
管理难度	设备分散、密钥分散； 系统各自独立，管理方式和工具各异。	**【集中、方便、省力】** 密码设备、密码服务、密钥集中管理，统一运维。
易用性	各密码产品系统服务模式各异，密码应用复杂度高，专业性强。	**【好用，应用对接简单】** 密码服务针对应用模式一体化设计，服务模式统一，易用性高。
资源利用	各单位密码服务建设不均衡，密码资源利用效能不足。	**【好扩展】** 密码服务按需获取，弹性扩充，密码资源统一管理，密码资源效能充分发挥。

图 产品简介-2中数国科密码服务平台对比传统应用方式的优势

3. 产品架构

中数国科密码服务平台在产品架构设计上秉承“合规化、平台化、服务化、易用性”的设计原则，采用云原生架构搭建高性能、高可用、分层解耦、弹性伸缩的多租户密码服务与运营体系。

密码服务平台以国家政策法规及安全规范为支撑，以分层模块化的结构为用户业务提供密码服务及数据安全服务接入能力。整个架构中，底层的是密码资源层与基础设施层，包含了各类密码设备、数据安全防护产品；最顶层的是应用层，包含了用户各类需要使用密码服务、数据安全服务的应用系统、终端系统；处于中间层次的即是密码服务平台层。产品架构如下图所示。

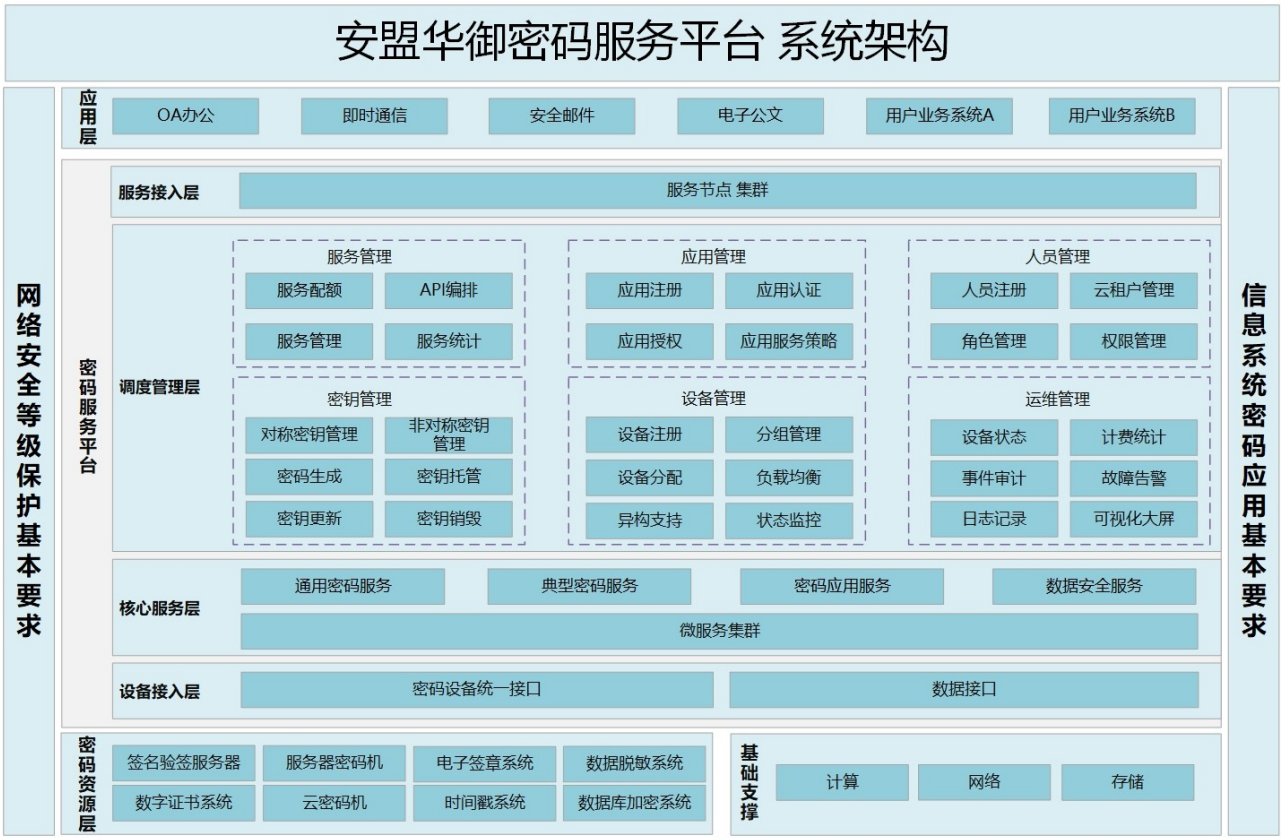

图 产品架构-3中数国科密码服务平台系统架构图

云服务器密码机、电子签章系统、时间戳系统、数字证书系统、数据库加密系统等设备和产品构成了密码服务平台的密码资源层。密码资源层的各产品系统是密码服务平台实现服务能力的基础，可通过增加底层资源系统的种类和同类型设备的数量，扩展密码服务的能力，提升密码服务的性能。

密码服务平台的核心服务层，由微服务集群组成。用于聚合、集成底层的密码设施、密码产品系统、数据安全防护系统，封装并形成服务平台的核心服务能力，包括通用密码服务、典型密码服务、密码应用服务、数据安全服务等。

调度管理层实现对各类应用的接入管理与认证，对各类服务进行管理，并可提供系统运维、租户管理、服务计费、服务策略管理、服务状态监控和审计、密码服务合规分析、密码服务综合态势呈现、密码设备资源管理等功能。

服务接入层由服务节点集群组成，是各应用系统的服务入口。服务节点提供动态、实时、高性能服务接入和调度能力，通过负载均衡、动态路由、灰度发布、服务熔断、应用认证、可观测性等关键技术实现丰富的流量管理功能，可以对各类密码和数据安全微服务实行控制管理。服务接入层采用一体化设计，以服务节点、SDK 形式提供 Restful、C、Java 等主流接口，方便用户应用集成。用户的应用系统或业务终端，以此调用并获取到各类通用密码服务、典型密码服务、数据安全服务等。

4. 产品关键技术

中数国科密码服务平台采用多项关键技术保障平台安全、可靠、易用。

(一) 云原生技术

利用云原生技术架构的容器化、微服务化、体系化、规模化方面的成熟特性，服务平台的设计聚焦于密码服务和数据安全服务的业务解耦，充分融合底层架构技术实现应用韧

性。

密码基础设施、数据安全系统、服务软件功能解耦，密码服务、数据安全服务分层。

(二) 多租户密钥安全隔离技术

从应用密钥管理系统、虚拟云服务器密码机、服务调度机制等多层次提供租户密钥隔离机制。

为各租户的各类密钥信息提供安全隔离机制，从密钥管理功能的全生命周期，包括密钥的产生、绑定、分发、更换、销毁等，提供安全保护。

(三) 细粒度服务配额与流控技术

采用多级消费者标识和流控技术，实现应用可信标识、安全访问鉴权和精细化限流。

基于租户、应用、服务等采用细粒度的资源分配与流量控制技术，可实现多维度的运维管理控制和计费服务。

(四) 密码服务弹性扩展技术

底层密码产品设备、数据安全系统能力动态扩展；采用弹性、高性能的密码服务和数据安全服务 API 管理、负载均衡和能力聚合技术，通过扩展后台支撑系统，实现快速、低成本、低风险地开放和扩展服务能力。

(五) 密码服务高可用技术

密码服务调用从接入层、服务层、资源层采用全流程双冗余机制，采用大容量、高并发、高稳定服务技术；密码服务资源采用集群调用，实现服务故障熔断自愈机制。

(六) 密码服务亲和技术

密码服务和数据安全服务在资源分配与调度环节采用亲和机制，保障资源分配、调度和切换过程保持亲和性，避免资源频繁迁移，降低负载压力，提供高效和稳健可靠的服务。

(七) API 服务编排技术

采用无代码技术和低代码开发技术实现服务编排。将 API 服务通过“拖拽”的方式进行组合编排，编排的插件共享上下文信息，最终实现场景化需求。

5. 产品主要功能

5.1. 密码和数据安全服务

密码服务平台以商密标准产品为基础，打造服务化、场景化，易于业务系统快速对接的密码服务和数据安全防护的开放性平台。

密码服务平台的服务接口采用一体化设计，消除各个服务之间的空隙，实现各服务之

间的平滑调度。平台为业务系统提供了丰富的密码和数据安全服务种类，并以服务节点、SDK 形态提供 Restful、C、Java 等主流接口，方便应用系统集成。

通过集成云服务器密码机、证书管理系统、身份认证系统、数据库加密系统等密码产品及数据安全防护产品，密码服务平台可提供以下服务。

5.1.1. 密码计算服务

平台可为用户提供适用于各类应用系统的高速的、多任务并行处理的密码计算服务,可满足应用系统数据的加密/解密、签名/验证的密码运算要求,保证信息的机密性、完整性和有效性。

提供对称运算、非对称运算、杂凑运算、随机数运算等服务。

为用户提供数据加解密服务、文件加解密服务，对称算法支持 SM1、SM4，加密、解密，非对称算法支持 SM2 算法加密、解密。

为用户提供数据完整性运算服务、文件完整性运算服务，支持 SM3 摘要运算。

为用户提供签名验签运算接口，支持 SM2 算法签名、验签运算。

5.1.2. 签名验签服务

平台可为各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并可验

证签名数据的真实性和有效性;支持不同 CA 的用户证书验证，提供基于根 CA/CRL/OCSP 等多种方式的证书有效性验证。满足用户在网络行为中真实性、不可否认性、完整性、机密性等需求。

提供数据签名验签服务接口、文件签名验签服务接口；提供数字信封服务接口，实现数据的数字信封加封解封功能；提供证书验证服务接口。

5.1.3. 应用密钥管理服务

服务平台支持集中统一管理密钥，提供方便便捷的密钥服务。

平台支持对称、非对称密钥的全生命周期管理，从密钥生成、更新，到注销、归档、删除，平台会记录密钥全生命周期的操作管理日志，便于进行密钥管理审计。

平台按照国家主管部门认可的密钥生成方法生成高质量随机数、对称密钥和非对称密钥，提供密钥存储保护机制，保证密钥生成及存储的安全性。平台支持密钥模板管理，便于业务统一规划密钥的属性，同时也支持基于密钥库方式的管理，适应各种不同场景的密钥管理需求。

密钥管理可对业务系统提供密钥互操作接口，符合 KMIP（密钥互操作协议）的规范，可与满足 KMIP 管理规范的系统平滑对接，快速为业务系统赋能。

5.1.4. 身份认证服务

平台可为用户提供统一的身份认证体系，帮助用户实现统一资源管理、统一授权管理统一身份认证、统一门户单点登录以及统一行为审计。

对于使用了多个云上应用的用户，可通过平台提供的合规的身份认证服务联通所有的业务应用，实现用户的跨云统一管理和单点登录。

身份认证服务通过统一的认证入口为用户提供集中式的办公体验，同时基于单点登录为用户提供“一次认证、全网通行”的便捷性体验。

身份认证服务通过多租户设计有效的保证不同租户数据隔离，提供认证等级、授权、二次认证等安全策略配置，提升应用安全，同时通过完善的日志审计，对管理员操作日志和用户访问日志进行审计，可进行事后追溯，保障应用安全。

身份认证服务以 PaaS 服务的方式提供服务，极大降低了各部门的运维成本，同时身份认证服务为业务应用提供便于集成的服务 SDK，可避免多个系统中身份认证和账户管理的重复建设，节约了大量的研发成本和人力成本。

身份认证服务通过标准化接口能够快速对接外部应用系统，使其能够快速响应业务需求，提升部门的敏捷性及创新能力。

5.1.5. 时间戳服务

时间戳服务广泛地用于网上招投标、电子病历、公文审批、版权保护等领域，对业务系统中关键业务和操作提供精确的、可信的且不可抵赖的时间服务。时间戳和原文绑定在一起可以证明某个时间的有效。

平台提供的时间戳服务通过生成可信时间戳可确定电子文件生成的精确时间，并防止电子文件被篡改，为电子数据提供可信的时间证明和内容真实性、完整性证明。

例如：对审计日志进行签名和时间戳，从而使业务发生时间具有权威可信的特征；在网上招投标系统中提供投标、开标等关键操作的时间认证，确保时间的有效性、合法性。

5.1.6. 扩展密码及数据安全服务

通过进一步集成密码产品及数据安全防护产品，密码平台可提供以下服务。

（1） 电子签章服务

平台可提供电子签章服务用于电子政务公文应用、电子票据、电子商务等应用场景。

以电子政务公文审批场景为例，用户在某一电子政务审批流程中需要签章时，可通过

PC 终端或移动终端加载 USBKey 或软件密码模块进行业务访问，通过数字证书服务为用户颁发数字证书，用户登录业务系统并进行身份认证，认证通过后向业务系统发起签章请求，由签章服务执行签章操作，进行版式文件生成并加盖电子印章，签章结果返回业务系统

电子签章服务提供安全合规的平台化电子签章服务，可为各类应用提供安全合规的电子签章服务，保障应用服务的安全性、可靠性、权威性。

电子签章服务可帮助用户单位将签章使用审批、签章验章操作、公文合同存档等原有线下工作流程全部线上化、电子化，电子政务全流程实现线上闭环，提升签章使用效率的同时，借助流程管理、模板管理、签章审计管理，进一步规范签章使用，高效同时确保安全。

服务平台以 API 方式为业务系统提供电子签章功能，业务系统无需改变原有签章审批操作业务流程，平台服务模式下无需额外采购硬件设备，电子签章服务 API 除签章、验章等基本电子签章功能外，同时考虑到电子签章使用各类场景需求，可以灵活的为用户提供所需如数字证书、短信、证照查验、人脸比对等第三方服务，用户业务系统仅需一站式集成电子签章服务 API 即可为原有业务快速实现电子签章服务。

（2） 数据传输保护服务

数据传输保护为数据在不同安全域上的传输构建安全通道，可支持用户单位安全访问

门户网站、移动办公、远程访问 OA 系统、数据共享管控等业务场景。数据传输保护服务是平台跨部门数据安全共享最重要的安全技术支撑。

服务平台可依托 VPN 安全网关、终端安全套件保障用户跨网络间数据传输安全、终端与应用之间的数据传输安全。

（3） 数据库加密存储服务

数据库加密存储服务，是服务平台提供给用户，用以保障数据库数据存储安全。该项服务，是基于数据库透明加密原理的数据库主动防御产品，具有高性能、透明加解密及完整性保护、密钥合规生命周期管理、多因素身份认证、基于加密的权限控制等功能特性。

数据库加密服务可防止数据库明文存储引发的数据泄密、突破边界防护的外部黑客攻击及内部高权限用户非法对数据的窃取。该服务使用密码技术对敏感数据进行加密和完整性保护，在数据写入数据表前保护数据，数据返回前解密或验证数据；密码运算过程是在数据库逻辑层面调用服务接口进行，对应用程序和用户完全透明无感知。

（4） 文件加密存储保护服务

依托服务平台的文件加密保护服务，用户可保护文件在存储过程中的安全。服务平台可为用户提供文件加解密服务、文件完整性运算服务，为应用系统文件加密提供密钥管理服务。

（5） 数据脱敏服务

服务平台可提供数据脱敏服务实现数据的隐私性保护。系统支持用户系统的隐私数据发现、数据提取、数据漂白、测试数据管理、数据装载等功能，多种脱敏算法（可选）对敏感数据进行变形、屏蔽、替换、加密。

数据脱敏服务可针对用户数据进行流程化管理，满足用户各种数据使用场景，既遵循了法规要求，又很好的保障了用户信息安全。可以针对不同的用户和数据处理情况设置不同的脱敏规则和算法以达到不同的脱敏效果，提升操作效率，满足审计及监管部门要求。

5.2. 运营管理功能

5.2.1. 设备集中管理

平台可对密码资源设施、密码基础设施、数据安全设施统一调度和集中管理，设备部署和服务能力可灵活便捷地动态伸缩扩展。

服务平台采用密码资源池的概念来集中管理各种密码设备。平台可以管理支持虚拟化的云密码机，也支持传统的密码设备和密码基础设施，如服务器密码机、签名验证服务器、密钥管理系统、数字证书系统等。

5.2.2. 运维管理

支持完备的运维管理，包括应用管理、资源管理、服务目录、服务日志、系统监控等功能，提供运维工单管理。

应用是指租户单位的各类应用业务系统，这些应用系统需要连接到服务平台并获取服务。应用业务系统在使用密码服务前，须完成应用信息在平台中的登记注册，并配置对应的应用认证策略。应用管理是从协助用户规划系统业务的角度出发，建立服务平台对应用的密码服务关系。

服务平台管理密码设备和系统、数据安全防护产品，聚合为统一的服务接口，在平台界面向租户单位展示可选取的密码服务目录。租户单位的应用与服务平台的某类的服务关系通过审批并建立，则应用可接入服务平台进行认证和获得对应的服务。

服务平台能够实时监控、分析密码资源的使用情况、密码服务的运行情况、业务应用的密码服务调用情况等，为密码管理、密码运维、密码运营等提供科学决策依据。

5.2.3. 云租户管理

支持多租户服务模式。租户是指最终需要使用密码和数据服务的客户单位实体。本服

务平台每个租户之间采用了安全隔离机制，确保各租户使用的密码资源相互隔离。服务平台为各租户单位建立管理员账号。租户单位管理员可通过安全通道登录密码服务平台，以本单位的租户管理视角进行应用、服务、资源配额、统计分析等功能操作。

5.2.4. 服务配额和计费管理

服务平台按租户分配密码资源，支持按应用、服务类型等进行配额管理。针对应用系统、密码服务类型、服务配额比例等进行细粒度的控制管理，针对不同类型的密码服务、数据安全服务提供多维度的计费模式。

服务平台对服务资源按租户进行统一分配及运维管理。服务资源分配至各租户后，租户可自行规划应用与服务资源的配额分配关系。

5.2.5. 数据报表

数据报表用于对系统中的设备资源数据、应用数据、服务数据、业务数据、运行日志等进行统计，生成必要的统计报告，以满足日常工作汇报、运营数据汇总的需要；结合测评合规需求，输出合规分析报告。

5.2.6. 可视化大屏

服务平台可将平台运营中的各种数据进行综合处理，以可视化大屏的方式进行宏观展示。大屏可从平台整体运维角度、租户单位租用服务角度，展示各类服务调用统计、流量统计，系统、设备、服务的实时运行状态、实时调用信息；应用、服务、计费的阶段统计及各类排名。

服务平台为平台运营单位、租户单位均可提供大屏展示。

图 产品主要功能-4中数国科密码服务平台大屏图

5.3. 高可用与弹性扩展

5.3.1. 高可用高可靠服务能力

服务平台提供密码服务调用从接入层、服务层、资源层的全流程双冗余机制，结合密码服务亲和技术，实现大容量、高并发、高稳定服务。

服务采用限流、熔断机制。密码服务可以针对 TPS 和吞吐流量限流，密码服务可设置熔断策略，通过熔断策略可以拒绝异常访问，并采用了故障熔断自愈机制。

5.3.2. 服务按需定制

服务平台可针对用户应用场景，按需定制密码应用设计。采用无代码技术和低代码开发技术实现服务编排，缩短用户定制业务上线周期。

服务平台具备优异的服务扩展能力，可快速集成第三方产品或系统，以统一的服务入口，为用户提供多样化的服务类型。

6. 优势亮点

6.1. 密码应用合规，数据全生命周期防护

以通过商密测评的基础密码产品为基础，设计符合等保 2.0 和密评标准体系，建设满足

密码测评要求和密码应用需求。

符合《数据安全法》、《工业和信息化领域数据安全管理办法》，提供数据全生命周期安全防护。

6.2. 聚合密码和数据安全防护能力，实现平台化交付

密码服务平台采用多模式资源集成技术，聚合各种密码设备和系统、数据安全防护产品，对外向用户业务应用系统提供统一的透明服务。

服务平台针对数据加密运算、签名验签运算、应用密钥管理等服务，平台服务节点网关采用服务集成模式，对应用进行认证、配额控制，实现多维度的服务量化管理；针对不宜再进行封装的密码产品系统、或为了快速集成第三方产品系统，平台采用管理集成模式，实现统一提供服务的目标，服务的配额控制、服务计量，由密码运营平台与提供服务的密码产品系统直接对接实现。

6.3. 云原生部署，服务能力弹性伸缩

支持云平台部署，支持丰富多样的底层密码产品设备、数据安全系统，服务能力可灵活便捷地动态伸缩扩展。

密码服务及数据安全资源集群调用，故障熔断自愈，提供大容量、高并发、高稳定服务。

采用 API 服务编排技术，缩短用户定制业务开发周期，快速扩展用户业务。

6.4. 多租户服务与流控计费，完备的服务运营支撑

支持多租户、多应用的细粒度服务配额与计费，提供丰富的运维管理和租户管理功能基于租户、应用、服务等提供细粒度的资源分配与控制，多维度的计费模式，运维工单管理、大屏展示。

采用多级消费者标识和流控技术，实现应用可信标识、安全访问鉴权和精细化限流。针对不同类型的密码服务，在配额管理和服务量化采用不同维度，如：带宽 Mbps、TPS、应用数、客户端数、用户数、证书数等。

服务平台可支持服务集成模式，基于运营平台分发服务策略，从服务带宽、TPS、服务调用次数等维度进行细粒度的服务计量和流量控制；服务平台可支持管理集成模式，密码运营平台对接各密码产品管理系统，基于各配额维度，进行服务量化控制。

例如，对于密码计算服务，可基于应用接入数量、加解密 TPS 进行配额、流控；身份认证服务，可基于应用对接数量、可认证用户数进行配额、流控；电子签章服务，可基于托

管签章数量、每月可盖章次数进行配额、计量；证书管理服务，可基于证书颁发数量（可分证书种类）进行配额、计量。

7. 产品部署

中数国科密码服务平台可应用于政务、金融、能源、交通、电力、装备制造等行业领域，助力建设各级政务云平台、国资云平台，为用户业务系统提供密码服务能力和数据防护能力，为用户提供数据加解密、数据签名验签、密钥管理、数字证书认证、时间戳签名、数据脱敏等密码、数据安全服务。

中数国科密码服务平台可灵活应用于传统网络国密改造、私有云平台合规建设、政府建云企业上云合规建设等场景。中数国科按用户要求，提供多样的建设和服务模式，帮助用户建设服务平台，支撑用户密码应用、数据应用系统快速对接上线；协助建设单位（或共建）服务平台，满足建设方按租赁模式运营。

下图是密码服务平台在云环境多租户模式下的部署图。

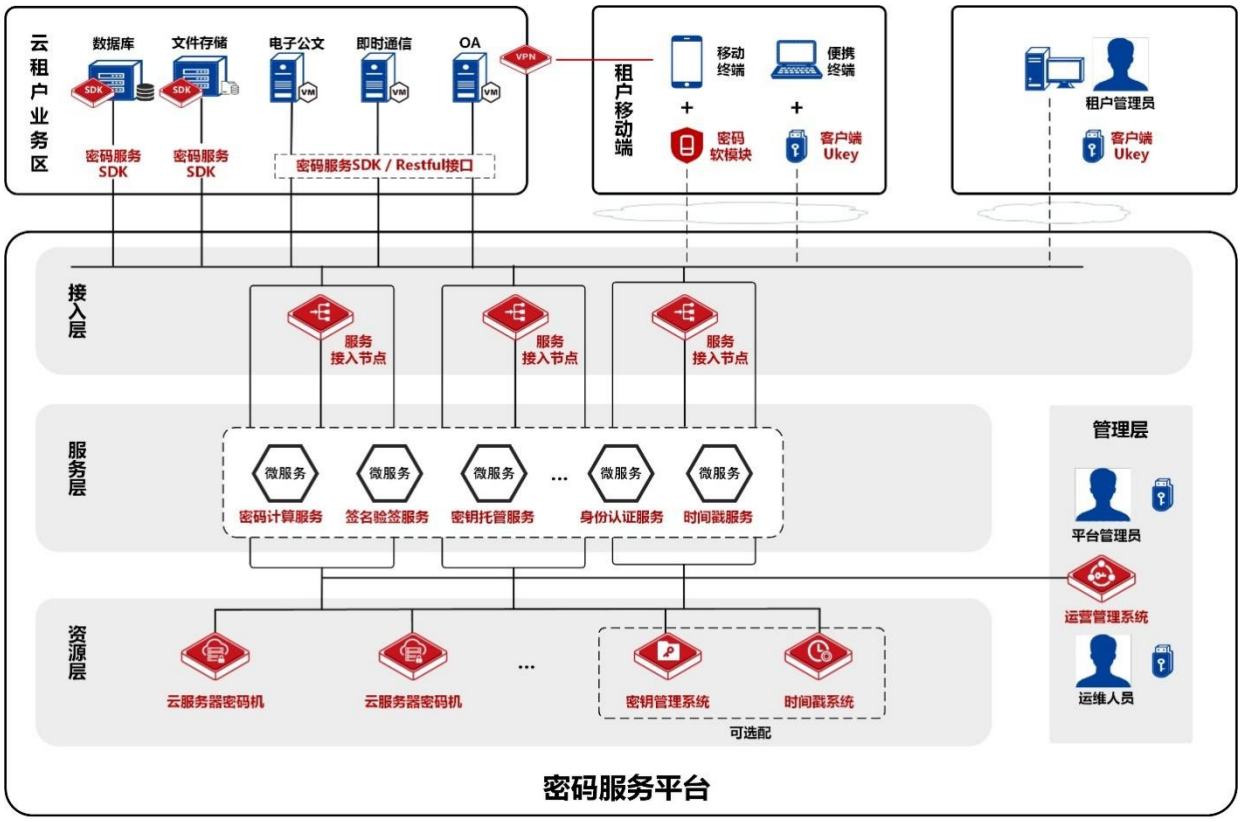

图 产品部署-5中数国科密码服务平台 多租户模式部署图

8. 性能与参数

密码服务平台具备优异的服务弹性扩充能力，可通过增加底层的密码资源设备、扩充IT设施，增加服务能力，满足用户系统建设需求。

- 支持的租户单位数：100 个
- 支持的租户管理员数：500 个
- 支持的应用系统数：1000 个

- 可部署的服务节点数：100 个
- 可管理的后台密码设备及数据安全防护产品数：200 个

9. 效果和收益

中数国科基于密码基因打造安全合规、统一管理、部署灵活、服务弹性可计量的服务平台，为用户业务应用系统提供密码服务、数据安全服务，致力于为用户打造数据全生命周期防护服务平台，筑牢数据安全新防线。

（1） 满足安全合规要求

符合密码法和等级保护相关管理和技术要求，采用经过商密检测的产品和技术，标准化提供密码服务，有效满足用户“安全、合规、便捷”应用密码的需求。

（2） 资源优化管理、服务量化可见

密码服务平台以密码服务、数据安全服务为运营对象，将资源最大力度优化，提供资源池化、弹性可扩展、泛在接入、按需购买、可计量的服务。

服务能力由密码产品化输出转向云密码服务化输出，让密码在用户中“流动”起来，密码价值看得见。

（3） 提高安全防护水平，缩短建设周期

通过基础及通用密码服务，从“云、管、端、边界”全方位保障用户业务和数据安全，整体提高安全风险防护水平。

用户使用平台提供的密码服务与应用系统对接，可实现业务快速上线，缩短用户业务建设周期。

（4） 实现降本增效

服务化引入密码能力，无需用户采购额外的硬件设备系统；全托管式服务，降低用户管理运维投入，最大限度在增强安全性同时，为用户实现降本增效。