中数国科密码应用监测平台
产品白皮书
（监测版）

（中数国科集团）

目录

1. 前言

近年来，随着《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》的颁布和实施，国家有关部门在密码应用建设方面提出了一系列的合规要求。2019 年，全国人大常委会通过了《密码法》，该法是我国密码领域首部国家层面的综合性、基础性法律，《密码法》的颁布和落实将充分发挥密码在保护我国网络空间安全的核心作用。同年，国务院办公厅发布《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号），要求政务信息化项目按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。2021 年，国务院颁布《关键信息基础设施安全保护条例》，明确界定了关键信息基础设施的范围，明确要求“采取技术措施或其他措施，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。”综合近年来不断出台的法律法规和政策文件，国家政务信息系统、关键信息基础设施、网络安全保护第三级以上的系统都需要进行密码应用安全性评估。但是，国内各地密码主管部门和信息系统运营单位难以及

时评估密码应用建设成效，识别密码运行风险和总结密码应用态势，因此无法针对自身业务系统的实际情况和安全防护体系的薄弱环节有的放矢地开展密码应用体系建设，严重制约各地密码应用建设合规化的进程。

为解决信息系统运营单位的上述问题，中数国科通过自主研发设计的中数国科密码应用监测平台融合密码应用行为分析技术，密码事件建模分析技术、多源数据融合技术等核心关键技术，将密码技术应用在密码应用检测控制、密码应用风险预警、密码应用态势感知、密码应用合规性检查等方面，实现一体化密码状态监测、一张图密码态势呈现、协同化密码风险预警和多样化密码管控处置，确保用户信息系统在规划、建设、运行等各个阶段密码应用合规性、有效性和正确性。

2. 产品概述

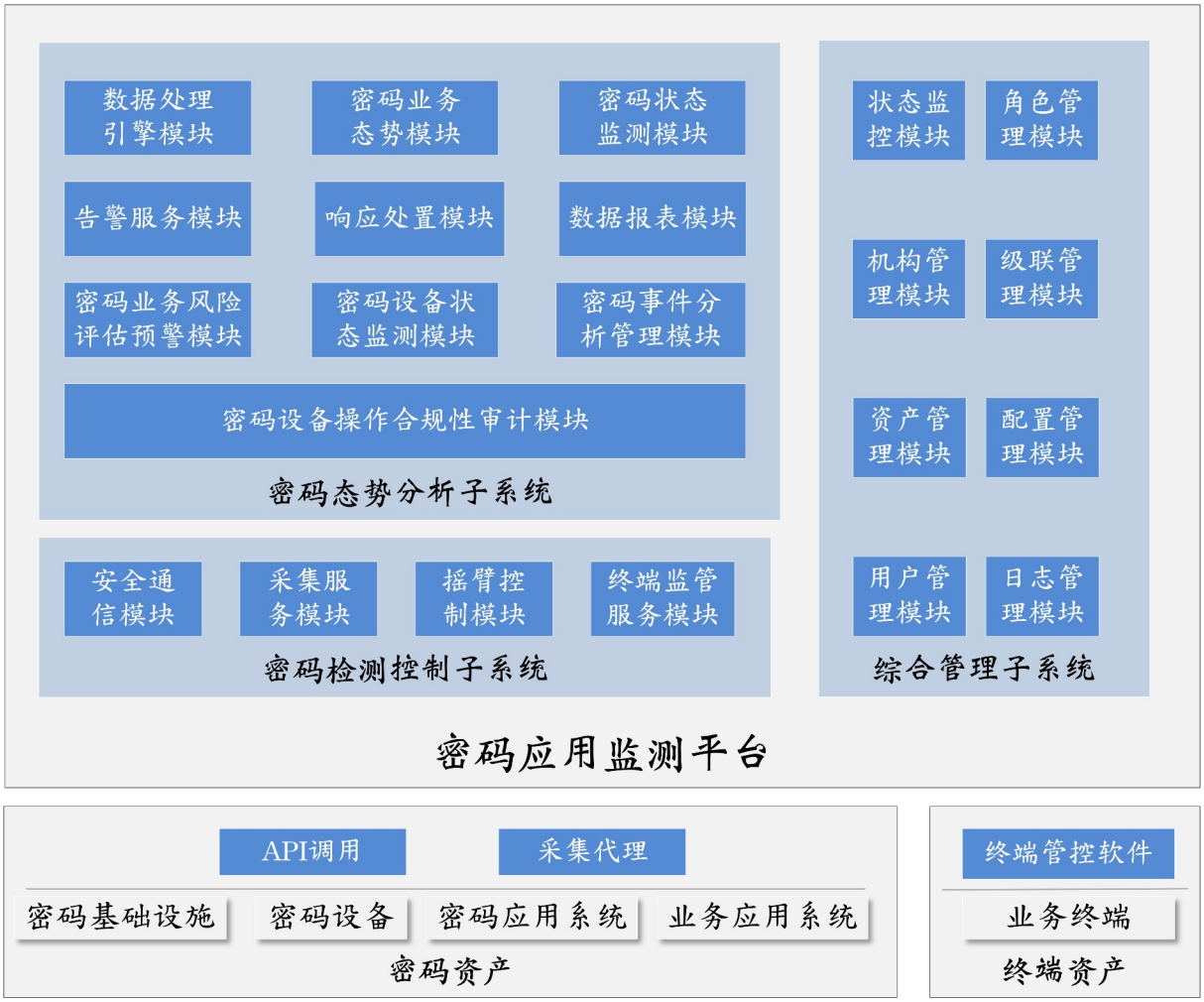
中数国科密码应用监测平台（以下简称密码应用监测平台）是中数国科集团严格遵照国家技术规范，融合密码管理监测技术与态势感知技术，面向密码主管部门和信息系统运营单位密码基础设施、密码设备、密码应用系统、业务应用系统、终端等提供多维度、全景式、智能化的检测控制与态势感知的新概念产品。

针对密码主管部门，部署本产品可帮助用户实时掌握自身密码应用合规性、有效性和正确性，并结合自身业务应用实际情况，进行策略下发和远程管控，并为应急处置和保障提供技术支撑。针对信息系统运营单位，部署本产品将帮助用户对其主管范围内的密码应用进行全面的态势感知，对密码应用建设成果进行展现，为用户开展密码应用检查、监督、指导等工作提供技术支撑。

3. 产品架构

中数国科密码应用监测平台在产品架构设计上秉承“模块化耦合、标准化设计、高安全架构、精细化管理、智能化分析、可视化呈现”设计原则进行产品架构设计，平台

由密码检测控制子系统、密码态势分析子系统、综合管理子系统三部分组成，各部分内部又分成若干个模块。产品功能架构如下图所示。



密码检测控制子系统通过 API 调用或采集代理的方式，负责与被监管设备对接实现密码相关数据的采集和相关控制指令的下达，由安全通信模块、采集服务模块、遥臂服务模块和终端监管服务模块四部分组成。

密码态势分析子系统负责整个系统的数据处理和业务逻辑实现，包括数据处理引擎、

密码设备监测、密码事件管理、密码设备操作合规性审计、密码业务风险评估和预警、告警服务、响应处理、数据报表、密码业务态势九大模块组成。

综合管理子系统是承担了整个系统的维护、配置和管理功能。包括状态监测、用户管理、角色管理、资产管理、机构管理、级联配置、配置管理和日志管理。通过综合管理子系统可以对系统所管理的机构、资产进行配置；也可以对系统的用户、角色权限进行配置；还可以查看系统所有的操作日志以及对系统运行参数进行配置。

4. 产品特点和优势

4.1. 一体化密码状态监测

中数国科密码应用监测平台可对泛在化的密码应用进行一体化监测，通过采集到的网络密码设备、密码应用设备、密码应用系统、业务应用系统的各种硬件信息、工作状态、软件服务状态，结合网络连通性和交互关系，对于整个业务各个节点工作情况进行监控，以建立起面向密码保障系统的一体化监测能力，从而保证关键业务系统持续正常工作。

4.2. 一张图密码态势呈现

中数国科密码应用监测平台通过收集各种数据并进行综合处理，以可视化大屏的方式进行宏观展示。基于系统中密码设备状态、管理员操作行为记录、密码事件和风险评估数据，和具体的单位、资产、业务系统、人、密码模块进行关联，形成密码业务态势，进行可视化展示。同时支持根据不同用户的需求定制展示内容和查看权限，并可与网络安全态势感知对接，构建整体安全态势。

4.3. 协同化密码风险预警

中数国科密码应用监测平台通过将用户身份信息、访问行为、其所处环境、上下文进行关联分析，形成各类密码事件，根据这些事件的类型、级别、风险度进行综合的量化，达到一定阈值后可以认为是风险访问并进行告警，从而快速、准确地发现密码业务中的高风险环节，预警密码事故的发生，并总结形成规则库、事件库和情报库实现横向协同和纵向支撑。

4.4. 多样化密码管控处置

中数国科密码应用监测平台提供日常策略下发和管控能力，保证全网设备的管控策略一致以及中心端的管控指令顺利下达和执行；针对远程的风险、告警和事件能够进行及时的应急处置，将单点风险的处置措施迅速同步至全网所有设备，避免安全、保密事件的发生和扩大。

5. 产品主要功能

5.1. 数据采集与摇臂控制服务

通过部署采集代理主要完成密码基础设施、密码设备、密码应用系统、业务应用系统、终端等资产的数据采集和执行摇臂控制指令或生效下发的管理策略并反馈执行结果。数据采集即数据接收，通过采集客户端将采集的数据通过安全通信模块上传至采集服务端。遥臂控制是指由采集服务端将遥控指令通过安全通信模块下发之客户端，客户端解析、执行指令并将执行结果反馈。

5.2. 终端监管服务

通过终端监管服务模块与平台在各个检测对象部署的终端管控软件协同工作，完成业务终端信息的采集。业务端采集的信息包括：业务终端运行状况、访问应用系统日志、业务终端程序运行日志、业务终端防病毒模块运行情况等。业务采集的各类信息将用于进行密码态势分析并以可视化的方式面向用户呈现。

5.3. 密码设备状态监测

通过采集到的密码相关业务系统包括网络密码设备、密码应用设备、密码应用系统、业务应用系统的各种硬件信息、工作状态、软件服务状态，结合基础的网络连通性和

交互关系，对整个业务各个节点工作情况进行监控，以保证关键业务系统持续正常工作。监测的信息包括各节点设备的 IP 地址、在线状态、CPU 使用率、内存使用率、硬盘使用率、累计的事件数量、告警数量、综合的风险评估得分等，通过这一模块还可以向下点击钻取对应的告警、事件等详细信息。

5.4. 密码事件分析管理

密码事件分析管理包括后台的密码事件识别和分类、前台的密码事件查询分析两部分。密码事件识别和分类是以业务用户使用日志为基础数据，配合系统中内置的密码事件规则定义，对用户的使用行为进行数据的关联分析，生成各种密码事件，同时对事件类型区分、级别定义、风险度评估，综合评价达到一定程度时可以进行告警和后续的处置。

5.5. 密码设备操作合规性审计

密码设备操作合规性审计模块是对系统集中收集、存储密码相关业务系统各节点设备的管理员操作日志进行分析处理，从而达到以下几个目的：

- □实现日志的集中存储、统一管理，使得日志管理满足国家相关的留存时间要求；
- □对管理员操作进行审计，检查其操作是否符合规范，是否存在人为的配置不当，甚至主观的破坏性行为；
- □一旦出现密码相关的事故可以作为存证数据进行溯源查询和分析。

5.6. 密码业务风险评估和预警

通过将用户身份信息、访问行为、其所处的环境进行关联分析，形成各类密码事件，根据这些事件的类型、级别、风险度进行综合的量化，达到一定阈值后可以认为是风险访问，进行告警，从而快速、准确地发现密码业务中的高风险使用，预警密码事故的发生。

5.7. 密码事件告警

基于收集到的资产数据、密码业务数据、运行环境数据、网络通联关系等进行关联分析、基线对比、数据统计，从大量的信息中发现违背规律性的、可疑的、高风险的事件进行告警。一般来说，告警事件都是系统中关键性的事情，也是需要重点关注和干预的，所以告警服务与响应处理服务对接，实现对告警事件的处理、跟踪、反馈的闭环。

5.8. 响应处置

响应处置是对系统中发现的异常事件的处理、响应、跟踪和反馈功能。将异常的事

件转化为工单，并推送给相应的人员，进行人工处理，从而实施系统与人的互动，将技术化的系统管理与制度化的人工管理相结合，真正将业务从技术和制度两个维度共同管理起来，实现相辅相成，共同促进的目标。

响应处理模块在系统中具体的体现方式是工单，工单从创建开始就是一个流程化的过程，创建之后可以进行分派、处置、反馈，最终关闭。在进行工单处理操作时又可以与密码检测控制子系统中的遥臂服务模块进行联动，对远端的密码业务设备进行诊断、配置下发等。本功能可实现与不同单位、不同业务、不同场景进行深度融合，做到真正符合用户需要，提供与既有工单系统、OA、事务处理系统的对接能力，根据业务场景需要进行对接联动。

5.9. 数据报表

数据报表用于对系统中的资产数据、密码业务数据等进行统计，生成必要的统计报告，以满足日常工作汇报、数据汇总的需要，结合测评合规需求，输出合规分析报告。

5.10. 密码业务可视化

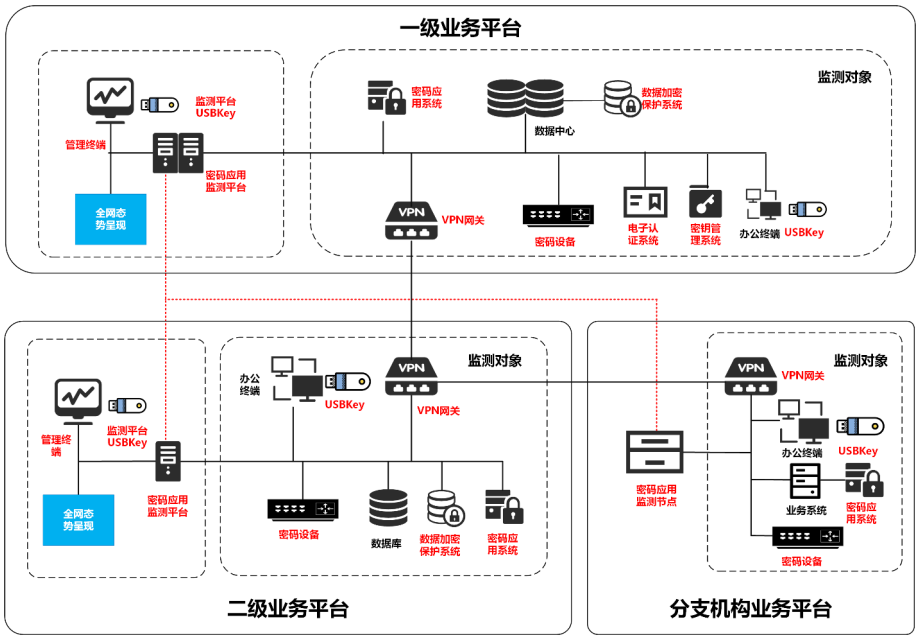
密码业务可视化模块是将系统中收集到的各种数据进行综合处理，以可视化大屏的方式进行宏观展示。基于系统中密码设备状态、管理员操作行为记录、密码事件和风险评估数据，与具体的单位、资产、业务系统、人、USBkey 进行关联，形成密码业务态势，进行可视化展示（如下图示意，具体根据项目进行定制开发），具体可以包括：

- 设备运行态势
- 设备管理行为审计
- 密码业务合规性评估
- 密码业务风险态势和预警
- 事件处置态势
- 密评合规一张图

6. 产品部署

中数国科密码应用监测平台可部署于密码主管部门数据中心或大型信息系统（政务云、公有云、大中型企业业务信息平台）数据中心，并支持级联部署，可在二级业务平台或分支机构部署密码应用检测系统主机或监测节点，已达到全面覆盖用户密码基

础设施、密码设备、业务应用系统、终端的目的。产品部署如下图所示：



7. 性能与参数

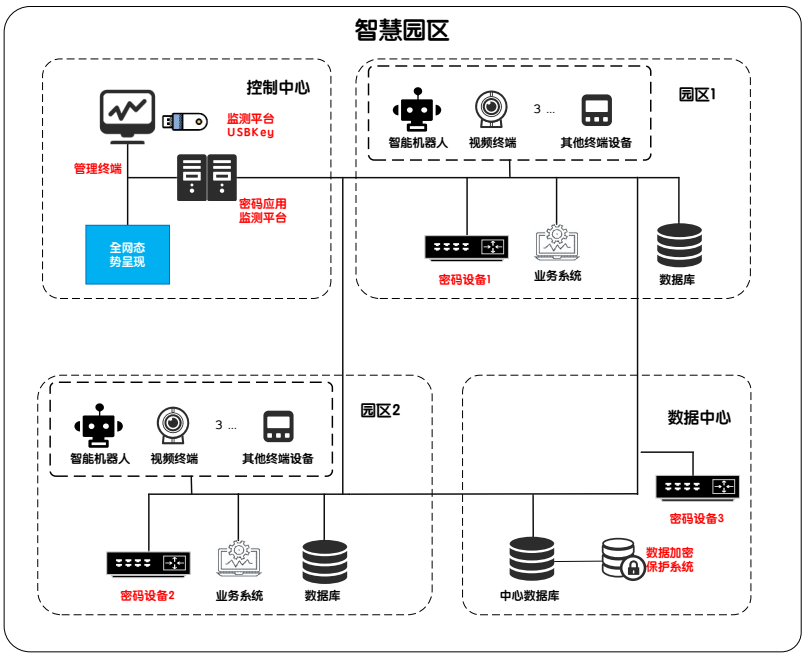
- 监测对象范围：密码基础设施（密钥管理系统、数字证书认证系统）、密码设备（服务器密码机、VPN 安全网关、PCI-E 密码卡、安全接入终端等）、密码应用系统（身份认证系统、电子签章系统等）、业务应用系统（部署 PCI-E 密码卡或软件密码模块的服务器等）和终端（PC 终端、移动终端）等；
- 可同时监测对象数量：10000 以上；
- 可同时摇臂控制对象数量：10000 以上；

- 日志平均处理能力（每秒日志解析能力 EPS）：20000EPS；
- 峰值日志处理能力（每秒日志解析能力 EPS）：30000EPS；

- 支持的数据采集方式包括不限于：SYSLOG、FTP/SFTP、HTTP、API 接口、专用代理插件等方式采集日志等；
  - 日志留存时间：六个月以上；
  - 可识别密码事件种类：18 类；
  - 密码事件识别准确率：99%以上；
  - 应急响应时间：1 分钟以内；
  - 平均无故障时间：10000 小时以上。

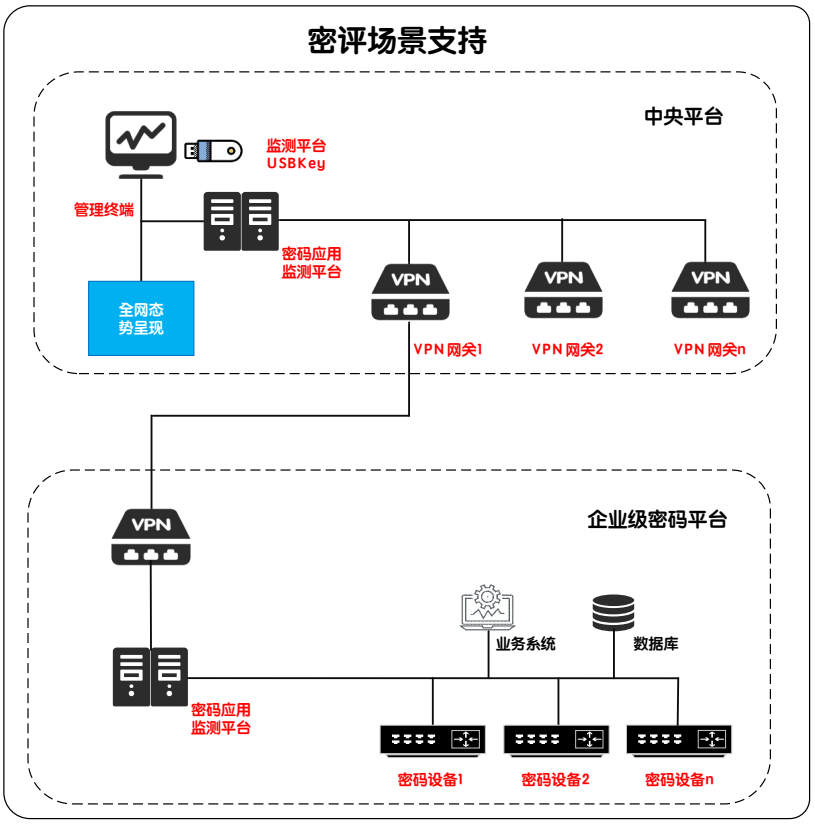
8. 应用场景

8.1. 本地密码设备监控



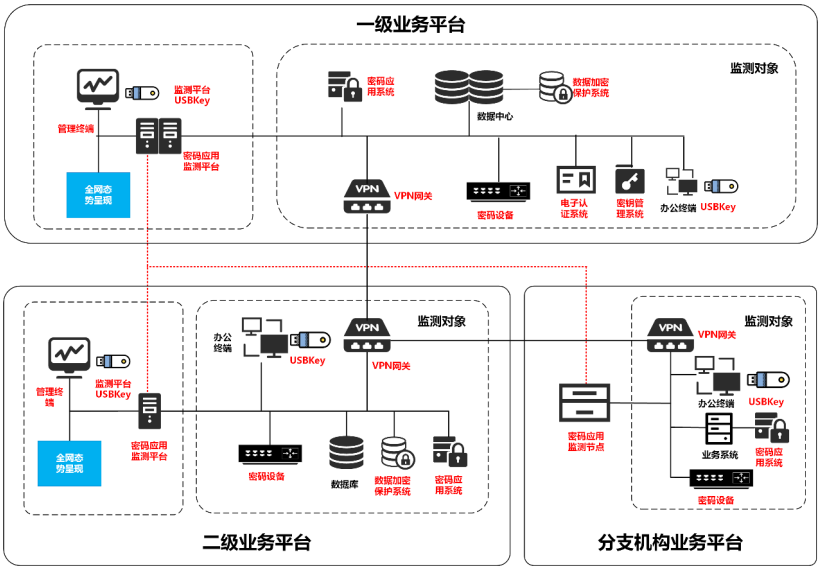
对零散分布密码设备进行监控，实现设备的统一管理。适用于中心对分布式节点（如分散的场站）的密码设备或泛在部署的密码设备（ 智慧园区、物联网安全设备）的集中监测。

8.2. 密码测评工作协助



从业务系统的视角，依据密评的合规项要求，对业务系统所涉及的各类密码设备和密码应用进行监测。适用于呈现出平台上应用系统在初次密评及定期密评中所需了解的密码应用使用情况，辅助密评机构完成密评。

8.3. 横纵向密码应用联动



在平台运行过程中，将学习获取的密码事件规则同步到其他密码监测平台上。适用于层级化部署的业务场景中，某个节点的密码态势和时间规则信息能够实施同步到部署平级和上下级的密码应用监测平台，实现态势联动和情报协同。

9. 效果和收益

中数国科密码应用监测平台的建设和部署将显著提升用户密码应用防护和管理能力，中数国科密码应用监测平台可以系统化指导密码合规建设和改造工作，为用户解决密码情况难掌握、密码应用难感知、密码风险难发现、密码赋能难统筹等技术和管理难

题，从而形成顶层的密码事件分析和应对能力，有效减少各类密码事件的发生及其造成的损失。