# 中数国科服务器密码机
# 产品白皮书

（中数国科集团）

# 目录

# 一、 前言

## 1.1 应用现状

现代社会被称为“信息社会”，信息技术渗透到政治、经济、产业、服务领域的所有部门，信息化产业在国民经济中占有的比重越来越大。信息化产业发展水平和信息基础设置建设水平，是衡量社会现代化的重要指标。随着互联网、物联网、移动互联网、大数据等领域的发展，社会信息化达到了前所未有的高度，极大刺激了我国的经济发展。社会信息化程度越高，产生的信息数据越多，信息安全的问题就越突出。在享有信息化高速发展带来便利和效率的同时，如何有效的保护信息安全，是摆在政府、企业、个人面前的共同问题。服务器密码机作为高端的商用基础密码产品，它既可以为信息安全传输系统提供高性能的数据加/解密服务，又可以作为主机数据安全存储系统、身份认证系统以及对称、非对称密钥管理系统的主要密码设备和核心构件，具有广泛的系统应用潜力。可广泛应用在银行、保险、证券、交通、邮政、电子商务、移动通信等行业的安全业务应用系统中。

服务器密码机具有高速多任务并行处理的密码运算能力，提供安全完善的密钥管理机制，支持所有国内国际主流的密码算法。同时服务器密码机以独立主机通过网络的形式提供密码服务，可以做到和其他应用系统松耦合，保证了其他应用系统和密码机的各自独立性，降低了使用方开发、应用、维护等各方面的难度和成本。综上所述，服务器密码机是一个能提供通用、易用和强大密码服务的完整主体，能够适用于各种应用密码方面的需求，有着广泛的市场需求和前景。

## 1.2 政策要求

根据《国家商用密码管理条例》规定“商用密码的科研成果，由国家密码管理机构组织专家按照商用密码技术标准和技术规范审查、鉴定，密码算法必须采用国家密码管理局审

批的硬件算法”，随着国家对信息安全的要求的提高，市场对国产服务器密码机产品有很迫切的需求。

从政策层面，网络安全已上升为国家战略，成为总体国家安全观的重要组成部分“没有网络安全就没有国家安全”。而密码技术作为网络安全重要的主动防护技术，在国家信息化进程中也得到了更多的应用和发展。国家持续提升在政策上对密码应用推广的扶持力度和密码测评的强制执行，制定和颁布了一系列法规和标准，对密码技术和密码服务的应用提出了要求。

# 二、 产品概述

## 2.1 产品简介

中数国科服务器密码机（以下简称服务器密码机）是由我公司自主研发的密码设备，适用于各类密码安全应用系统进行高速的、多任务并行地处理各种密码运算，可以满足应用系统数据的签名/验证、加密/解密、完整性校验、密钥生成和管理等服务，保证传输信息的机密性、完整性和真实性，同时提供安全、完善的密钥管理机制。

中数国科服务器密码机可以独立为应用系统提供高性能的数据加解密服务，也可作为身份认证系统、密钥管理系统等系统的主要密码设备和核心构件。密码应用系统通过调用密码机提供的标准 API 函数来使用密码机的服务，密码机 API 与密码机之间的调用过程对上层应用透明，应用开发商能够快速地使用密码机所提供的安全功能。密码机 API 接口符合《密码设备应用接口规范》，通用性好，能够平滑接入各种系统平台，满足大多数应用系统的要求，在应用系统安全方面具有广泛的应用前景。

## 2.3 产品形态

中数国科服务器密码机是应用层密码机，是一个物理安全的实体，承担主机安全模块

（Host Security Module）的作用，能够实时地为主机提供密钥管理、对称密码算法运算、非对称密码算法运算、杂凑运算、随机数生成等密码服务，可以保证应用数据在产生、传输、存储到使用等各个阶段的机密性、完整性、真实性等。该密码机采用专用的密码设备——自研的密码卡，作为密码运算和密钥管理的核心部件。

## 2.4 产品组成

中数国科服务器密码机采用国产安全平台，包括国产处理器，国产操作系统，自研的PCI-E 密码卡。服务器密码机支持 SM1、SM2、SM3、SM4 国家密码算法，同时支持 RSA 1024/2048、AES、3DES、DES、SHA1、SHA256、SHA512、SHA384、SHA224、MD5 等国际密码算法。

## 2.5 产品架构

服务器密码机具有初始化、密码运算、密钥管理、随机数生成和检验、访问控制、设备管理、日志审计、设备自检等功能。为了实现以上的功能，设计上，服务器密码机由系统平台层、中间层、业务层组成，如图 3.1 所示。

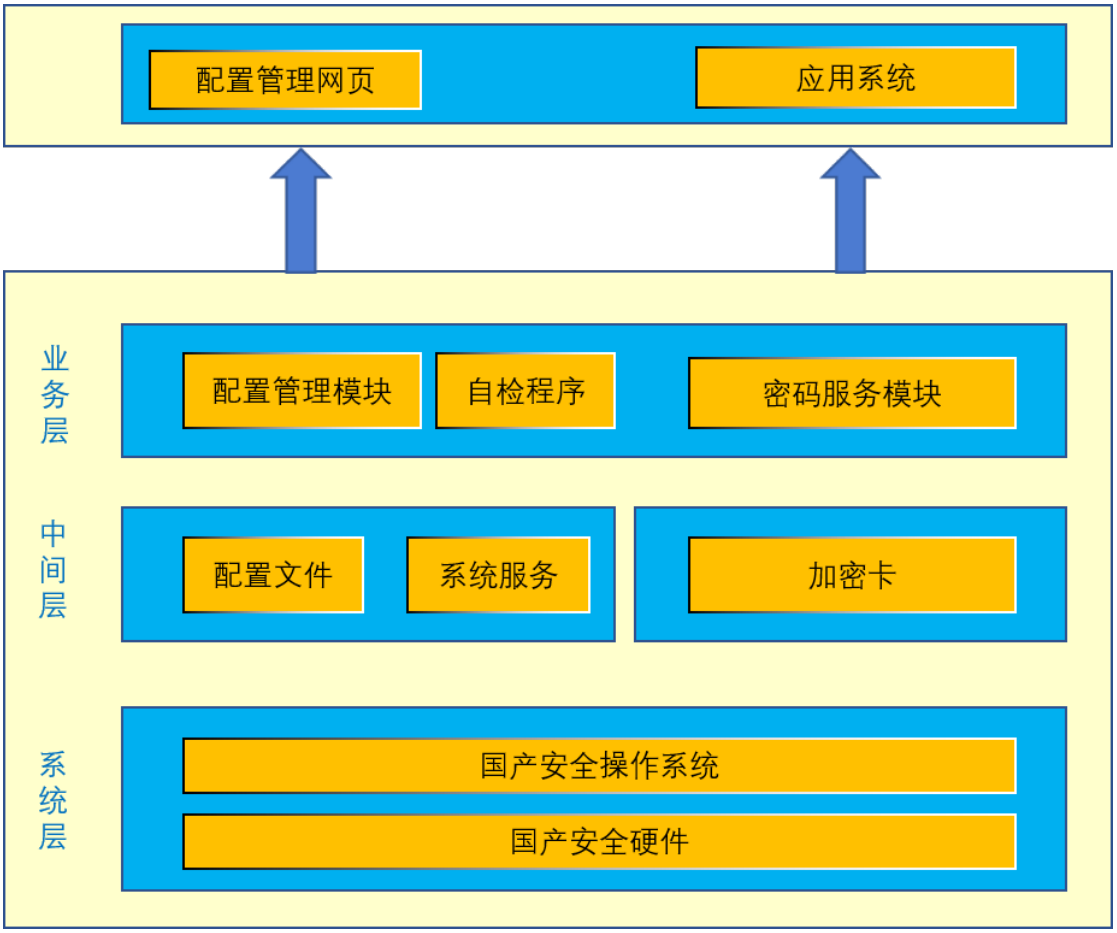


图 3.1 服务器密码机架构图

系统平台层硬件采用国产飞腾平台。操作系统采用已加固的麒麟操作系统。

中间层由密码卡、配置文件、系统服务组成。

密码卡提供密码服务的硬件支撑。密码卡包含密码卡实体硬件、驱动程序和调用接口，提供底层的密码服务硬件支撑。

配置文件记录各种配置和状态信息，供多个模块使用。

系统服务提供所需的操作系统功能。

业务层由配置管理程序、密码服务程序、自检程序组成，是服务器密码机对外提供密码服务、配置管理的功能主体。

配置管理程序包含了所有的配置管理功能：初始化、密钥管理、网络管理、客户白名单管理、权限和访问控制、日志以及备份恢复等。

密码服务程序以程序接口的形式对外提供密码运算服务，包含部署于业务主机的客户端和部署于服务器密码机的服务端两部分。并且密码服务程序包含了销毁事件监听线程，用于响应销毁事件并执行密钥销毁操作。

自检程序执行各项自检操作。

## 2.6 标准和规程

在服务器密码机设计、研发、测试的全过程中，遵循以下标准：

《GB/T 9813 微型计算机通用规范》

《GM/T 0005-2012 随机数检测规范》

《GM/T 0018-2012 密码设备应用接口规范》

《GM/T 0028-2014 密码模块安全技术要求》

《GM/T 0059-2018 服务器密码机检测规范》

《GM/T 0039-2015 密码模块安全检测要求》

《GM/T 0030-2014 服务器密码机技术规范》

# 三、 主要功能

服务器密码机为业务系统提供密码安全服务和各项配置管理功能。

# 3.1 密钥管理

➢密钥生成

采用双物理噪声源随机数芯片生成真随机数，可生成各类对称密钥(SM1、SM4、AES、3DES、DES)和非对称密钥(SM2、RSA 1024/2048 )。

➢密钥更新

支持各类对称密钥和非对称密钥的更新。

➢密钥安全存储

设备密钥对、用户密钥对及密钥加密密钥 KEK 使用管理密钥加密保护，以密文的形式存储在服务器密码机内部的密码硬件中，且授权管理员的 USBKey 登录并验证身份后，才能够提供服务。

服务器密码机内部支持 500 个对称密钥和 1000 个非对称密钥的安全存储。

➢多级密钥管理体系

设备采用三级密钥管理体系，三级密钥分别为：管理密钥，设备密钥对/用户密钥对/密钥加密密钥 KEK，会话密钥，逐层加密。

设备密钥对、用户密钥对及密钥加密密钥 KEK 使用管理密钥加密保护，以密文的形式存储在密码硬件中。

➢密钥的备份与恢复

支持基于备份密钥保护下的密钥和业务数据的备份和恢复功能，保证了安全应用系统的安全性和可靠性。采用基于密钥分割的方式，输出备份密钥分量到用户 KEY 中，保障备份数据的安全性。采取高强度的密钥分割算法，只有满足最少数量的管理员才能进行恢复操作，已备份的密钥和其他业务数据可恢复到相同型号的服务器密码机中。

➢密钥销毁

支持通过管理界面删除指定的对称和非对称密钥，支持通过物理开关对设备内全部密钥进行销毁。具有防暴力拆盖密钥自毁机制，销毁后通过任何技术手段均无法恢复。

➢密钥销毁开关接通后 10 毫秒内硬件自动销毁密钥。

## 3.2 密码服务

➢随机数生成

采用由国家密码管理局批准使用的双物理噪声源芯片生成随机数。

➢签名/验证

签名和验签的服务支持国密算法 SM2,以及国际算法 RSA。

➢非对称加解密

支持国密算法 SM2,以及国际算法 RSA。

➢对称加解密

支持国密算法 SM1、SM4,以及国际算法 AES、3DES、DES。

➢密钥协商基于国密算法 SM2，协商出通信双方可以使用的对称密钥，保障通信安全。

➢摘要运算

支持国密算法 SM3,以及国际算法 SHA1、SHA256、SHA512、SHA384、SHA224、MD5。

➢消息鉴别码

支持基于国密 SM1、SM4 算法的 MAC 产生和验证。

➢数字信封

支持基于 RSA/ECC 密码算法的数字信封功能，并支持由内部密钥保护到外部密

钥保护的数字信封转换功能。

## 3.3 设备管理

➢权限管理

用户访问权限控制：采用两级权限控制模式，管理员、操作员各司其职，提高了密码模块自身的安全性。

用户访问权限控制载体：提供 UKEY 管理机制，实现权限控制中的身份认证和机密数据的安全存储、传递。

➢日志审计

支持审计员对服务器密码机的管理操作行为进行审计。

# 四、技术指标

## 4.1 硬件规格

| | |
|---|---|
| 外观规格 | 2U |
| 尺寸 | 440mm×89mm×560mm |
| 网络电口 | RJ-45 10/100/1000Mb *6 |
| 网络光口 | SFP 1000Mb *4 |
| 电源 | 双模块冗余电源 |
| MTBF | 大于 50000 小时 |
| 工作协议 | TCP/IP |
| 工作电源 | 220V 50Hz |
| 最大功耗 | 120W |
| 工作温度 | 0°C ~50°C |
| 工作环境相对湿度 | 20%～90%RH |
| 存贮环境温度 | -10℃～70℃ |
| 存贮环境相对湿度 | 20%～90%RH |
| 大气压力 | 86～106KPa |

## 4.2 性能指标

| | |
|---|---|
| SM1 加解密 | 840Mbps |
| SM4 加解密 | 830Mbps |
| 随机数生成 | 10Mbps |
| SM3 杂凑 | 880Mbps |
| SM2 非对称密钥生成 | 30000 次/秒 |
| SM2 签名 | 25000 次/秒 |
| SM2 验签 | 21000 次/秒 |
| SM2 加密 | 17000 次/秒 |
| SM2 解密 | 22000 次/秒 |
| RSA 签名 | 1300 次/秒 |
| RSA 验签 | 10000 次/秒 |
| RSA 加密 | 5000 次/秒 |
| RSA 解密 | 1000 次/秒 |

# 五、产品特点及关键技术

## 5.1 安全性设计

➢安全的密钥管理体系

1）利用真随机数发生器产生各类对称密钥和非对称密钥。

2）三级密钥管理体系：分别为管理密钥，设备密钥对、用户密钥对及密钥加密密钥 KEK，会话密钥，逐层加密。

3）设备密钥对、用户密钥对及密钥加密密钥 KEK 使用管理密钥加密保护，以密文的形式存储在加密硬件中。

➢安全的权限控制方式

1）用户访问权限控制：采用两级权限控制模式，管理员、操作员各司其职，提

高了密码模块自身的安全性。

2）用户访问权限控制载体，提供 UKEY 管理机制，实现权限控制中的身份认证和机密数据的安全存储、传递。

➢物理安全

服务器密码机的机箱采用防拆、防撬结构设计。利用全密封机壳、物理锁控制开启面板等技术为密钥的安全管理提供了强有力的保护，且在暴力拆解下密钥将自动销毁。

➢白名单

当用户的主机的 IP 地址在白名单数据库时，用户的主机才能访问服务器密码机，服务器密码机提供 ip 包过滤功能，只有授权的用户主机才可以访问密码机使用密码服务。

➢密钥使用授权

用户密钥对的私钥的使用采用私钥授权码机制，用户在使用非对称密钥的私钥时，需要验证私钥授权码，实现了对每一个用户密钥对的认证，进一步提高了系统的安全性。

# 5.2 产品优势

➢支持多种国密和国际算法

国密算法：公钥密码算法为 SM2；对称密码算法为 SM1、SM4；

杂凑密码算法为 SM3。

国际算法：公钥密码算法为 RSA2048；对称密码算法为 AES、DES、3DES；

杂凑密码算法为 SHA1、SAH256、SHA512、SHA384、SHA224、MD5。

➢真随机数发生器

随机数是系统中关键基础数据，随机数的安全性会影响系统中各种密钥的质量。

➢服务器密码机的设计中采用以下措施保障随机数的随机性：

1）芯片选择：

采用物理噪声源芯片产生随机数，随机数满足国家随机数检测标准。

2）随机数生成：

采用双随机数芯片，提高随机数芯片的冗余能力，避免单片芯片失效；正常工作状态下，每片芯片随机数单独采集。

3）随机数的随机性检验：

通过硬件上电自检、出厂检验、管理程序上电自检、周期性检验和单次检验，确保服务器密码机使用的随机数发生器工作正常，产生的随机数的随机性满足检验规范的要求。

➢密钥快速销毁

密钥销毁开关接通后 10 毫秒内硬件自动销毁密钥。

➢定制的 Linux 操作系统

密码机采用的是定制的 Linux 操作系统。

操作系统是从源代码开始构建的，能够根据自身需要选择、删除、修改操作系统组件，同时，我们采用的是具有优越性能的 64 位的操作系统，因此定制后的操作系统具有很高的运行效率和安全性。

➢高可靠性

1）密钥备份及恢复：支持密钥的备份和恢复功能，保证了安全应用系统的安全性和可靠性。

2）服务器密码机的平均无故障工作时间（MTBF） 大于 50,000 小时。

➢冗余电源供电

采用双模块冗余电源供电，保证电源的稳定可靠。当一个模块出现故障时，能自动切换到另一个模块供电，不会影响系统正常工作。并且电源支持热插拔，可以在线更换故障电源，不必断电。这有效地提高了服务器密码机的可用性，保证系统的连续运行。

➢服务器密码机国产化

服务器密码机采用国产处理器。

➢安全的密钥管理技术

服务器密码机采用高性能、高可靠性的 PCIE 接口密码卡作为核心密码部件，采用三级密钥管理体系，分别为管理密钥，设备密钥对、用户密钥对及密钥加密密钥 KEK，会话密钥，逐层加密。设备密钥对、用户密钥对及密钥加密密钥 KEK 使用管理密钥加密保护，以密文的形式存储在密码卡的存储芯片中。除公钥以外任何密钥的明文不出密码卡。用户访问权限控制采用两级权限控制方式，管理员、操作员各司其职，提高了密码模块自身的安全性。

➢简单易用

可通过 WEB 管理网页轻松的对其进行配置和监控。

# 六、典型部署

中数国科服务器密码机的典型应用场景如下图所示，分为常规应用环境和跨网段用环境。

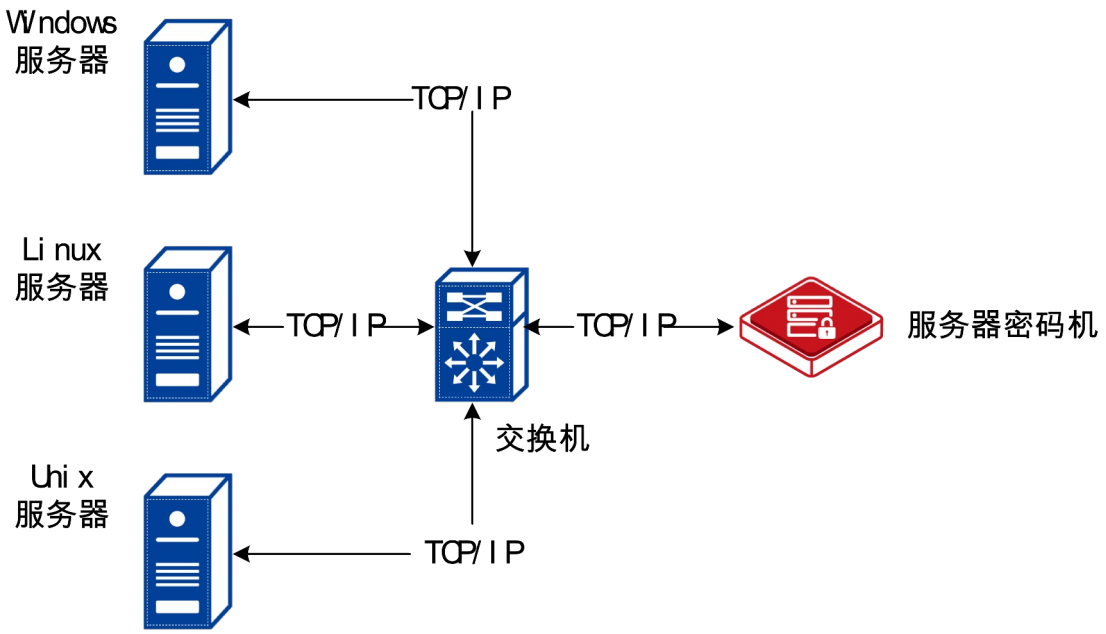


图 6.1 中数国科服务器密码机常规应用环境

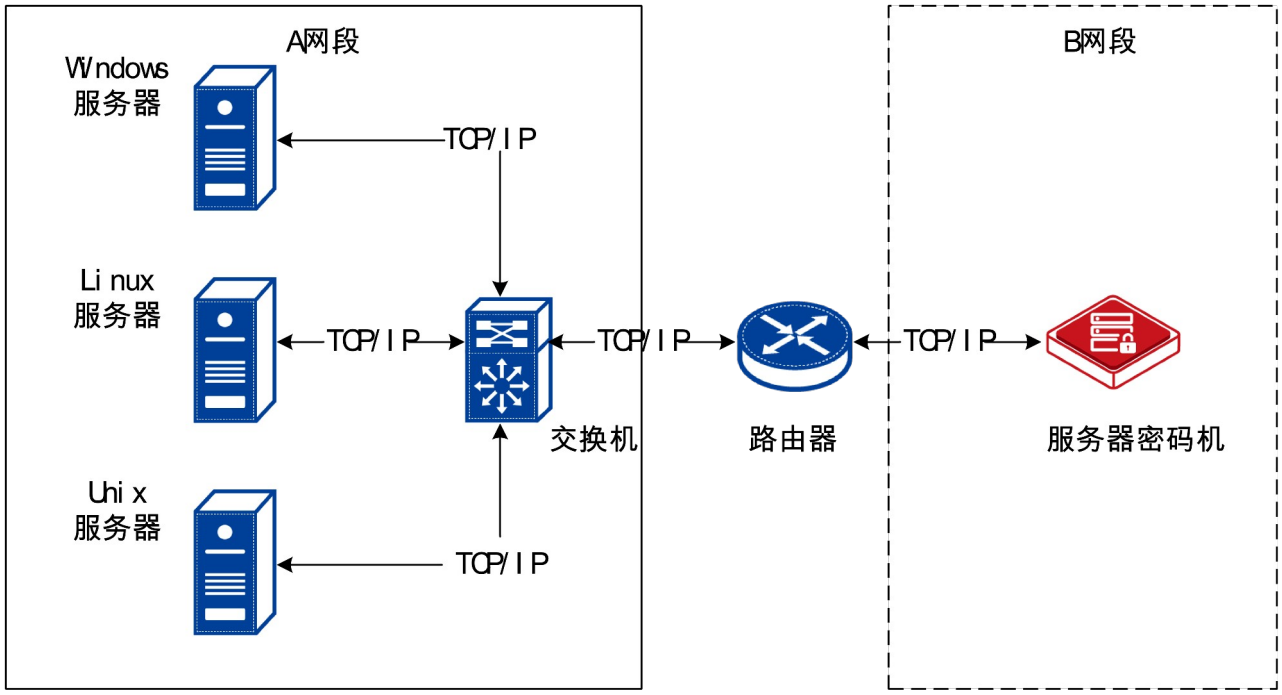


图 6.2 中数国科服务器密码机跨网段应用环境