中安云科
SINOCIPHER

中安云科 金融数据密码机

技术白皮书

V2.4

中安云科科技发展（山东）有限公司

2026-02

特别提示

由于产品版本升级、调整或其他原因，本文档的内容将做不定期性的变更，恕不另行通知。更改的内容将不会补充到本文档，且会在本文档发行新版本时予以更新。本文档仅用于为最终用户提供信息或使用指导，文档中的陈述、信息和建议不构成任何明示或暗示的担保。您所购买产品的配置、功能、特性或服务等应受本公司商业合同和条款约束。本公司不做任何明示或默许担保，其中包括本文档的内容的适售性或符合特定使用目的的默许担保。

联系我们

感谢您使用我们的产品，如果您对我们的产品有什么意见和建议，可以通过电话或电子邮件等方式向我们反馈。

电话：0531-58205218

邮箱：business@sinocipher.com

网址：www.sinocipher.com

公司地址、各地分公司与办事处地址请前往官方网站查阅。

目录

1 产品简介 1
2 产品外观 2
3 产品特性 3
4 产品功能 4
5 技术指标 5
6 依据标准 6
7 典型应用 7
8 产品资质 8
8.1 商用密码产品认证证书 8
8.2 计算机软件著作权登记证书 9
附录 A 公司简介 10

1 产品简介

金融数据密码机（以下简称密码机）是由我公司自主研发的服务器类密码设备，密码机具有密钥安全存储、设备管理、访问控制、高速金融密码运算、真随机数生成、日志审计和设备自检等功能，通过 TCP/IP 协议对外提供金融密码服务，支持多种主流操作系统，具有很强的环境适用性。该款密码机支持通过配置终端进行管理和维护，具有易用性高、管理方便等优点。

该款金融数据密码机以高性能、高稳定性的硬件平台为基础，以高效的任务调度为中心，以不同金融密码运算模块化、支持高并发为原则，以金融数据密码机技术规范中的标准命令集为窗口，为金融支付与电子交易等业务系统提供高性能、高可靠性、高实时性的金融密码运算服务。

该密码机是应用层设备，支持 SM1、SM2、SM3、SM4 等多种国产密码算法以及 DES/3DES、RSA、SHA256 等国际密码算法。可以为金融行业的应用系统提供密钥管理、身份认证、数据加解密、消息验证等密码服务。适用于银行核心业务系统、数据准备系统、密钥管理系统等各种类型的安全应用系统，尤其适用于跨地区、跨机构的金融交易系统。

2 产品外观

产品规格	B3000
外观类别	机架式 2U
外观	
尺寸	430(宽)×550(深)×89(高)mm
工作电源（额定）	220V（100-240V）,550W 冗余电源
功耗 (最小/典型/最大)	100W/130W/150W
电源线	3C 认证国标/欧标可选
直流	支持,240V(190-310V)
网络接口	2 个 RJ-45 千兆电口，可扩展
外包装尺寸	608(宽)×749(深)×270(高)mm
规格	2U
MTBF	≥50000 小时
工作环境温度	0℃～60℃
非凝结的工作湿度	5%～90%
存储环境温度	-20℃～80℃
非凝结的存储湿度	5%～95%

3 产品特性

- 密码算法由硬件实现，支持并发访问，性能高；
- 算法安全。支持 SM1/SM2/SM3/SM4 系列密码算法；
- 具有完善的密钥保护机制。具有密钥加密存储、密钥销毁功能；
- 具有完善的系统监测功能，可监测密码机硬件及软件的运行状态，并可对故障进行自动恢复；
- 采用智能密码钥匙 USBKEY 作为身份认证和密钥存储介质；
- 安全的密钥管理体系：
  - ✓ 密钥产生：利用真随机数产生 RSA 密钥对、SM2 密钥对。
  - ✓ 三层密钥机制：分别为主密钥、传输密钥及应用密钥，分层保护，逐层加密。保护原则为“自上向下逐层保护”，即：主密钥保护传输密钥，传输密钥保护应用密钥。
  - ✓ 密钥存储：主密钥、传输密钥和应用密钥存放到加密卡内。
  - ✓ 密钥注入：如果主密钥和传输密钥由外部设备产生，则采用手工注入的方式导入至密码机内部。
  - ✓ 密钥销毁：为了保证密钥在特殊情况下的安全性，密码机提供了密钥销毁功能。
  - ✓ 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。

4 产品功能

- 对称密码算法：支持国产 SM1/SM4 算法以及国际通用算法 DES、AES 等算法。
- 非对称密码算法：支持 SM2、RSA 等算法。
- 摘要算法：支持国产 SM3 和通用 SHA1/SHA256 等算法。
- 配置管理功能：包括管理员身份认证、管理员权限划分、密码机参数配置、日志管理、口令修改。
- 密钥管理功能：包括对称密钥和非对称密钥的生成、密钥安全存储、密钥导出/导入、密钥状态查看、密钥销毁等功能。
- 磁条卡应用功能：支持密钥产生、导入导出、合成 ZMK、LMK 加密密钥、生成密钥校验值、PIN 的产生、PIN 的验证、PIN 的转加密及消息鉴别码 MAC 运算等功能。
- 基础密码服务功能：支持 SM2 密钥对产生、SM2 加密/解密、SM2 签名/验签、产生消息摘要及数据加解密等功能。
- 真随机数产生功能。
- 系统故障检测功能：包括开机自检和实时监控功能。
- 远程管理：在有远程集中管理需求时，密码机具有设备远程集中管理功能，方便设备的维护和升级。
- 连接白名单：通过对连接白名单的支持，实现了密码机对应用服务器的授权认证，进一步提高了系统的安全性。
- 日志审计：密码机提供了日志记录的功能，同时支持日志的查看和导出，更方便了后期对设备的维护。

5 技术指标

产品名称		中安云科金融数据密码机
商用密码产品认证型号		SC600
产品规格		B3000
性能参数		
非对称（SM2）	生密钥	3000tps
	签名/验签	10000tps/10000tps
	加密/解密	23000tps/11000tps
RSA2048	生密钥	45tps
	签名/验签	3500tps/40000tps
	加密/解密	40000tps/3500tps
对称密钥生成		5000tps
对称密钥加解密（SM4）		500Mbit/s
摘要算法（SM3）		500Mbit/s

注：

1、标配不含光纤网卡，若对光口指标有需求请联系销售

2、测试客户端为 单 E5 服务器，对称算法的数据包长 4K,操作系统：centos 7.6

3、不同测试环境中性能会略有差异

6 依据标准

《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》

《GM/T 0009-2012 SM2 密码算法使用规范》

《GM/T 0010-2012 SM2 密码算法加密签名消息语法规范》

《GM/T 0004-2012 SM3 密码杂凑算法》

《GM/T 0002-2012 SM4 分组密码算法》

《GM/T 0005-2021 随机性检测规范》

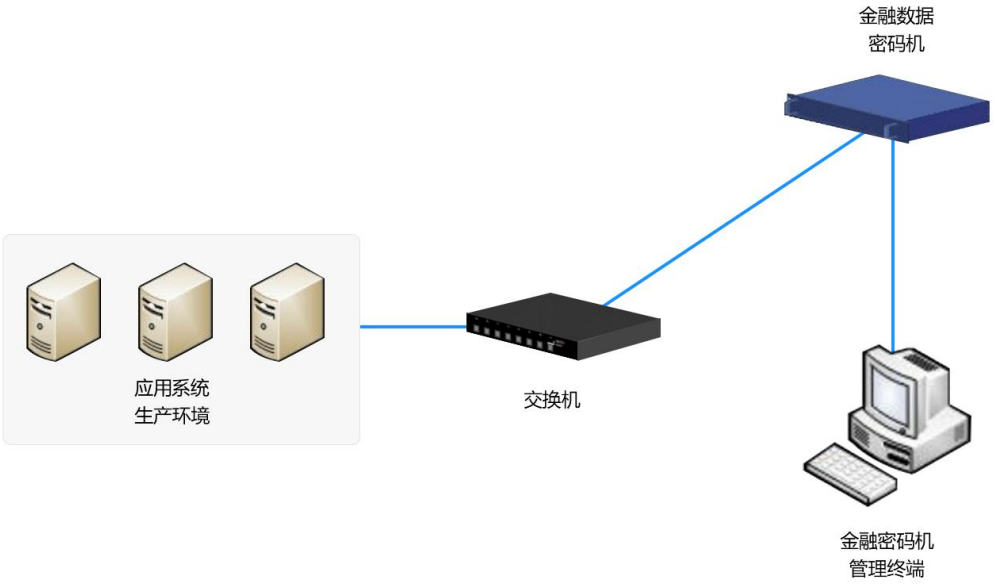
《GM/T 0006-2023 密码应用标识规范》

《GM/T 0045-2016 金融数据密码机技术规范》

《GM/T 0046-2016 金融数据密码机检测规范》

7 典型应用

在客户正式生产环境部署我公司金融数据密码机服务器，用于保证传输信息的机密性、完整性和有效性，其部署架构如下图所示：



8 产品资质

8.1 商用密码产品认证证书

商用密码产品认证证书

证书编号：GM013710920220149

委托人名称及所在地

中安云科科技发展（山东）有限公司
中国（山东）自由贸易试验区济南片区经十路 7000 号汉峪金谷 A7-4 栋 1768

生产者（制造商）名称及所在地

中安云科科技发展（山东）有限公司
中国（山东）自由贸易试验区济南片区经十路 7000 号汉峪金谷 A7-4 栋 1768

生产企业名称及所在地

中安云科科技发展（山东）有限公司
中国（山东）自由贸易试验区济南片区经十路 7000 号汉峪金谷 A7-4 栋 1768

产品名称和型号、版本

中安云科金融数据密码机
SC600　V1.0.1

产品标准和技术要求

GM/T 0045《金融数据密码机技术规范》
GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2025 年 5 月 1 日　　有效期至：2027 年 3 月 30 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

商用密码检测认证中心

中国·北京·南四环西路188号　www.scctc.org.cn 证书通过此网站查询

8.2 计算机软件著作权登记证书

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第5104000号

软件名称：中安云科金融数据密码机系统 V1.0

著作权人：中安云科科技发展(山东)有限公司

开发完成日期：2019年08月16日

首次发表日期：2019年08月19日

权利取得方式：原始取得

权利范围：全部权利

登记号：2020SR0225304

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局 计算机软件著作权登记专用章

2020年03月09日

No. 05415465

附录 A 公司简介

中安云科科技发展(山东)有限公司（以下简称中安云科），成立于 2016 年，作为一家全栈式密码产品与密码服务提供商，专注于密码核心技术的革新探索、密码产品的研发、市场推广和服务，致力于为客户提供全方位、一站式的密码服务，积极促进密码技术在关键基础设施领域的深度应用，助力客户构建完善的网络和信息系统密码防护体系。

中安云科创立于密码产业大省-山东省省会济南，是一家深耕于密码行业多年的国家级高新技术企业。公司先后与中科院、山东大学等学术院所建立了紧密的产学研合作关系，核心团队汇集了来自山东大学、北京邮电大学等高校的密码学专家，联合来自于奇安信、奇虎 360、阿里和百度等全球知名上市公司在云计算、信息安全、数据安全和密码学等领域的产品、技术和营销专家，共同构成了一个融合产学研、协同创新的卓越团队。

自成立以来，中安云科先后荣获“国家高新技术企业”、“省市专精特新”、“省市瞪羚企业”等称号，通过了 CMMI5、ISO9001、ISO27001 等权威体系认证、知识产权管理体系认证、武器装备质量管理体系认证、持有四十余项商用密码产品认证证书，十余项公安部销售许可、三十余项发明专利，四十余项计算机软件著作权。密码产品及解决方案多次赢得权威部门的认可。

秉承“用密码的力量，让每个用户的生活更简单、更安全”的使命，中安云科遵循“一个中心七个区域”的营销战略，以北京为营销中枢，辐射全国七大区域中心，现已构筑起覆盖全国 31 个省(直辖市、自治区)的销售与服务网络，广泛渗透于政府、运营商、军队、军工、金融、能源、交通、医疗、教育等领域，立志于铸就信息安全的铜墙铁壁，为数字中国的稳健前行保驾护航。