格尔软件
KOALSOFTWARE

服 务 器 密 码 机
产 品 白 皮 书

格尔软件股份有限公司

目 录

1 背景

1.1 应用现状

目前我国电子政务、金融、医疗、能源等领域信息化已全面普及，对计算机网络的安全也越来越重视。密码安全作为信息安全的基础性核心技术，是信息保护和网络信息体系建设的基础，是保障网络空间安全的关键技术。充分利用密码技术能够有效地保障网络安全等级保护制度的落实，科学合理的利用密码技术及其产品，是落实信息安全体系建设最为有效、经济和便捷的手段。

服务器密码机作为基础的商用密码产品，可以独立为应用系统提供高性能的数据加/解密服务，也可以作为数据安全存储系统、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组件，能够广泛应用在电子政务、金融、能源、移动通信、交通等领域的应用系统中。

1.2 政策要求

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。

1) 《密码法》第二十七条法律、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，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

2) 《信息安全技术 网络安全等级保护基本要求》中要求按照等级使用密码技术。以等保 2.0 三级安全通用要求为例，在安全通信网络（通信传输）、安全计算环境（身份鉴别、数据传输完整性、数据传输保密性、数据存储完整性、数

据存储保密性）、安全管理中心（集中管控）、安全建设管理（产品采购和使用、测试验收）、安全运维管理（密码管理）等五个层面，共十三个安全要求项中提出了密码技术和管理的要求。

3) 《商用密码应用安全性评估管理办法（试行）》第三条、第二十条要求涉及国家安全和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位应当健全密码保障体系，实施商用密码应用安全性评估。重要领域网络和信息系统包括：基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上信息系统。

4) 《信息安全技术 关键信息基础设施安全防护能力评价方法》（征求意见稿）要求关键信息基础设施安全防护能力评价前，关键信息基础设施应首先通过相应等级的等级保护测评和相关密码测评。

5) 《中华人民共和国网络安全法》第十条、第十八条、第二十一条相关规定要求防止网络数据泄露或者被窃取、篡改，采用数据分类、重要数据备份和加密等措施，维护网络数据的完整性、保密性和可用性。

6) 《中华人民共和国个人信息保护法(草案)》第五十条明确了采取相应的加密、去标识化等安全技术措施，确保个人信息处理活动符合法律、行政法规的规定,并防止未经授权的访问以及个人信息泄露或者被窃取、篡改、删除。

7) 《国家政务信息化项目建设管理办法》第十五条要求项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

2 产品概述

2.1 产品简介

格尔服务器密码机能够满足各类应用系统的密码安全应用需求，提供高速的、

多任务并行处理的密码运算，可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和真实性。同时提供安全、完善的密钥生命周期管理机制，通过专门加固的、防止恶意攻击的软硬件设计，可以保障密码机内部密钥的安全管理、运行和存储。

格尔服务器密码机运用先进和成熟的嵌入式系统设计技术，遵循国家密码管理局规范《GM/T 0030-2014 服务器密码机技术规范》以及《GM/T 0018-2012 密码设备应用接口规范》，具有集成性高、安全性高、可靠性强、性能高、规范性强等特点。

2.2 产品形态

格尔服务器密码机是一个具备自身物理安全防护能力的实体硬件设备，能够实时地为应用提供密钥管理、密码运算、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、有效性、完整性、不可抵赖性等。

密码应用系统通过调用密码机提供的标准应用接口 API 函数来使用密码机提供的密码服务，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的使用密码机所提供的密码服务功能。

2.3 产品组成

格尔服务器密码机采用自主研制的 x86 嵌入式安全平台，包括嵌入式主板、PCI-E 密码卡和智能密码钥匙等核心部件，支持 SM1、SM2、SM3、SM4、SM9、ZUC 密码算法，同时支持 AES、3DES、RSA 1024/2048/4096、SHA-2 系列等国际密码算法扩展。

3 产品功能

3.1 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生成随机数，符合国家密码管理局颁布的《随机数检测规范》。

● 非对称加解密

支持国密算法 SM2、SM9，以及国际算法 RSA。

● 对称加解密

支持 SM1、SM4 分组算法、ZUC 序列算法，以及国际算法 AES、3DES 等。

● 摘要运算

支持国密算法 SM3,以及国际算法 SHA-2 系列(SHA-224、SHA-256、SHA-384、SHA-512)、SHA1、MD5 等。

● 消息鉴别码

支持基于国密 SM1、SM3、SM4 算法，以及国际算法 SHA-2 系列(SHA-224、SHA-256、SHA-384、SHA-512)、SHA1 的 MAC 产生和验证。

● 签名/验证

签名/验签支持国密算法 SM2、SM9，以及国际算法 RSA。

● 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。

● 身份鉴别

遵循《GBT 15843.3-2008 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制》采用核准的数字签名技术来进行身份鉴别。

3.2 管理功能

● 角色与身份认证

管理用户采用三权分立的模式，保障设备的安全访问，划分为系统管理员、安全管理员、审计管理员、系统操作员员四种类型。所有管理员的身份需通过密码机上的 USBKEY 内的数字证书进行双因子认证。

● 密钥生成

采用由国家密码管理局批准使用的双物理噪声源生成随机数，采用了国家密码管理局批准使用的密码卡可生成各类对称密钥（SM1、SM4、AES、3DES 等）和非对称密钥（SM2、SM9、RSA 1024/2048/4096）。

● 密钥安全存储

设备内部支持 500 个对称密钥和 200 个非对称密钥的安全存储。密码机的内部密钥都位于内置的加密硬件中，且必须与授权管理员的 USBKey 进行密码运算，才能够提供服务。

● 密钥统计

展示设备内部现有密钥数量，并根据密钥类型进行分类展示。

● 密钥销毁

支持通过管理界面删除指定的对称或非对称业务密钥，也支持销毁全部业务密钥。支持通过密钥销毁钥匙对安全区内的密钥进行清空操作。

● 密钥备份与恢复

采用基于密钥分割的方式备份密钥和安全数据，保障备份数据的安全性。采取非对称密钥加密的门限算法，只有满足最少数量的管理员才能进行恢复操作，且支持在相同型号的其它加密机设备间进行恢复数据。

● 服务管理

支持在服务器密码机管理界面上进行密码服务的管理，包括查看服务运行状态、连接数、启停密码服务、服务日志信息配置、服务接口跟踪日志以及客户端

IP 白名单配置等功能。

- 系统管理

支持对服务器密码机的网卡、系统日志、系统时间、授权文件等进行配置。

- 安全审计

审计管理员对系统操作日志进行审计操作，并支持对日志文件进行签名下载。

3.3 支持接口

- 国密标准接口

提供符合《GB/T 36322-2018_信息安全技术 密码设备应用接口规范》的标准化接口。

- PKCS#11 接口

国际通用标准接口，提供各种通用标准对称加解密、非对称加解密、数字签名、HASH 算法。

- JCE 接口

国际通用标准接口，JAVA 编程语言，提供完善的统一的安全应用解决方案。

4 产品特点

4.1 安全性

格尔服务器密码机在自身软硬件、应用接口以及管理手段上，都采取完善的安全体系，确保密码机自身的安全以及上层服务接口的安全：

- 设计上严格遵循国家密码管理局相关技术要求和商用密码行业规范，国产密码算法使用硬件实现，密钥产生存储和密码服务应用符合标准要求。
- 物理安全采用防拆、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保护设备。
- 采用严格的多级密钥管理体制和权限分离的设备机制，确保密钥安全和

设备管控安全。

- 密码机内部密钥都位于内置的加密硬件中，授权管理员必须完成基于管理员 USB Key 内数字证书的验证，密码机才能够提供服务。
- 密钥备份采取高强度的密钥分割算法，只有少量有权限的管理员才能进行恢复操作。
- 内置白名单技术，提供 IP 包过滤，只有授权的用户才可以访问密码机，使用密码机的安全功能。
- 用户密钥采用私钥授权码，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。
- 采用 SM3 摘要算法对每条日志记录进行运算和比对，保证密码机内日志数据的不可篡改和真实性。
- 管理员与 SDK 均可以通过 SSL 安全通道访问服务器密码机。

4.2 易用性

- 全面支持国产密码算法以及常用国际密码算法，包括 SM1、SM2、SM3、SM4、SM9、ZUC、RSA 1024/2048/4096、AES 128/256、3DES、SHA-2 系列、SHA1、MD5 等。
- 提供符合《GB/T 36322-2018_信息安全技术 密码设备应用接口规范》的标准化接口，接口支持 C、Java、Python、Go 等主流编程语言，便于应用厂商进行开发和集成。
- 支持 B/S 模式的本地管理页面。

4.3 可靠性

- 支持断链修复功能，当网络异常导致设备断开连接时，服务器密码机能够自动尝试修复链接。
- 支持多机并行及负载均衡，避免单点故障。

- 支持对设备 CPU/内存资源的使用率、当前并发连接数量、服务进程状态等进行实时监控，能够实时掌握设备状态。

5 产品规格

5.1 设备外观

产品型号	正面	背面
KHSM-SG		
KHSM-100		

KOAL-HSM S3		
KOAL-HSM S4		
KOAL-HSM S7		

5.2 硬件规格

	KHSM-SG	KHSM-100	KOAL-HSM S3	KOAL-HSM S4	KOAL-HSM S7
外观规格	2U	2.5U	2U	2U	2U
网络接口	千兆网口 x6	千兆网口 x3	千兆网口 x6	千兆网口 x6 光口 x2	千兆网口 x6 光口 x4
电源	双模块冗余电源	双模块冗余电源	双模块冗余电源	双模块冗余电源	双模块冗余电源
最大功耗	120W	120W	300W	300W	300W
工作温度	0℃～40℃	0℃～40℃	0℃～40℃	0℃～40℃	0℃～40℃
存储温度	-40℃～70℃	-40℃～70℃	-40℃～70℃	-40℃～70℃	-40℃～70℃
CPU	兆芯 C4600/4 核 /2.2GHz	Intel Pentium G4560 2 核/3.5GHZ	Intel I5-6500 4 核 /3.2GHz	海光 C86 3250 16 核 /2.8GHz	海光 C86 5380 32 核 /2.5GHz
内存	4GB	4GB	8GB	16GB	32GB

硬盘存储器	4GB SATADOM	4GB SATADOM	256G SSD	256G SSD	256G SSD

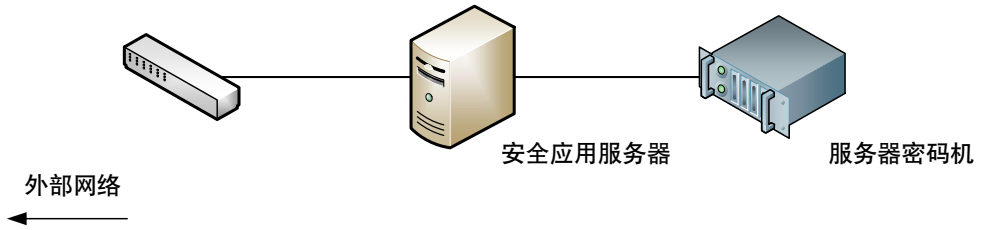
5.3 性能指标

算法	KHSM-SG指标	KHSM-100指标	KOAL-HSM S3指标	KOAL-HSM S4指标	KOAL-HSM S7指标
SM1 算法加解密速率	490Mbps	550Mbps	4800Mbps	5000Mbps	8500Mbps
SM4 算法加解密速率	520Mbps	800Mbps	4800Mbps	4700Mbps	8500Mbps
SM2 密钥对产生速率	6600 对/秒	39000 对/秒	80000 对/秒	200000 对/秒	300000 对/秒
SM2 签名速率	3000 次/秒	38000 次/秒	57000 次/秒	230000 次/秒	240000 次/秒
SM2 验签速率	4500 次/秒	28000 次/秒	36000 次/秒	100000 次/秒	100000 次/秒
SM2 算法加密速率	2.5Mbps	19000 次/秒	38000 次/秒	51000 次/秒	52000 次/秒
SM2 算法解密速率	7.23Mbps	30000 次/秒	68000 次/秒	61000 次/秒	62000 次/秒
SM3 计算 Hash 速率	2671Mbps	870Mbps	19000Mbps	19000Mbps	19000Mbps
随机数产生性能	40Mbps	35Mbps	129Mbps	130Mbps	130Mbps

6 典型部署

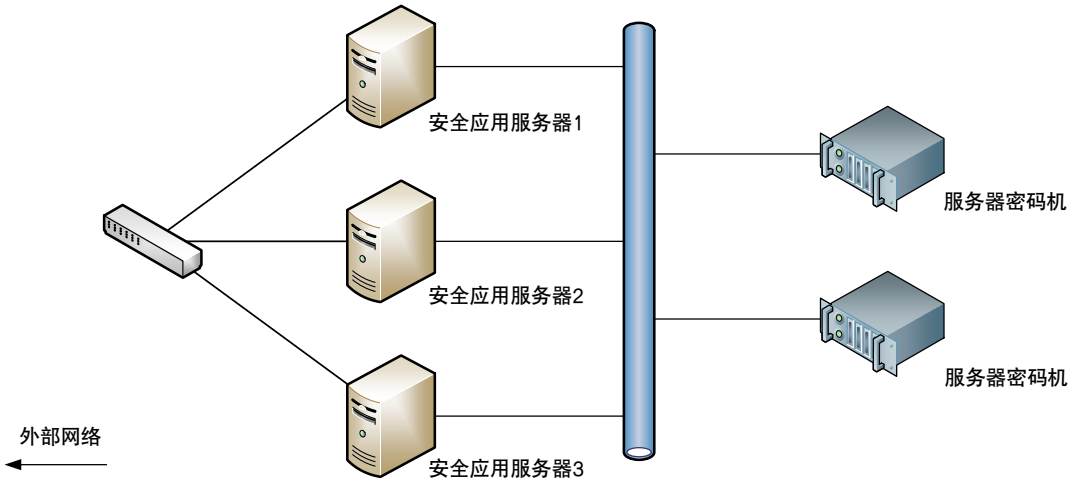
6.1 单机部署

用户应用系统和密码服务需求较少时，可以选择单机部署模式，密码机与应用服务器直连，为应用系统提供密码服务。



6.2 集群部署

当用户使用多个应用系统、对密码服务性能和稳定性要求较高时，可以选择集群部署模式，多台服务器密码机组成的集群使用专用网络与应用服务器连接，为不同的应用系统提供密码服务。



7 建设效益

标准合规支持	满足密评、等保等密码相关标准指标要求，帮助用户网络和应用系统通过合规评估
标准国密密码服务	全面支持国密算法，达到国产密码替代目标
规范合规接口	提供统一规范接口，保障业务密码应用安全合规
灵活适配	接口支持多种主流开发语言，便于开发集成
提高密码安全专业性	专业的密码服务能力，可提高整体网络的密码安全专业性
密码安全服务体系	可与格尔数字证书体系、身份认证体系和安全应用系统共同构成密码安全服务体系

8 产品资质

商用密码产品认证证书

证书编号：GM003111020210213

委托人名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产者（制造商）名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产企业名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

产品名称和型号、版本

格尔服务器密码机
KHSM-100　V1.0.0

产品标准和技术要求

GM/T 0030《服务器密码机技术规范》
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：2021 年 6 月 21 日　　有效期至：2026 年 6 月 20 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。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

商用密码产品认证证书

证书编号：GM003111020210439

委托人名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产者（制造商）名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产企业名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

产品名称和型号、版本

格尔服务器密码机
KHSM-SG V1.0.0

产品标准和技术要求

GM/T 0030《服务器密码机技术规范》
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：2021 年 11 月 4 日　　有效期至：2026 年 11 月 3 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。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

商用密码产品认证证书

证书编号：GM003111020230351

委托人名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产者（制造商）名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

生产企业名称及所在地

格尔软件股份有限公司
上海市静安区江场西路 299 弄 5 号 601 室

产品名称和型号、版本

格尔服务器密码机
KOAL-HSM S3

产品标准和技术要求

GM/T 0030《服务器密码机技术规范》
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：2023 年 4 月 28 日　　有效期至：2028 年 4 月 27 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。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询