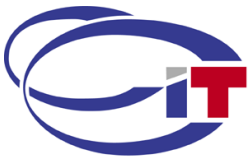
密钥管理系统

产品白皮书



北京创原天地科技有限公司

Creative Century Information Technology Co., Ltd

您的意见和建议请发送至：

北京创原天地科技有限公司

北京海淀区学清路 38 号金码大厦 B 座 2010-2012，100083

电话：010-62395838

传真：010-62395896

电子邮箱：marketing@ccit.com.cn

目　录

1 概述

1.1 产品简介

密钥管理系统是北京创原天地科技有限公司独立自主研发的高性能专用密码设备，符合国家密码管理局颁布的 GM/T 0038-2014《证书认证密钥管理系统检测规范》、GM/T 0051-2016 《密码设备管理对称密钥管理技术规范》，通过国家密码管理局商用密码检测中心检测认证，并获得商用密码产品认证证书。

密钥管理系统内置经国家密码管理局鉴定并批准的高速密码模块，全面支持国产商密码算法和国际标准算法，密码运算和密钥生成均由内置高速密码模块实现，保证密码运算安全和密钥生成、存储安全，为用户提供合规、安全、高效的密钥管理服务。

密钥管理系统具有完善的对称密钥和非对称密钥管理体系，支持 SM1/2/3/4、RSA、AES、SHA256 等算法，提供 CA 证书密钥管理、分散密钥管理、对称密钥管理和非对称密钥管理等服务，实现密钥的生成、更新、存储、分发、归档、备份、恢复和销毁等全生命周期管理，保障密钥生命周期中各环节的安全。

密钥管理系统负责整个密码服务基础设施的核心数据-密钥的安全管理，为平台服务商、密码使用单位/个人等用户提供密钥管理相关安全服务，如密钥生成服务、密钥分发服务、密钥安全隔离和存储服务、密钥安全访问服务、密钥策略控制服务、基于托管密钥的加解密服务、密钥使用的日志记录服务、密钥高可用服务等，满足用户密钥管理、密钥托管等需求。

1.2 产品规格

产品名称	密钥管理系统	密钥管理系统（国产化）
产品型号	SYT1301	SYT1920-G
产品外观	 正面  背面	 正面  背面

	 整体效果图	 整体效果图
规格	2U	2U
外形尺寸（宽 x 深 x 高）	440x550x88mm	440x550x88mm
工作电源	550W 冗余电源	550W 冗余电源
网络接口	4 个 RJ-45 千兆电口，可扩展光口	2 个 RJ-45 千兆电口，可扩展光口
配置参数	4 核 CPU/8GB DDR/1TB	兆芯 8 核 CPU/8GB DDR/1TB，麒麟操作系统
加密模式	硬件密码卡	硬件密码卡
工作环境温度	0℃～60℃	0℃～60℃
非凝结的工作湿度	5%～90%	5%～90%
存储环境温度	-20℃～80℃	-20℃～80℃
非凝结的存储湿度	5%～95%	5%～95%

1.3 依据技术标准

GM/T 0051-2016 密码设备管理 对称密钥管理技术规范

GM/T 0050-2016 密码设备管理 设备管理技术规范

GM/T 0038-2014 证书认证密钥管理系统检测规范

GM/T 0014-2012 数字证书认证系统密码协议规范

GM/T 0034-2014 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

2 产品组成

密钥管理系统由密钥管理服务平台、密钥管理服务接口和密钥管理服务 SDK 三部分组成。用户可根据业务系统应用需求选择调用密钥管理 SDK 或密钥管理 API 接口，实现密钥管理服务能力的调用。

产品组成图如下

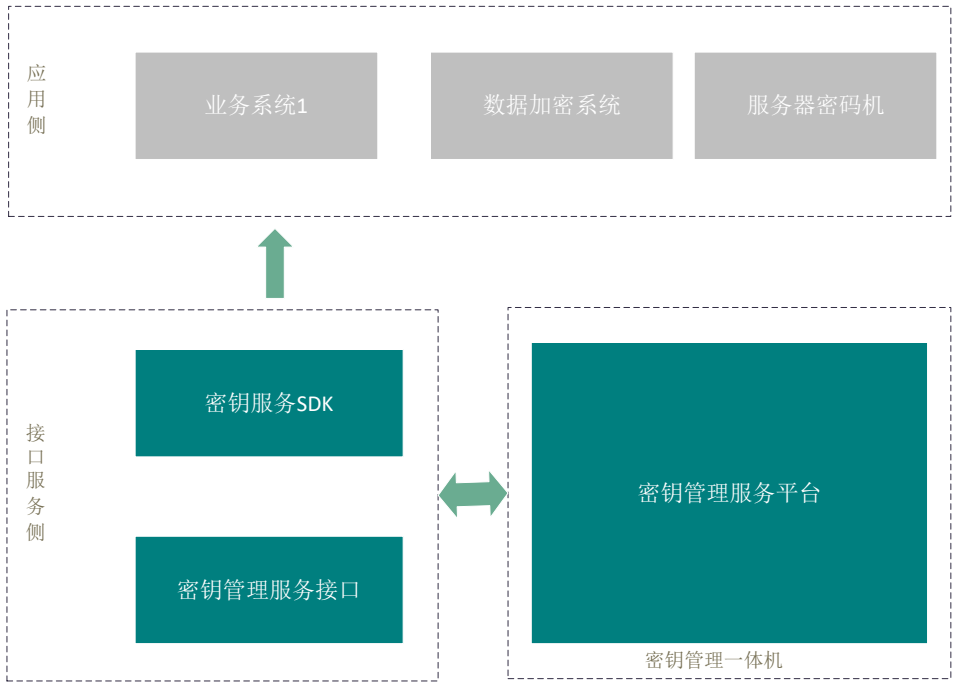


图 1 产品组成图

2.1 密钥管理服务平台

密钥管理服务平台提供密钥生成管理、密钥分发管理、密钥服务接口以及系统配置、应用管理、安全备份、监控监测、安全审计、密钥备份恢复以及其他密钥生命周期管理等功能。

2.2 密钥管理服务 SDK

密钥管理服务 SDK 是运行在业务系统服务器主机上的软件包，业务系统通过集成密钥管理服务 SDK，进行与密钥管理系统进行密钥申请、密钥分发、密钥启用、密钥销毁等操作。SDK 按照标准要求进行数据格式封装和消息发送，与密钥管理中心建立安全连接。

2.3 密钥管理服务接口

密钥管理接口服务为业务系统提供密钥申请、密钥分发、密钥启用、密钥销毁等密钥服务 API。业务系统通过 HTTP/HTTPS 的方式调用密钥管理服务能力。

3 产品功能

3.1 对称密钥管理

对称密钥管理提供对称密钥生成、存储、备份、恢复、获取、更新和销毁等全生命周期管理，为数据加密系统、密码机等密码产品及业务系统提供对称密钥服务。

支持生成 SM1、SM4、AES、3DES 等对称密钥，支持批量生成或单个索引生成。支持密钥长度和算法的选择；调用密码卡随机生成对称密钥，通过密钥保护密钥加密保存在密钥管理系统中。支持制定密钥生成与密钥更新策略，密钥更新后旧密钥迁移至历史密钥库。

3.2 派生密钥管理

派生密钥管理是指使用分散因子实现密钥的派生，提供密钥更新策略配置、密钥绑定和密钥分发等功能。

支持时间周期、一次一密和固定密钥三种密钥更新策略。

3.3 非对称密钥管理

非对称密钥管理提供非对称密钥生成、存储、备份、恢复、获取、更新和销毁等全生命周期管理，为密码产品和业务系统提供非对称密钥服务。

支持批量生成或者单个索引生成 SM2、RSA 密钥对，每一对密钥占用一个密钥索引号。支持根据密钥用途生成签名密钥、加密密钥等。密钥生成时可选择密钥算法、密钥模长和密钥用途等。通过密码卡随机生成非对称密钥对，并使用密钥保护密钥加密保存在密钥管理系统中。密钥更新后旧密钥迁移至历史密钥库。

3.4 数字证书密钥管理

证书密钥管理提供证书密钥生成、存储、备份、恢复、获取、更新和销毁等全生命周期管理，配套数字证书认证系统（CA）使用。

支持 CA 系统的添加、删除、启停等管理。支持配置 CA 服务器证书。支持密钥生成计划设置，提供 SM2、RSA 算法密钥预生成。

3.5 司法取证

根据司法取证需要，司法取证员可查询密钥管理系统密钥信息，并通过司法取证及管理员 UKEY 可将密钥加密导出到安全介质。

3.6 应用管理

实现对调用密钥管理系统的应用系统进行添加、删除、修改。根据在系统配置的应用标识和应用证书，对密钥管理 SDK 的合法性进行安全认证。支持多个应用系统调用，在密钥管理系统完成应用添加后即可使用密钥服务。

3.7 安全管理

系统采用“三权”分立的机制，保障整个系统的安全性，管理用户分为管理员、操作员、审计员三类角色，按照角色类型配置相应的权限列表。管理员权限包括用户管理、系统管理等。操作员可依照分配的权限对密钥的全生命周期进行管理。审计员权限包括日志查看、日志审计等。系统支持管理员采用数字证书（USBKEY）进行身份鉴别。

3.8 安全审计

系统提供可视化管理控制台，可查看操作内容、操作时间、操作结果、操作人员等密钥管理的日志记录，具有日志查询、导出、审计等功能。支持对操作日志和业务日志进行安全审计，防止日志记录被篡改。

3.9 密钥统计

支持按证书密钥、派生密钥、对称密钥及非对称密钥等密钥类型，对系统中在用密钥库、历史密钥库和备用密钥库的密钥数量、新增密钥数量等进行统计。支持密钥使用情况的统计，可按照时间周期统计密钥使用次数。

4 产品特点

4.1 支持多种密钥类型

密钥管理系统支持对称密钥管理、非对称密钥管理、派生密钥管理、认证密钥管理等多种密钥体系管理，满足多应用系统多场景下对密钥使用的需求。

支持 SM1、SM2、SM3、SM4 等国家标准密码算法，同时支持 AES、RSA、SHA256、SHA512 等国际标准密码算法。

4.2 支持多种服务模式

密钥管理系统服务支持 SDK 和 API 两种调用方式，满足不用场景、不同开发环境下密钥管理、密钥使用等需求。支持数字信封、KMIP、国密标准协议等多种密钥分发协议。

4.3 支持多级密钥管理体系

支持一级密钥管理中心、二级密钥管理中心等多级密钥管理体系。由一级密钥管理中心负责管理二级密钥中心的主密钥，二级密钥管理中心管理各密码产品、业务系统以及密码设备所使用的密钥。

4.4 支持多业务系统

密钥管理系统支持加密机、业务系统多个应用系统同时使用密钥服务，系统支持应用系统的添加、删除、修改、认证等管理功能，便于多个应用系统接入和认证。

4.5 高可用性

密钥管理系统支持双机热备、系统自检、数据错误忽略、备份恢复等技术，使密钥管理系统具备高可用和异常故障处理能力。

5 产品部署

密钥管理系统即可为与密钥管理系统部署在同一机房的业务系统、密码产品/设备提供密钥管理服务，也可通过安全分发的方式为异地机房的业务系统、密码产品/设备提供密钥管理服务。

部署示意图如下：

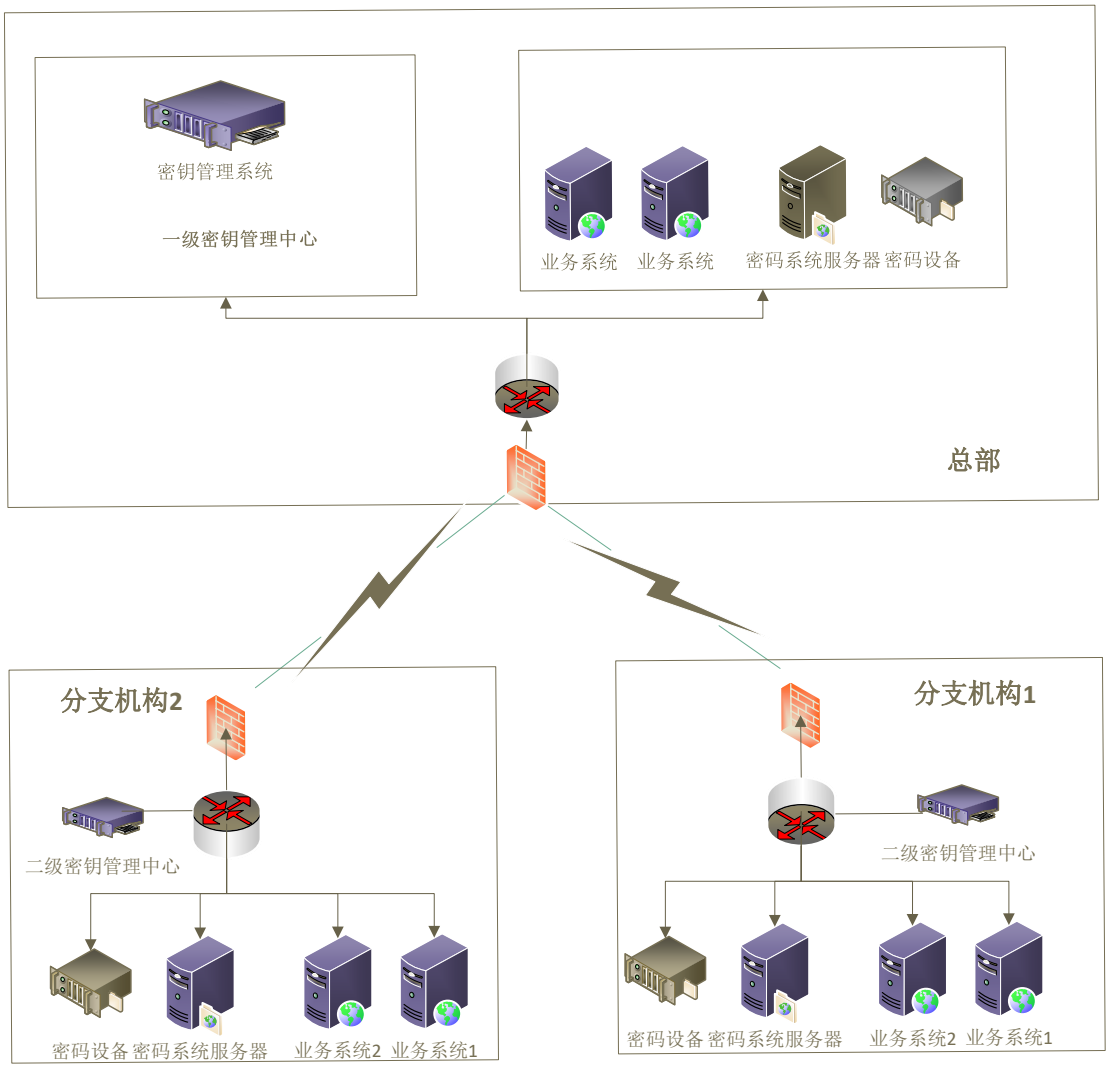


图 2 密钥管理系统部署示意图

6 应用场景

6.1 IC 卡密钥管理

密钥管理系统负责 IC 卡系统的密钥产生、传输、分散、使用等，保障 IC 卡存储数据的安全性。密钥管理系统支持多级密钥管理体系，如图所示。

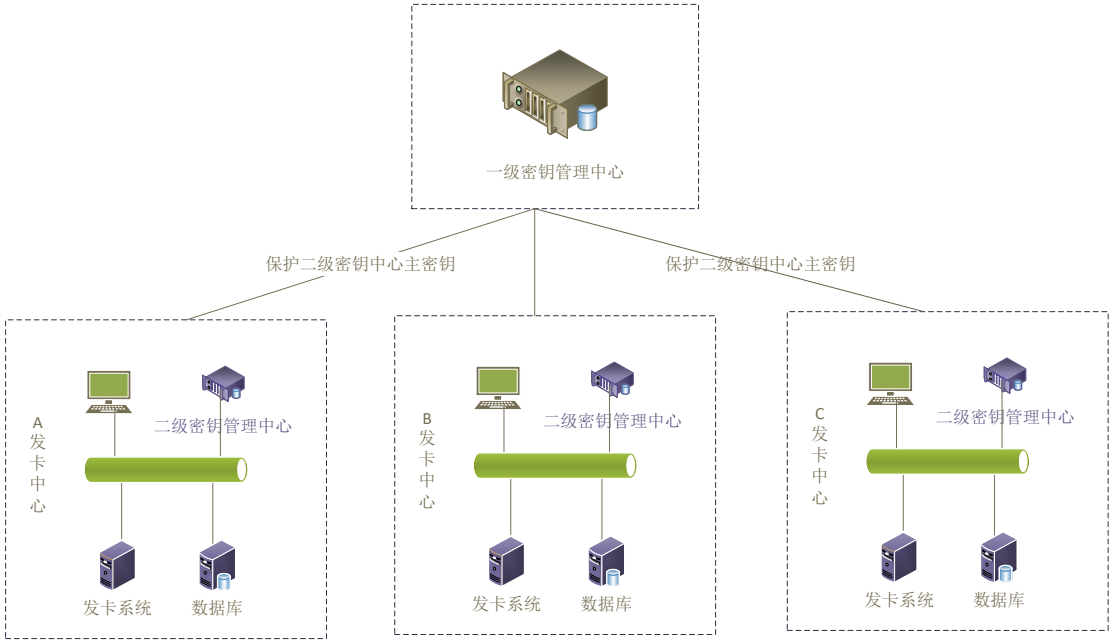


图 3 IC 卡密钥管理应用场景

一级密钥管理负责各二级密钥管理中心主密钥的生成、分发、加密保护。二级密钥管理中心负责分散生成、分发和加密存储 IC 卡密钥。

6.2 数据加密系统密钥管理

数据加密系统密钥管理应用场景如图所示：

图 4 数据加密系统密钥管理场景

密钥管理系统负责数据加密系统应用主密钥的生成和加密存储。在数据加密系统需要进行数据加密处理时，向密钥管理系统请求数据加密密钥；密钥管理系统根据应用主密钥和分散因子，分散生成数据加密工作密钥；通过安全传输的方式，将数据加密工作密钥下发到数据加密系统。

6.3 CA 系统密钥管理

密钥管理系统可作为独立的密钥管理中心为 CA 系统提供密钥管理服务。应用场景如图所示。

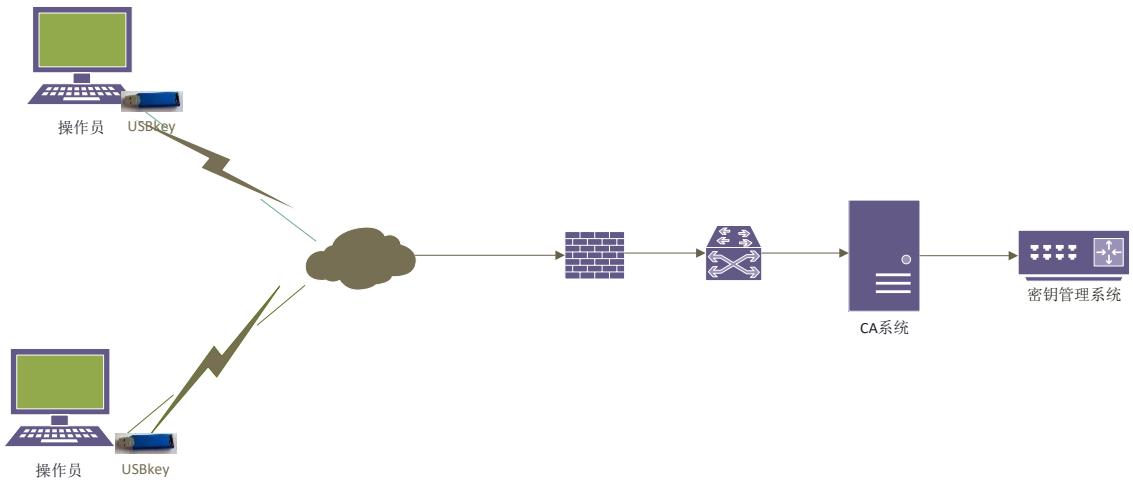


图 5 CA 系统密钥管理场景

密钥管理中心可对 CA 系统的加密密钥进行管理，包含密钥生成、密钥备份/恢复、密钥查询、密钥更新、密钥销毁等。

7 资质证书

- 国家密码管理局颁发的《商用密码产品认证证书》（普通版）

商用密码产品认证证书

证书编号：GM001119920201192

委托人名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

生产者（制造商）名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

生产企业名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

原商用密码产品型号证书批准型号

SYT1301 密钥管理系统（原证书编号：SXH2019051 号）

依据商用密码产品型号证书换发。

颁发日期：2020 年 12 月 14 日　　有效期至：2024 年 02 月 08 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

- 国家密码管理局颁发的《商用密码产品认证证书》（XC）

商用密码产品认证证书

证书编号：GM001119920201769

委托人名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

生产者（制造商）名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

生产企业名称及所在地

北京创原天地科技有限公司
北京市海淀区学清路 38 号 B 座 18 层 2011

原商用密码产品型号证书批准型号

SYT1920-G 密钥管理系统（原证书编号：SXH2019634 号）

依据商用密码产品型号证书换发。

颁发日期：2020 年 12 月 14 日　　有效期至：2024 年 12 月 08 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