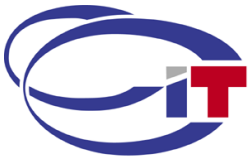
数据和数据库加密系统

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

数据和数据库加密系统是北京创原天地科技有限公司自主研发的高性能数据加密专用设备，符合国家密码管理局颁布的 GM/T 0028-2014《密码模块安全技术要求》，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，符合密码模块第二级要求。

数据和数据库加密系统内置经国家密码管理局商用密码检测中心检测认证的高速密码模块，支持 SM2、SM3、SM4 等商用密码算法，所有密码运算均由内置高速密码模块实现，保证密码运算安全和密钥存储安全，为用户提供安全、高效的数据加密服务。

数据和数据库加密系统为应用系统提供数据加解密服务，用户可选择性地对系统敏感数据、重要数据进行加密处理，以密文的形式进行存储，保证数据存储的机密性和完整性。系统支持重要数据信息加密服务、数据库敏感字段加密服务、文件/对象加密服务、数据库透明加密服务等多种服务场景。基于业务场景的数据加密服务，实现敏感数据以密文的形式存储，能保证即使在存储介质被窃取或数据文件被非法复制的情况下，敏感数据仍然安全，并通过密码技术实现三权分立，避免因 DBA 密码丢失造成批量数据泄漏风险。应用系统使用数据和数据库加密系统可实现对重要数据进行加密存储，符合密评关于数据存储的机密性和完整性保护的要求。

1.2 产品规格

产品名称	数据和数据库加密系统	数据和数据库加密系统（国产化）
产品型号	CY-DBES-V3000	CY-DBES-V3000A
产品外观	 正面  背面  整体效果图	 正面  背面  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，可扩展千兆光口和万兆光口	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，麒麟操作系统
密码实现模式	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 0003-2012《SM2 椭圆曲线公钥密码算法》

GM/T 0004-2012《SM3 密码杂凑算法》

GM/T 0002-2012《SM4 分组密码算法》

GM/T 0005-2012《随机性检测规范》

GM/T 0028-2014《密码模块安全技术要求》

2 产品组成

数据和数据库加密系统分加密网关模式和 SDK 加密模式两种实现数据加密服务。

2.1 加密网关模式

加密网关模式下，数据和数据库加密系统是以数据库加密网关的形式实现数据库透明加密。

产品组成如下：

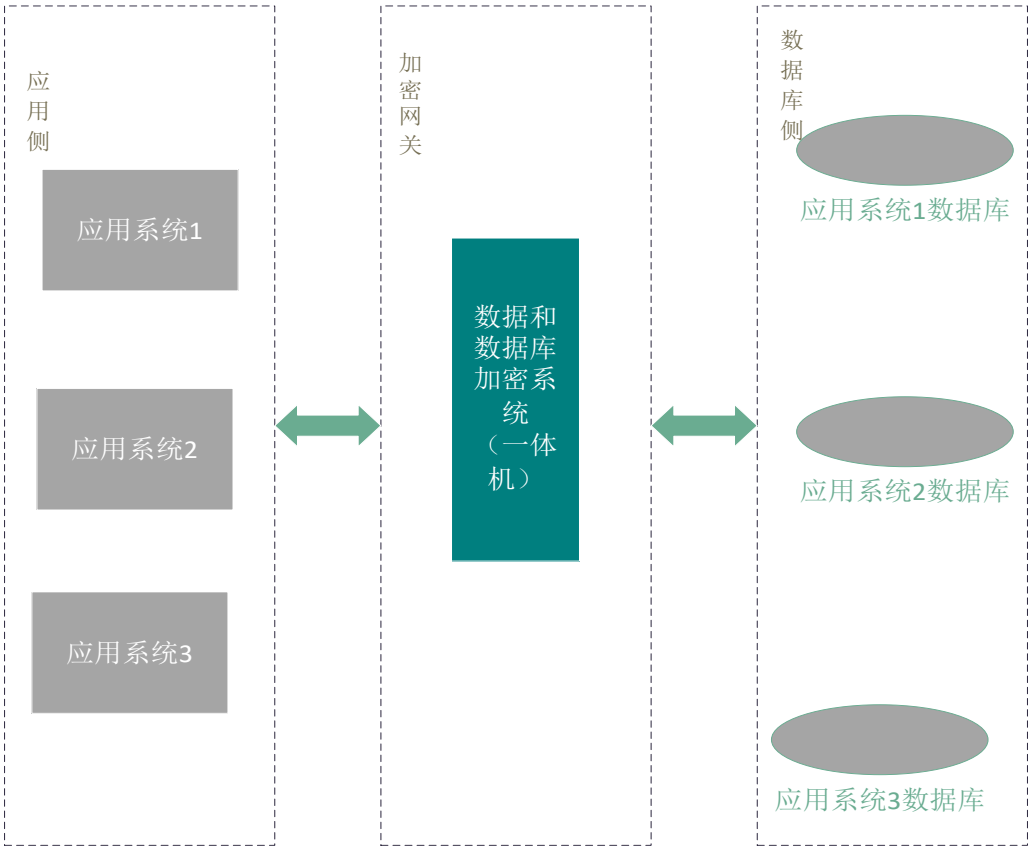


图 1 加密网关模式产品组成图

数据和数据库加密系统提供数据库透明数据加密、密钥管理、应用管理、安全管理和安全审计等功能服务。向应用系统提供数据库透明加密服务，自动完成指定数据库字段的加解密。

2.2 SDK 加密模式

SDK 加密模式下，数据和数据库加密系统由数据加密服务平台和数据加密 SDK 组成。

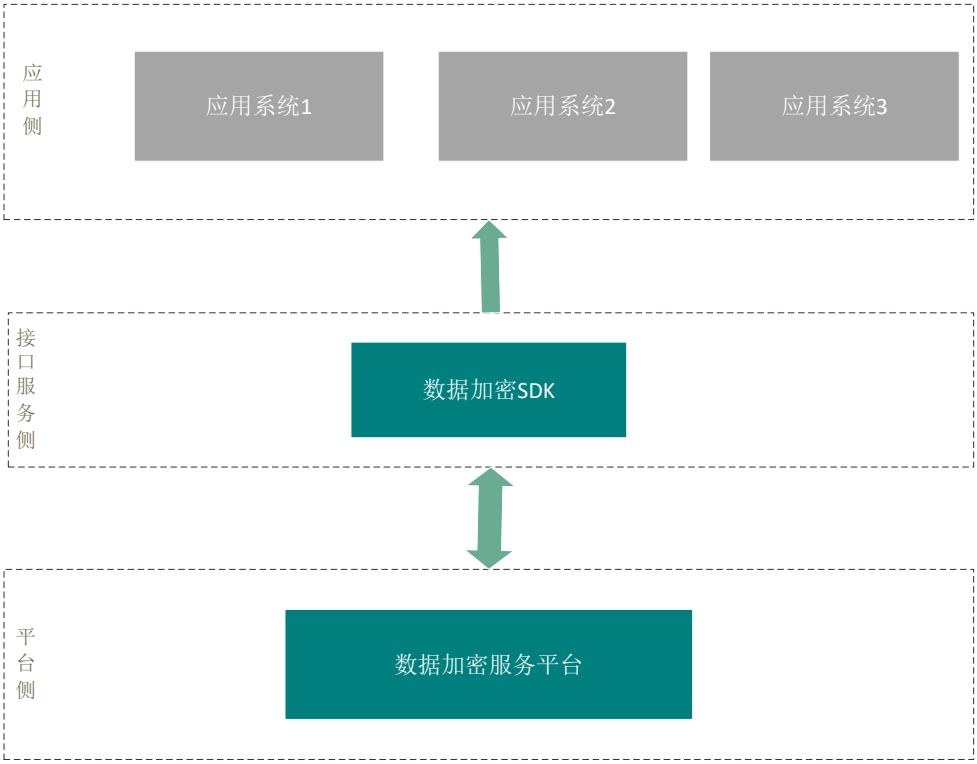


图 2 SDK 加密模式产品组成图

2.2.1 数据加密服务平台

数据加密服务平台提供密钥管理、应用管理、安全管理和安全审计等功能服务。向应用系统提供数据加密配置服务，完成数据库字段、数据内容、文件等加解密配置；向加密 SDK 提供安全可靠的密钥管理和密钥分发服务。

2.2.2 数据加密 SDK

数据加密 SDK 以软件开发包 SDK 的方式向应用系统提供数据/文件加解密功能服务。数据加密 SDK 与数据加密服务平台进行交互，获取服务平台分发的密钥及安全策略，根据策略完成数据/文件加解密处理。

3 产品功能

3.1 数据库加密

3.1.1 数据库加密网关模式

数据和数据库加密系统以数据库加密网关服务的方式为应用系统提供数据库透明加解密处理。应用系统无须进行改造和数据库适配。

支持系统对目标数据库的 IP、端口及代理端口进行配置。通过配置的数据库名、表名和列名，实现对数据库对应表和列写入或读出的数据进行加密或解密处理。

3.1.2 数据库 SDK 加密模式

数据和数据库加密系统提供数据加密 SDK 嵌入应用系统，为应用系统提供数据库字段加解密功能。应用系统通过调用数据加密 SDK 接口，实现对数据库重要字段进行加解密处理，以密文的形式存储在数据库中，保证数据存储的机密性。

3.2 数据加密

数据加密以 SDK 的方式与应用系统进行集成对接，为应用系统提供数据加解密处理功能。

3.3 文件加密

文件加密以 SDK 的方式与应用系统进行集成对接，为应用系统提供文件加解密处理功能。

3.4 保留格式加密

实现对数据的保留格式加密服务，加密后密文长度和原文一致。支持对 varchar，int 等常用数据库字段的保留格式加密，实现数据库免改造。

3.5 密钥管理

实现密钥的生成、存储、分发、导入、导出、备份和恢复等安全管理。支持工作密钥的生成和安全分发。

支持历史密钥统统计、在用密钥统计及密钥调用次数统计。

支持密钥生成策略配置，可按照时间周期、一次一密等细粒度策略生成密钥，维护密钥的安全性。

3.6 应用管理

实现对调用数据和数据库加密系统的应用系统进行添加、删除、修改。根据在数据和数据库加密系统配置的应用标识和应用证书，对数据加密 SDK 的合法性进行安全认证。支持多个应用系统调用，在数据和数据库加密系统完成应用添加后即可使用数据加密服务。

3.7 安全管理

数据和数据库加密系统采用“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；操作员权限包括密钥管理、策略管理、应用管理等；审计员权限包括日志查看、日志审计等。支持管理用户采用数字证书（USBKEY）进行身份鉴别。

3.8 安全审计

数据和数据库加密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、操作人员等密码应用服务的日志记录。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。

4 产品特点

4.1 支持多应用模式

系统支持多个应用系统同时使用数据加密服务，系统支持应用系统的添加、删除、修改等管理功能，便于多个应用系统接入和认证。

支持数据库透明加密场景，可以实现对数据库字段进行自动加解密处理，应用系统无须改造即可完成数据加密存储。

支持数据加密场景，应用系统可按需对数据内容进行加密处理和加密存储，满足应用系统个性化加密需求。

支持文件加密场景，应用系统可按需对文件进行加密处理和加密存储，满足应用系统对文件加密的个性化需求。

4.2 保留格式加密

数据加密后保留原数据格式，加密后密文长度和原文一致。满足常用数据库字段类型加密，包括整型类型，字符串类型。应用系统集成无需改造数据库。

4.3 应用系统免改造

通过在应用系统中配置数据透明加密网关的方式，即可实现数据库敏感字段加密和解密，以密文形式存储于数据库中，让用户在无感知的情况下保护其敏感数据不被泄露，无需应用系统开发改造和适配数据库。

4.4 高可用性

数据和数据库加密系统支持双机热备、透明故障切换、数据错误忽略、备份恢复等技术，使数据和数据库加密系统具备高可用支持和异常故障处理能力。

5 产品部署

数据和数据库加密系统根据加密模式不同，产品部署分两种方式。

5.1 数据库加密网关模式

数据库加密网关模式中，数据和数据加密系统与应用系统、应用系统数据库部署在同一网络区域，数据和数据加密系统作为透明加密网关，则需要与应用系统和应用系统数据库建立连接。部署示意图如下。

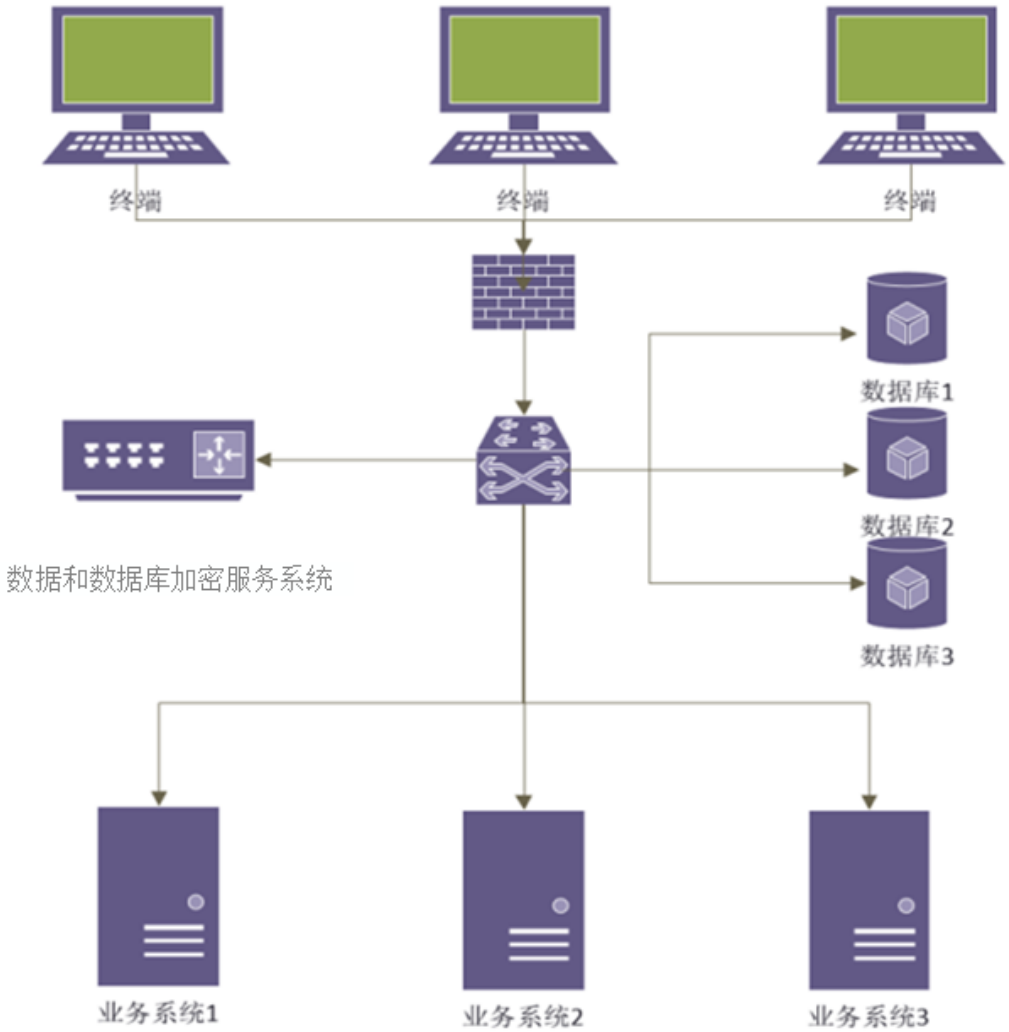


图 3 数据库加密网关模式系统部署示意图

5.2 SDK 加密模式

数据加密模式中，数据和数据加密系统与应用系统部署在同一个局域网中。部署示意图如下

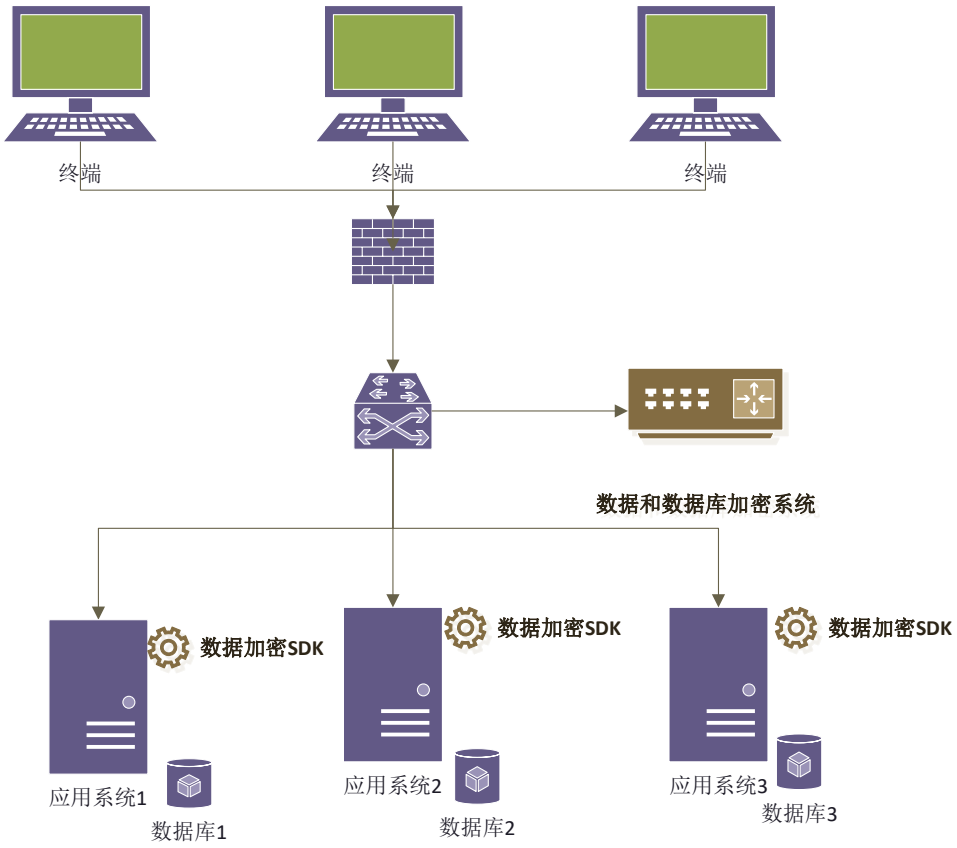


图 4 SDK 加密模式系统部署示意图

应用系统需集成数据和数据库加密系统 SDK，实现数据加解密服务功能的调用。数据和数据库加密系统只负责将数据明文加密成密文，或将数据密文解密明文数据的读写操作由应用系统完成。

6 应用场景

6.1 政务行业数据加密应用

政务信息化系统涉及政府信息、个人身份信息、民生数据等众多重要数据，需要通过数据库透明加密手段实现对重要数据的机密性保护，数据库透明加密场景如图所示。

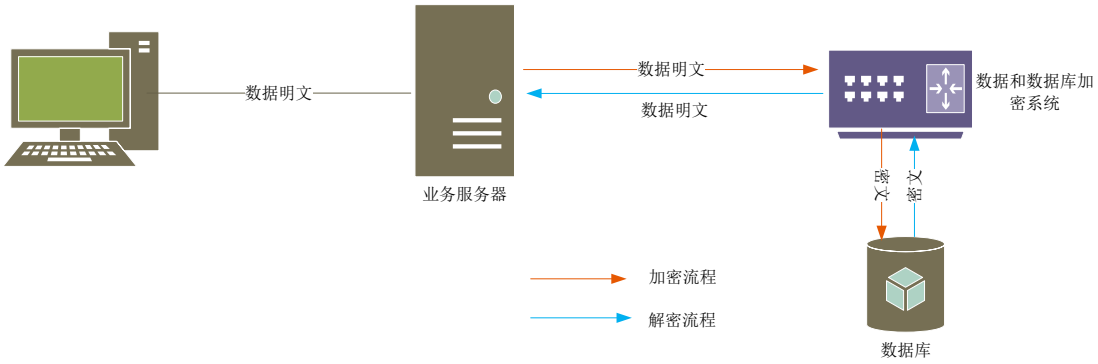


图 5 政务行业数据加密应用场景

政务信息系统配置连接数据和数据库加密系统服务地址和端口。数据和数据库加密系统将按照加密策略自动对需要加密的重要数据进行加密，然后自动将密文存在数据库指定的位置；当使用者在打开或编辑指定数据时，数据和数据库加密系统自动对已加密的数据进行解密。数据在数据库中以密文形式进行存储，一旦离开使用环境，由于应用程序无法使用自动解密服务所以无法得到数据明文，从而起来保护数据内容的效果。

6.2 教育行业数据加密应用

教育行业涉及学生身份证号、学号、家庭住址等重要数据，需要使用加密手段来保障这些重要数据机密性，防止学生数据被非法泄露。数据加密场景如图所示。

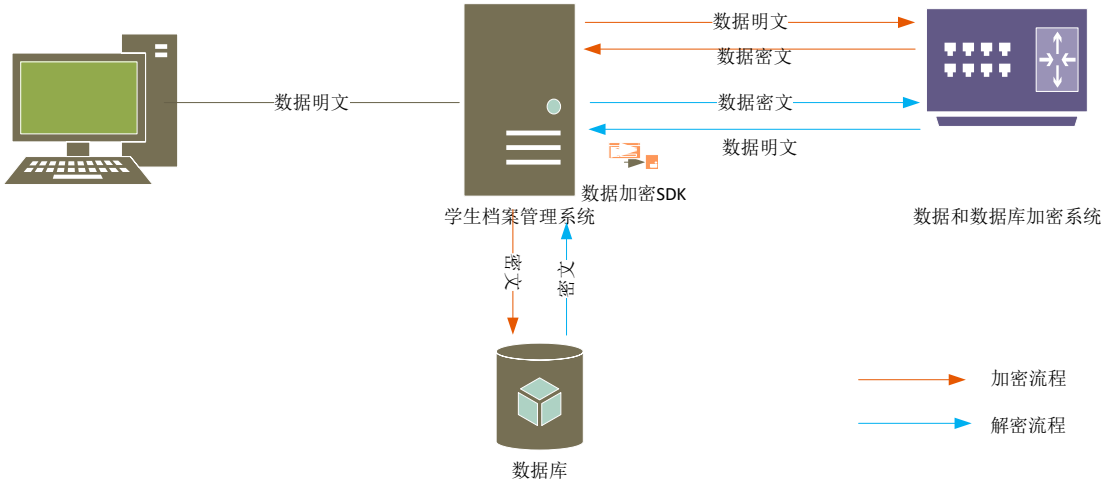


图 6 教育行业数据加密应用场景

教育信息系统如学生档案管理系统等，通过调用数据加密 SDK 实现对重要数据加密处理，然后以密文的形式进行存储，确保只有合法用户才能看到数据明文，非法用户或系统管理员只能看到数据密文。在数据读取时，调用数据加密 SDK 解密接口，对数据进行解密处理，得到数据明文。

6.3 医疗行业电子病历加密应用

电子病历文件涉及患者身份信息、病情等众多隐私数据，为了保障患者隐私数据不被泄露，医院信息化系统需要将电子病历文件加密存储。电子病历文件加密应用场景如图所示：

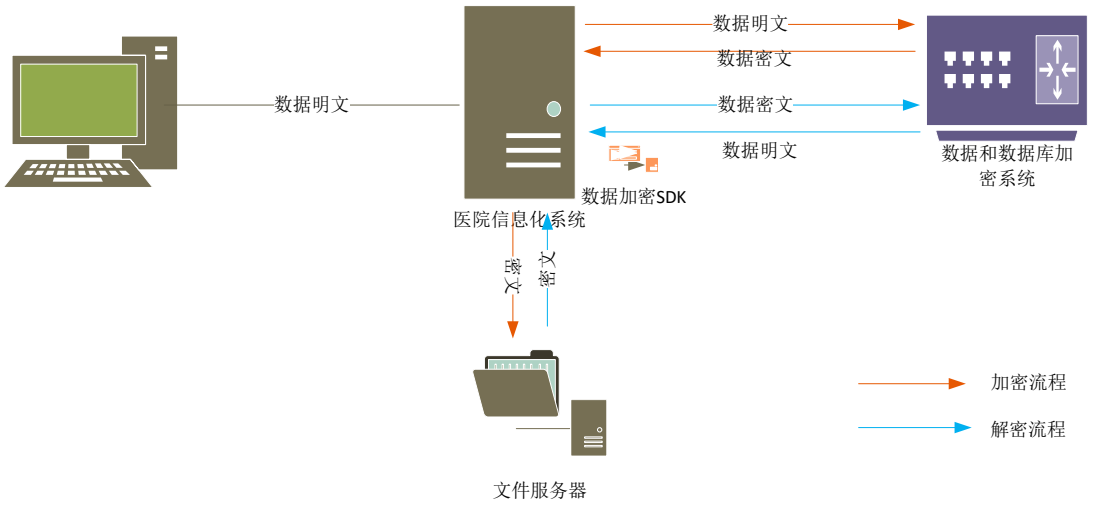


图 7 医疗行业电子病历加密应用场景

医院信息化系统调用数据加密 SDK 对电子病历进行加密处理，将电子病历以密文的形式存储在服务器中，确保只有合法用户才能看到电子病历明文，非法用户或系统管理员只能看到电子病历密文。在电子病历读取时，调用数据加密 SDK 解密接口，对电子病历进行解密处理。

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》

商用密码产品认证证书

证书编号：GM001112220220060

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

产品名称和型号、版本

数据和数据库加密系统密码模块
CY-DBES-V3000 V1.0.0

产品标准和技术要求

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：2022 年 2 月 7 日　　有效期至：2027 年 2 月 6 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