AiTDE透明数据库加密系统

技术白皮书

**目录**

[1 市场背景 1](#_Toc91064145)

[1.1 市场环境 1](#_Toc91064146)

[1.2 法规要求 1](#_Toc91064147)

[2 产品定位 2](#_Toc91064148)

[3 产品架构 3](#_Toc91064149)

[3.1 产品组成 3](#_Toc91064150)

[3.2 工作原理 4](#_Toc91064151)

[4 产品功能 7](#_Toc91064152)

[4.1 数据库透明加密 7](#_Toc91064153)

[4.2 支持多种算法 7](#_Toc91064154)

[4.3 密文密钥分离机制 7](#_Toc91064155)

[4.4 兼容多种环境 7](#_Toc91064156)

[4.5 高效检索能力 8](#_Toc91064157)

[4.6 完善的访问控制机制 8](#_Toc91064158)

[4.7 三权分立机制 8](#_Toc91064159)

[5 产品优势 8](#_Toc91064160)

[5.1 安全合规 8](#_Toc91064161)

[5.2 应用透明 9](#_Toc91064162)

[5.3 高可用性 9](#_Toc91064163)

[5.4 部署便捷 9](#_Toc91064164)

[6 产品参数 10](#_Toc91064165)

[7 产品部署 11](#_Toc91064166)

[8 参考标准 12](#_Toc91064167)

[9 资质证书 12](#_Toc91064168)

[10 行业案例 12](#_Toc91064169)

# 市场背景

## 市场环境

大数据时代，信息技术日益发达，应用范围越来越广泛，许多行业开始利用计算机信息技术构建数据库。数据库中包含许多重要信息和数据，许多企业需要借助数据库处理、存储大量重要信息。数据库甚至会涉及到诸多内部敏感信息，一旦出现问题，后果不堪设想。因此，在用户享受业务处理和数据交互便利的同时，数据安全保护需求交织上升，内部运维、外部攻击、新技术应用等带来的安全风险也日益严峻。

数据是信息系统中最核心的资产，因此数据库已经成为黑客的主要攻击目标，因为它存储着大量有价值和敏感的信息数据。一旦被丢失、破坏或泄漏，很可能会给企业带来难以估量的损失。因此在数据存储环节对数据库中的数据进行加密保护，对整个信息系统来说至关重要。

## 法规要求

针对日益严峻的信息安全形势，我国出台了《网络安全法》，自2017年6月1日起施行，从法律层面规范了网络业务运营者需要对应用平台中用户数据安全尽到的法律职责以及违法处罚办法。网络运营者应保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。同时也颁布了《中华人民共和国密码法》和信息安全技术网络安全等级保护基本要求等相关的政策法规，对密码技术要求进行了加强，主要包括：安全通信网络中通信传输要求使用加密技术，安全计算环境中身份鉴别、数据完整性、数据保密性使用密码技术，保证传输和存储的加密，安全建设管理和安全运维管理中包括安全测试报告应包含密码应用安全性测试相关内容等，安全通用要求中在4层面，7大类，11测评项都有密码相关要求，足以说明国家对密码技术的重视。

此外，国家市场监管总局、国家标准化管理委员会发布公告，2021年10月1日正式实施GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，该标准从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面提出了密码应用技术要求,以及管理制度、人员管理、建设运行、应急处置等密码应用管理要求。其中，39786标准中第三级密码应用基本要求中规定，应采用密码技术保护重要数据存储机密性，并且在中国密码学会密评联委会发布的《信息系统密码应用高风险判定指引》中提到，重要数据存储机密性此条款无缓解措施，该安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

为了顺应互联网时代严峻的网络安全形势和法规政策对数据库存储方面的需求，我司推出了数据库透明加密产品。

数据库透明加密产品为互联网应用提供第三方数据加密保护解决方案，解决业务提供者在数据存储环节发生的安全问题，从数据本身层面着手，有效防护数据泄露的风险。

# 产品定位

AiTDE透明数据库加密系统是一款基于国产密码的数据库加密系统，无需更改代码即可实现数据库加密，为用户提供安全合规、易部署的透明存储加密方案，产品通过国家密码管理局检测，具备《商用密码产品认证证书》，满足商用密码应用安全性评估要求。

数据库透明加密系统产品核心价值在于：

1. 安全合规：采用SM2、SM3、SM4算法，符合国密要求；
2. 透明加密：应用无需改造，业务访问对加解密过程无感知；
3. 部署便捷：不改变现有系统网络架构，易于安装部署；
4. 访问控制：支持应用白名单，实现进程级别的访问控制。

# 产品架构

## 产品组成

AiTDE透明数据库加密系统拥有完善的密钥管理体系，由数据库加密软件组成、数据库透明加密系统和专属硬件服务器组成。

1. 数据库加密软件：安装于数据库系统，实现数据透明加密；
2. 数据库透明加密系统：为数据库加密软件提供密码服务，实现密钥安全管理和数字签名认证；
3. 专用硬件服务器：数据库透明加密系统部署在专用硬件服务器中，硬件服务器符合国家密码管理局对真随机生成的设计要求，实现密钥的生成、存储等功能。

## 工作原理

### 技术实现架构

通过将要加密的数据表的数据存储路径配置在具备加解密功能的数据库加密软件中，数据库在设备上写入数据时，该加密软件中将设备的写入数据第一时间加密后将数据以密文形式写入物理设备，数据库读出数据时也需要先从物理设备读出密文然后解密返回给上层调用方，可在不修改原有数据库应用程序的情况下实现数据的存储加密。

数据库透明加密系统技术实现架构如图2-1所示：

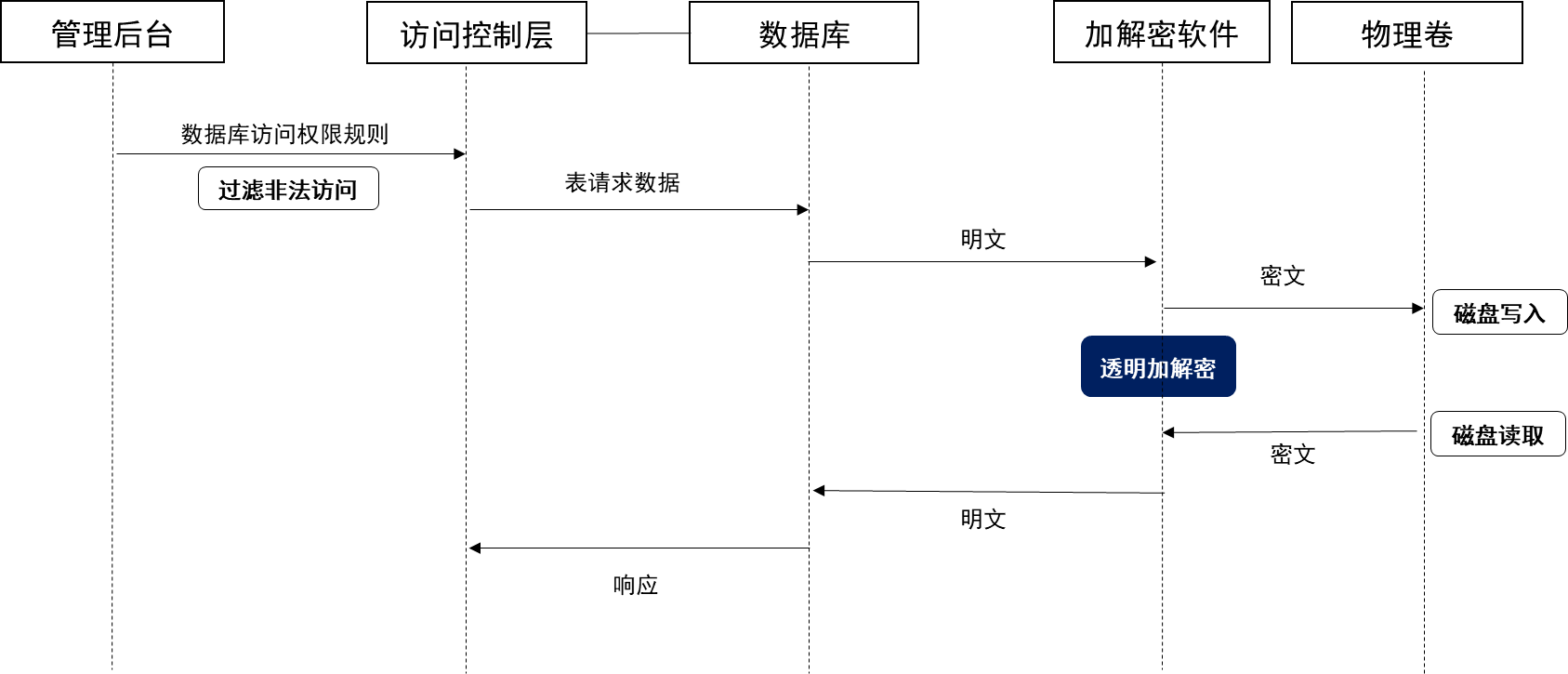


图 3‑1数据库透明加密系统技术实现架构

### 密钥管理体系

数据库透明加密系统密钥管理体系涉及产品组成部分包括数据库加密软件、数据库透明加密系统。

**数据库加密软件：**

提供数字签名接口、密钥获取接口、数据加解密接口，自动与协同服务、密钥管理服务进行网络交互。

**数据库透明加密系统：**

数据库透明加密系统主要负责如下工作：

* 加解密密钥的生成、分发、管理、保存。
* 支撑加解密系统实现数据的加解密功能。
* 负责安全生成数字签名，完成用户的身份认证。确保数据的完整性和抗抵赖性。

**密钥分发：**

加密软件申请密钥时，数据库透明加密系统只有在加密软件合法性验证通过后才会分发密钥；密钥分发过程严格采用非对称公钥加密体制，用加密软件的会话密钥加密密钥，密钥在分发和传输过程中都是密文，再在加密软件用会话密钥进行解密得到加密密钥，非对称加密技术确保只有加密软件才能解开加密数据得到密钥。

一个典型的密钥分发流程如下图所示：



图 3‑2密钥分发流程

# 产品功能

## 数据库透明加密

采用透明加密形式，对上层应用及部署无影响，无需更改代码即可加密数据库敏感数据，通过把数据库的表存储文件路径配置在加解密系统中，可实现数据库表文件的自动加解密。对数据库而言，存储加密数据文件的加解密系统与普通存储设备没有区别。功能上加解密操作对数据库层无感知。

## 支持多种算法

本产品综合采用SM2、SM3、SM4国家商用密码高强标准加密算法，符合《中华人民共和国密码法》对商用密码的相关要求，同时支持AES等国际算法，为数据加密提供高效的密码运算和加解密服务，保证敏感数据的机密性、真实性、完整性。

## 密文密钥分离机制

本产品具备独立于数据库系统的密钥管理体系，采用密钥和加密数据分离存储的理念，保证密钥不出设备，确保即使被拖库，数据依然安全。通过密钥分割和协同签名技术，解决针对数据库系统数据加密中私钥存放的安全问题，可保证私钥在数据库存储和使用的安全性。

## 兼容多种环境

本产品可兼容多种环境，支持绝大部分主流Mysql、Oracle、Postgresql、MongDB、ElasticSearch、influxDB、Hadoop、Kafka、Hive等数据库系统，支持CentOS、中标麒麟、RedHat等操作系统。

## 高效检索能力

支持对数据库系统进行加密后，对密文数据提供索引能力，同时对性能损耗极小。

## 完善的访问控制机制

提供安全访问控制功能，除数据库原有权限控制外，可限制访问数据库的具体进程等。基于进程与数据库用户绑定进行访问控制增强，同一用户只能通过指定的进程访问密文，而无法使用命令行等其他方式访问密文数据，可有效防止合法用户违规操作引发的数据安全隐患。

## 三权分立机制

实现系统管理员、安全管理员和审计管理员三权分立。其中安全管理员完成日常的加密数据配置、数据库用户的密文权限控制等安全维护和管理操作；审计管理员进行审计开关的控制，检索、分析密文访问操作的审计信息工作；系统管理员则负责进行系统配置，如IP，端口等的配置。

# 产品优势

## 安全合规

本产品中密码计算采用SM2、SM3、SM4国密算法，已获得国密局授权商用密码产品型号证书，可满足等保2.0以及商用密码应用安全性评估应用和数据安全层面数据存储机密性和完整性保护的合规要求。

## 应用透明

加解密对上层应用访问过程完全透明，无需用户系统做任何改动，将对其他系统影响最小化。

## 高可用性

本产品可支持高可用的多台设备热备灾备方案,多台服务器互为主备,单台服务器故障时,其他服务器主动接管作业及IP地址,保证加密工作平稳运行。同时可实现“同城灾备”、“异地灾备”等灾备模式。

为保证数据库加密软件在高负载状态下的稳定性，支持数据库原有的冗余机制，确保数据的高可用性。

## 部署便捷

数据库透明加密系统的部署分为软件安装和硬件部署。

软件安装部分只需在数据库系统中安装数据库加密软件，不需要用户另行集成开发，对用户现有的数据库系统结构无影响，对原有操作习惯无影响。

硬件部署主要为完成专用硬件服务器的部署工作，支持独立部署，可根据系统负载需要支持弹性扩容，不需要更改用户现有的网络规模，对整体系统结构无影响，可轻便的适用于复杂的系统环境。

# 产品参数

|  |  |  |
| --- | --- | --- |
| 产品名称 | 数据库透明加密系统 | |
| 产品型号 | DAS-ABL-AiTDE-E10 | |
| 产品规格 | 规格项 | 产品参数 |
| 通用项 | 硬件规格 | 2U |
| 网络接口 | RJ-45 10/100/1000Mb\*6，可拓展 |
| 电源 | 提供冗余电源 |
| 性能指标 | 加解密速率 | 300MB/s |
| 可靠性指标 | 平均无故障时间MTBF | ≥5000h |
| 电压 | 工作电压 | ~220V±25%、50HZ |
| 环境参数 | 工作温度 | 0℃~40℃ |
| 工作湿度 | 10%~90%无凝结 |

# 产品部署

数据库加密软件安装在数据库系统中，提供数据库文件透明加解密服务，数据库透明加密系统和专属硬件服务器部署在网络路由可达位置。

当业务系统传输数据到数据库，数据直接通过数据库加密软件进行自动加密，加密后的数据以密文的形式存储在数据库指定的加密分区中，用户层面无感知，在技术实现上具有良好的安全性和处理能力，并能在不修改原有数据库系统架构的情况下透明接入系统。产品部署如下图所示：

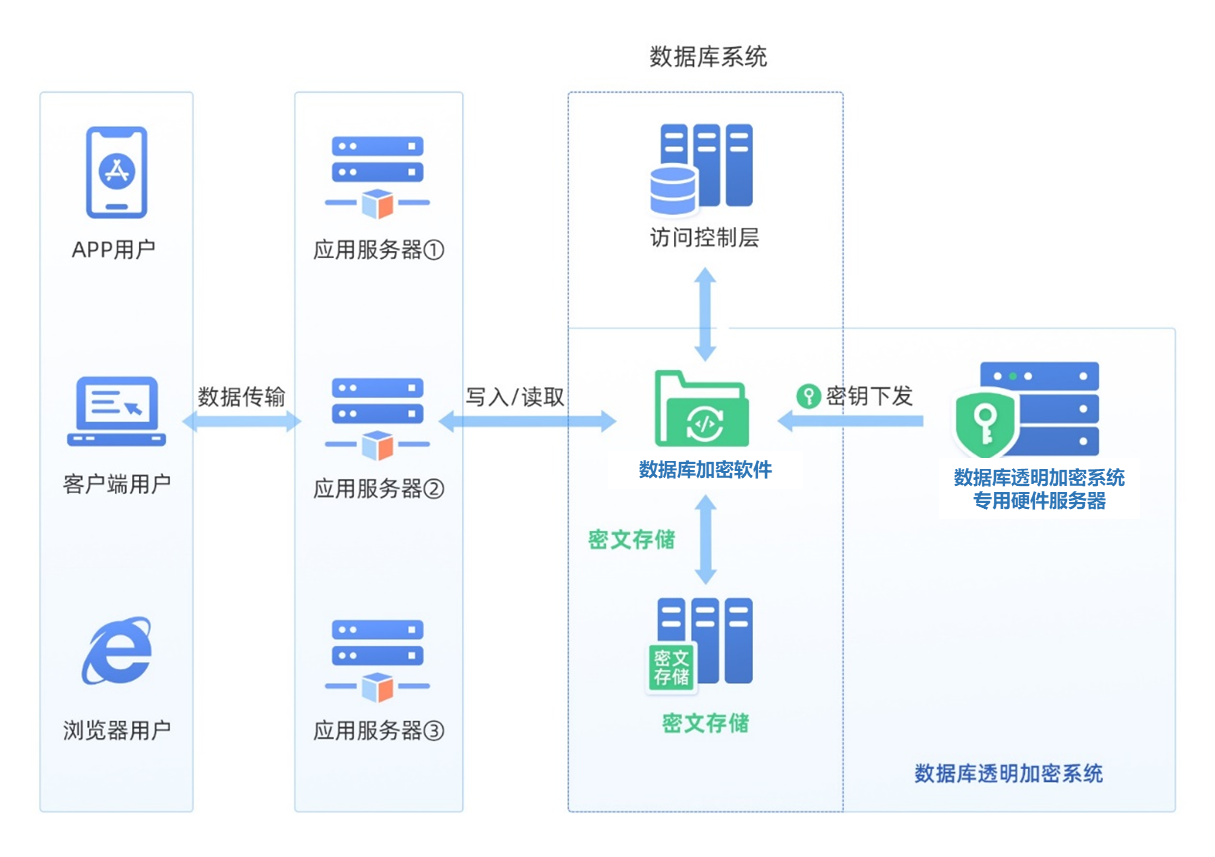


图 7‑1产品部署图

# 参考标准

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 0006-2012 《密码应用标识规范》

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 0006-2012 《密码应用标识规范》

GM/T 0028-2014《密码模块安全技术要求》

GM/T 0051-2016《密码设备管理 对称密钥管理技术规范》

# 行业案例

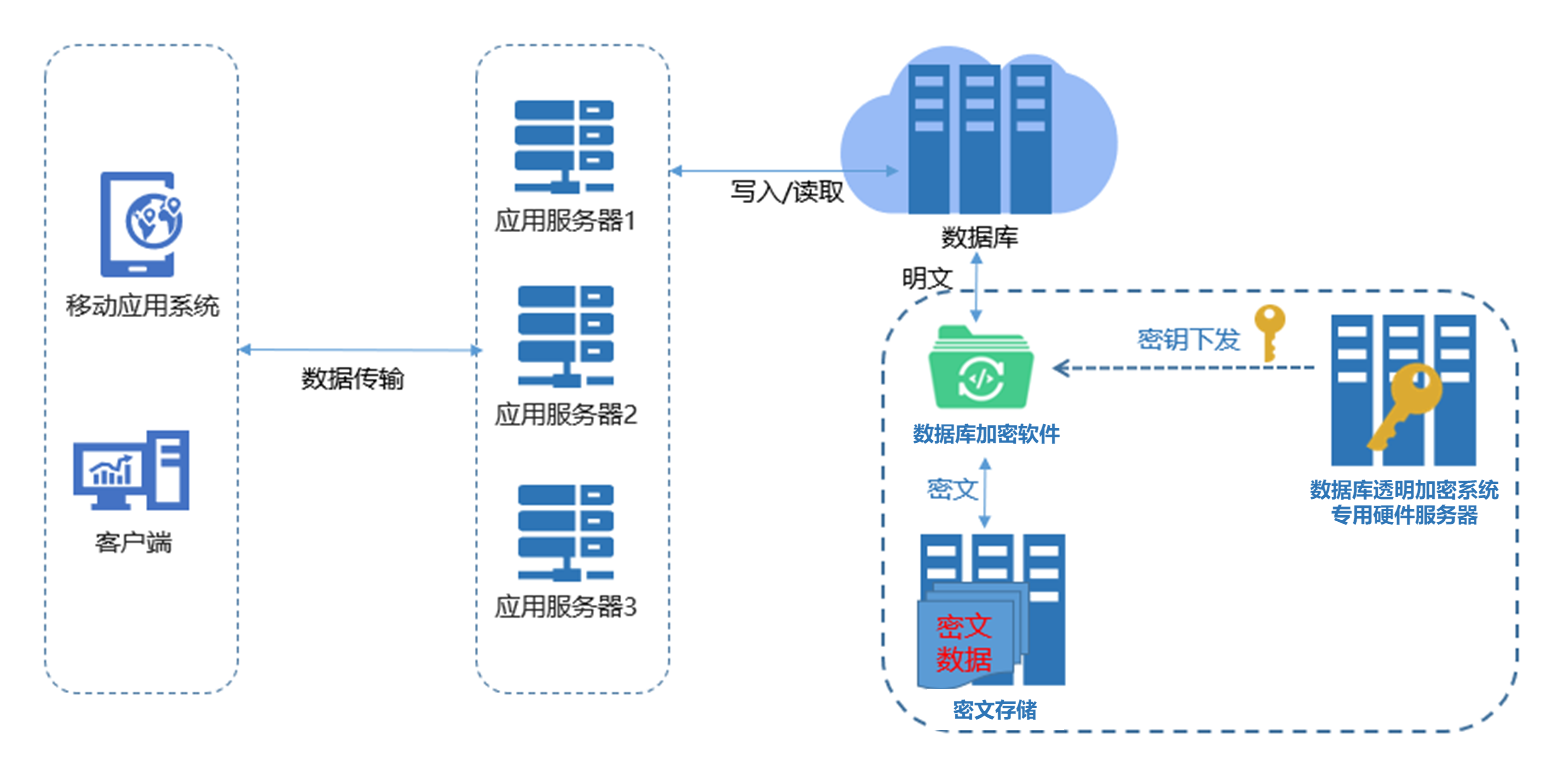
数据库透明加密产品推向市场后，受到了市场欢迎，得到了广泛应用。本产品能很好地解决政府、公安、金融、教育、医疗、企业等重要领域用户对数据存储环节的安全性和私密性、合规性的需求。

自然研究部某研究所的内部各类重要数据和重要信息存储在云服务器中，由于数据在云端存储面临的安全风险增多，数据存储防护薄弱等都会导致出现数据泄露等问题。尤其是涉及用户内部敏感信息和重要数据的云计算场景下，更是迫切有数据库加密的需求。

**用户需求:**

在不更改用户原有系统架构的前提下，统一采用国密算法针对数据存储环节进行加密，为了顺应上述需求，采用数据库透明加密产品。

**解决方案**



1.在DMZ区部署数据库透明加密系统和专用硬件服务器，同时在数据库中安装数据库加密软件。

2.当业务系统传输数据到数据库，数据直接通过数据库加密软件进行自动加密。

3. 加密后的数据以密文的形式存储在数据库指定的文件中，用户读出数据时也需要先从物理设备读出密文然后解密返回给上层调用方，不改变用户操作习惯。