项目需求

|  |  |
| --- | --- |
| 项目名称 | 数据库加密系统 |
| 需求内容：1、提供一套支持国密算法的数据库加密系统对医院外网重要信息系统数据进行加密存储，且加解密过程不影响业务逻辑，对现有应用系统无侵入、无需代码改造，能够无缝接入我院数据安全平台，实现在平台内进行统一资产管理、身份管理、联动处置等，提高运营效率。2、本次提供的系统需满足国密要求3、功能授权需求说明：（一）数据加解密（1）支持根据数据库查看加密资产的信息，以库加密、schema加密、表加密、列加密、表空间加密等维度查询当前的加密资产（2）至少支持整库、表空间、schema、表、列等数据加密粒度；支持针对不同敏感等级的数据进行加密（3）支持多种加密模式，支持业务在线加密，不需要业务停机。（4）支持以下特殊数据类型和索引类型的加密正常读写、等值查询和范围查询：BLOB数据、CLOB数据、IOT表的Mapping表、B\*Tree索引、Bitmap索引、全局索引等；（5）支持通过指定进程或指定目录，新增进程白名单（6）无需修改应用系统代码，业务系统及数据库访问工具如PL/SQL、JDBC、ODBC等访问数据库时不受影响，实现透明加密（7）支持离线加解密工具下载，通过离线加解密工具，可对敏感数据文件进行加密，保障数据文件安全；实时记录用户名、邮箱、电话、加密内容、加密地址等信息；接收方需获取授权并验证信息后才可解密密文数据文件（二）加密资产授权（1）资产访问默认密文，支持通过工单审批机制，实现加密数据资产访问授权（2）支持基于身份的密文访问控制，身份要素至少包括应用名称、应用签名、IP地址、主机名、数据库用户等，根据用户权限进行数据库返回结果控制，只有拥有合法权限的数据库用户才可看到明文，无合法权限的用户返回经过加密数据（三）密钥管理（1）加密算法至少应支持3DES168、AES128、AES192、AES256等国际密码算法，SM4等国密算法（2）支持在加密前，根据不同加密算法，进行加密结果预览（3）支持分层密钥管理体系，通过引入主密钥，加密工作密钥，生成可备份保存的加密密钥（4）支持多级密钥管理体系，同一数据库中不同的数据表使用独立的工作密钥（5）支持对密钥进行更新；支持密钥备份至本地离线保存；支持通过将密钥导入至系统，实现密钥恢复；进入加密平台后，需再次经过当前安全管理用户的密码校验后，才能进行密钥更新、备份、恢复操作（6）支持对接三方密码设备，至少包括密码卡、密码服务平台、密码管理系统等（四）集中化管理能力（1）支持数据权限功能，通过设置数据权限组，控制用户可见的资产范围；分配到对应权限组的用户，可进行对应资产的管理，否则此用户无法管理此资产，以实现数据隔离（2）支持通过敏感类型以及资产选择，进行敏感数据发现（3）支持对告警信息进行详细的订阅设置，包括告警接受的对象、接收方式、资产范围、告警范围、风险类型、告警发送时间、告警频次等信息；支持通过短信、邮件、专有钉、钉钉、企业微信等多种告警方式发送风险提示（4）安全运营工作台支持多层级部门管理，实时监测各部门资产的安全状态，集中展示风险事件；提供部门级资产基本统计数据，明确资源分布与安全配置状态（5）支持对接第三方数据安全设备，实现数据收集、数据外发、任务联动；支持监控数据安全子设备运行状态，可直观呈现子设备的CPU、内存、磁盘使用率、网络接发情况及其趋势 |
| 使用科室制定需求 |  |
| 信息工程师审核 |  |