## 电子数据存证系统建设项目用户需求书

## 项目概况

为实现将各医疗系统中数字证书使用过程的电子签名数据进行集中、安全、长期存储及查验，需建设一套电子数据存证系统。同时，需要实现每笔签名业务按系统、按科室、按患者信息等维度进行数据记录，实现每笔签名业务对应的签名结果按原文、签名值、时间戳签名值、签名者、签名时间进行存储。

除了需要解决电子签名数据统一存储的问题，还有以下几个方面需要通过电子数据存证系统解决：

医疗业务的特殊性决定了电子签名数据的增长是非常快速的，随着时间的推移，电子签名数据的增长会给医疗业务系统带来一定的存储压力，进而影响医疗业务系统的响应效率。需要通过电子签名数据存证系统的应用，实现电子签名数据的统一存储，减轻各个医疗业务系统的存储压力。

目前医院各业务系统缺少对签名应用效果监测手段。需要通过电子数据存证系统，从侧面对各个医疗业务系统的电子签名业务进行监管，所有电子签名数据推送到电子数据存证系统上时，存证系统都会对电子签名数据进行验证，确保签名结果是正确无误的，才进行存储，避免部分开发商没有完全按照CA的开发规范进行集成，导致最后产生的电子签名数据存在问题的情况。

随着医院电子签名应用推广和签名业务量增长，目前缺少电子签名数据的统计与展示。需要通过电子签名数据统一存储后，直观地展示出电子签名应用的情况，比如每个科室的应用情况、每个业务系统的应用情况等，通过这些统计数据为医院提供一定的决策辅助支撑。

此前各业务系统各自存储签名结果，需要从各个业务系统分别查询调取签名数据，工作量大效率低下，通过电子数据存证系统，对电子签名数据、电子签名数据的验证等材料进行检索、验证和导出结果，以快速满足电子病历评级的相关要求。

## 需求清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 数量 | 维保期 |
| 1 | 电子数据存证系统 | 1项 | 三年 |

## 报价要求

本次报价对整个项目整体报价，报价中包含项目设计、开发、实施、运输、安装、培训以及所有税费等。

## 功能参数

|  |  |  |  |
| --- | --- | --- | --- |
| **模块** | **二级功能序号** | **二级功能** | **三级功能** |
|
| 1.管理员功能 | 1.1 | 系统配置管理：可以对一些系统相关的参数进行配置管理，以便于其他模块的调用。包括了查询系统配置、修改系统配置、重置系统配置。 | 要求提供服务地址配置、存储路径配置、存储年限配置、单位logo配置等 |
| 要求提供第三方日志开关； |
| 要求提供定时任务记录开关； |
| 1.2 | 系统用户管理：管理员可以对操作员、审计员等系统用户进行有效的管理和监控，不同的系统用户可以分配不同的角色，不同角色有不同权限，通过有效的用户管理，可以确保只有经过授权的用户才能访问系统资源。 | 要求提供新增系统用户功能：可以新增管理员、操作员、审计员等不同系统用户。 |
| 要求提供删除系统用户功能：支持删除指定系统用户。 |
| 要求提供导出系统用户证书功能：采用证书登录，可以将系统用户绑定数字证书，实现强身份认证。 |
| 要求提供批量冻结/解冻系统用户功能：支持临时冻结/解冻系统用户，禁止非法用户访问。 |
| 要求提供系统用户详情：支持查询系统用户状态查看以及详细信息。 |
| 要求提供系统用户查询：支持多个不同维度进行查询系统用户。 |
| 要求提供修改系统用户功能：支持对系统用户进行修改。 |
| 1.3 | 用户权限管理：对系统中的用户进行权限的分配和管理，以确保用户只能访问其被授权的资源和执行其被授权的操作。 | 要求提供定义权限功能：权限划分为多个层级，例如模块级别的权限，每个权限可以用一个唯一的标识符来表示，以便于管理和控制。 |
| 要求提供角色创建功能：系统管理员可以创建系统设置不同的角色层级以及权限组合。 |
| 要求提供角色分配功能：将用户按照其职责和需要的权限划分为不同的角色。 |
| 要求提供权限控制功能：根据用户的权限和角色，对用户的操作进行控制。在用户登录系统时，通过验证用户的身份后，还需要对用户进行权限验证。 |
| 要求提供用户权限查询功能：管理员可以查询给用户分配的不同权限设置。 |
| 要求提供用户激活/冻结功能：管理员可以通过冻结或激活进行控制用户，冻结的用户不可用，激活的用户可以正常使用。 |
| 1.4 | 项目管理：可以支持以项目维度进行管理电子存证的不同数据，实现不同项目之间的数据进行逻辑隔离，不同的用户可以查看到不同的项目中的业务数据。 | 要求提供新增项目功能：记录项目编号、项目名称、状态、创建时间等信息。 |
| 要求提供删除项目功能：系统提供删除项目的操作，管理员可以通过此功能移除不再需要的项目。删除操作会彻底移除项目的所有相关数据和配置信息，确保数据的整洁性。 |
| 要求提供项目信息详情：系统提供查看项目详细信息的功能，管理员可以查看项目的编号、名称、状态、创建时间、最后修改时间等详细信息，以便更好地管理和监控项目。 |
| 要求提供项目信息查询：系统提供项目信息查询功能，管理员可以通过项目编号、项目名称、状态等条件进行快速查询，方便管理和定位项目。 |
| 要求提供批量冻结/解冻建项目功能：系统提供批量冻结和解冻项目的功能，管理员可以通过此功能快速批量处理项目状态，冻结的项目将无法进行数据操作，解冻后项目恢复正常运行。 |
| 要求提供修改项目信息功能：系统提供修改项目信息的功能，管理员可以对项目的编号、名称、状态等信息进行更新，以适应项目的变化和管理需求。 |
| 1.5 | 第三方接入管理：可以对接入电子数据存证系统的第三方业务系统进行管理，为这些第三方业务系统创建接入账号信息并配置认证密钥。只有在本系统注册了第三方接入配置，提供第三方系统接入编号才允许通过本系统提供的对外服务接口进行合法调用，以此实现接口鉴权与认证。 | 要求提供新增第三方应用功能。可录入接入名称，生成认证密钥、设置存储时长等； |
| 要求提供编辑第三方应用功能。可对接入名称、接入状态、默认标签、接入厂商名称、默认时长等信息进行修改 |
| 要求提供认证密钥功能。认证密钥是第三方应用接入的身份标识，支持国产密码算法； |
| 要求提供批量冻结/解冻第三方应用功能。在第三方应用不再符合接入要求时，可对其进行冻结操作；当第三方应用再次符合接入要求时，可进行解冻； |
| 要求提供检索、查看第三方应用详情。包括入接入名称，认证密钥、设置存储时长等信息； |
| 要求提供密码技术实现接口鉴权功能。以国产密码技术为核心，采用非对称密钥技术，对接入的第三方应用进行接口鉴权； |
| 1.6 | 定时任务管理：可以对当前系统内运行的定时任务情况做一个管理，并且可以启动、停止定时任务。定时任务包含了热库数据迁移至冷库定时任务、热库已归档数据表清理定时任务、缓存数据落库定时任务等多种任务运行管理。 | 要求提供热库数据迁移至冷库定时任务功能。通过预设指定的时间周期内自动将热库数据从一个数据库迁移到另一个数据库，将热库数据迁移到冷库数据库，以优化主数据库的性能。减少人工干预，降低错误率，定时任务可以快速完成数据迁移，提高工作效率，支持设定不同的迁移策略和时间，提高灵活性。 |
| 要求提供热库已归档数据表清理定时任务功能。一种数据库维护策略，主要功能是定期清理热库中已归档的、不再需要频繁访问的数据表。通过自动化清理操作，可以释放存储空间，优化数据库性能，并确保数据的合理管理和存储。 |
| 要求提供缓存数据落库定时任务功能。是将缓存中的数据按照一定的时间周期定期写入到数据库中，并在每次写入前创建新的数据表，用于处理大量实时数据，确保数据的持久化和可追溯性。 |
| 要求提供历史数据迁移任务功能。通过预设指定的时间周期内自动将历史数据从一个数据库迁移到另一个数据库，将历史数据迁移到归档数据库，以优化主数据库的性能。减少人工干预，降低错误率，定时任务可以快速完成数据迁移，提高工作效率，支持设定不同的迁移策略和时间，提高灵活性。 |
| 要求提供摘要数据生成存证报告功能.通过预设指定的时间周期内自动对存证系统中摘要数据生成存证报告，并将凭证存储到文件系统中。通过定时异步方式减轻了主数据库的压力，提高性能。 |
| 要求提供摘要数据加固时间戳.通过预设指定的时间周期内自动对存证系统中摘要数据进行加盖时间戳加固，防止数据篡改。 |
| 要求提供查询不同定时任务状态、停止定时任务、启动定时任务等管理。 |
| 1.7 | 数据迁移策略管理：可以对数据迁移策略进行管理，该策略用于将数据从热库迁移至冷库，保护数据的完整性和准确性。 | 支持创建多个不同的数据迁移策略。可根据实际的需求自定义创建数据迁移策略。包括数据归档迁移时间、表迁移后保留时间等； |
| 支持修改已有的数据迁移策略。 |
| 查看不同的数据迁移策略。 |
| 转存热库数据到冷库，有效防止热库数据增大。 |
| 1.8 | 历史数据迁移表管理：针对医疗业务系统中存量的电子签名数据，可以支持将多个医疗业务系统中的历史数据迁移到本系统中，通过定义的中间表进行建立数据连接，并完成迁移。 | 要求提供新建历史数据迁移：支持建立多个数据源获取历史数据，支持测试连接。 |
| 要求提供验证数据合法性：支持对历史数据进行校验，设置不同验证级别，实现数据合法性和完整性。 |
| 要求提供定时迁移历史数据：支持指定时间段和策略进行定时迁移历史数据，实现错峰迁移。 |
| 支持终端迁移任务继续迁移，保证数据迁移直至完成。 |
| 操作员功能 | 2.1 | 电子签名数据存储管理：可以对签名数据的存储情况进行查看，其数据来源是经电子签名存储接口传入的数据，且能够控制只能管理归属于具有管辖的项目的电子签名。 | 要求提供电子签名查询功能：支持对数据编号、应用、项目、患者、业务流水号、时间等多种条件进行查询电子签名数据。 |
| 要求提供电子签名验签功能：支持对签名人的签署的电子签名进行验证，自动对签名结果进行验证，展示是否被篡改，保证电子签名的合法性。 |
| 要求提供时间戳验证：支持对电子签名值进行解析时间戳并验证。 |
| 要求提供导出电子签名数据功能：支持导出电子签名数据，并支持外部工具输入验证。 |
| 要求提供电子签名数据详情查看：支持详细查看完整的电子签名数据。 |
| 要求提供电子签名数据凭证信息查看：支持对每个电子签名数据产生凭证报告，证明数据的完整性。 |
| 要求提供导出电子签名数据凭证功能：支持对凭证报告进行导出并展示。 |
| 2.2 | 摘要数据存储管理：可以对摘要数据的存储情况进行查看，其数据来源是经摘要数据存储接口传入的数据，且能够控制只能管理归属于具有管辖的项目的摘要数据。 | 要求提供摘要查询：支持对数据编号、应用、项目、业务流水号、时间等多种条件进行查询摘要数据。 |
| 要求提供导出摘要数据功能：支持导出摘要数据下载。 |
| 要求提供摘要数据详情查看：支持详细查看完整的摘要数据与分类。 |
| 要求提供导出摘要数据凭证功能：支持对每个摘要数据产生凭证报告，证明数据的完整性，以及导出凭证报告。 |
| 2.3 | 电子文件存储管理：可以对电子文件的存储情况进行查看，其数据来源是经电子文件存储接口传入的数据，且能够控制只能管理归属于具有管辖的项目的电子文件。 | 要求提供电子文件查询：支持对数据编号、应用、项目、患者、业务流水号、时间等多种条件进行查询电子文件。 |
| 要求提供电子文件验签：支持对签名人的签署的电子文件进行验证，自动对签名结果进行验证，展示是否被篡改，保证电子文件的合法性。 |
| 要求提供导出电子文件功能：支持导出电子文件并下载。 |
| 要求提供电子文件详情查看：支持详细查看完整的电子文件。 |
| 要求提供电子文件凭证信息：支持对每个电子文件产生凭证报告，证明数据的完整性。 |
| 支持多种电子文件存储方式。 |
| 2.4 | 统计分析管理：可以对电子签名数据、电子签名文件、摘要数据存入量、接口接入情况进行查看、导出。 | 支持按项目和应用两个不同维度进行统计分析。 |
| 要求提供业务统计功能：统计业务数据总量，近3个月业务数据总量，当前数据总量，当天数据总量。 |
| 要求提供年数据量:展示近3年的数据量柱状图。 |
| 要求提供月数据量:展示近12个月的数据量柱状图 |
| 要求提供日数据量:展示近30日的数据量柱状图。 |
| 3.审计员功能 | 3.1 | 系统操作日志管理：可以全面记录用户在系统上的各种操作行为，包括但不限于登录、修改数据、删除数据等关键操作。每个事件都包含时间戳、事件类型、事件描述和其他相关属性。有助于审计员了解系统的运行状态和用户的操作行为。 | 要求提供系统操作日志查询； |
| 要求提供系统操作日志详情功能； |
| 要求提供导出系统操作日志功能； |
| 3.2 | 接口日志管理：可以能够全面收集API请求和响应的详细信息，包括但不限于请求参数、请求头、响应状态码、响应体、执行时间等。接口日志数据可以用于后续的分析、报告和审计。 | 要求提供接口日志查询功能 |
| 要求提供接口日志详情功能 |
| 要求提供导出接口日志功能 |
| 4.数字证书CA登录访问控制 | 4.1 | 支持管理员、操作员、审计员系统用户，采用数字证书UKey的物理硬件强身份认证方式进行登录系统，登录过程进行了数字签名与验签，系统则会验证证书的合法性和有效性，保证其行为不可篡改和不可否认性，确保只有合法用户才能访问系统，从而提高了系统安全。 | UKey登录产生随机数 |
| UKey登录进行数字签名 |
| 验证数据签名和证书有效性 |
| 验证身份和角色权限 |
| 5.与医疗系统对接外部接口模块 | 5.1 | 电子签名数据存储接口 | 提供一个安全的接口，用于将电子签名数据从医疗业务系统传输到电子数据存证系统。接口支持多种数据格式，确保数据的完整性和一致性。 |
| 5.2 | 电子签名数据查询接口 | 允许医疗业务系统查询存储在电子数据存证系统中的电子签名数据。支持按数据编号、应用、项目、患者、业务流水号、时间等多种条件进行查询。 |
| 5.3 | 电子签名数据验签接口 | 提供一个接口，用于验证存储在电子数据存证系统中的电子签名数据的合法性。接口会自动对签名结果进行验证，展示是否被篡改。 |
| 5.4 | 电子签名数据验签下载 URL | 提供一个安全的下载链接，用于下载经过验证的电子签名数据。链接会设置有效期，确保数据的安全性。 |
| 5.5 | 摘要数据存储接口 | 提供一个接口，用于将摘要数据从医疗业务系统传输到电子数据存证系统。接口支持多种数据格式，确保数据的完整性和一致性。 |
| 5.6 | 摘要数据查询接口 | 允许医疗业务系统查询存储在电子数据存证系统中的摘要数据。支持按数据编号、应用、项目、业务流水号、时间等多种条件进行查询。 |
| 5.7 | 摘要数据凭证生成接口 | 提供一个接口，用于生成摘要数据的凭证报告，证明数据的完整性和合法性。凭证报告会包含数据的摘要信息、签名信息等。 |
| 5.8 | 摘要数据凭证报告下载接口 | 提供一个安全的下载链接，用于下载摘要数据的凭证报告。链接会设置有效期，确保数据的安全性。 |
| 5.9 | 文件数据存储接口 | 提供一个接口，用于将电子文件数据从医疗业务系统传输到电子数据存证系统。接口支持多种数据格式，确保数据的完整性和一致性。 |
| 5.10  | 文件数据查询接口 | 允许医疗业务系统查询存储在电子数据存证系统中的电子文件数据。支持按数据编号、应用、项目、患者、业务流水号、时间等多种条件进行查询。 |
| 5.11 | 文件数据下载接口 | 提供一个安全的下载链接，用于下载存储在电子数据存证系统中的电子文件数据。链接会设置有效期，确保数据的安全性。 |

## 项目工期要求

项目工期30天内完成系统上线运行。

## 项目实施要求

1. 实施过程应严格执行相关的规范，并保证安全。
2. 应在规定的时间内，保证质量，完成系统建设。
3. 实施过程中应科学、合理地掌握与其他工作的协调、交叉。

## 售后服务要求

1. 免费维保
	1. 从项目总体验收合格之日（从双方代表终验签字之日起计算）起，提供三年软件维保服务。
	2. 免费维保期结束后，软件维保费用不高于总价格的8%。
	3. 维保期内须每季度安排工程师对系统巡检一次，安排经验丰富的、任职一年以上的运维工程师提供巡检服务。
2. 技术服务

为确保本项目系统稳定正常运行，需长期提供优良的技术支持，保修期间的维护服务不收取任何额外费用，质量保证期后，以合理价格提供软件功能改进技术服务，保修期后的具体服务价格双方另行协商。

1. 系统维护与支持的具体内容如下：

（1）电话支持

对应用系统的运行、维护提供24小时的实时技术支持。以热线电话或Email、传真等方式随时回答用户各种技术问题并在48小时内提出解决方案。需提供7X24小时内的全天服务热线。

（2）远程技术支持

当系统出现故障，需提供7X24小时的远程技术服务。

（3）现场服务

当系统运行环境出现严重故障，或因更换服务器等原因需要重新搭建系统时，通过远程支持不能及时解决问题时，需要派技术支持人员赶赴现场，协助用户完成故障排除、升级或迁移操作，对系统进行完整性检查并跟踪运行。

（4）故障响应

7 x 24小时的实时故障响应。对于电话方式无法解决的问题或系统发生严重故障时，质保期内出现质量问题，需在接到通知后的4小时内给予响应，24小时内响应到场，48小时内完成维护（以上响应时间不含从出发到达甲方的路途时间），并承担维护的费用。

1. 定期跟踪

项目验收完毕后，需定期电话、现场跟踪系统使用情况，听取意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，需派遣技术人员去现场解决存在的问题。

1. 系统升级

提供定时或不定时巡检服务，做到有问题早发现早解决。并及时向用户通报系统软件升级情况，若用户需要对系统软件升级，需提供升级版本和相应的支持服务。

1. 服务器操作系统要求

电子数据存证系统部署于内网，服务器由医院按需提供，电子数据存证系统支持部署在国产服务器和国产操作系统环境。

1. 系统安全

必须配合需求方对该软件进行安全检测时发现的安全隐患进行限期修复，在等保测评中发现的系统漏洞、安全漏洞等做整改并安全加固。

## 其他要求

培训要求：

1、培训内容与课程要求

对系统的使用，操作，维护进行培训。培训时提供安装使用维护说明书，以确保需求方能够对系统有足够的了解和熟悉，能够独立进行系统的日常维护和管理。培训所需一切资料由服务商提供。

2、培训费用

培训过程中所发生的一切费用（含培训教材费）均包含在报价中。