**福建中医药大学电子认证服务平台建设项目技术参数**

# 一、电子认证服务中台

（一）总体要求

1、系统要求采用微服务技术架构、平台化开发，支持容器化部署，使用界面直观明了、简单方便，操作简便。

2、系统采用私有化部署方式在学校本地部署，系统服务器端须支持windows、linux等主流操作系统，支持Mysql、Oracle等主流数据库。

3、系统须支持PC端和移动端应用，支持客户化开发，电子认证服务中台软件厂商须具备自主知识产权。

4、系统应提供完备的日志和审计功能，系统应保存不少于6个月的日志。

5、系统应能适配国产操作系统和国产数据库，应能支持统一部署在学校提供的国产环境。并承诺在学校要求支持对信创产品的兼容适配时，可平滑过度，免费迁移。

（二）系统应用接口

1、内部用印接口

支持需加盖内部组织印章与教职工签名的业务场景安全应用，适用如内部审批文件的签名/盖章等。需调用内部用印接口，由电子认证服务中台判断其是否有相应的印章使用权限的情况下，实现对电子文件的电子签章。接口包括：获取个人签字图片、获取公章图片、获取授权印章、获取印章授权对象、采集员工个人签字、电子签章、文档下载、申请/更新/吊销数字证书、创建/删除个人用户信息、创建组织、查看组织、导入组织数字证书、企业证书数字签名/解密等。

2、在线签约接口

基于Restful API接口，支持外部用户签名或签章场景应用，接口包括：注册用户、查询用户、查询印章、上传或生成印章、作废用章、申请/导入/吊销证书、电子签章/签名、人脸识别/短信验证、消息签名/验签、数据存证等。

（三）运营管理后台

面向运营管理人员提供丰富的管理功能，包括证书管理、公章管理、用印管理、组织管理、员工管理、角色管理、账号管理、日志管理、接入管理、预警管理、RA管理、第三方服务管理等，满足系统在使用与运营过程中集中安全管控要求。

1、个人中心

支持系统账号退出登录、修改密码，支持统一身份认证登录。

2、账号管理

账户管理功能展示当前登录账号的账号名称、账号所属组织、账号ID、数据权限、账号中心内容，支持修改密码。

3、统计查询

支持公章统计、授权印章统计、文件签署数统计、组织及员工统计。

（1）公章统计：统计有效公章数、已失效公章数。

（2）授权印章统计：统计有效授权印章数、已撤销授权印章数。

（3）文件签署数统计：统计文件签署数、文件签署记录数。

（4）组织及员工统计：统计所有组织数量以及组织下对应的员工数。

4、证书管理

证书管理是对平台证书、组织证书及个人证书的管理。支持对即将过期的证书进行预警通知和展示。支持按照组织、证书的有效时间及其他关键字检索，支持上传证书、在线申请证书以及组织证书共享功能。

5、公章管理

公章管理提供公章数据看板、公章管理列表、查询公章、管理公章标签、创建公章、编辑公章、授权公章、管理授权标签、撤销授权等公章生命周期管理功能。

（1）公章数据看板：提供公章数据看板，在公章管理菜单下，展示内部所有公章是否有效的状态的数量，包括有效公章数量、已失效公章数量、所有公章数量。

（2）支持公章列表：公章列表根据状态分为三类：有效公章、已失效公章、所有公章，对应公章列表展示。公章列表的详细信息包含公章的基础信息以及编辑管理功能，基础信息包含公章、公章ID、生成方式、印章名称、创建日志、公章标签、所属组织；编辑管理功能根据权限进行管理，所有权限包含禁用、作废、变更、用印授权。公章授权根据类型分为三类：人员、标签、应用，对有效授权进行撤销操作后，该条授权记录即变为已撤销）。

（3）查询公章：通过输入公章名称、创建时间范围、创建人、公章所属组织、公章标签进行筛选查询。

（4）设置公章标签：支持自定义公章标签名称，对公章标签的增加、删除。

（5）创建公章：支持创建内部组织印章，创建方式支持在线生成与自定义上传两种方式，支持对印章类型进行选择，支持对印章的形状、规格、颜色、中央刊图进行选择，支持自定义印章的上弦文、横向文、下弦文，创建公章时支持上传申请公章的相关证明材料。

（6）编辑公章：支持对公章的授权、禁用/启用、作废、变更及用印授权等全生命周期管理功能。

（7）授权公章：支持创建组织公章授权，按公章/员工/应用进行授权，支持通过excel表格批量导入方式进行批量公章授权。支持创建个人印章授权。

（8）管理授权标签：支持管理用印授权标签，支持对用印授权标签的增加、删除。

（9）撤销用印授权：支持对用印授权进行撤销操作，支持批量撤销授权。

查询用印授权：可通过输入公章ID/公章名称/个人签名的用户名称进行筛选查询。

6、用印管理

（1）用印记录提供用印数据看板、API用印列表、查询用印记录功能。

（2）API用印列表：提供API用印列表，API用印列表的详细信息包含签署的主要操作信息。

（3）查询用印记录：支持用印记录查询，通过输入关键字、应用、签署时间范围、公章、签署人/操作人进行筛选查询。

7、组织管理

组织管理提供组织树、组织管理、员工管理、印章管理、管理证书功能。

（1）组织树：提供组织树，系统将创建的组织数据以树结构的方式进行展示。展示组织的基本信息，如组织名称、系统ID、上级组织以及操作日志。

（2）组织管理：支持组织管理，包括组织新增、编辑等功能，支持对组织的公章与证书进行管理，可设置组织负责人和签发员工或组织证书的RA连接。

（3）员工管理：支持新增员工，支持对组织内的员工进行新增及管理功能，包括员工的所属组织、账号、姓名、邮箱、手机号码、身份证号等基本信息及签字样式和颜色。

（4）印章管理：提供印章管理功能，支持查看、新增印章，包括查看印章的标签、授权人及操作日志。

（5）管理证书：提供组织证书管理功能，支持上传证书、在线申请证书以及组织证书共享功能。

8、员工管理

员工管理支持对所有组织下的员工进行管理，包括每个组织的负责人、被授权员工所授权的印章等其他信息。支持对组织内的员工进行新增及管理功能，包括员工的所属组织、账号、姓名、邮箱、手机号码、身份证号等基本信息及签字样式和颜色。

9、文件盖章

支持自定义上传电子文件，通过可视化方式对电子文件进行电子签章，支持拖拽方式对电子文件添加个人电子签名、单位电子签章。

10、角色管理

角色管理提供角色管理列表、角色管理、角色查询功能。

（1）角色管理列表：提供角色管理列表，系统提供基于角色的访问控制。

（2）角色管理：提供角色创建、编辑、删除功能。

（3）角色查询：支持角色查询，系统支持快速搜索与高级搜索。

11、账号管理

账号管理提供账号管理列表、账号列表、账号管理、账号查询功能。

（1）账号管理列表：提供账号管理列表，系统提供基于角色的访问控制。

（2）账号列表：提供账号列表，用户账号主要用于系统的访问，主要管理工作涉及到用户账号的添加、修改和删除。

（4）账号管理：提供系统账号创建、编辑、禁用等功能。

（5）账号查询：支持账号查询，系统支持快速搜索与高级搜索。

12、日志管理

日志管理提供日志记录列表、查询日志记录、导出日志记录功能。

（1）日志记录列表：提供日志记录列表，系统管理员在系统中的操作行为展示在列表中，包括记录时间、系统模块、操作类型、操作描述等。

（2）查询日志记录：支持查询日志记录，可支持按日志记录时间段、系统模块、操作类型进行搜索。

（3）导出日志记录：支持导出日志记录，支持按条件搜索后列表记录的导出。

13、接入管理

接入管理提供接入管理数据看板、接入应用列表、接入应用管理、查询应用功能。

（1）接入管理数据看板：提供接入管理数据看板，面板显示系统已接入应用的数量。

（2）接入应用列表：提供接入应用列表，应用列表显示已设置好的应用，列表中每行显示接入应用的基本信息。

（3）接入应用管理：支持接入应用管理，支持应用创建、编辑、禁用/启用、查看应用详情等功能。支持对接入应用进行可视化页面配置，可对文件同步的机制进行配置，支持SFTP、COS方式。支持配置应用的公章授权列表，支持对应用的在线签约API配置、企业用印API配置、签约平台配置、存证配置。

（4）查询应用：查询应用支持接入应用查询，对列表个别字段进行模糊搜索和组合搜索。

14、预警管理

预警管理提供预警事项里列表、指定敏感操作预警、预警事项管理功能。

（1）预警事项列表：支持敏感操作预警，对一些敏感关键操作时通过系统进行通知，如公章管理的关键操作。支持组织证书到期提醒，对即将到期的组织数字证书列表提醒管理员及时更新。

（2）预警事项管理：支持对预警事件的开启、关闭功能。

15、RA连接管理

RA连接管理提供RA连接列表、创建/编辑RA连接功能。

（1）RA连接列表：支持展示已经完成配置的 RA 连接，默认的 RA 连接边框进行高亮边框显示。

（2）创建/编辑RA连接：提供创建/编辑RA连接功能，支持对连接名称、接口地址、账号、密码、证书有效期、签名算法、代理设置等进行配置。

16、第三方服务管理

支持对连接的第三方的认证服务进行配置，包括短信服务、个人实名认证、企业实名认证进行配置。

17、定时任务

支持导入定时任务，支持切换为实时调度和整点调度。支持对系统数据同步、数量统计、文件归档、敏感数据脱敏等策略进行配置。

18、基本配置

支持切换系统主题皮肤颜色，至少包含5种默认颜色选择。支持对平台证书进行上传配置，支持双签模式。

19、操作日志

展示当前登录账号的所有修改操作，包含登录账号、增删改查印章签字文档合同。

20、服务监控

服务监控提供API调用记录和回调管理功能。

（1）API调用记录：提供API趋势图和API调用记录表，支持入站请求和出站请求API记录表，支持查看请求时间、API地址、请求参数、响应内容、响应时间、执行状态等信息，支持按请求时间、执行状态、请求参数、调用应用、API地址进行API记录的精准查询。

（2）回调管理：提供系统回调列表，用于管理回调功能，支持查看回调ID、回调信息、创建时间，支持回调重试功能。支持按回调名称、回调参数、回调状态、创建时间进行精准查询。

# 二、数字证书服务

为给各业务系统及用户提供合法合规的电子签章服务，需要基于第三方CA的数字证书服务，以满足《中华人民共和国电子签名法》等法律法规要求。包括：

（一）单位数字证书（国际算法）

标识学校及二级单位/部门、外部单位的真实身份，用于对文件进行电子签章。单位数字证书数量为1张，证书服务期为三年。

（二）个人数字证书（国际算法）

标识学校教职工、学生、外部个人用户的真实身份，用于对电子数据进行电子签名。个人数字证书数量为200张，证书服务期为三年。

# 三、校自助打印系统扩展

（一）证明文件电子档自助申请模块

1.系统登录

系统支持对接学校统一身份认证，也可以根据学校的安全性需求，实现学号+密码等多种方式组合认证，确保用户的隐私不被泄露。

2.电子档项目选择页面

用户登录后，进入电子档申请项目选择页面，用户根据需求选择需申请的电子档项目进行申请操作。

3.电子档项目预览页面

选择证明文件电子档项目后，点击项目进入证明文件预览页面，用户在该页面对证明文件报表进行预览查看，确认报表内容完整准确。确认报表的准确性后，即可点击“继续”按钮生成证明文件电子档申请订单。

4.电子档申请完成页面

预览电子证明文件报表内容，确认无误后，即可进入申请订单完成页面，在该页面，用户可以点击“发送至邮箱”按钮将证明文件电子档发送至用户指定的邮箱中，或可以点击“下载”按钮将证明文件电子档下载到本地。

5.电子档项目申请记录

已申请的记录可以在登录后的电子档项目选择页面通过点击“查看历史记录”进入证明文件电子档申请记录列表页面中进行查看，同时针对于已申请的记录，并且该记录未超过有效期可以再次点击“发送至邮箱”按钮再次发送证明文件电子档至申请时填入的邮箱中，或下载限制次数的可点击“下载”按钮再次下载到本地。

6.自动注销

系统提供自动注销功能，管理员可以设置页面没有操作情况下超出空闲时间进行自动退出登录，以防止用户忘记退出，保护用户的数据信息安全。

7.报表定制

提供对实现学生成绩单、在读证明、在职证明等学校各类许可证明材料自助打印服务，可以针对不同终端不同角色设置自助终端打印服务项目，打印报表的建设可根据采购人个性化样式需求设计并实施；

（二）电子证明文件验真

1.电子证明文件扫防伪码验真

系统对每份生成的电子报表进行存档，并生成唯一的二维码粘贴在电子报表上，用户只需要扫描二维码，就可以对电子报表文档进行真伪校验，实现数据内容的真伪校验功能。

2.电子证明文件防篡改验真页面

通过第三方应用对接，或扫码证明文件上二维码验真页面为入口进入到电子真实文件在线验真的网页中，然后上传需验真的电子证明文件，点击“点击验真”按钮，即可获取验真的结果，确认文档自签发后是否有篡改。

3.电子证明文件防篡改验真实现

电子证明文件防篡改验真功能我们使用了2种技术对电子证明文件的真伪保驾护航。

（1）电子档加盖可信CA签章

CA签章是电子签章，是电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。

同时，加盖了CA签章的文件，使用PDF工具查看时，可以查看电子档文件签章的签发状态和文件是否已被篡改的一个状态信息，查看该证明文件电子档文件是否已被修改，从而保证电子档的真实性。

（2）输出电子档文件MD5溯源

针对项目现场没有签章系统，或证明文件盖章不在本系统中时，则通过生成文件的MD5加密信息进行比对，确认该电子证明文件是否已被篡改。

在可信证明文件申请生成时，将生成的PDF文件的MD5进行获取，并将其保存至数据库中，标识该申请出去的此份PDF文件。

在验真页面上传电子档PDF文件，通过获取上传电子档文件的MD5到数据库查询溯源，确认系统中是否有该MD5值得存档证明文件数据，如果存在则该份文件为有效证明材料文件。

# 四、系统集成服务

（一）项目本期需完成电子认证服务平台与学校现有身份认证平台、主数据管理平台进行对接。

（二）项目本期需完成4个业务系统集成对接：

系统需与自助打印系统对接，实现线下打印成绩单等证明文件的电子签章应用。

系统需与OA系统对接，实现审批流程中领导签批、部门签章的电子签章应用。

系统需与网上办事大厅对接，实现业务流程中领导签批、部门签章的电子签章应用。

系统需与一站式服务大厅对接，实现业务流程中领导签批、部门签章的电子签章应用。

1. 需承诺免费进行对接并承担第三方对接所产生费用。

# 五、质保和供货要求

合同签订后60天内部署并调试至可验收状态；质保期三年。