广东医科大学顺德妇女儿童医院线上 CA 项目需求书

一、功能要求

医院有多种医疗信息化终端，本次引进电子签名产品，必须支持所有的医疗信息系统终端，包括 PC 终端、安卓移动终端、苹果移动终端、PDA 移动医疗终端，必须全方位支持医疗行业中存在各类型电子签名业务，主任医生与实习医生之间的授权签名，医生与医生之间的协同签名等为更好的维护医疗业务的连续性，实现电子签名与业务的轻度耦合，甚至零耦合，实现各种故障下的医疗业务连续性。

1、 手机扫码身份认证

以手机扫码的方式取代原有 USBKey 数字证书的身份认证方式，完成业务系统验证与登录。

2、 手机扫码电子签名

以手机扫码的方式取代原有 USBKey 数字证书电子签名方式，签名应用支持移动端和 PC 端，在首次签名的时候或者认证有效期失效的时候需要进行身份认证。

3、 即时签名

医护人员在进行身份认证通过后，立刻对提交的数据进行签名。第一次签名时需要进行身份认证，在认证的有效期内（可自定义，如 2 小时），以后的签名过程中不需要再进行身份认证。

4、 非即时签名

医护人员在提交完数据后，不会立刻对提交的数据进行签名。签名数据仍会在医疗信息系统中流转，在合适的时候再打开手机上的专用 APP，进行身份认证后，对所有提交的数据进行补签名。

5、 授权签名

主任医师授权给实习医师，使得实习医师可以调用主任医师的数字证书进行电子签名。

6、 升级优势

完全兼容医院已有 USBKEY 电子认证数字证书体系兼容，完全兼容医院已有电子印章、电子认证网关。无需改动医院已有数字证书体系、电子印章、电子认证网关服务器及其相关应用接口。

7、本项目线上 CA 系统包括以下内容：云密钥安全管理服务 1 套和云密钥安全管理服务器 2 台

二、安全管理需求

云密钥安全管理服务功能需求：

项目名称	需求说明
证书管理	● ▲证书生命周期管理，包括单个/批量申请证书、单个/批量续期证书。证书下载，通过用户名、用户标识查询证书，可下载证书；证书绑定，用户标识与证书进行绑定；密码管理，包括修改密码、密码解锁。 ● 证书申请，支持单个申请，一键批量申请；支持应用通过接口在线申请； ● 支持数字证书、续期、注销、变更等全生命周期服务管理，支持一键批量操作； ● 支持数字证书口令在线解锁； ● 支持证书发放数量统计；

身份认证管理	● ▲身份认证方式：通过多因子认证（口令认证、口令认证+刷脸认证、口令认证+短信认证、口令认证+指纹认证、口令认证+设备认证）、扫码认证方式进行身份认证。 ● ▲身份认证方式管理：对认证方式进行查询、修改、添加操作。用户完成登录认证后，在一定时间内免扫码认证或免密签名，可设置免密时间长短； ● ▲认证提醒：第三方应用发起认证时，提醒用户进行认证确认。
授权管理	通过授权管理实现用户之间进行互相授权的操作。 ● ▲授权用户管理：对授权用户进行查询、修改、添加授权操作。 ● ▲申请授权：授权用户申请授权；删除授权：删除已经授权的信息；确认授权：授权人确认授权行为； ● ▲冻结/解冻授权：授权人可冻结授/解冻授权； ● ▲授权续期:授权人可对授权用户的授权时间、授权使用次数进行续期；
电子签名管理服务	通过电子签名管理服务实现各场景签名应用。 ● ▲授权签名：授权人可指定授权用户代授权人进行签名。 ● ▲非实时签名：支持提交签名文件后，在 APP 上确认后才对文件进行签名。 ● ▲协同签名:提交协同签名文件，可设置并行多人签名、多级串行签名； ● ▲属性选项:提交签名文件时可配置是否添加签名时间戳、内容时间戳、吊销信息（CRL 信息、OCSP 信息）、证书链。
电子印章	● 支持 PDF 文件电子印章功能 ● 印章管理，包括印章/个人手写签名图样采集、印章上传、印章下载 ● 电子签章，包括不带时间戳的签章、带时间戳的签章、指定位置签章、指定域签章
用户管理	● 对证书用户和系统管理员信息进行管理 ● 批量导入用户信息 ● 支持删除、冻结用户
日志管理	● 支持管理员操作日志、接口调用日志，便于操作行为溯源； ● 支持关键操作查询和统计
安全通信	● 移动端与服务端之间的通信全部建立在安全加密信道的基础上，确保信息传输安全
跨平台支持	支持 Windows、Linux、 Android/IOS 移动端，微信小程序等平台

安全性	● 用户密钥双重加密存储 采用密码设备叠加用户设置的口令对用户的密钥进行加密存储，实现更安全的双重加密 ● 多因子认证 结合用户指纹验证、用户口令进行多因子认证 ● 全面支持国产 SM 系列密码算法 遵从国家密码局对签名算法的相关要求，全面支持 SM2 国密签名算法，同时兼容 RSA 等国际通用算法 ● 分组加密技术 对用户的私钥资源池进行分组，采用不同的加密密钥进行分组加密，增加密钥加密存储安全性，提高加解密效率。 ● 签名私钥不出密码设备 用户在整个电子签名过程中，所有签名运算均在专用密码设备中进行，签名私钥不出密码设备，确保用户签名私钥的安全性
电子签名长久保存解决方案	▲结合电子签名、时间戳等技术为电子病历归档与长期保存解决方案，解决电子病案等电子档案电子签名独立验证、时间链条可追溯，实现可靠的电子档案保护策略等。

云密钥安全管理服务器技术需求：

项目名称	需求说明
密钥管理	密钥生成：支持生成 SM2 密钥对、RSA 密钥对、对称密钥（通信密钥）等。 密钥销毁：支持销毁 SM2 密钥对、RSA 密钥对和通信密钥的功能。 密钥备份：在满足权限的情况下能够将密码设备内的密钥等重要信息加密后进行备份，并且可以恢复到相同型号的设备中。
密码算法	非对称加解密算法：支持 SM2 和 RSA 算法； 分组对称密码算法：支持 SM1、SM4、3DES、AES 算法； 摘要算法：支持 SM3、SHA1、SHA256、SHA3 系列等算法。 SM2 算法：SM2 签名≥1000 次/秒，验签≥500 次/秒；
密码应用	数据加解密：支持对称加解密和非对称加解密 数字签名：支持 SM2、RSA 类型密钥对对信息进行数字签名。 支持数字信封和 SignedData、时间戳。
标准接口	符合国密局《公钥密码基础设施应用技术体系密码设备应用接口规范》的接口、PKCS#11、MS CSP、JCE 及其高层封装接口、X.509 等接口；

三、维保要求

2、免费维保期　使用期间免费维保

3、后续

证书维护费　不超过 30 元/人/证书/年

电子印章维护费　不超过 50 元/人/证书/年

四、参考评分

项目评分项	分值
公司证照齐全、合法有效。	一票否决
价格部分。	**30**
公司 2018 年后至今同类项目的业绩经验对比。	10
公司技术方案比较。	40
公司提供响应时间比较。	10
公司提供售后服务的内容 (包括质保期、维护保养方案、补充承诺等)比较。	10
合计	**100**