### 四、项目技术要求

1. 国密建设

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **产品** | **参数** | **数量** |
| 1 | 签名验签服务器 | 1、标准高度：2U；Intel Xeon Bronze 3206R@1.9GHz；内存： 32GB DDR4 ECC REG；硬盘：4TB SATA企业级硬盘 | 1 |
| 2、身份认证功能:实现基于数字证书的身份认证，支持不同CA的用户证书验证，提供多种验证证书有效性的方式。 |
| 3、数据签名功能:达到对各种类型电子数据的数字签名功能,满足多个格式的数字签名。 |
| 4、验证签名功能:达到对签名数据的验证功能,对签名的真实性与有效性进行验证。 |
| 5、系统备份功能:系统可以备份当前所有配置信息,保证系统瘫痪时的快速恢复。 |
| 6、日志管理功能:系统可以自己进行日志的记录,也可以把日志发送到指定服务器。 |
| 7、CRL连接配置：签名验签服务器应支持CRL连接配置功能，通过配置管理界面，提供从CRL发布点获取CRL、导入CRL等功能。 |
| 8、证书管理和验证功能：签名验签服务器应具有对应用实体证书、用户证书、根证书或证书链的导入、存储、验证、使用以及备份和恢复等功能。签名验签服务器管理的证书包括应用实体证书和用户证书。 |
| 9、访问控制功能：签名验签服务器的管理界面应具备完善的身份认证机制，通过智能密码钥匙、智能IC卡与口令相结合的方式实现管理员身份的认证。管理员登录成功后，通过管理界面进行初始化、应用管理、证书管理、系统配置以及日志查询等管理操作。 |
| 10、性能：SM2 Detach 签名≥750；RAS Detach 签名≥2500；SM2 Detach 验签≥1200；RAS Detach 验签≥800；SM2 Attach 签名≥750；RAS Attach 签名≥3000；SM2 Attach 验签≥1200；RAS Attach 验签≥750；RSA数字信封加密≥3000；RSA数字信封解密≥2500；SM2数字信封加密≥600；SM2数字信封解密≥700； |
| 11、产品遵循GM/T 0018-2012《密码设备应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》、GM/T 0029《签名验签服务器技术规范》及SM系列密码算法标准。 |
| 12、▲产品具备国家密码管理局颁发的商用密码产品认证证书（提供相关证明并加盖厂商公章） |
| 2 | 高性能密码机 | 1、标准高度2U，冗余电源，≥2个千兆电口，内存≥64G，配置960GB SSD固态盘，配置液晶屏显示服务状态面板和冗余电源； | 1 |
| 2、物理随机数的产生：采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的真随机数。 |
| 3、对称加解密：支持SM1、SM4对称密码算法和支持ECB、CBC、CFB、OFB运算模式。 |
| 4、消息鉴别码产生和验证：支持基于SM1、SM4算法的MAC产生及验证。 |
| 5、数据杂凑产生和验证：数据杂凑产生和验证。 |
| 6、数字签名的产生和验证：同时支持使用内部的密钥或外部导入密钥进行签名和验证。 |
| 7、非对称加解密：支持SM2加解密算法。 |
| 8、密钥体制：三层密钥管理体制，支持系统保护密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥三层结构。 |
| 9、密钥生成：支持产生RSA和SM2算法密钥对，支持产生SM1和SM4算法密钥。 |
| 10、密钥存储：设备内可静态存储SM2密钥对和SM1/SM4密钥。 |
| 11、密钥备份及恢复：支持以密文的形式将密钥备份导出；支持门限秘密共享机制确保备 |
| 12、份密钥的安全；支持将备份密钥恢复到同型号的密码机中。 |
| 13、密钥销毁：支持密钥的紧急销毁功能。 |
| 14、访问权限控制：基于管理员、操作员、审计员三种角色采用UKey作为身份凭证介质的访问控制，提高了密码设备自身的安全性。 |
| 15、设备管理：支持多台设备同时提供密码服务；支持双机热备功能，密码机故障时可自动切换；支持基于连接密码的客户端访问授权；支持基于IP地址的白名单访问控制。 |
| 16、日志管理：系统可以自行记录日志，方便系统维护和跟踪管理。 |
| 17、性能：SM1算法加解密速率≥1000Mbps；SM4算法加解密速率≥3000Mbps；SM2密钥对产生速率≥30000对/秒；SM2签名速率:75000次/秒；SM2验签速率≥24000次/秒；SM2加密速率≥18000次/秒；SM2解密速率:24000次/秒；SM3杂凑速率≥2800Mbps；SM2密钥对存储容量≥3500对；SM1/SM4密钥存储容量≥500个； |
| 18、产品遵循GM/T 0018-2012《密码设备应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》、GM/T 0030-2014《服务器密码机技术规范》及SM系列密码算法标准。 |
| 19、产品具备国家密码管理局颁发的商用密码产品认证证书（提供相关证明并加盖厂商公章） |
| 3 | 时间戳服务器 | 1、数字时间戳：支持对数据制作时间戳；支持验证时间戳结果 | 1 |
| 2、可信时间源：支持通过NTP时间服务器手动或自动同步系统时间，为用户提供精确的时间数据，实现系统时间的可信 |
| 3、支持多证书：实现基于数字证书的身份认证，支持不同CA的用户证书进行签发和验证时间戳 |
| 4、支持多平台：支持多平台、多开发语言调用，提供JAVA、COM、C等多种类型的接口函数 |
| 5、高安全性：基于高强度的双向身份认证，确保了管理者的合法身份 |
| 6、日志管理：提供数据库管理功能，可对时间戳业务数据、按策略留存和自动存档，方便用户检索查询，产品提供时间戳序列号、签发时间等检索方式 |
| 7、支持NTP/SNTP时间同步协议 |
| 8、PKI算法支持PKCS7/PKCS12/SM2/RSA；哈希算法支持SHAI/SM3 |
| 9、支持多样数据传入方式，可直接传入数据或传入数据存储的路径 |
| 10、性能：RSA签发效率：750TPS；RSA验证效率：1200TPS；SM2签发效率：3000TPS；SM2验证效率：1200TPS；授时精度：0.5-3ms；守时精度：＜1ms； |
| 11、产品遵循 GM/T 0033《时间戳接口规范》、GM/T 0028《密码模块安全技术要求》及SM系列密码算法标准。 |
| 12、▲产品具备国家密码管理局颁发的商用密码产品认证证书。（提供相关证明并加盖厂商公章） |
| 4 | PKI安全中间件 | （1）支持国家相关标准的数字证书及PKI/CA公钥体系；支持CSP协议，支持USBKEY介质数字证书读取；提供数字证书验证、根据证书验证、CRL验证功能； | 1 |
| （2）实现基于数字证书的数字签名和验签功能，支持PKCS#1、PKCS#7等数字签名格式，使用SM2非对称算法和SM4对称加密算法，支持SM3摘要算法，支持多人数字签名； |
| （3）使用RSA、SM2、SM3算法加密；支持SM4、DES、3DES、AES、RC4等对称加密；能够满足数据加密解密业务需求； |
| （4）数据编码：提供BASE64编码； |
| （5）二次开发接口：提供Java、Com、DLL等版本接口，支持JavaScript、Java、ASP.NET、VC、Delphi等多种开发语言； |
| （6）▲产品具备SM2安全中间件软件著作权登记证；（提供相关证明并加盖厂商公章） |
| 5 | 密钥管理系统 | 1、密钥管理系统由密钥生成、密钥管理、密钥库管理、用户权限管理、安全审计、密钥恢复和密码服务等核心组件组成，为证书认证中心提供加密证书密钥对相关服务。 | 1 |
| 2、提供了对生命周期内的加密证书密钥对进行全过程管理的功能。密钥过程主要包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管理等。 |
| 3、产品遵循国家密码管理局制定的GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》、GM/T 0051《密码设备管理对称密钥管理技术规范》。 |
| 4、产品具备国家密码管理局颁发的商用密码产品认证证书（提供相关证明并加盖厂商公章） |
| 6 | 国密浏览器(3年授权) | 1、提供客户端数字证书认证、加密通道建立和国密算法支持，支持国密算法SM2、SM3、SM4。在Chrome内核、IE内核下均支持国密SSL协议 | 10 |
| 2、产品具备国家密码管理局颁发的商用密码产品认证证书（提供相关证明） |
| 7 | USB key | 1、采用32位高性能智能卡芯片，存储容量≥64K； | 200 |
| 2、支持CSP及 PKCS#11，MS CSP, X.509 v3, SSL v3，PC/SC、ISO7816-1/2/3等接口标准; |
| 3、存储时间≥10年； |
| 4、可擦写次数≥100,000 次； |
| 5、支持国产SM密码算法数字证书； |
| 6、▲产品具备国家密码管理局颁发的商用密码产品认证证书（提供相关证明）并加盖厂商公章 |
| 8 | 数字证书(证书有效期一年) | 1. 依托《电子签名法》标识个人信息系统用户网络身份； | 200 |
| 2. 证书格式标准遵循ITU X.509 Version3标准； |
| 3. 数字证书应支持SM2等国产密码算法，数字签名算法支持RSA、SM2、SM3，摘要算法支持SHA-1，证书及私钥的存储格式采用国际标准的DER、PEM和PKCS#7、PKCS#12格式，证书请求支持PKCS#10格式； |
| 4. 支持自定义证书扩展域管理； |
| 5. ▲证书签发系统通过公安部信息安全等级三级认证并备案。（提供相关证明并加盖厂商公章） |
| 6. 服务响应：证书提供方提供7×24小时实时服务，对于系统在使用过程中出现的问题，在1小时内响应。 |
| 7、数字证书提供方应具有国家工业和信息化部颁发的、具有国家密码管理局颁发的《电子认证服务使用密码许可证》、具有国家密码管理局颁发的《电子政务电子认证服务机构》（提供相关证明并加盖厂商公章）； |
| 9 | SSL 证书 | 1、使用Https加密协议访问网站，可建立客户端浏览器到网站服务器之间SSL加密通道（SSL协议），实现加密传输，防止传输数据被泄露或篡改，确保信息在网上传输的安全。 | 4 |
| 2、▲证书签发系统通过公安部信息安全等级三级认证并备案。（提供相关证明） |
| 3、服务响应：证书提供方提供7×24小时实时服务，对于系统在使用过程中出现的问题，在1小时内响应 |
| 4、数字证书提供方应具有国家工业和信息化部颁发的、具有国家密码管理局颁发的《电子认证服务使用密码许可证》、具有国家密码管理局颁发的《电子政务电子认证服务机构》（提供相关证明）； |
| 10 | 方案设计 | 商用密码改造方案编写 | 两套 |
| 11 | 系统集成 | 承担项目的实施、业务系统改造、技术指导、咨询提供设计文件、技术资料 | 1次 |
| 12 | 院内产品升级 | 1、院内疗养系统完成国密建设升级 | 1次 |
| 2、院内检前问卷及检前预约系统系统完成国密建设升级 | 1次 |
| 3、院内餐饮预约系统系统完成国密建设升级 | 1次 |
|  |  |  |  |

1. 疗养一码通

|  |  |  |
| --- | --- | --- |
| **模块名称** | **功能** | **说明** |
| 统一认证 | 用户认证 | 用户认证平台帐号(支持多手机号认证)。 |
| 用户修改 | 用户修改个人信息。 |
| 主界面展示 | 根据用户角色显示用户可访问主界面。 |
| 身份认证 | 确认访问者身份，可以限制访问不同的业务平台。 |
| 一码通 | 展示 | 用户在院内任何需要扫码的地点展示个人二维码。 |
| 使用 | 任何业务扫码后，记录扫码时间及对应的业务，后续统计分析使用。并可根据配置限制使用等。 |
| 扫码付款 | 操作员登陆平台可以现场扫码收费,平台可根据业务提前传输过来的订单进行付款。 |
| 展示收款记录 | 可以人工查看当前使用二维码收款相关记录，总额等，便于确认端口数量，费用等数据。 |
| 登陆 | 验证权限、安全限制等。 |
| 标题维护 | 业务主界面显示标题。 |
| 通知维护 | 业务主界面显示通知。 |
| 认证修改通知 | 用户认证或修改个人信息时通知各业务系统。 |
| 一码通设置 | 可以设置院内一码通是否允许多次使用,定时更新时单等. |
| 追缴设置 | 是否允许经费消费欠费，以及用户扣费余额不足或者额度不足时通过其他方式完成支付，设置系统自动提醒周期，次数等。 |
| 个人年度消费限额 | 维护已有业务是否限额消费、限额度等。可以设置限额业务码，支持不同码(不同业务)之间不共用限额。 |
| 统计 | 用户统计 | 查询已认证用户，查询、显示、导出、打印等。 |
| 扣费统计 | 包括按业务类型，费用类型，结果类型统计等 |
| 欠费统计明细 | 用户在消费时，超过了指定额度，剩下的费用需要使用其他方式支付。这里可以查看还有多少欠费未支付。 |
| 二维码使用统计 | 查看二维码使用场所，针对使用较多场所可以重点维护，便于后续业务扩展。 |
| 二维码收款统计 | 可以查看指定日期内二维码收款的记录，确认数量，总费用等。 |
| 欠费追缴 | 追缴通知 | 按类型、时间段查出，扣费失败并且未完成支付记录，人工追缴，人工短信通知、电话通知，追缴完成等操作。 |
| 系统按配置定时查询扣费失败并且未完成支付记录，发送补缴短信通知。 |
| 自动追缴 | 系统在扣费时发现余额不足或者额度不足时直接发送补缴短信通知。 |
| 补缴方式 | 1.支持短信链接显示界面显示补缴余额等信息，直接点击补缴链接缴费，短信提示点击链接补缴及公众号内回复补缴方式。 |
| 2.院内公众号回复指定内容，系统显示补缴链接，点击缴费。 |
| 3.人工支持现场扫码缴费。 |
| 操作员 | 操作员维护 | 可使用后台的用户维护，增加、修改、删除、权限控制等。 |
| 操作记录 | 可以查看操作员对后台的操作记录,可跟踪业务数据变化情况. |
| 异常处理 | 短信通知 | 系统内所有发送短信明细查询、显示、导出，发送失败短信可以单独、批量重新发送。 |
| 业务调用 | 系统和第三方系统流转时异常数据展示，查询、显示、导出等。 |
| 内部异常 | 系统内部运行异常数据展示，查询、显示、导出等。 |
| 系统提供接口 | 短信发送 | 院内其他各子业务提供发送短信通知。 |
| 主界面展示 | 院内其他各子业务平台转回主界面展示。 |
| 用户识别 | 为各子业务平台提供当前用户是否是平台合法用户，根据配置返回用户认证时间等信息 |
| 信息通知 | 用户认证/修改信息时，可根据配置通知相应的平台。 |
| 余额查询 | 查询经费余额，可用额度等。 |
| 二维码验证 | 验证当前一码通所提供二维码的有效性、是否使用等 |
| 一码通使用 | 接收并记录当前一码通二维码使用场景。 |
| 费用查询 | 查询扣费、退费结果等 |
| 费用冻结 (预扣费) | 用户确定某个业务消费时，提前锁定用户金额。 |
| 取消冻结 (预扣费) | 用户确定消费某个业务后了用户金额，由于某种原因取消业务消费，取消冻结金额。 |
| 费用扣除 | 用户正式消费时正式扣除经费，并可根据实际情况发送短信提示等。支持额度限制，是否允许欠费等多种模式。 |
| 退费 | 用户正式消费后，由于某种原因退还用户费用，支持部分退款，同一订单允许多次退款等。 |
| 费用对帐 | 针对固定时间段核对正式消费或者冻结金额总额。 |
| 后台服务 | 短信发送 | 后台检查需要发送短信通知或者发送失败短信二次处理，时时将信息发出。 |
| 通知信息 | 用户认证/修改信息等根据配置需要通知其他平台的，第一次通知错误时，启用再次定时通知，最多通知三次。 |
| 余额同步 | 定时同步核对人员费用信息,确认数据准备。 |
| 异常处理 | 后台定时检测异常、恢复等其他业务服务。 |
| 国密标准 | 疗养平台有及体检预约平台 | ▲具有国家密码管理局授权的商用密码产品认证证书 |
| ▲满足符合国密标准的身份鉴别。 |
| ▲重要数据机密，安全性，修改时需要使用符合国密标准的CA认证。 |
| ▲重要数据机密，安全性，需要使用国密标准SM2加密存储。 |
| ▲网络和通信通道需要使用国密标准SSL加密 |
| ▲需要提供符合国密标准授权浏览器 |
| 其他 | 数据兼容 | 平台上线后要兼容院内历史数据。 |
| 疗养接口 | 与院内疗养平台完成接口对接。 |
| 问卷接口 | 与院内检查问卷完成接口对接。 |
| 餐饮预约 | 与院内餐饮预约完成接口对接。 |
| 其他 | 与院内现有其他业务完成接口对接。 |

1. 交付

|  |  |
| --- | --- |
| 1、▲提供与院内疗养系统对接证明，确保整个项目顺利交付完成。 | |
| 2、▲提供与院内检前问卷系统对接证明，确保整个项目顺利交付完成。 | |
| 3、▲提供与院餐饮预约系统对接证明，确保整个项目顺利交付完成。 | |
| 4、▲提供与院内无人超市系统对接证明，确保整个项目顺利交付完成。 | |
| 5、系统部署 | 云服务器 |
| CentOS系统 |
| 国产数据库 |
| 6、项目整体建设要符合国密二级标准，通过第三方审核，完成密码局备案工作 | |

### 五、项目商务要求

（一）服务期限：

（1）甲方支付完首付款30工作日内要启动调研、开发、部署工作。

（2）项目总工期为8个月，以支付首付款日期开始计算。

（3）项目当中如遇延期或者其他可能影响项目进展的事情，需向甲方书面说明。

（二）付款方式：以合同签订为准

（三）质量考核验收标准及违约金

1.质量考核验收标准：项目最终验收以系统通过国密第三方测评机构评审，报告送至市密码局，并收到备案回执为最终目标。

（四）免费保修期

1.质保期五年，质保期从设备完成验收并签署验收报告之日起开始计算质保期。保修期内，中标人免费维护，对易损耗材，配件等损坏，中标人只收取零部件的成本费，不收人工服务费用。无论在保修期（维护期）内或保修期（维护期）外，法定工作时间内均提供终身售后服务。

2. 项目验收以后免费维护一年，后续维护费不超过总价10%

（五）售后运维服务能力

（1）为保证售后到位及时，要求投标人在本地有售后服务机构；

（2）技术支持：提供7×24小时的服务热线，随时接收故障的反馈和申报；

（3）根据项目需求设立产品培训计划。

### 六、投标报价

1.本项目服务费采用包干制，应包括服务成本、法定税费和企业的利润。由企业根据招标文件所提供的资料自行测算投标报价；一经中标，投标报价总价作为中标单位与采购人签定的合同金额，合同期限内不做调整。

2.投标人应根据本企业的成本自行决定报价，但不得以低于其企业成本的报价投标；评标时，评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.投标人的投标报价，应是本项目招标范围和招标文件及合同条款上所列的各项内容中所述的全部，不得以任何理由予以重复，并以投标人在投标文件中提出的综合单价或总价为依据。

4.除非政府集中采购机构通过修改招标文件予以更正，否则，投标人应毫无例外地按招标文件所列的清单中项目和数量填报综合单价或总价。投标人未填综合单价或总价的项目，在实施后，将不得以支付，并视作该项费用已包括在其它有价款的综合单价或总价内。

5.投标人应充分了解项目的位置、情况、道路及任何其它足以影响投标报价的情况，任何因忽视或误解项目情况而导致的索赔或服务期限延长申请将不获批准。

6.投标人不得期望通过索赔等方式获取补偿，否则，除可能遭到拒绝外，还可能将被作为不良行为记录在案，并可能影响其以后参加政府采购的项目投标。各投标人在投标报价时，应充分考虑投标报价的风险。