**东华大学一网通办电子签章平台采购**

**一、项目建设内容**

（1） 建设校级电子签章平台，应用电子签名、电子签章和电子认证技术措施确保业务系统中重要业务数据的真实性和完整性，确立符合法律要求的责任认定和抗抵赖机制。

（2） 针对校办及各行政部门、教学单位及科研教辅单位各个业务部门生成的多种电子凭证，提供电子签章及CA认证。

（3） 依托电子签名技术，生成可信电子服务凭证。

（4） 基于公安人口库，实时、在线核验新生身份。与高校微信企业号或高校校园APP结合，实现远程报到时，身份核验的应用。

**二、采购产品一览表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 单位 | 数量 | 质保期 |
| 1 | 可信电子签章密码应用支撑平台 | 套 | 1 | 1年 |
| 2 | 单位数字证书（国产算法） | 张 | 1 | 1年 |
| 3 | 时间戳数字证书（国产算法） | 张 | 1 | 1年 |
| 4 | Adobe单位证书（国际算法） | 张 | 1 | 1年 |
| 5 | Adobe时间戳证书（国际算法） | 张 | 1 | 1年 |
| 6 | 云签名认证网关 | 套 | 1 | 1年 |
| 7 | 校内个人签名用户数 | 个 | 1000 | 1年 |
| 8 | 个人事件型证书服务 | 1万次 | 1 | 1年 |
| 9 | 与教育部权威机构（学信网）验证平台对接服务 | 项 | 1 |  |
| 10 | 产品维保服务 | 年 | 1 | 1年 |
| 11 | 系统集成服务 | 项 | 1 |  |

**三、主要产品指标要求和实施方案**

**“*斜体加粗下划线*”内容代表最关键指标，不满足该指标项则为无效投标**，**▲**代表重要指标，无标识则表示一般指标项。

**1、电子签章系统（软硬一体设备）**

|  |  |
| --- | --- |
| 1 | 主要用途：专用密码设备，底层依托密钥管理与密码计算能力，向各类校级业务系统提供数据指纹提取、PDF签章、时间戳等服务，支持校级各类系统的电子签章功能的实现和应用。 |
| 2 | 技术要求：密码应用支撑平台主要用来实现与密码相关的各种运算和配置管理，包括密钥管理、证书管理、电子签章及验证、时间源管理、时间戳签发及验证等功能，支持校内各类系统功能的实现和应用。设备应具备可扩展性，支持集群部署。 |
| 3 | 证书管理：需要包括证书信任链管理、签名服务器证书管理等，遵循PKCS公钥密码学标准及X509 v3证书国际标准。 |
| 4 | 签名密钥管理：支持RSA、SM2等签名算法的签名密钥管理。 |
| 5 | 电子签章/验证：对文档提供电子签章及验证功能。 |
| 6 | **▲**安全二维码：能够在文档中加入安全二维码，安全二维码实现在QR二维码中加入数字签名。安全二维码技术具有自主知识产权**（需提供实质性证明文件，包含软件著作权证书或专利证明）。** |
| 7 | **▲**PDF骑缝章签章服务：支持对PDF文档进行骑缝章签章功能，支持左右骑缝、签章位置比例分配设定功能，支持骑缝章首页签名或每页签名，并可设置文档安全控制。 |
| 8 | **▲**签章规则管理：对PDF签章制定相关的规则与标准，支持关键字定位与坐标定位，可以根据自身业务特点设置个性化签章规则，并且基于该规则进行PDF查看预览，同时可设置对签章后的文档进行安全保护。 |
| 9 | 权威时间同步：基于SNTP协议，从指定时间源设备获取标准时间并同步。 |
| 10 | **▲**PDF文档安全控制：支持对签章后的PDF文档进行安全控制，包括无限制、仅允许复制、仅允许打印、仅允许复制和打印、全部禁止。 |
| 11 | **▲**权威国家时间源：内置国家授时中心时间源。 |
| 12 | 签发/验证时间戳：签发可信时间戳、验证时间戳有效性。 |
| 13 | 系统备份与恢复：系统支持备份当前系统所有的配置，保证系统瘫痪时快速恢复。 |
| 14 | 审计日志：系统能够对管理员的操作日志进行记录和审计。 |
| 15 | 三权分立：系统支持初始化成系统管理员、安全管理员和审计管理员三权分立模式。 |
| 16 | 高可用性：支持双机并行、负载均衡。 |
| 17 | 设备高度：2U； |
| 18 | 网络接口：100/1000M自适应网口\*2； |
| 19 | 电源指标：冗余电源； |
| 20 | 应用平台：支持Windows Server、Linux、AIX等应用平台； |
| 21 | 应用接口：支持Java、COM、C等； |
| 22 | 算法标准：支持SM2、SM3、RSA、SHA256等。 |
| 23 | 签章性能：千兆网络环境下，签发200K PDF文件效率不小于280次/秒。 |
| 24 | **▲**产品资质：电子签章系统同时具有《商用密码产品认证证书》、《公安部检测报告》、《信息技术产品安全测试证书》、《软件著作权登记证书》 |

**2、学校单位数字证书(国产算法+国际算法)**

|  |  |
| --- | --- |
| 1 | 主要用途：代表签发单位的网上真实身份。使用该证书进行的电子签章能在国内外范围被广泛认可和验证。 |
| 2 | 用于标识签发单位的网上真实身份。 |
| 3 | 数字证书采用SM2/RSA算法签发。 |
| 4 | 证书格式遵循x．509v3标准。 |

**3、时间戳数字证书 （国产算法+国际算法）**

|  |  |
| --- | --- |
| 1 | 主要用途：由合法第三方电子认证服务机构颁发的数字证书，基于标准时间源，为应用系统提供精准、安全和可信的时间认证服务。使用该证书进行的电子签章能在国内外范围被广泛认可和验证。 |
| 2 | 采用先进精准的时间源和时间同步技术保证时间的真实可靠。 |
| 3 | 数字证书采用SM2/RSA算法签发。 |
| 4 | 证书格式遵循x．509v3标准。 |

**4、云签名认证网关**

|  |  |
| --- | --- |
| 1 | 支持用户通过云签名认证网关注册，并为用户申请签发数字证书 |
| 2 | 为应用提供认证服务接口，提供基于数字证书的身份认证方式 |
| 3 | 提供数据签名服务接口，把业务系统签名请求安全提交到云签名服务端与用户手机完成协同签名 |
| 4 | 可验证PKCS1/PKCS7标准格式的电子签名，基于标准PKI验证过程，包括签名验证、证书有效性验证等 |
| 5 | 提供用户注册服务接口、登录认证服务接口、数据和文档签名接口，提供业务系统通过JAVA SDK接口集成 |

**5、移动端APP/SDK**

|  |  |
| --- | --- |
| 1 | 支持主流的手机终端设备，android 4.2以上，IOS 8以上 |
| 2 | 支持用户在线完成注册和服务激活功能 |
| 3 | 支持用户使用手机APP完成基于实名证书的身份认证功能，包含APP登录认证与扫描二维码登录认证。 |
| 4 | **▲**支持用户使用手机APP完成基于实名证书电子签名，包括对数据的电子签名和扫描二维码方式形成电子签名。 |
| 5 | **▲**支持用户通过APP定制独有手写笔迹，用于电子签章。 |
| 6 | 用户基于同一实名身份，可以使用多台客户端设备进行认证签名，APP提供管理功能，用户可删除多余的设备。 |
| 7 | 能够有效防止证书被盗用、暴力猜测PIN口令；采取密钥分割方式，分别在手机和云端加密保存，每次的认证及电子签名需要用户、手机客户端、业务系统、个人签名服务共同参与完成。 |
| 8 | 客户端支持用户使用签名口令方式、指纹验证方式进行用户认证 |

**6、个人云签名服务**

|  |  |
| --- | --- |
| 1 | 主要用途：面向个人用户，通过云服务模式实现认证、数字签名、签章等服务，含个人证书服务。 |
| 2 | 签发数字证书前应对用户进行有效身份鉴证，确保网络身份与真实身份一致，鉴证强度应不低于用户姓名、身份证号信息对比鉴证。 |
| 3 | 密码运算服务：支持SM1、SM2、SM3、SM4等国产算法，RSA等国际算法的运算。 |
| 4 | 身份认证服务：提供通过验证数字签名进行身份认证的服务。 |
| 5 | 证书验证服务：支持数字证书有效性验证，包括完整的证书链以及证书有效期。 |
| 6 | **▲**密钥管理服务：支持密钥由移动终端和云服务平台协商产生，各产生一部分，实现异地分体安全存储。 |
| 7 | 提供密钥生成、存储、销毁、归档、统计产销等功能。 |
| 8 | 用户管理服务：提供用户注册功能，支持短信通知激活方式。 |
| 9 | 支持个人用户和企业用户等多种用户身份。 |
| 10 | 账户管理服务：提供注册云服务账户功能，支持批量、单个用户注册，注册后为用户生成唯一标识码。 |
| 11 | 提供账户状态管理功能，包括：冻结、解冻、注销、更换手机号等操作。 |
| 12 | 运营安全性：提供7\*24小时服务，保证系统不间断运营。 |
| 13 | 密钥安全性：支持用户密钥分割，分别在手机和云服务平台加密保存，在用户未参与情况下，云服务平台无法单独操作密钥。 |
| 14 | 在协同签名的过程中，分别在移动终端和云服务平台进行，移动终端和云服务平台均不能有完整密钥出现。 |
| 15 | 签发数字证书前应对用户进行有效身份鉴证，确保网络身份与真实身份一致，鉴证强度应不低于用户姓名、身份证号信息对比鉴证。 |

**7、身份核验服务**

|  |  |
| --- | --- |
| 1 | 主要用途：面向个人用户，通过云服务模式实现个人身份核验服务。 |
| 2 | ▲与公安部门、银联、电信运营商等多家可信认证源深度合作，保障数据准确齐全。 |
| 3 | 身份核验服务仅采集核验模式所需的个人信息，符合《信息安全技术个人信息安全规范》、《中华人民共和国个人信息保护法》中的个人信息安全基本原则。 |
| 4 | 提供纯云端 API、H5 及移动端 SDK 等多种接入方式，满足客户在不同场景下的身份核验需求。 |
| 5 | 支持APP和H5应用接入。 |
| 6 | 支持手机机主与个人身份一致性核实。 |
| 7 | 支持活体检测或者人像比对的方式核实。 |
| 8 | 支持身份核验完成后进行个人签章。 |
| 9 | 运营安全性：具备 7\*24 小时的系统运维能力，具备完善的故障监控、自动告警、快速定位、快速恢复等一系列故障应急响应机制，有效保障身份核验服务的正常运行。 |

**8、与学信网对接服务**

|  |  |
| --- | --- |
| 1 | **▲**主要用途：实现与教育部权威机构（学信网成绩单验证平台）对接。 |

**9、产品维保服务：1年**

|  |  |
| --- | --- |
| 1 | 主要用途：提供软硬件1年质保，单位证书、时间戳证书等共4张证书1年的免费售后服务。质保期内所有投标软硬件的升级、维护均免费（除人为损坏、自然灾害情况外）。服务商应明确质保期后的售后服务内容和收费标准。 |

**10、系统集成服务：1项**

|  |  |
| --- | --- |
| 1 | 主要用途：配合及支持我校完成学校业务系统与可信电子签章服务系统集成，实现数据对接以及可信电子凭证、重要文件可信化处理等的应用；考虑到后续的信息化建设，能支持对接自助打印终端。 |
| 2 | 服务商应将可信电子签章系统、数字证书等部署到用户指定地点。 |