**湖北省政府采购电子交易数据交换汇聚平台**

**UsbKey厂家对接规范**

**湖北省财政厅政府采购管理处**

**2023年3月**

**目录**

[1. 范围 1](#_Toc129858069)

[2. 规范性引用文件 1](#_Toc129858070)

[3. 对接准备 1](#_Toc129858071)

[3.1. 对接主体 1](#_Toc129858072)

[3.2. 对接材料清单 2](#_Toc129858073)

[4. 数字证书及电子印章技术要求 3](#_Toc129858074)

[4.1. 介质集成技术要求 3](#_Toc129858075)

[4.1.1. 技术要求清单 3](#_Toc129858076)

[4.1.2. 密码服务接口 4](#_Toc129858077)

[4.2. 数字证书技术要求 4](#_Toc129858078)

[4.2.1. 技术要求清单 4](#_Toc129858079)

[4.2.2. 证书扩展域及其数据结构 4](#_Toc129858080)

[4.3. 电子印章技术要求 5](#_Toc129858081)

[4.3.1. 技术要求清单 5](#_Toc129858082)

[4.3.2. 电子印章接口技术要求 5](#_Toc129858083)

[4.3.3. 电子印章数据格式 5](#_Toc129858084)

[附件1 湖北省政府采购数据交换汇聚平台UsbKey对接调试申请表 6](#_Toc129858085)

# 范围

本标准规范用于湖北省政府采购数据交换汇聚平台Usbkey厂商对接。

# 规范性引用文件

以下文件的相关条款通过引用而成为本规范的内容。凡是加注日期的引用文件，其随后所有的修改或修订版（勘误的内容除外）均不适用于本规范，但鼓励根据本规范达成协议的各方经协商一致适用以下文件的修订版本。凡是未加注日期的引用文件，其修订版本应自动适用于本规范。

GM/T 0002 SM4分组密码算法

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

GM/T 0009 SM2密码算法使用规范

GM/T 0015 基于SM2密码算法的数字证书格式规范

GM/T 0016智能密码钥匙密码应用接口规范

GM/T 0027 智能密码钥匙技术规范

GB/T 20518信息安全技术 公钥基础设施 数字证书格式

GB/T 38540-2020 信息安全技术 安全电子印章密码技术规范

# 对接准备

## 对接主体

用于电子化招投标的UsbKey一般由介质、CA证书和电子印章组成，介质、CA证书和电子印章有可能是不同的厂商。为了对接时沟通方便，同时在对接之后由固定的厂商向UsbKey用户提供客服服务。要求UsbKey只能由一个厂商成为总集成方申请对接。

## 对接材料清单

UsbKey厂商在对接调试之前需要提供以下材料：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **材料名称** | **数量** | **说明** |
|  | 对接调试申请表 | 1 | 格式见[附件1](一张网#_附件1 湖北省政府采购) |
|  | CA证书链、CA根证书、LDAP目录服务系统和OCSP证书在线状态查询 | 1 | 1.提供CA机构的证书链、根证书；  2.提供CRL列表发布LDAP地址、WEB验证地址；  3.提供证书在线状态查询OCSP地址(及demo和相关状态码表)。 |
|  | 数字证书主题规则解析策略 | 1 | 1.证书主题规则或扩展项说明；  2.一个单位多个USBKey数字证书主题规则说明；  3.数字证书必须包含用户实体的唯一标识（个人用户：身份证号码；法人用户：统一社会信用代码），方便进行证书用户身份识别（注：标识OID不符合GB/T 20518要求，需说明规则）。 |
|  | USBKey数字证书 | 1 | USBKey数字证书（含电子印章）  需提供至少3套（每套6枚）用于测试验证。  每套包含如下：   1. 包含公章3枚（机构证书）、3枚法人\个人证书； 2. 其中2枚机构证书分别灌制对应机构名称测试印章，1枚法人\个人证书灌制个人姓名测试印章（包含名字方章和手写签字章），具体测试印章名称在制作前由项目组提供。 3. UKEY中的数字证书需要包含签名证书和加密证书 |
|  | USBKey驱动程序 | 1 | 智能密码钥匙可视化工具。 |
|  | JAR包 | 1 | 对符合国密SKF的UKEY动态链接库(动态库需符合GM/T 0016-2012)在封装的JAR包（含API接口文档及demo） |
|  | 商用密码产品认证证书 | 1 | 智能密码钥匙、电子印章获得国家密码管理部门颁发的商用密码产品认证证书，提供资质证书。 |

# 数字证书及电子印章技术要求

## 介质集成技术要求

### 技术要求清单

|  |  |
| --- | --- |
| **功能项** | **功能描述** |
| 功能要求 | **JAR包：**   * CA厂商需提供.jar包及其依赖的包（访问共享库资源的jna包建议使用3.3.0版本） * jar包的命名应当能够明确的表明自身的使用身份、己方完整厂商名称等信息。jar包格式：“UKEY\_介质厂商名称.jar”。命名示例：UKEY\_xxKey.jar。 * jar包是对动态依赖库“.dll”和“.so”的在封装（动态依赖库需符合GM/T 0016-2012），jar包中的接口名称、参数传入顺序需和动态链接库保持一致，同时保持对32位/64位系统和信创环境的支持。 * .dll”和“.so”动态链接库需符合C99标准形式，同时支持多进程调用。 * jar包需要对Wintel运行环境及信创运行环境进行支持。 * jar包API接口详细说明需要提供（注：“SKF\_ECCPrvKeyDecrypt”接口需要提供）。 * Jar包中的API实现请按照附件进行： * 为提高整合效率需提供对JAR包中的接口调用案例 |
| **设备管理：**   * 智能密码钥匙应支持设备管理功能，如：设备认证密钥的更新、PIN校验、解锁等。 * 设备管理相关要求符合GM/T 0027 智能密码钥匙技术规范。 |
| 功能要求 | **密码运算**：   * 智能密码钥匙支持SM4分组密码算法，并符合GM/T 0002的要求；(至少支持ECB、CBC模式） * 智能密码钥匙支持SM2公钥密码算法，并符合GM/T 0003的要求;智能密码钥匙支持SM3密码杂凑算法，并符合GM/T 0004的要求； * 智能密码钥匙对消息鉴别码的处理应符合GM/T 0017 的要求。 |
| **容器管理：**   * 出厂的智能密码钥匙可包含一个或多个容器。如包含多个容器，需提供可通过接口读取有效容器名称； * 数字证书（单证或双证）都需存放在同个容器内； * CA厂商在USBKey证书制作签发过程中应杜绝空容器的情况。 |
| 硬件要求 | * 智能密码钥匙的硬件接口需支持USB接口； * 智能密码钥匙的核心芯片需经过国家密码管理部门的审批； * 智能密码钥匙硬件的相关要求符合GM/T 0027智能密码钥匙技术规范的要求。 |

### 密码服务接口

密码服务接口函数提供对称算法运算、非对称算法运算、密码杂凑算法运算、密钥管理、消息鉴别码计算等功能。密码服务接口应符合GM/T 0016要求。

## 数字证书技术要求

### 技术要求清单

|  |  |
| --- | --- |
| **功能项** | **功能描述** |
| 证书延期 | 证书续期后的加密CA证书的公钥和私钥与原加密CA证书应保持一致,不允许发生变化，以满足对加解密业务的持续支持能力 |

### 证书扩展域及其数据结构

证书扩展域及其数据结构应符合《GB/T 20518 信息安全技术 公钥基础设施 数字证书格式》要求。

基于上述要求，结合实际业务，本标准将部分扩展项标记为关键性扩展，要求如下：

1. 个人身份标识码，当证件号码中有中文字符时，请采用UTF8编码。
2. 企业组织机构代码，为标识企业身份，主要存放“统一社会信用代码”，因其可以代替税务登记证、企业营业执照、组织机构代码证，当证件号码中有中文字符时，请采用UTF8编码。

## 电子印章技术要求

### 技术要求清单

|  |  |
| --- | --- |
| 功能项 | 功能描述 |
| 软件功能要求 | 电子印章厂商提供的电子印章数据结构体，协同“湖北政采证书签章助手”的电子印章功能模块，在PDF/OFD/HTML5等电子文档上进行电子签章； |
| 印章结构体要求 | 电子印章数据结构符合《GB/T 38540-2020 信息安全技术 安全电子印章密码技术规范》中“6.1数据格式”章节规定。  注：自定义数据属性，需根据实际项目需求增加信息。 |

### 电子印章接口技术要求

获取印章接口若需先通过证书PIN码验证，需要在API文档接口中说明。

企业圆章建议尺寸42\*42mm，个人方章建议尺寸20\*20mm。

### 电子印章数据格式

电子印章数据符合《GB/T 38540 信息安全技术 安全电子印章密码技术规范》要求；

电子印章中所有的字段除可选项外全部不能为空，须赋值；

基于上述要求，结合实际业务，自定义数据信息需增加关键扩展字段标识（如下）:

|  |  |
| --- | --- |
| **extnID** | **说明** |
| 1.2.156.xxxxx.7.1 | extnID中的xxxxx为系统ID编号，如湖北省政府采购一体化的系统在某厂家的编号是234324，某厂家发的UK **extnID**就可以是 1.2.156.234324.7.1 |