# 组成架构体系设计

## 背景

因自研需要ca服务，且运营ca收费较高，故有此极简版自建ca，不采用安全设备，仅用于实验室级别的测试使用。

## 范围

自研项目的实验室级别测试使用，所颁发的证书都不含证书颁发机构的详细信息。

## 组成

### RA

提供用户和CA之间的业务接口，包括但不限于 注册申请信息、变更、延期、撤销的功能

### CA

证书制作颁发、变更、延期、撤销、吊销列表的生命周期管理

### KM

密钥管理中心，即保证密钥产生过程、传输、认证安全的系统，实际应在专门机构管理下（密码局）；本简易系统采用模拟方式，应严格限制其应用范围。

### pps

发布系统用于发布证书信息，提供证书下载、吊销列表查询和下载的功能。本简易系统仅提供证书下载，不提供查询。

### 目录服务器

为证书的存储服务器，与ca和pps相关。本简易系统不作要求。

## 内容

## 界面

见原型图

### 功能

#### API用户

ra角色，提供注册在本系统的用户，采用每次请求都认证的单向认证方式。

认证信息包括： 租户编号、项目编号、单次token（rndA + rndB + uPin）enc，加密方式由项目编号决定

本简易系统均采用同步方式返回数据，实际业务可视情况增加异步。

注册申请

变更

延期

撤销

#### 口令用户

##### 管理员

用户管理：注册、修改、冻结、解冻、注销

证书统计：已注册、变更、延期、注销

##### 操作员

各类委办操作：根据线下申请，代理证书的各类申请操作

注册申请

变更

延期

撤销

下载：证书、吊销列表

## 数据库设计

口令用户表

user\_info

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| uid | 账号 | String |  |
| uname | 账号名 | String |  |
| pin | 口令 | String |  |
| utype | 用户类型 | int | 0-管理员；1-操作员 |
| RD\_TIME | 记录时间 | datetime |  |
|  |  |  |  |

接口用户表（租户表）

rent\_info

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| uid | 租户账号 | String |  |
| uname | 账号名 | String |  |
| pin | 租户口令 | String |  |
| RD\_TIME | 记录时间 | datetime |  |
| LIM\_TIME | 有效截止时间 | datetime |  |
|  |  |  |  |

租户项目表

rent\_proj\_rd

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| uid | 租户账号 | String |  |
| prj\_id | 项目编号 | String |  |
| algType | 算法类型 | String | rsa1024、 rsa2048、sm2 |
| authType | 请求参数认证类型 | String | sha1、sha256、sm2\_sign |
| authPuk | 认证用参数/公钥 | String |  |
| RD\_TIME | 记录时间 | datetime |  |
|  |  |  |  |

证书申请信息表

req\_data\_rnd

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| uid | 租户账号 | String |  |
| req\_data | 申请数据 | mediumBlob | 申请数据 |
| biz\_type | 申请类型 | int | 0-查询、1-注册、2-变更、3-延期、4-注销 |
| cer\_type | 证书类型 | int | 0-个人， 1-单位， 2-机构 |
| req\_id | 记录编号 | String | uuid |
| code | 任务执行结果 | String | 0-完成， 非0-失败 |
| err\_msg | 执行失败时的错误信息 | String |  |
| RD\_TIME | 记录时间 | datetime |  |

证书记录表

cert\_rnd

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| serial\_number | 序列号 | String | 证书序列号 |
| cert\_type | 证书类型 | int | 0-个人， 1-单位， 2-机构 |
| algType | 算法 | String | rsa1024、 rsa2048、sm2 |
| dn | 主题 | String | {cn=xxx,o=xxx,s=xx,c=cn} |
| valid\_st | 有效期起 | datetime |  |
| valid\_end | 有效期止 | datetime |  |
| cer\_data | 证书数据 | mediumBlob |  |
| RD\_TIME | 记录时间 | datetime |  |
| status | 状态 | int | 0-正常， 1-冻结， 2-注销 |
| pre\_serial | 序列号-变延前 | String | 进行变更和延期，原证书将被注销，此处记录变更或延期前的证书序列号，用于关联顺序 |

双证表

cert\_db\_rel

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| uuid | 记录编号 | String | uuid |
| sign\_serial | 签名证书序列号 | String |  |
| enc\_serial | 加密证书序列号 | String |  |
| prt\_alg | 主题 | String | rsa1024、 rsa2048、sm2 |
| epk\_prt\_data | 加密密钥保护结构密文数据 | mediumBlob | 根据算法进行的加密密钥保护结构数据 |
| RD\_TIME | 记录时间 | datetime |  |
|  |  |  |  |

吊销列表

cert\_revoke\_rnd

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 含义 | 类型 | 注释 |
| ID | id | int | pri |
| serial\_number | 证书序列号 | String |  |
| pre\_sts | 吊销前证书状态 | int | 1. 1 |
| rev\_msg | 吊销原因 | String | 变更、延期、注销 |
| rev\_date | 吊销日期 | date | 存在申请时间晚于吊销日期的情况，故设此 |
| rd\_time | 记录时间 | datetime |  |
|  |  |  |  |

## api接口参数设计

### 获取token

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| rentId | String | 是 | 租户编号 |
| projId | String | 是 | 项目编号 |
| rndA | String | 是 | 随机数rndA |
|  |  |  |  |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |
| data | String | 否 | 返回数据： 随机数rndB |
|  |  |  |  |

### 业务请求

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| token | String | 是 | 一次token：由租户信息、随机数A和B运算所得，具有一次性和时效性。 |
| data | String | 是 | 请求数据、待签名数据, base64字符串 |
| signValue | String | 是 | 签名值的base64字符串 |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |
| data | String | 否 | 返回数据，当失败时，可没有此项 |
|  |  |  |  |

data数据项详解

#### 注册申请业务

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| taskCode | String | 是 | applyCert |
| reqType | int | 是 | 0:p10, 1: dn+pubkey |
| certType | int | 是 | 0:个人， 1-单位， 2-机构 |
| body | String | 是 | 取决于reqType, 0: csr的base64字符串，1：为 {“dn”:””, “pk”:””}的json字符串的utf-8编码的base64字符串 |

示例

|  |  |
| --- | --- |
| {  ”reqType”: 0,  “certType”: 0,  “body”: “xxxxxxxxxxxxx”  } | |
| p10 | body = base64(p10) |
| dn + pukey | body = base64(  {  “dn”: “”,  “pk”: “”  }  ) – utf-8 |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |
| data | String | 否 | 返回数据 |
|  |  |  |  |

data的示例

|  |
| --- |
| {  ”signCert”: “”,  “encCert”: “”,  “ekpStr”: “xxxxxxxxxxxxx”  } |

#### 变更申请业务

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| taskCode | String | 是 | modifyCert |
| certType | int | 是 | 0:个人， 1-单位， 2-机构 |
| serialNumber | String | 是 | 证书序列号 |
| dn | String | 是 | cn=xx,o=xx,s=xx,c=cn的utf-8的base64 |

注：变更时证书类型，证书有效期不得修改。变更后开始有效期为申请时间，结束有效期为原证书的结束有效期，不顺延。

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |
| data | String | 否 | 变更后的证书Base64编码字符 |
|  |  |  |  |

注：目前仅进行单证书变更，即签名证书和加密证书不同时变更

#### 延期申请业务

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| taskCode | String | 是 | delayCert |
| certType | int | 是 | 0:个人， 1-单位， 2-机构 |
| serialNumber | String | 是 | 证书序列号 |

注： 延期仅改变有效期，其它如 证书类型，证书主题不发生变化。新证书的开始有效期为申请时间，结束有效期为自申请时间起延后一年。

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |
| data | String | 否 | 变更后的证书Base64编码字符 |
|  |  |  |  |

注：目前仅进行单证书延期，即签名证书和加密证书不同时延期。

#### 撤销申请业务

请求参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| taskCode | String | 是 | delayCert |
| certType | int | 是 | 0:个人， 1-单位， 2-机构 |
| serialNumber | String | 是 | 证书序列号 |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 | 类型 | 是否必须 | 描述 |
| code | String | 是 | 结果码 |
| msg | String | 是 | 结果描述 |

注：正常和冻结状态的证书可以撤销，已撤销的证书不再重复撤销，code仍为0，msg中会告知“已经撤销过，无需重复操作”。