**公私钥加密js1.0接口**

文档历史

|  |  |  |  |
| --- | --- | --- | --- |
| 修订日期 | 修订内容 | 修订版本 | 修订人 |
| 2017/12/7 | 独立的js1.0版本 | 1.0.0.0 | 时昌雪 |

目录

[1. 设计目的 1](#_Toc500433273)

[2. 前提条件 2](#_Toc500433274)

[3. 变更点 2](#_Toc500433275)

[4. 控件脚本SDK接口定义 2](#_Toc500433276)

[4.1. 方法 2](#_Toc500433277)

[4.1.1. 生成公钥和私钥 2](#_Toc500433278)

[4.1.2. 私钥加密函数 2](#_Toc500433279)

[4.1.3. 公钥解密函数 3](#_Toc500433280)

[4.1.4. 公钥加密函数 3](#_Toc500433281)

[4.1.5. 私钥解密函数 3](#_Toc500433282)

[4.1.6. 私钥签名函数 3](#_Toc500433283)

[4.1.7. 公钥验证函数 4](#_Toc500433284)

[4.1.8. P10文件生成函数 4](#_Toc500433285)

# 设计目的

实现一个js文件，统一封装和调用RSA公私钥的加密算法和签名算法，以及P10文件的生成，便于第三方调用和应用接入。

# 前提条件

1. Windows XP版本以上操作系统.
2. 32位的IE、Chrome、FireFox及部分使用这3种内核的浏览器，确保浏览器为正常设
3. 配置nodejs环境，使用npm安装"encoding": "^0.1.12", "ursa": "^0.9.4", "underscore": "1.4.x", "underscore.string": "2.3.x"依赖包.
4. 首先调用PKI( )函数，生成公私钥文件，之后调用签名等函数

# 变更点

暂无变更点

# 控件脚本SDK接口定义

## 方法

### 生成公钥和私钥

PKI();

参数：

无；

说明：

该函数调用此函数，公私钥文件会直接生成在根目录下，私钥命名为client\_private.key，公钥命名为client\_public.pub。

### 私钥加密函数

priEncrypt(string plain)；

参数：

string plain；

默认值为‘fenyukejiyouxiangongsi’；

返回值：

加密之后的密文。

说明：

对输入的字符串进行加密，例如PFD文件的数字指纹。

### 公钥解密函数

pubDecrypt(cipher);

参数：

cipher;

私钥加密的密文

返回值：

解密后的明文。

说明：

将私钥加密的密文作为参数传入，得到明文。

### 公钥加密函数

pubEncrypt（string plain）；

参数：

string plain；

默认值为‘fenyukejiyouxiangongsi’’；

返回值：

加密之后的密文。

说明：

对输入的字符串进行加密，例如PFD文件的数字指纹。

### 私钥解密函数

priDecrypt(cipher);

参数：

cipher;

公钥加密的密文

返回值：

解密后的明文。

说明：

将私钥加密的密文作为参数传入，得到明文。

### 私钥签名函数

sign(string plain);

参数：

plain;

需要签名的字符串。

默认参数：‘fenyukejiyouxiangongsi’’

返回值：

签名值

说明：

将字符串作为参数传入，得到签名之后的值。

### 公钥验证函数

verify(string plain);

参数：

signature

私钥签名值

plain

被签名的字段

默认参数：‘fenyukejiyouxiangongsi’

返回值：

bool true || false

说明：

验证数字签名。

### P10文件生成函数

csrgen(domain, options, callback);

参数：

domain

域名

optiions参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 类型 | 默认值 | 是否必选 | 描述 |
| outputDir | String | 无 | 是 | P10文件输出地址 |
| read | bool | 无 | 是 | 是否生成可读文件，参考值：true |
| country | string | ‘US’ | 是 | 国家 |
| company | String | 无 | 否 | 公司信息 |
| email | String | 无 | 否 | 电子邮箱 |

callback：回调函数function(err,keys)

说明：

生成P10文件，文件名默认为domain.csr