**CFCA方案**

评测报告v0.2

## 修改记录

|  |  |  |
| --- | --- | --- |
| 时间 | 修改人 | 修改说明 |
| 2019-03-06 | 吴志民、齐奇、周锐 | 初版 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

目 录

[修改记录 1](#_Toc2950255)

[背景 3](#_Toc2950256)

[目标 4](#_Toc2950257)

[1. 产品简介 4](#_Toc2950258)

[2. 整体方案 4](#_Toc2950259)

[3. 功能特性 4](#_Toc2950260)

[4. 性能 5](#_Toc2950261)

[4.1 接口性能 5](#_Toc2950262)

[4.2 加解密性能 5](#_Toc2950263)

[4.3 签章性能 5](#_Toc2950264)

[5. 可靠性&安全 5](#_Toc2950265)

[6. 兼容性&易用性 5](#_Toc2950266)

[6.1 浏览器兼容性 6](#_Toc2950267)

[6.2 易用性 6](#_Toc2950268)

[7. 市场情况 6](#_Toc2950269)

[8. 报价方案 6](#_Toc2950270)

[9. 评估结论 6](#_Toc2950271)

## 背景

随着互联网的普及和网络应用的快速发展，网络应用的风险也日益凸显。越来越多的网络应用系统对安全提出了要求，数字证书安全应用方案（PKI安全）是当前网络应用中最理想的整体安全解决方案，可以解决身份认证、数据安全、电子签名等各方面的安全需求。

平安医药团队自主研发的药品xx平台，具有招投标、在线合同等业务模块，客户是面向医疗机构和药企，对安全性要求非常高，客户在平台上的操作需要经过严格的身份验证，同时平台的电子合同需要符合国家电子签名法的有关规定，故需要接入CA方案。

## 目标

对各大厂商的产品从技术指标和商务指标进行评估，其中技术指标包括整体方案、功能特性、可靠性、兼容性等维度评估，最终选用一家成熟的CA机构，能够满足xx项目对身份认证的业务流程：CA登录、招投标信息加解密、在线合同签章等。

## 产品简介

中国[金融](https://baike.baidu.com/item/%E9%87%91%E8%9E%8D/860" \t "_blank)认证中心（China Financial Certification Authority，简称CFCA）是经中国人民银行和国家信息安全管理机构批准成立的国家级权威安全认证机构，是国家重要的金融信息安全基础设施之一。在《中华人民共和国电子签名法》颁布后，CFCA成为首批获得电子认证服务许可的电子认证服务机构之一。

## 整体方案

详见文档*《平安医疗在线招投标及采购平台解决方案.pdf》*

## 功能特性

**CFCA产品体系如下：**

* **RA系统**：必选产品，用于向CA申请数字证书，并导入UKEY
* **无纸化签章系统**：必选产品，用于完成电子签章及PDF电子合同生成
* **UKEY**：必选产品，作为各参与方数字证书载体
* **证书应用工具包**：必选产品，通过证书应用工具包可调用UKEY中数字证书签名及加解密
* **加密机**：必选，平台方使用加密机对投标文件二次加解密
* **网银助手**：可选产品，解决投标人及采购方由于电脑配置，无法完成相关操作问题，一键修复操作系统及浏览器配置

详细功能参考：*《CFCA产品功能列表.docx》*

## 性能

### 接口性能

### 加解密性能

### 签章性能

详细功能参考：*《CFCA无纸化电子印章系统性能测试报告.doc》*

## 可靠性&安全

官方描述：CFCA机房具有两地三中心，含同城灾备、异地灾备中心保证服务的高可用性。CA机房供电采用双回路且自备发电机，CA机房故障自动切换对用户透明无感。同时对外服务满足高可靠性，满足单机构600+TPS服务（可扩容）。CFCA数字认证系统CA的服务可用性连续3年超过99.99%。

提供7\*24小时运维自动化服务，每个系统，有明确的角色定义和责任划分，以便能快速、准确地定位问题原因，并及时地进行修复和处理。建立了流程化的故障处理机制和跟踪记录，确保能够高效处理故障并实现故障记录的可追踪。监控人员和运维工程师负责7\*24的系统运维监控，当发生异常情况时，确保能第一时间处理故障。

**服务端使用硬件加密机：**

加密机通过硬件实现SM2，和通过软算法实现，理论上计算结果是一样的，主要存在的问题在于安全性。  
 第一是密钥的使用和保护，如果你通过软算法实现，密钥必然要保存在你的PC或者服务器上，如何能够安全地保存是个问题。  
 第二是计算过程，用软算法实现必然要在服务器内存中进行加解密计算，这也是存在安全隐患的。而加密机实现的话，可以认为是个安全的计算环境，不容易被窃取。  
 第三是SM2算法计算中需要随机数参与，而随机数的随机性一般也是要靠硬件噪声源保证的，这也需要加密机内置的噪声源芯片。

## 兼容性&易用性

### 浏览器兼容性

支持IE，Edge, chrome, firefox。低版本的IE 不支持websocket，但可以使用COM方式调用，接口形式一样。(高版本中间件支持)。

详见*《CFCA兼容性测试.xlsx》*

### 易用性

* SDK接口文档不够齐全、不够专业；
* 没有具体改造方案，集成、改造较为复杂；
* 经常出现卡顿现象；

## 市场情况

**唯一拥有金融行业数字证书案例千家以上企业：**

客户包括人民银行、中国工商银行、中国农业银行、中国建设银行、民生银行、交通银行、招商银行、中信银行、浦发银行、光大银行、平安银行、广发银行、兴业银行等共2300余家银行客户。以及上千家非银行客户，包括国家电网、北京市国税局、中国华能集团、海尔、中远集团、中国南方航空公司、苏宁电器、清华同方等。目前证券行业客户包括招商证券、海通证券、东方证券、长城国瑞证券等。

**资质优势：**

* CFCA证书入根全球五大证书库（中国唯一）
* 唯一经过监管机构认可的解决方案
* 最丰富的数字签名鉴定经验、最全面的司法鉴定服务

## 报价方案

共计6个产品，必选产品5个，一次性费用35万，企业证书+UKEY共104元/年，系统维护费2万元/年；

详见*《平安医疗在线招投标及平台报价函.pdf》*

## 评估结论