**网证通CA方案**

评测报告v0.2

## 修改记录

|  |  |  |
| --- | --- | --- |
| 时间 | 修改人 | 修改说明 |
| 2019-02-26 | 吴志民，周锐，齐奇 | 初版 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

目 录

[修改记录 1](#_Toc2956982)

[背景 4](#_Toc2956983)

[目标 4](#_Toc2956984)

[1. 产品简介 4](#_Toc2956985)

[2. 整体方案 4](#_Toc2956986)

[2.1 技术架构 4](#_Toc2956987)

[2.2 部署架构 5](#_Toc2956988)

[3. 功能特性 6](#_Toc2956989)

[4. 性能 7](#_Toc2956990)

[4.1 接口性能 7](#_Toc2956991)

[4.2 加解密性能 7](#_Toc2956992)

[4.3 签章性能 7](#_Toc2956993)

[5. 可靠性&安全 7](#_Toc2956994)

[6. 兼容性&易用性 7](#_Toc2956995)

[6.1 浏览器兼容性 7](#_Toc2956996)

[6.2 其他兼容性 8](#_Toc2956997)

[7. 市场情况 8](#_Toc2956998)

[8. 评估结论 8](#_Toc2956999)

## 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

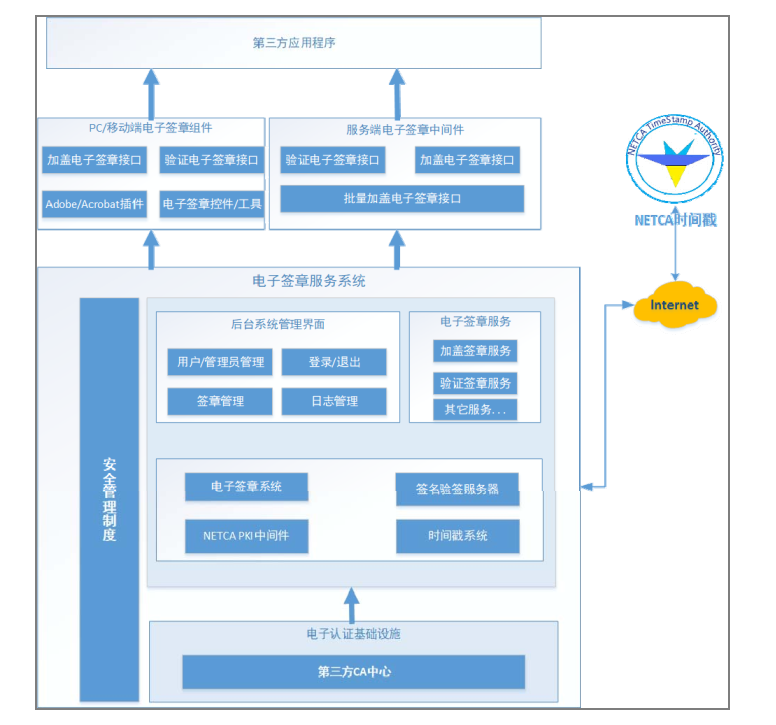
对各大厂商的产品从技术指标和商务指标进行评估，其中技术指标包括整体方案、功能特性、可靠性、兼容性等维度评估，最终选用一家成熟的CA机构，能够满足xx项目对身份认证的业务流程：CA登录、招投标信息加解密、在线合同签章等。

## 产品简介

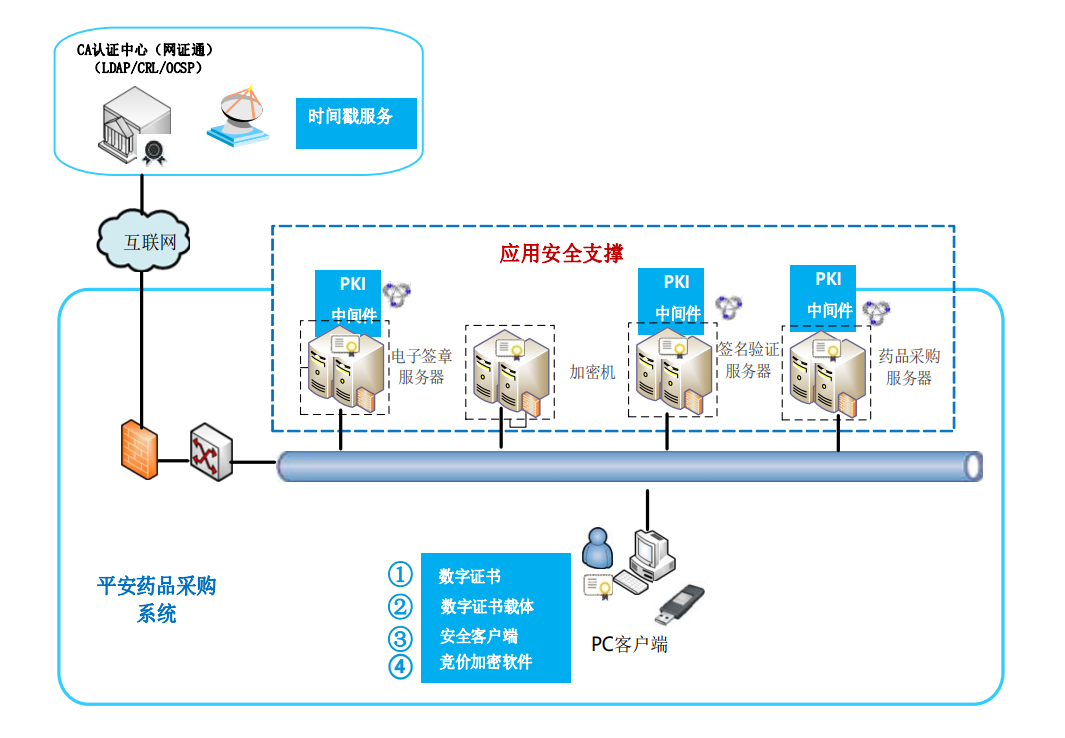
选用一个成熟的API，需要具备安全、稳定、高可用的特点，除此之外，未来平台提供的API服务多种多样，API网关应该具备以下基础功能，如对外API的全生命周期进行便捷管理、鉴权、限流、计费、监控、统计、端对端调用、API市场等。

## 整体方案

### 技术架构



### 部署架构



整体方案参考：*《<药品采购CA安全解决方案.pdf>》*

## 功能特性

网证通平台由服务端和客户端两大部分组成。

**服务端包括：**

* 签名验证服务器
* 证书密码服务器
* 时间戳服务器
* 电子签章系统

**客户端包括：**

* 数字证书（单位/单位员工/公务员）
* 电子密钥（USBKEY）

详细功能参考：*《<网证通CA功能列表.pdf>》*

## 性能

### 接口性能

官方给出的性能测试报告

通过测试得出性能指标

详细功能参考：*《[NETCA签名验签服务器V1.1.0\_TCFP测试报告20190219.doc](资料/相关资料/签名验证服务器/NETCA签名验签服务器V1.1.0_TCFP测试报告20190219.doc)》*

### 加解密性能

加密机实现加解密

详细功能参考：*《[SJJ507服务器密码机用户使用手册\_V1.0.pdf](资料/相关资料/证书密码服务器/SJJ507服务器密码机用户使用手册_V1.0.pdf)》*

### 签章性能

客户端由 Adobe Reader/Acrobat 加载，在 Adobe Reader/Acrobat 中使用 NETCA 的签章

服务端批量签章，逐个签章

详细功能参考：*《[网证通电子签章软件V3.0.5.3\_TCFP测试报告\_20190131.docx](资料/相关资料/电子签章系统/网证通电子签章软件V3.0.5.3_TCFP测试报告_20190131.docx)》*

*《[网证通电子印章管理系统V2.0.3\_TCFP测试报告20180820.docx](资料/相关资料/电子签章系统/网证通电子印章管理系统V2.0.3_TCFP测试报告20180820.docx)》*

## 可靠性&安全

加密算法：RSA/SM2；

依赖于第三方竞价规则的安全加密解密方式；

加密解密过程，安全方面由网证通负责；

## 兼容性&易用性

### 浏览器兼容性

支持chrome，IE兼容性差。

### 其他兼容性

系统兼容性：

客户端winXp，win7，win10

服务端：RedHat企业版5、6、7（32/64bit），Windows server 2008及以上

## 市场情况

## 评估结论