

**网证通中间件小程序插件**

**V1.1.0.2009041214测试报告**

编制单位：广东省电子商务认证有限公司

责任部门：运维部

目 录

[1 升级内容 1](#_Toc50129604)

[2 测试结论 1](#_Toc50129605)

[2.1 功能测试 1](#_Toc50129606)

[2.2 性能测试 2](#_Toc50129607)

[3 测试信息 3](#_Toc50129608)

[3.1 测试策略 3](#_Toc50129609)

[3.2 测试执行情况与记录 3](#_Toc50129610)

[3.3 各个系统/软件模块版本及对应升级内容 4](#_Toc50129611)

[3.4 测试过程总结 4](#_Toc50129612)

[4 测试环境与配置 4](#_Toc50129613)

[4.1 服务器环境（智能移动终端安全密码模块协作系统） 4](#_Toc50129614)

[4.2 客户端环境 5](#_Toc50129615)

[5 功能测试结果 5](#_Toc50129616)

[6 性能测试结果 5](#_Toc50129617)

[7 遗留缺陷报告 6](#_Toc50129618)

[7.1 新发现未解决的缺陷 6](#_Toc50129619)

[7.2 历史版本遗留的缺陷 6](#_Toc50129620)

# 升级内容

本次测试中，网证通中间件小程序插件由V1.0.3升级到V1.1.0.2009041214，主要升级了以下内容：

1. 新增PDF签章功能；
2. 新增设备数据管理功能；

参考资料：

1. 测试申请单：<http://192.168.0.123:8080/browse/RODT-2001> ；
2. 需求文档：[http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/文档/小程序/NETCA-T01-PR03-RE04 微信小程序平台中间件产品需求说明书.docx](http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/文档/小程序/NETCA-T01-PR03-RE04%20微信小程序平台中间件产品需求说明书.docx)

# 测试结论

本次测试类型有：功能测试、性能测试。

该版本剩余残留问题，经初步评估对用户影响可控，可暂不解决，评估为**测试通过**。

## 功能测试

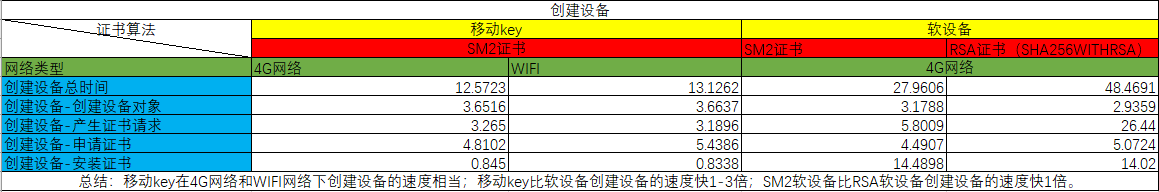
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **版本号** | V1.1.0.2009041214 | | **测试结果** | | **测试通过** | |
| **测试结论** | 1. PDF签章，测试通过； 2. 设备数据管理，测试通过； 3. 回归测试，测试通过：设备管理、修改设备密码、计算哈希、计算HMAC、签名验签、SignedData、对称加解密、非对称加解密，测试通过。 | | | | | |
| **需求情况** | 未实现需求 | | | 未测试需求 | | 测试覆盖率 |
| 无 | | | 无 | | 100% |
| **测试用例执行情况** | 共执行用例数 | 通过用例数 | 失败用例数 | | 阻塞用例数 | **通过率** |
| 54 | 53 | 1 | | 0 | 98.15% |
| **缺陷情况** | 新发现缺陷数 | 缺陷率 | 已解决缺陷数 | | **本次测试残留缺陷数** | **最终缺陷率** |
| 14 | 25.93% | 13 | | 1 | 1.85% |
| 注：1. 本版本存在历史残留缺陷，故共残留缺陷4个，缺陷情况请查看第[7](#_遗留缺陷报告)章遗留缺陷报告；  2. 测试覆盖率计算方式：已测试的需求测试用例数/本次共执行测试用例数（未实现的不包括在内）。 | | | | | | |

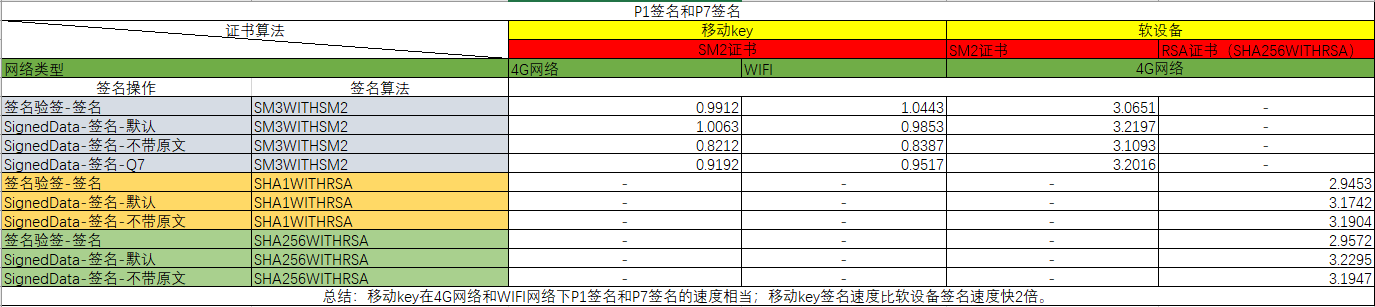
## 性能测试

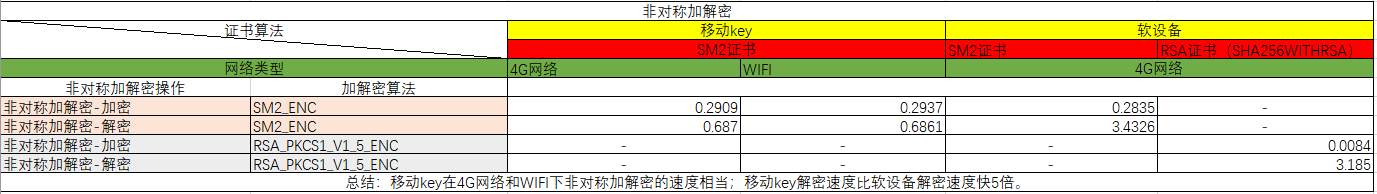
本次性能测试主要对移动key和软设备两种设备的各功能的平均响应时间进行测试，测试设备为vivo iQoo Pro，使用支付宝小程序进行测试；移动key设备仅支持SM2证书；RSA证书的测试结果仅节选签名算法为 SHA256WITHRSA 的数据，测试结论如下：

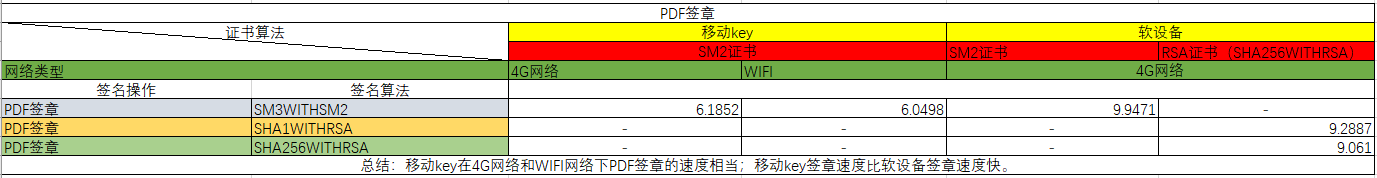
1. 创建设备：移动key在4G网络和WIFI网络下创建设备的速度相当；移动key比软设备创建设备的速度快1-3倍；SM2软设备比RSA软设备创建设备的速度快1倍。
2. P1签名和P7签名：移动key在4G网络和WIFI网络下P1签名和P7签名的速度相当；移动key签名速度比软设备签名速度快2倍。
3. 非对称加解密：移动key在4G网络和WIFI下非对称加解密的速度相当；移动key解密速度比软设备解密速度快5倍。
4. PDF签章：测试使用的PDF大小为4KB，移动key在4G网络和WIFI网络下PDF签章的速度相当；移动key签章速度比软设备签章速度快。

测试结果如下表，详细测试结果见第[6](#_问题列表_1)章：









注：性能测试结果跟上个版本（测试设备为荣耀V10）差距较大，经确认属于测试设备性能问题。

# 测试信息

## 测试策略

1. 使用Android和iOS手机，在支付宝小程序上测试各项功能；
2. 哈希、HMAC、验签、SignedData验签、非对称加密使用CryptoTestTool进行交叉验证；
3. PDF签章使用Adobe Reader进行验签；
4. 使用vivo iQoo Pro手机，在支付宝小程序上，进行创建设备的测试，使用例程中连续测试的功能，分别在4g和wifi两种网络下，测试创建移动key设备10次，记录各步骤的时间和平均时间；在wifi网络下测试创建软设备10次，记录各步骤时间和平均时间；
5. 使用vivo iQoo Pro手机，在支付宝小程序上，进行P1签名、非对称加密、非对称解密、SignedData签名、SignedData不带原文签名、SignedData使用国密Q7签名（仅SM2算法）、PDF签章各10次，记录各步骤时间和平均时间。
6. PDF签章，选择STREAM的PDF返回方式时，由于支付宝小程序不支持复制到剪贴板且PDF较大时复制会导致小程序崩溃，因此本次测试使用4KB的PDF文件进行测试，以便复制到PC中使用Adobe进行验签。性能测试主要目的是对比不同网络条件、设备和算法之间的性能差距，因此也使用4KB的PDF进行测试。实际上，PDF签章支持较大PDF的签名。

## 测试执行情况与记录

### 人力资源情况

|  |  |
| --- | --- |
| 主要开发人员 | 杜炳坚 |
| 主要测试人员 | 陈碧玉 |
| 用例评审人员 | 廖远贵 |
| 测试时间 | 本次测试耗时：20200827－20200904（总工时5人日） |
| 测试版本 | 本次测试共测试8个版本  最终版本号：V1.1.0.2009041214  测试过程版本数：8 |

### 测试过程记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 执行用例数 | 发现缺陷数 | 备注 |
| V1.1.0.0 | 20 | 5 | 大部分缺陷为新功能引入 |
| V1.1.0.2008280901 | 10 | 1 | 新功能引入，修复4个缺陷 |
| V1.1.0.2008280952 | 15 | 2 | 新功能引入，修复3个缺陷 |
| V1.1.0.2008281455 | 20 | 5 | 修复缺陷引入、新功能引入，修复2个缺陷 |
| V1.1.0.2009011631 | 10 | 0 | 修复2个缺陷、调整接口参数 |
| V1.1.0.2009021612 | 5 | 0 | 优化兼容性 |
| V1.1.0.2009031212 | 45 | 1 | 修复缺陷引入、修复1个问题 |
| V1.1.0.2009041214 | 25 | 0 | 修复1个问题 |

### Rmsis最后版本测试用例统计结果如图：

| Name | Description | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 86\_中间件小程序V1.1.0\_支付宝小程序 | 支付宝小程序 | V1.1.0 | Android/iOS | 27 Aug 2020 | 4 Sep 2020 | 53 passed, 1 failed | 中间件小程序插件V1.1.0 |

## 各个系统/软件模块版本及对应升级内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统名称** | **最终版本号** | **本次升级** | **升级次数** | **主要升级内容** |
| 中间件小程序插件 | V1.1.0.2009041214 | 是 | 8 | 1. 新增PDF签章功能； 2. 新增设备数据管理功能； |

## 测试过程总结

本次测试过程测试时间耗时长，迭代版本8个，缺陷率高，经总结主要有以下原因：

1. 本版本为支付宝小程序首测版本，前期发现的缺陷较多，且修复缺陷会引进新缺陷，因此耗时较多；
2. 需要与电子印章管理系统联测；
3. 需要进行性能测试，测试运行时间长；
4. 有部分缺陷为支付宝的问题，需经过实施跟对接方协商确定是否未来版本解决；

针对以上问题，后续改进建议有：

1. 修复缺陷后要对相关功能进行全面的回归测试，尽早发现修复缺陷引进的新缺陷。

# 测试环境与配置

## 服务器环境（智能移动终端安全密码模块协作系统）

|  |  |
| --- | --- |
| CPU | Intel(R) Xeon(R) E3-1220 v5/3.00GHz \* 4 |
| 内存 | 8G/DDR4/2133 |
| 硬盘 | 1T |
| 网络通道 | eno1 |
| 操作系统OS | CentOS Linux release 7.5.1804 (Core) |
| 支持环境JDK | JDK1.8.0\_172 64位 |
| WEB服务 | Springboot 2.2.4 |
| 数据库系统 | MYSQL8.0.4-rc-log |
| 中间件 | V5.7.0.1（Java-Linux64位） |
| 虚拟机/物理机 | 物理机 |

## 客户端环境

|  |  |
| --- | --- |
| 中间件微信小程序 | V1.1.0.2009041214，扫描二维码获取，二维码见工单：  <http://192.168.0.123:8080/browse/RODT-2001> |
| 测试手机系统 | vivo iQoo Pro Android10  iPhone7 iOS12.1.4 |
| 支付宝版本 | Android端：V10.2.0.9000  iOS端：V10.2.0 |
| 业务平台 | <https://124.71.15.76:6300> |
| 密码模块服务器 | <http://124.71.15.76:7091> |
| 时间戳服务器 | <http://tsa.cnca.net> |

# 功能测试结果

共执行用例54个，通过 53个用例，通过（存在可允错误）0个用例，失败1个用例，阻塞0个用例，通过率为98.15%。具体测试结果，请查看以下文件。

文件格式为：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Run Name** | **Test Case ID** | **Test Case Name** | **Test Case Status** | **Artifact ID** | **Artifact Summary** | **Artifact Priority** |



# 性能测试结果

具体数据可查看下面的文件。



# 遗留缺陷报告

## 新发现未解决的缺陷

新发现未解决的问题共1个。详情请查看以下文件。文件格式如下：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **标识** | **主题** | **优先级** | **严重性** | **状态** | **影响版本** | **创建人** | **创建日期** | **备注** |



## 历史版本遗留的缺陷

历史版本遗留的问题共3个。详情请查看以下文件。文件格式如下：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **标识** | **主题** | **优先级** | **严重性** | **状态** | **影响版本** | **创建人** | **创建日期** | **备注** |

