

**网证通安全中间件**

**V5.8.0.2\_回归测试报告**

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 3](#_Toc28705055)

[2 测试结论 3](#_Toc28705056)

[3 限制条件/建议 4](#_Toc28705057)

[3.1 例程限制 4](#_Toc28705058)

[4 测试信息 4](#_Toc28705059)

[4.1 测试策略 5](#_Toc28705060)

[4.2 测试执行情况与记录 5](#_Toc28705061)

[4.3 各个系统/软件模块版本及对应升级内容 6](#_Toc28705062)

[5 测试环境与配置 6](#_Toc28705063)

[5.1 客户端配置 6](#_Toc28705064)

[5.2 测试环境 7](#_Toc28705065)

[6 功能测试结果 7](#_Toc28705066)

[7 问题列表 8](#_Toc28705067)

[7.1 新发现未解决的问题 8](#_Toc28705068)

[7.2 历史版本遗留的问题 8](#_Toc28705069)

# 升级内容

网证通安全中间件V5.8.0.2与上个版本V5.7.2.0相比，升级了以下内容：

1. 随机数发生器允许配置直接使用设备产生的随机数，并可以配置进行随机数测试
2. 允许配置使用其他设备进行公钥运算，尤其是在验证证书签名的时候
3. 增加SignedAndEnvelopedData的支持，包括C和纯JAVA
4. 增加PKCS#8的私钥格式的支持
5. 纯JAVA增加JOSE的支持
6. 修复获取证书非DER编码的时候，由于指针转换错误导致在某些系统中崩溃的BUG
7. NETCA\_URL2修复URL中使用IPV6地址解析错误的BUG，支持断点续传和文件上传，增加TLS1.3的支持，添加日志
8. 去掉企业级CA证书链

参考资料：

1. 测试申请单： <http://192.168.0.123:8080/projects/RODT/issues/RODT-1595>

# 测试结论

本次测试是Test Case First Pass（简称TCFP），主要进行的测试类型有：功能测试。

剩余残留问题，对用户影响可控，可暂不解决，就提测内容中第1、4点及回归测试情况，评估为**测试通过**，因时间和资源有限，其他内容后续测试后再出测试报告。具体如下。

测试内容总结：

1. 随机数发生器允许配置直接使用设备产生的随机数，并可以配置进行随机数测试，测试通过；
2. 增加PKCS#8的私钥格式的支持，在邮箱申请应用插件测试通过，见http://192.168.0.11:8081/svn/rdrelease/软件发布/统一介质管理工具/install/测试版/标准版/Windows/应用安装包/邮箱申请应用插件/测试文档/邮箱申请应用插件V1.0.0.5\_TCFP测试报告20191220.doc；
3. 对称加解密、非对称加解密、数字信封加解密、P1签名、Signeddata签名、hash运算、base64编解码等功能，回归测试通过；
4. 剩余部分新增功能，暂时未测，后续再安排测试。

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 | 需求测试覆盖率 |
| 743 | 742 | 1 | 0 | 99.87% | 100% |

用例详情请查看第[6](#_功能测试结果)章节。

缺陷情况：

|  |  |  |  |
| --- | --- | --- | --- |
| 新发现缺陷数 | 缺陷率 | 最终残留缺陷数 | 最终缺陷率 |
| 1 | 0.13% | 1 | 0.13% |

详细问题请查看第[7](#_问题列表_1)章节。

# 限制条件/建议

## 例程限制

1. （新增）因例程没有实现，除随机数发生器允许配置直接使用设备产生的随机数，并可以配置进行随机数测试、增加PKCS#8的私钥格式的支持外，其余新增功能均没有进行测试。
2. （新增）win7x86系统下，由于大文件加密所需时间长，没有详细测试，仅针对100k大小文件进行测试。
3. （历史）详见例程限制.docx，svn地址：http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/安全中间件测试报告/例程限制.docx

# 测试信息

## 测试策略

由于暂时没有提供中间件V5.8大部分升级项内容的测试例程，且因邮箱申请应用插件发布目前需要使用该版本中间件，时间和资源有限，故本次测试重点为关键功能回归测试和满足邮箱申请应用插件的测试。其他升级内容将后续进行测试。

中间件测试需依托“网证通安全客户端”测试,本次测试采用的依托版本为V4.2.0.6

鉴于系统、IE和第三方软件的版本较多，在此采用交叉测试，如下表：（空格代表不测）

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Win7 32（IE11）** | **Win7 64（IE10）** | **Win10 64（IE11）** |
| Cryptotesttool | √ | √ |  |
| Office应用 |  |  | 2016 |
| PDF |  |  |  |
| 中间件2.0例程页面 |  |  | √ |
| 制证 | 业务平台 | 业务平台 |  |
| 其他（如能够实现测试的升级项等） | √ |  | √ |

鉴于测试介质的数量繁多，考虑到测试交付日期，采用交叉测试，如下表：

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Win7 32（IE11）** | **Win7 64（IE10）** | **Win10 64（IE11）** |
| 介质 | 文鼎创、飞天3000GM（重点）+剩余8种介质（只测试客户端能正常读取） | 飞天3003、海泰普通（重点）+剩余8种介质（只测试客户端能正常读取） | 飞天3000GM（重点）+剩余9种介质 （只测试客户端能正常读取） |

## 测试执行情况与记录

人力资源情况：

|  |  |
| --- | --- |
| 主要开发人员 | 赵敏 |
| 主要测试人员 | 谭嘉豪、叶利乔、陈碧玉 |
| 测试时间 | 本次测试耗时： 20191212-20191231  （实测5天） |
| 测试版本 | 本次测试共测试2个版本  最终版本号：V5.8.0.2  测试过程版本数：2 |

Rmsis测试集统计结果如图：

| Name | Description | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 65\_网证通安全中间件5.8.0 win7 32位（IE11） | 升级测试 | V5.8.0 | win7 32位 IE11 | 11 Dec 2019 | 31 Dec 2019 | 234 passed | V5.8.0 |
| 64\_网证通安全中间件5.8.0 win7 64位（IE10） | 升级测试 | V5.8.0 | win7 64位 IE10 | 12 Dec 2019 | 31 Dec 2019 | 465 passed | V5.8.0 |
| 63\_网证通安全中间件5.8.0 win10（IE11） | 升级测试 | V5.8.0 | win10 IE11 | 11 Dec 2019 | 31 Dec 2019 | 43 passed, 1 failed | V5.8.0 |

## 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** |
| *网证通安全中间件* | *V5.8.0.2* | *是* | *2* | *去掉企业级CA证书链等* |

# 测试环境与配置

## 客户端配置

|  |  |
| --- | --- |
| 客户端硬件 | *PC1: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81GHz 8G（win7x64）* |
| *PC2: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81GHz 2G(虚拟机) （win7x86）* |
| *PC3: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz 3.19GHz 8G（win10x64）* |
| PC操作系统 | *Win7 32位，Win7 64位，win10 64位* |
| 浏览器版本 | *IE10、IE11* |
| 网证通安全客户端 | V4.2.0.6，svn地址：http://192.168.0.11:8081/svn/rdrelease/软件发布/统一介质管理工具/install/测试版/标准版/Windows/网证通安全客户端/V4.2/网证通安全客户端.exe |
| 网证通安全中间件 | V5.8.0.2，svn地址：  http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/安装包/NETCA\_Crypto.exe |

## 测试环境

|  |  |  |
| --- | --- | --- |
| 制证环境 | 业务平台制证系统，V4.13，<https://192.168.0.59/certbpms/> | |
| 测试用例 | RMsis测试用例集（项目：安全中间件32位）：  65\_网证通安全中间件5.8.0 win7 32位（IE11）  64\_网证通安全中间件5.8.0 win7 64位（IE10）  63\_网证通安全中间件5.8.0 win10（IE11） | |
| 支持介质类型 | 10种介质，  微柏、飞天3003、飞天3000GM、海泰、海泰全算法、文鼎创、明华2版、明华3版、文鼎创蓝牙、飞天蓝牙、华大SD | |
| 设备驱动 | 海泰 | NETCA\_Devices(HTSM2COS).exe V2.0.0.33 |
| 飞天3000GM | NETCA\_Devices(FT3000GM).exe V4.1.0.14 |
| 飞天3003 | NETCA\_Devices(FT3003).exe V1.1.0.27 |
| 飞天蓝牙 | NETCA\_Devices(FTBluetoothKey).exe V1.0.0.11 |
| 文鼎创 | NETCA\_Devices(ES).exe V1.1.2.14 |
| 文鼎创蓝牙 | NETCA\_Devices(ESBluetoothKey).exe V1.0.0.3 |
| 龙脉OTG | NETCA\_Devices(LongMaiOTG).exe V1.0.0.18 |
| 明华二版三版 | NETCA\_Devices\_x86(MWV2V3).exe V1.1.0.22 |
| 华大SD卡 | NETCA\_Devices(HDSDCard).exe V1.0.0.11 |
| 中间件测试例程NetcaPKITest.htm | http://192.168.0.11:8081/svn/rdrelease/软件发布/PKI 项目应用改造例程/NetcaPkiCOM调用例程/JavaScript/2.0.0版本 | |
| 32位cryptotesttool | 1.7.0.0，http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool.exe | |
| 64位cryptotesttool | 1.7.0.0，http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool\_x64.exe | |

# 功能测试结果

共执行用例743个，通过 742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99.87%。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** |



# 问题列表

## 新发现未解决的问题

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** |



## 历史版本遗留的问题

历史版本遗留的问题10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** |

