

**网证通安全中间件**

**V5.10.0.0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](#_Toc42159723)

[2 测试结论 3](#_Toc42159724)

[3 测试信息 4](#_Toc42159725)

[3.1 测试策略 5](#_Toc42159726)

[3.2 测试执行情况与记录 5](#_Toc42159727)

[3.3 各个系统/软件模块版本及对应升级内容 6](#_Toc42159728)

[4 测试环境与配置 7](#_Toc42159729)

[4.1 介质支持算法 7](#_Toc42159730)

[4.2 客户端配置 7](#_Toc42159731)

[4.3 测试工具 8](#_Toc42159732)

[4.4 测试脚本 8](#_Toc42159733)

[5 功能测试结果 8](#_Toc42159734)

[6 问题列表 9](#_Toc42159735)

[6.1 新发现未解决的问题 9](#_Toc42159736)

[6.2 历史版本遗留的问题 9](#_Toc42159737)

[6.3 其他风险及规避措施 9](#_Toc42159738)

# 升级内容

网证通安全中间件V5.10.0.0与上个版本V5.9.0.3相比，升级了以下内容：

1. C和纯JAVA支持GM/T 0031和GB/T 38540的电子印章和电子签章；
2. C和纯JAVA支持PKCS#5第二版使用口令导出密钥进行加密的EncryptedData；
3. KM的加密加密私钥的数字信封支持SM4算法；
4. 使用回调对象的JNI签名和解密，提供IGetErrorMessage接口来获取错误描述。

**参考资料：**

1. 测试申请单：<http://192.168.0.123:8080/browse/RODT-1874>
2. 参考手册：

（1）[http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/文档/NETCA PKI API Cookbook.doc](http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/文档/NETCA%20PKI%20API%20Cookbook.doc)

（2）[http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/文档/NETCA PKI API参考手册.doc](http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/文档/NETCA%20PKI%20API参考手册.doc)

# 测试结论

本次测试类型有：功能测试。

无残留问题，就提测内容，评估为**测试通过**。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本号** | V5.10.0 | | **测试结果** | 测试通过 | |
| **测试结论** | 1. C和纯JAVA支持GM/T 0031和GB/T 38540的电子印章和电子签章，**测试通过**； 2. C和纯JAVA支持PKCS#5第二版使用口令导出密钥进行加密的EncryptedData，**测试通过**； 3. KM的加密加密私钥的数字信封支持SM4算法，**测试通过**；   说明：目前支持SM4算法的设备有龙脉、文鼎创安可和软设备，由于暂无正常的文鼎创安可key可用，故此次仅测试龙脉key（pid为E618）和软设备。   1. 使用回调对象的JNI签名和解密，提供IGetErrorMessage接口来获取错误描述，**测试通过**； 2. 回归测试关键功能，**测试通过**：   （1）软件设备，**回归测试通过**：   1. 对称加解密、Hash和Base64编码解码，测试通过   （2）硬件设备，**回归测试通过**：   * + 1. 对称加解密、非对称加解密、数字信封加解密，测试通过     2. Hash和Base64编码解码，测试通过     3. 签名验签和SignedData签名验签，测试通过   （3）中间件应用，**回归测试通过**；   1. 业务平台制作证书，测试通过； 2. Adobe Acrobat Reader签名验签，测试通过； 3. Outlook签名验签和加密解密，测试通过； 4. 多浏览器应用插件PKI接口，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 |
| 456（自动化用例251） | 456 | 0 | 0 | 100% |
| **缺陷情况** | 新发现缺陷数 | 缺陷率 | 已解决缺陷数 | 最终残留缺陷数 | 最终缺陷率 |
| 0 | 0 | 0 | 0 | 0 |
| 注：1.本版本还存在其他风险及其规避措施请仔细告查看本报告[6.3章节](#_其他风险及规避措施)；  2.历史版本缺陷情况请查看[第6章](#_遗留缺陷报告)遗留缺陷报告；  3.测试覆盖率计算方式：已测试的需求测试用例数/新增测试用例数（未实现的不包括在内）。 | | | | | |

# 测试信息

## 测试策略

1. 重点测试本版本的升级内容；
2. 回归测试中间件的算法和应用；
3. 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V4.3.5；
4. 根据测试要求，且鉴于操作系统、浏览器、第三方软件和测试介质的数量繁多，在此采用交叉测试，如下表：（空格代表不测）

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Win7 32** | **Win7 64** | **Win10 64** |
| 升级内容 |  | √ | √ |
| Cryptotesttool | 自动化 | 自动化 |  |
| Office应用 |  |  | 2016 |
| PDF |  |  | Acrobat Reader DC |
| 制证 |  |  | 业务平台（IE11） |
| 多浏览器应用 |  |  | √（IE11、Edge、FrieFox、Chrome） |
| 介质 | 文鼎创、飞天3000GM | 飞天3000GM、  海泰 | 文鼎创、海泰、龙脉 |

## 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 | 吴晓霞、叶利乔 |
| 打包人员 | 吴晓霞 |
| 用例评审人员 | 梁宁宁 |
| 测试时间 | 本次测试耗时： 2020601-2020604  （实测3天） |
| 测试版本 | 本次测试共测试1个版本  最终版本号：V5.10.0.0  测试过程版本数：1 |

### 测试过程记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 执行用例数 | 发现缺陷数 | 备注 |
| V5.10.0 | 455（自动化用例251） | 0 |  |

### Rmsis测试集统计结果如图：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Description | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| 81\_中间件PC版 V5.10.0 win7 32 | 升级测试 | 5.10.0 | win7 32 | 3 Jun 2020 | 4 Jun 2020 | 84 passed | V5.10 |
| 80\_中间件PC版 V5.10.0 win10 | 升级测试 | 5.10.0 | win10 | 1 Jun 2020 | 3 Jun 2020 | 106 passed | V5.10 |
| 79\_中间件PC版 V5.10.0 win7 64 | 升级测试 | 5.10.0 | win7 64 | 1 Jun 2020 | 3 Jun 2020 | 266 passed | V5.10 |

## 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 | V5.10.0.0 | 是 | 1 | 1. 支持GM/T 0031和GB/T 38540的电子印章和电子签章，包括C和纯JAVA； 2. 支持PKCS#5第二版使用口令导出密钥进行加密的EncryptedData，包括C和纯JAVA； 3. KM的加密加密私钥的数字信封支持SM4算法； 4. 使用回调对象的JNI签名和解密，提供IGetErrorMessage接口来获取错误描述。 |

# 测试环境与配置

## 介质支持算法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **介质** | **RSA1024** | **RSA2048** | **SM2** | **是否支持64位应用** |
| 飞天3000GM | √ | √ | √ | √ |
| 文鼎创 | √ | √ | √ | √ |
| 海泰 | √ | √ | √ | √ |
| 飞天3003 | √ | √ | 不支持 | √ |
| 微柏 | √ | √ | 不支持 | √ |
| 明华2/3 | √ | 不支持 | 不支持 | 不支持 |
| 龙脉OTG | √ | √ | √ | √ |
| 飞天蓝牙 | √ | √ | √ | √ |
| 文鼎创蓝牙 | √ | √ | √ | √ |
| 华大SD卡 | √ | √ | √ | 不支持 |

## 客户端配置

|  |  |
| --- | --- |
| 客户端硬件 | PC1: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz 3.40GHz 8G |
| PC2: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.30GHz 12G |
| PC3: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81GHz 8G |
| PC操作系统 | Win7 32, Win7 64, Win10 |
| 浏览器版本 | IE11、Edge、Chrome、Firefox |
| 网证通安全客户端 | <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/V4.3/测试中/网证通安全客户端.exe>  版本：4.3.5.0 |
| 网证通安全中间件 | <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/安装包/NETCA_Crypto.exe>  版本：5.10.0.0 |
| 支持介质类型 | 11种介质，  微柏、飞天3003、飞天3000GM、海泰、龙脉、文鼎创、明华2版、明华3版、文鼎创蓝牙、飞天蓝牙、华大SD、软设备 |
| 制证平台 | 业务平台：<https://192.168.0.67/certbpms/>  版本：V5.6.1 |

## 测试工具

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **用途** | **名称** | **版本** | **地址** |
| 1 | 自动化测试工具 | HP Unified Functional Testing | 11.5 | \\192.168.0.8\software\应用软件\QTP |
| 2 | Office签名、签名加密邮件 | Office | 2016 | \\192.168.0.8\software\办公软件 |
| 3 | PDF签名测试 | Adobe Reader  Adobe Acrobat | DC | \\192.168.0.8\software\办公软件\Acrobat |
| 4 | 32位cryptotesttool测试 | cryptotesttool测试 | 1.7.0.0 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool.exe |
| 5 | 64位cryptotesttool测试 | cryptotesttool测试 | 1.7.0.0 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool\_x64.exe |

## 测试脚本

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **地址** |
| 1 | QTP测试脚本 | http://192.168.0.11:8081/svn/rdrelease/测试文档/03\_测试工具/QTP/crypto算法 |
| 2 | LUA脚本 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/例子/lua的例子 |
| 3 | 纯JAVA脚本 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/例子/Java的例子/pure |

# 功能测试结果

共执行用例456个（其中251个为自动化脚本执行，占比：55.04%），通过456个用例，失败0个用例，阻塞0个用例，通过率为100%。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

无。

## 历史版本遗留的问题

历史版本遗留的问题12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** |



## 其他风险及规避措施

1. （历史）详见例程限制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