

**网证通安全中间件**

**V5.8.0.2新增功能测试报告**

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](#_Toc35010519)

[2 测试结论 1](#_Toc35010520)

[3 测试信息 2](#_Toc35010521)

[3.1 测试策略 2](#_Toc35010522)

[3.2 测试执行情况与记录 2](#_Toc35010523)

[3.3 各个系统/软件模块版本及对应升级内容 3](#_Toc35010524)

[4 测试环境与配置 3](#_Toc35010525)

[4.1 客户端环境 3](#_Toc35010526)

[5 功能测试结果 4](#_Toc35010527)

[6 遗留缺陷报告 4](#_Toc35010528)

[6.1 新发现未解决的缺陷 4](#_Toc35010529)

[6.2 历史版本遗留的缺陷 4](#_Toc35010530)

# 升级内容

网证通安全中间件V5.8.0.2在上个版本V5.7.2.0基础上，新增以下功能：

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；
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. 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/browse/RODT-1595>；
2. NETCA PKI API参考手册：[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)
3. NETCA PKI Java API使用手册：[http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/文档/NETCA PKI Java API使用手册.doc](http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/文档/NETCA%20PKI%20Java%20API使用手册.doc)
4. JAVADOC文档：<http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/文档/NetcaJCryptodoc.zip>

# 测试结论

本次测试类型有：功能测试。

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**测试限制性通过**；

回归测试结果为**测试通过**，结果详见：<http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/安全中间件测试报告/网证通安全中间件V5.8.0.2_回归测试报告20191231.docx>。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **版本号** | V5.8.0.2 | | **测试结果** | | 测试限制性通过 | |
| **测试结论** | 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. 允许配置使用其他设备进行公钥运算，测试通过； 3. SignedAndEnvelopedData，包括C和纯JAVA，测试限制性通过：    1. SignedAndEnvelopedData使用签名回调函数进行SM2签名，验签失败（[CRPT-173](http://192.168.0.123:8080/browse/CRPT-173)），V5.9版本修复。 4. PKCS#8的私钥格式，测试通过； 5. 纯JAVA的JOSE ，测试限制性通过：    1. net.netca.pki.encoding.json.jose.impl.netcajni.NetcaMyStore实现有问题，JWE解密失败（[CRPT-175](http://192.168.0.123:8080/browse/CRPT-175)）,JWT解密有相同问题，是因为证书同时带有加密密钥和密钥协商位时处理有问题导致的，V5.9版本修复。 6. 去掉企业级CA证书链，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 |
| 31 | 26 | 5 | | 0 | 83.87% |
| **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 |
| 2 | 6.45% | 0 | | 2 | 6.45% |
| 注：1.缺陷情况请查看[第6章](#_遗留缺陷报告)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/新增测试用例数（未实现的不包括在内）。 | | | | | | |

# 测试信息

## 测试策略

本次测试主要测试新增功能，回归测试之前已完成，结果详见: <http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/安全中间件测试报告/网证通安全中间件V5.8.0.2_回归测试报告20191231.docx>

## 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 | 陈碧玉 |
| 用例评审人员 | 廖远贵 |
| 测试时间 | 本次测试耗时：20191216－20200313（总工时共19个工作日）  测试环境测试时间：19个工作日 |
| 测试版本 | 本次测试共测试3个版本  最终版本号：V5.8.0.2  测试过程版本数：3 |

### 测试过程记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 执行用例数 | 发现缺陷数 | 备注 |
| V5.8.0.0 | 6 | 1 | 新功能引入 |
| V5.8.0.1 | 10 | 1 | 新功能引入 |
| V5.8.0.2 | 31 |  |  |

### 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 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 71\_网证通安全中间件V5.8.0新增功能 |  | V5.8.0 | win10/win7 32 | 12 Mar 2020 | 13 Mar 2020 | 26 passed, 5 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 | 3 | 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.去掉企业级CA证书链。 |

# 测试环境与配置

## 客户端环境

|  |  |
| --- | --- |
| 客户端硬件 | PC1: Intel(R) Core(TM) i5-3350P CPU @3.10GHz 3.10GHz 8G |
| PC2: Intel(R) Core(TM) Duo CPU T7700 @ 2.40GHz 2.20 GHz 4G |
| PC操作系统 | Win7 32位，win10 |
| 测试工具 | NetBeans IDE 8.2、Microsoft Visual Studio 2010 |
| 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 |
| 网证通客户端 | 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 |

# 功能测试结果

共执行用例31个，通过 26个用例，通过（存在可允错误）0个用例，失败5个用例，阻塞0个用例，通过率为83.87%。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** |



# 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2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11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** |

