

**网证通安全中间件**

**V5.11.4.2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](#_Toc60819334)

[2 测试结论 3](#_Toc60819335)

[3 测试信息 4](#_Toc60819336)

[3.1 测试策略 4](#_Toc60819337)

[3.2 测试执行情况与记录 5](#_Toc60819338)

[3.3 各个系统/软件模块版本及对应升级内容 6](#_Toc60819339)

[4 测试环境与配置 6](#_Toc60819340)

[4.1 介质支持算法 6](#_Toc60819341)

[4.2 客户端配置 7](#_Toc60819342)

[4.3 测试工具 7](#_Toc60819343)

[4.4 测试脚本 8](#_Toc60819344)

[5 功能测试结果 8](#_Toc60819345)

[6 问题列表 8](#_Toc60819346)

[6.1 新发现未解决的问题 8](#_Toc60819347)

[6.2 历史版本遗留的问题 8](#_Toc60819348)

[6.3 其他风险及规避措施 8](#_Toc60819349)

# 升级内容

网证通安全中间件V5.11.4.2与上个版本V5.10.3.1相比，升级了以下内容：

1、增加了使用SCVP协议进行委托路径构造和委托路径验证；

2、修复[~~YSB-37~~](http://192.168.0.123:8080/browse/YSB-37)SignedData验签存在多余数据的时候导致程序崩溃问题；

3、证书选择框增加单位信息的显示。

**参考资料：**

1. 测试申请单：<http://192.168.0.123:8080/browse/RODT-2191>；
2. 参考手册：
3. [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)；
4. [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** | V5.11.4.2 | | **测试结果** | **测试通过** | |
| **测试结论** | 1. SignedData验签存在多余数据时导致程序崩溃的问题，本版本验证正常，**测试通过**； 2. 证书选择框显示单位信息相关功能，**测试通过**； 3. 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，测试通过   2. Hash模块，测试通过   3. Base64编码模块，测试通过   （2）硬件设备，**回归测试通过**：   * 1. 对称加解密，测试通过   2. 非对称加解密，测试通过   3. Hash模块，测试通过   4. Base64编码模块，测试通过   5. 数字信封加解密，测试通过   6. 签名验签，测试通过   7. SignedData签名验签，测试通过   8. 验证用户、管理员密码，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； | | | | |
| **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 |
| 168 | 168 | 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SignedData验签导致程序崩溃的问题及证书选择选择框显示证书单位信息的功能；
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** | **Win10** |
| Cryptotesttool | 32位 | 32位\64位 |
| Office应用 | 2013 | 2016 |
| PDF | Acrobat Reader 11 | Acrobat Reader DC |
| 制证 |  | 业务平台（IE11） |
| 介质 | 文鼎创、飞天3000GM、明华2&3 | 文鼎创、海泰、飞天3003 |

## 测试执行情况与记录

### 人力资源情况

|  |  |
| --- | --- |
| 主要开发人员 | 赵敏、梁宁宁、林少柳 |
| 主要测试人员 | 廖远贵 |
| 评审人员 | 谭嘉豪、叶利乔 |
| 打包人员 | 叶秋菊 |
| 测试时间 | 本次测试耗时： 20210104-20210106  （实测2.5人日） |
| 测试版本 | 本次测试共测试2个版本  最终版本号：V5.11.4.2 |

### 测试过程记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 执行用例数 | 发现缺陷数 | 备注 |
| V5.11.4.1 | 140 | 0 | 升级程序，引入新功能 |
| V5.11.4.2 | 60 | 0 | 打包修改配置文件hash值 |

### Rmsis测试集统计结果如图：

| Name | Description | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 98\_中间件PC版V5.11.4 win7x32 | 升级测试 | V5.11.4 | win10 IE11 | 31 Dec 2020 | 6 Jan 2021 | 84 passed | V5.11 |
| 97\_中间件PC版V5.11.4 win10 | 升级测试 | V5.11.4 | win7 32位 | 31 Dec 2020 | 6 Jan 2021 | 84 passed | V5.11 |

## 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 | V5.11.4.2 | 是 | 2 | 1. 增加了使用SCVP协议进行委托路径构造和委托路径验证；  2．修复[~~YSB-37~~](http://192.168.0.123:8080/browse/YSB-37)SignedData验签存在多余数据的时候导致程序崩溃问题；  3. 证书选择框增加单位信息的显示 |

# 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 2G |
| PC2: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz 3.40GHz 8G |
| PC操作系统 | Win7 32, 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/V4.4/网证通安全客户端.exe>；  版本：4.4.1.1 |
| 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：5.11.4.2 |
| 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 |
| 制证平台 | 业务平台：<https://192.168.0.59/certbpms/>  版本：V5.16 |

## 测试工具

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **用途** | **名称** | **版本** | **地址** |
| 1 | Office签名、签名加密邮件 | Office | 2013、2016 | \\192.168.0.8\software\办公软件 |
| 2 | PDF签名测试 | Adobe Reader  Adobe Acrobat | 11、DC | \\192.168.0.8\software\办公软件\Acrobat |
| 3 | 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 |
| 4 | 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 | Python测试脚本 | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/安全中间件测试报告/测试脚本/SignedData验证导致崩溃 |

# 功能测试结果

共执行用例168个，通过168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. （新增）由于未找到有效方法测试SCVP协议，故本次未测试SCVP协议进行委托路径构造和委托路径验证相关功能；
2. （历史）详见[例程限制](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)