

**网证通安全中间件**

**V5.8.1.0\_TCFP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](#_Toc31719380)

[2 测试结论 3](#_Toc31719381)

[3 限制条件/建议 4](#_Toc31719382)

[3.1 例程限制 4](#_Toc31719383)

[4 测试信息 5](#_Toc31719384)

[4.1 测试策略 5](#_Toc31719385)

[4.2 测试执行情况与记录 5](#_Toc31719386)

[4.3 各个系统/软件模块版本及对应升级内容 6](#_Toc31719387)

[5 测试环境与配置 7](#_Toc31719388)

[5.1 介质支持算法 7](#_Toc31719389)

[5.2 客户端配置 7](#_Toc31719390)

[5.3 测试工具 8](#_Toc31719391)

[6 功能测试结果 8](#_Toc31719392)

[7 问题列表 9](#_Toc31719393)

[7.1 新发现未解决的问题 9](#_Toc31719394)

[7.2 历史版本遗留的问题 9](#_Toc31719395)

# 升级内容

网证通安全中间件V5.8.1.0与上个版本V5.8.0.2相比，升级了以下内容：

1. NETCA\_CRYPTO\_UI.dll，修复多浏览器管理员权限弹密码框失败的问题。（[CRPT-174](http://192.168.0.123:8080/browse/CRPT-174)）
2. NETCA\_URL2.dll，增加HTTPS 2.0的支持，修正TLS1.3因序列号用错导致加密出错的BUG，增加LDAPS的支持。

**参考资料：**

1. 测试申请单： <http://192.168.0.123:8080/browse/RODT-1668>

# 测试结论

本次测试是Test Case First Pass（简称TCFP）。

无残留问题，就升级内容中的第1点和回归测试，评估为**测试通过**。其余升级内容因暂未有项目使用且缺少测试例程，故暂不测试。具体如下：

1. NETCA\_CRYPTO\_UI.dll，修复多浏览器管理员权限弹密码框失败的问题，测试通过；
2. 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
3. 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
4. 采用Cryptotesttool工具测试的具体情况如下：
   1. Cryptotesttool测试脚本运行的实测文件大小情况，详见svn文档：<http://192.168.0.11:8081/svn/rdrelease/测试文档/03_测试工具/QTP/crypto算法/crypto算法模块用例说明表.xlsx>
   2. 非对称加解密中算法实测文件大小测试结果如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **算法** | **推荐的文件大小** | **实际测试文件大小** | **测试结果** | **注** |
| RSA1024 | 小于等于117字节 | 0字节、1字节、116字节、117字节、118字节 | 当文件大于117字节时，加密失败 |  |
| RSA2048 | 小于等于245字节 | 0字节、1字节、244字节、245字节、246字节 | 当文件大于245字节时，加密失败 |  |
| SM2 | 小于等于32字节 | 0字节、1字节、153字节、154字节、155字节、25KB | 加密空文件（0字节）失败；当文件小于等于154字节时，加解密成功；当文件大于154字节时，加密成功，解密失败 | （1）经过与开发讨论确认：中间件SM2加密通常是用软件实现，因此没有长度限制。但解密是用密码设备实现的，通常会有长度限制，不同的密码设备限制不同。SM4密钥是16个字节，SM4密钥+IV是32个字节，这两种可能是最常用的。目前通过对常用介质（飞天3000GM、海泰、文鼎创）的非对称解密文件大小最大可为154字节，但为了保险起见，推荐32位字节。  （2）中间件是不允许SM2加密0字节的，通常一般应用也极少要求加密0字节的数据 |
|  | | | | |

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 |
| 550 | 550 | 0 | 0 | 100% | 50% |

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 |
| 0 | 0 | 0 | 0 |

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）本版本增加HTTPS 2.0的支持，修正TLS1.3因序列号用错导致加密出错的BUG，增加LDAPS的支持，因暂未有项目使用且缺少测试例程，暂不测试；
2. （历史）网证通安全中间件v5.8.0.2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。
3. （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

# 测试信息

## 测试策略

1. 根据项目的升级内容，本次测试主要对中间件V5.8.1做相对于V5.8.0的回归测试；
2. 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V4.2.5；
3. 鉴于操作系统、IE、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）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **XP SP3（IE8、Firefox）** | **Win7 32（IE9、chrome）** | **Win7 64（IE10、360）** | **Win10 64（IE11、Edge）** |
| Cryptotesttool |  |  | 自动化 |  |
| Office应用 |  | 2010 |  | 2016 |
| PDF |  | Acrobat 10 |  |  |
| 中间件2.0例程页面 |  | √ |  | √ |
| 制证 |  |  |  | 业务平台 |
| 多浏览器应用 | √ | √ | √ | √ |
| 介质 | 文鼎创 | 文鼎创、飞天3000GM | 飞天3003、  海泰 | 飞天3000GM |

## 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、谭嘉豪 |
| 测试时间 | 本次测试耗时： 2020119-20200204  （实测3天） |
| 测试版本 | 本次测试共测试1个版本  最终版本号：V5.8.1.0  测试过程版本数：1 |

Rmsis测试集统计结果如图：

| Name | Description | Build/Version Details | Environment | Start Date | End Date | Summary Report | Release Id |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 69\_网证通安全中间件V5.8.1XP SP3（IE8、Firefox） | 升级测试 | 5.8.1 | XP SP3（IE8、Firefox） | 19 Jan 2020 |  | 4 passed | V5.8.1 |
| 68\_网证通安全中间件5.8.1 Win7 32（IE9、chrome） | 升级测试 | 5.8.1 | Win7 32（IE9、chrome） | 19 Jan 2020 |  | 37passed, 2 passed with exception | V5.8.1 |
| 67\_网证通安全中间件5.8.1 Win10 64（IE11、Edge） | 升级测试 | V5.8.1 | Win10 64（IE11、Edge） | 19 Jan 2020 |  | 39passed, 2 passed with exception | V5.8.1 |
| 66\_网证通安全中间件5.8.1 Win7 64（IE10、360） | 升级测试 | V5.8.1 | Win7 64（IE10、360） | 19 Jan 2020 |  | 466passed | V5.8.1 |

## 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* | *V5.8.1.0* | *是* | *1* | 1. *NETCA\_CRYPTO\_UI.dll，修复多浏览器管理员权限弹密码框失败的问题。* 2. *NETCA\_URL2.dll，增加HTTPS 2.0的支持，修正TLS1.3因序列号用错导致加密出错的BUG，增加LDAPS的支持。* |

# 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) i5-8400 CPU @ 2.80GHz 2.81GHz 8G |
| PC2: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81GHz 2G |
| PC3: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz 3.19GHz 8G |
| PC4: Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz 3.19GHz 8G |
| PC操作系统 | XP.SP3, Win7 32, Win7 64, Win10 |
| 浏览器版本 | IE8、IE9、IE10、IE11、Edge、Chrome、Firefox、360 8.1.1 |
| 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/V4.2/网证通安全客户端.exe>  版本：4.2.5.5 |
| 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：5.8.1.0 |
| 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：V4.16 |

## 测试工具

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **来源** | **用途** | **名称** | **版本** | **地址** |
| 外部软件 | 自动化测试工具 | HP Unified Functional Testing | 11.5 | \\192.168.0.8\software\应用软件\QTP |
| Office签名、签名加密邮件 | Office | 2016 | \\192.168.0.8\software\办公软件 |
| PDF签名测试 | Adobe Reader  Adobe Acrobat | 9、10、11、DC | \\192.168.0.8\software\办公软件\Acrobat |
| 内部开发 | 制证安装控件 | NetCaCtl | 2.0.2.0 | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/得安读卡器/NetCaCtl-v2.0.exe |
| 中间件测试例程 | NetcaPKITest.htm | NA | 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 |
| 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 |

# 功能测试结果

共执行用例550个（其中462个为自动化脚本执行，比率：84%），通过546个用例，通过（存在可允错误）4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** |

