# 测试背景

因云认证平台项目需求，首次将江南天安云加密机接入到中间件。本次主要测试云密码机，是否可以正常使用，比如签名、非对称解密、对称加解密等基本功能。测试其运算速度、稳定性、负载等性能。

参考资料：

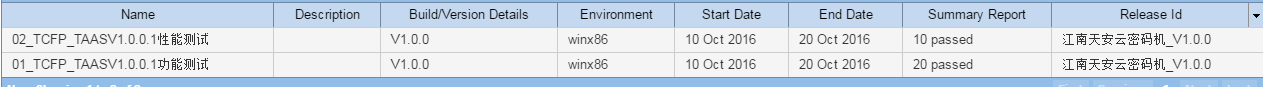
1. 开发提交的测试申请单：http://192.168.0.123:8080/browse/RODT-138
2. 需求文档：

\\192.168.0.8\项目交接资料\001-云认证平台项目资料\003-项目实施\实施参考文档\云认证平台-产品规划方案.docx

# 测试结论

本次测试是Test Case First Pass（简称TCFP），共执行用例30个（20个功能测试用例，10个性能测试用例），Pass 30个用例，通过率为100 %。就提测的内容，评估为测试通过。

RMsis测试集统计结果如下图：



测试总结：

JAVA版时间戳系统配置了云加密机，时间戳签名测试通过：

1. 使用NETCA\_GMTDEMO.exe工具，获取时间戳签名成功；
2. PDF文档中配置默认时间戳服务器后，签名成功；

Windows环境下，配置了云加密机驱动和中间件后，使用CryptotestTool工具测试，签名、对称加解密、非对称加解密等功能测试通过：

1. 使用SM1算法，对称加解密成功；
2. RSA、SM2算法的签名及验证、SignedData签名及验证，数字信封加解密、非对称加解密成功。

连接云加密机测试的JAVA版时间戳服务系统，最佳并发用户数为300：300个并发用户运行8小时，事务执行成功率为100%，平均响应时间为1.499秒。

# 限制条件

1. 仅部署在Java版时间戳服务系统进行了云加密机的应用测试，其他如电子认证网关、业务平台，因开发未提供部署文档，没有进行测试。

# 测试策略

1. 因云加密机是部署到JAVA版时间戳服务系统中，所以选用时间戳服务进行性能测试；
2. 因云加密机是部署到JAVA版时间戳服务系统中，但仅应用到其签名功能，所以在windows测试机上再次部署中间件环境和连接云加密机的配置，使用CryptotestTool工具验证其对称加解密等功能。

# 测试要项

|  |  |  |
| --- | --- | --- |
| **测试对象** | 江南天安云密码机 | |
| **提测版本** | TassVsmSDF.dll（v1.0.0.1） | |
| **生产单位** | 广东省电子商务认证中心 开发部 | |
| **测试单位** | 广东省电子商务认证中心 运维部 | |
| **测试类型** | 功能测试、性能测试 | |
| **测试依据** | 测试申请单：http://192.168.0.123:8080/browse/RODT-138 | |
| **测试用例** | RMsis测试集：  01\_TCFP\_TASSV1.0.0.1功能测试  02\_TCFP\_TASSV1.0.0.1性能测试 | |
| **制证平台&**  **证书模板** | 06系统：<http://192.168.0.28/netca>  证书模板：服务器证书下的TSA项目、ClassBCA内部测试项目  业务平台：<https://192.168.0.59/certbpms>  证书模板：  1，RSA 2048：南方产权s项目下的服务器模板20160601  2，SM2：南方产权s项目下的SM2服务器证书（域名） | |
| **测试环境** | Win7 32：Intel(R) Core(TM) i5-3350P CPU @3.10GHz 3.10GHz 4G内存 | |
| **测试工具** | Adobe reader DC | \\192.168.0.8\software\办公软件\Adobe\_Acrobat\_Reader\Reader DC 2015 |
| Loadrunner11 | \\192.168.0.8\software\tools\测试工具\LoadRunner11 |
| 时间戳获取程序（NETCA\_GMTDEMO.exe） | http://192.168.0.11:8081/svn/rdrelease/测试文档/03\_测试工具/NETCA\_GMTDEMO.exe |
| CryptoTestTool | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/工具/CryptoTestTool.exe |
| **中间件** | [http://192.168.0.11:8081/svn/rdrelease/](qq://txfile/)软件发布/NETCA\_CRYPTO/current/安装包/NETCA\_Crypto.exe （V2.0.11.4） | |
| **时间戳系统** | http://192.168.0.126/NETCATimeStampServer/TSAServer.jsp（V3.1.1） | |
| **部署文档** | <http://192.168.0.11:8081/svn/rdrelease/>软件发布/NETCA\_CRYPTO/current/winX86/设备驱动/江南天安加密机/云加密机/天安云加密机的部署文档.docx | |
| **测试人员** | 彭叶苹 | |
| **测试日期** | 2016-10-10至2016-10-20 | |

# 测试结果

## 功能测试

本次测试是Test Case First Pass（简称TCFP），共执行用例20个，passed 20个,通过率为100%。测试结果文件格式如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Run Name**  **测试集名称** | **Test Case ID**  **测试用例编号** | **Test Case Name**  **测试用例名称** | **Test Case Status**  **用例结果** | **Artifact ID**  **缺陷编号** | **Artifact Summary**  **缺陷主题** | **Artifact Priority**  **缺陷优先级** |



## 性能测试

本次测试是Test Case First Pass（简称TCFP），共执行用例10个，passed 10个,通过率为100%。测试结果文件格式如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Run Name**  **测试集名称** | **Test Case ID**  **测试用例编号** | **Test Case Name**  **测试用例名称** | **Test Case Status**  **用例结果** | **Test Case Comments**  **详细的性能数据** |



详细的性能测试数据，表格形式如下面的两个表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **测试项** | **运行时长**  **（分钟）** | **最小响应时间（秒）** | **最大响应时间（秒）** | **平均响应时间（秒）** |
| 1\_10用户 | 10 | 0.44 | 4.051 | 0.063 |
| 2\_20用户 | 15 | 0.048 | 3.661 | 0.115 |
| 3\_30用户 | 20 | 0.048 | 2.228 | 0.17 |
| 4\_50用户 | 30 | 0.051 | 4.185 | 0.271 |
| 5\_200用户 | 10 | 0.054 | 2.53 | 0.97 |
| 6\_400用户 | 10 | 0.05 | 3.133 | 1.539 |
| 7\_500用户 | 10 | 0.054 | 5.007 | 1.82 |
| 8\_310用户 | 30 | 0.05 | 3.486 | 1.472 |
| 9\_300用户 | 30 | 0.05 | 3.078 | 1.425 |
| 10\_300用户的稳定性测试 | 480 | 0.05 | 7.794 | 1.499 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **测试项** | **事务总数（条）** | **成功事务数（条）** | **失败事务数（条）** | **中断事务数（条）** | **事务执行成功率** | **平均响应时间（秒）** |
| 1\_10用户 | 95273 | 95273 | 0 | 0 | 100.00% | 0.063 |
| 2\_20用户 | 156548 | 156544 | 0 | 4 | 100.00% | 0.115 |
| 3\_30用户 | 211985 | 211983 | 0 | 2 | 100.00% | 0.171 |
| 4\_50用户 | 333565 | 333561 | 0 | 4 | 100.00% | 0.271 |
| 5\_200用户 | 131974 | 131971 | 0 | 3 | 100.00% | 0.97 |
| 6\_400用户 | 148460 | 146507 | 1951 | 2 | 98.68% | 1.539 |
| 7\_500用户 | 158614 | 154334 | 4279 | 1 | 97.30% | 1.82 |
| 8\_310用户 | 387527 | 387301 | 216 | 10 | 99.94% | 1.472 |
| 9\_300用户 | 391589 | 391589 | 0 | 0 | 100.00% | 1.425 |
| 10\_300用户的稳定性测试 | 5775424 | 5775424 | 0 | 0 | 100.00% | 1.499 |

分析：

从上面2个表可知，整体趋势是平均响应时间随着用户数的增多而增加。在用户数是400、500时，并发时有失败响应记录，事务执行成功率均低于99%。降低用户数为310，仍有失败记录；降低用户数至300，事务执行成功率为100%，平均响应时间1.499秒，满足时间戳签名实际需求。

# 参考文档

JAVA版时间戳服务系统V3.1.1的测试报告：

<http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCASERVER/NETCATimeStampServer/Java版/测试报告/JAVA版TOMCAT7服务器时间戳服务V3.1.1测试报告20160203.doc>