# 测试背景

为了云认证平台项目，江南天安云加密机10月已完成远程访问测试，现将云加密机设备部署到我司，并接入到中间件，进行本地测试。本次主要回归测试云密码机签名、非对称解密、对称加解密等基本功能是否正常，并回归测试其运算速度、稳定性、负载等性能，以验证本地实测云加密机与远程访问云加密机的测试结果是否有差异。

参考资料：

1. 测试申请单：http://192.168.0.123:8080/browse/RODT-190
2. 需求文档：
3. [\\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](file:///\\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)
4. http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南天安加密机/云密码机/

# 测试结论

本次测试是Test Case First Pass（简称TCFP），共执行用例18个（14个功能测试用例，4个性能测试用例），Pass 16个用例，pass with exception 2个用例，通过率为100%。发现2个bug，缺陷率为11.11%，厂家未修复bug，故最终缺陷率仍为11.11%。问题详见[章节9](#_问题列表)。就测试的内容，评估为测试**限制性通过**。

RMsis测试集统计结果如下图：



测试总结：

1. 云加密机一台VSM的管理工具可产生64对RSA算法密钥（RSA1024或RSA2048），及64对SM2算法密钥，管理工具限制只能输入1-64的索引号，如果RSA算法和SM2算法使用同一个索引号，会导致修改密钥对密码失败（TASS-4），因此考虑到密钥密码安全性，一台VSM的管理工具现只能支持64对密钥（可混合不同密钥算法），而不是厂家宣称的“64对RSA算法+64对SM2算法”，故测试**限制性通过**；
2. 云加密机目前管理工具不支持ECC及RSA4096算法（TASS-5），故测试**限制性通过**；
3. 连时间戳应用、签名、对称加解密、非对称加解密等功能测试通过；
4. 连接本地云加密机测试JAVA版时间戳服务系统，与远程访问加密机测试相比，总体性能结果相对较好。[平均响应时间，对于相同并发数，本地访问耗时大部分比远程访问耗时少；而且400并发本地成功率更高（本地测试99%以上，远程访问99%以下）]，测试通过；
5. 连接本地云加密机RSA2048执行1w次，平均签名速度约为3.7755ms/次（厂家提供的签名速度为0.143ms/次）。

# 限制条件

1. 本次测试是基于公司内网测试，仅对部署在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。
2. 由于江南天安云加密机VSM集群尚未调通，故本次不涉及测试集群相关用例。
3. 对于第2章第5点RSA2048签名测速结果，开发提供的测速工具属于串行测试工具；厂家只提供相关性能参数，并未提供测试环境条件及测试说明，因此本测试未能证实厂家的参数。。

# 测试策略

1. 本次测试主要回归远程访问云加密机的测试用例，以确认本地实测与远程访问云加密机的功能性能上的差异，对于云加密机集群相关测试，在此处暂不涉及。
2. 由于加密机密钥最常用到的是签名功能，故在远程访问云加密机回归用例基础上，增加密钥签名速度测试。
3. 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。

# 参考文档

1. 远程测试云加密机V1.0.0.1测试报告：

http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/安全中间件测试报告/江南天安云加密机V1.0.0.1TCFP测试报告20161020（远程）.docx

1. JAVA版时间戳服务系统V3.1.1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>

# 测试要项

|  |  |
| --- | --- |
| **测试对象** | 江南天安云密码机 |
| **提测版本** | VSM服务（HS0.02.12）  TassVsmSDF.dll（v1.0.0.1） |
| **生产单位** | 江南天安、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-190 |
| **测试用例** | RMsis测试集：  05\_TCFP\_TASS测试（本地） |
| **测试人员** | 孙玉洁 |
| **测试日期** | 2016-12-5至2016-12-6 |

# 测试环境

## 测试环境

|  |  |  |
| --- | --- | --- |
| **#** | **设备** | **信息** |
| 时间戳服务器 | 虚拟机 | 1. CPU：2个；内存：6.1G；硬盘:200G 2. 操作系统：64位redhat 6.4 3. JVM version： 1.7.0\_60   4，所在实体机配置:2\*INTEL 至强E5-2630 V3 2.4G\6\*8G RDIMM DDR4-2133\6\*600G SAS 10K RPM 2.5寸硬盘\PERC H730P RAID控制器/2G缓存； 3，操作系统： win2012R2标准版 64位 |
| 云加密机主机 | 实体机 | 1，CPU： E5-2630V3 X 2，内存:16GB X 4，加密卡SJK1322 X 4 |
| 客户机 | Win7 32 | AMD FX(tm)-4100Quad-Core Processor 2.75GHz |
| Win7 64 | Intel(R)CORE（TM） i7-6700 CPU @3.4Ghz 3.4Ghz 8GB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 |
| 测试签名速度工具 | http://192.168.0.11:8081/svn/rdrelease/测试文档/03\_测试工具/云加密机性能工具/签名及非对称解密测速工具.exe |
| VSM管理工具  VsmManager\_Unified\_1.2.2.1 | http://192.168.0.11:8081/svn/rdrelease/软件发布/证书介质/驱动及开发包/江南天安加密机/云密码机/云加密机管理工具及手册.zip |

# 测试结果

## 测试结果

本次测试是Test Case First Pass（简称TCFP），共执行用例18个（14个功能测试用例，4个性能测试用例），Pass 16个用例，pass with exception 2个用例，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**  **详细数据备注** | **Artifact ID**  **缺陷编号** | **Artifact Summary**  **缺陷主题** | **Artifact Priority**  **缺陷优先级** |



## 测试数据

本地加密机性能测试结果与远程加密机测试数据情况如下：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 备注 | 测试用例 | 成功数/次 | 失败数/次 | 成功率 | 平均响应时间/s | 最大响应时间/s | 最小响应时间/s | 平均吞吐量(byte/s) |
| 1 | 本地测试 | 1\_200users\_10min | 257329 | 0 | 100% | 0.191 | 1.782 | 0.016 | 1577445.375 |
| 2 | 240603 | 15 | 99.99% | 0.219 | 2.359 | 0.016 | 1573276.375 |
| 3 | 远程访问 | 131971 | 0 | 100% | 0.97 | 2.53 | 0.054 | / |
| 4 | 本地测试 | 2\_400users\_10min | 252693 | 1195 | 99.53% | 0.41 | 4.211 | 0.017 | 1517771.813 |
| 5 | 285744 | 1126 | 99.61% | 0.305 | 2.483 | 0.016 | 1571191.875 |
| 6 | 远程访问 | 146507 | 1953 | 98.68% | 1.539 | 3.133 | 0.05 | / |
| 7 | 本地测试 | 3\_300users\_8h | 7416097 | 523 | 99.99% | 1.874 | 79.385 | 0.016 | 1132808.266 |
| 8 | 远程访问 | 5775424 | 0 | 100% | 1.499 | 7.794 | 0.05 | / |

# 问题列表

发现2个bug，缺陷率为11.11%。

