# 测试背景

为了云认证平台项目，江南天安云加密机2016年10月已完成远程访问测试，2016年12月进行本地测试（把一台云加密主机部署到我司，并接入我司中间件）。后者测试分为两个阶段，第一阶段为单个VSM环境，第二阶段为集群VSM环境。第一阶段测试情况已出[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20161207（本地单个VSM）.docx)，测试结果为限制性通过。现在进行第二阶段测试，验证云加密机签名、非对称解密、对称加解密等基本功能是否正常，并验证其运算速度、稳定性、负载等是否正常，云加密机集群VSM与单个VSM的性能对比，以及云加密机与江南天安加密机SJJ1507实体机的性能对比。

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 Run（简称TCFR），共执行用例34个（7个功能测试用例，27个性能测试用例），通过15个，通过存在可允错误15个，失败4个，通过率为88.2%。发现8个bug，缺陷率为23.5%，厂家未修复bug，故最终缺陷率仍为23.5%。Bug问题详见[章节9](#_问题列表)。测试详细情况详见[章节8](#_测试结果)。就测试的内容，功能测试评估为**限制性通过**，性能测试**不通过**。

RMsis测试集统计结果如下图：



## 功能

**测试结论：限制性通过。**

1. **一台云加密机主机支持32台VSM虚机，每台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”（TASS-4）；
2. 云加密机管理工具**不支持ECC算法**（TASS-5，可支持RSA1024、RSA2048、RSA4096及及SM2算法）；
3. 云加密机控制中心，VSM的**CPU占比无法显示正确数据**（TASS-6）。VSM重启关机**有时会报错**，重新操作后可正常关机（TASS-11）；
4. 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。

## 性能

**测试结论：不通过。**

1. 云加密机单VSM签名速度为SJJ1507实体机的**一半**（TASS-10）；
2. 集群VSM总体性能**不如**单个VSM性能**好**（TASS-8，TASS-11）；
3. 使用我司内部工具验证厂家提供的参数，**大部分无法达到厂家的速度水平**（只有RSA产生密钥对速度高于厂家水平，其余参数均低于厂家水平）。我司测试环境与厂家测试环境详见[第3.3章节](#_测试环境_1)：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | **RSA1024** | | | **RSA2048** | | | **SM2** | | |
| 我司工具 | 厂家参数 | 我司：厂家 | 我司工具 | 厂家参数 | 我司：厂家 | 我司工具 | 厂家参数 | 我司：厂家 |
| **产生密钥对速度(对/s)** | 85 | 5 | 快1600% | 12 | 1 | 快1100% | 1666 | 7000 | 慢76% |
| **签名(次/s)** | 876 | 2000 | 慢56% | 281 | 400 | 慢30% | 1504 | 3000 | 慢50% |
| **非对称解密(次/s)** | 858 | 2000 | 慢57% | 277 | 400 | 慢31% | 833 | 1100 | 慢24% |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | **SM1-ECB加密（Mbps）** | | | **SM1-ECB解密（Mbps）** | | | **SM1-CBC加密（Mbps）** | **SM1-CBC解密（Mbps）** |
| 我司  工具 | 厂家参数 | 我司：厂家 | 我司  工具 | 厂家参数 | 我司：厂家 | 我司工具 | 我司工具 |
| **100K** | 3.68 | 15 | 慢75% | 3.56 | 15 | 慢76% | 3.46 | 3.48 |
| **50K** | 3.66 | 15 | 慢76% | 3.45 | 15 | 慢77% | 3.34 | 3.66 |
| **10K** | 3.22 | 15 | 慢79% | 3.32 | 15 | 慢78% | 3.52 | 3.75 |

1. 不同VSM同一密钥算法的签名速度**基本一致**，同一VSM同一算法不同密钥对的签名速度**基本一致。**但**180VSM除外，其**重启后签名速度下降一半，多次重启，没有重现重启前的速度，其重启后的签名速度与其他VSM基本一致。（厂家初步确定VSM算法芯片可能有问题，具体原因尚在定位。TASS-9，180VSM是由江南天安实体机SJJ1507执行密钥备份到云加密机的VSM，其他VSM是在云加密机中直接创建密钥的VSM）。

# 限制条件

## 云加密机限制

1. 容量：一台云加密机主机最多包含32台VSM虚机。
2. 热备：一台主机的VSM与VSM之间无法热备（当VSM故障，密钥不会自动漂移到另外一台VSM），只能主机与主机之间才能进行热备。由于目前只有一台主机，无法测试热备情况。
3. 负载均衡：厂家提供云加密机负载均衡工具，以达到VSM集群的目的（此处集群，仅指提前将一台VSM的密钥同步到其他VSM后利用工具进行负载均衡，集群组内的每个VSM中密钥要保持一致。若集群组中的某VSM故障，应用可使用集群组内的其他VSM），但受云加密机负载均衡工具限制，每个集群组最大支持10台VSM（即一个应用最多使用10台VSM进行负载）。

## 工具限制

1. 我司提供的签名测试并行工具，最大连接数为1500。超过1500个连接数，工具会报错。受此限制，用我司工具只测试到最大连接数1500的情况。
2. 我司Loadrunner破解版工具，只支持1w个用户并发。超过1w个并发，工具会报错。受此限制，用Loadrunner只测试到最大并发1w的情况。

## 测试环境限制

1. 我司工具由开发部提供，与中间件对接，在一台客户机对云加密机主机进行测试；厂家提供的性能参数的测试环境，是在一台配置比云加密机性能高的服务器上，部署多个客户端对云加密机进行压力测试。
2. 厂家没有提供SM1-CBC加解密的性能参数，故无对比数据。

## 应用限制

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. 厂家的管理工具宣称支持产生RSA4096算法密钥，但受限于我方底层驱动尚未支持，无法测试RSA4096算法相关用例。

# 测试策略

1. 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工具验证功能。

# 参考文档

1. 本地单个VSM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20161207（本地单个VSM）.docx

# 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）  VSM管理工具V1.2.2.7 |
| **生产单位** | 北京江南天安科技有限公司（云加密机等）  广东省电子商务认证中心开发部（中间件） |
| **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：  06\_\_TCFR\_TASS集群测试（本地） |
| **测试人员** | 孙玉洁 |
| **测试日期** | 2016-12-7至2016-12-12 |

# 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；操作系统： win2012R2标准版 64位 |
| 云加密机主机 | 实体机 | 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 |
| 测试签名及非对称解密速度工具（串行） | 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 |
| 测试签名与非对称解密速度工具（并行） | <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/MultThread_RSAOperation.exe>  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/MultThread\_SM2Operatian.exe |
| 测试SM1-ECB对称加解密工具 | 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/MultThread\_SM1ECB.exe |
| 测试SM1-CBC对称加解密工具 | 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/MultThread\_SM1CBC.exe |
| 测试产生密钥对速度工具（并行） | <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/MultThread_GenerateRSA1024Keypair.exe>  <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/MultThread_GenerateRSA2048Keypair.exe>  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/MultThread\_GenerateSM2Keypair.exe |
| VSM管理工具  VsmManager\_Unified\_1.2.2.7 | 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/VsmManager\_1.2.2.7.zip |
| 云加密机控制中心 | 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34个（7个功能测试用例，27个性能测试用例），通过15个，通过存在可允错误15个，失败4个，通过率为88.2%。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** |



## 概述

### 功能情况

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”；
2. 云加密机管理工具**不支持ECC算法**（TASS-5，可支持RSA1024、RSA2048、RSA4096及及SM2算法）；
3. 云加密机控制中心，VSM的**CPU占比无法显示正确数据**（TASS-6）。VSM重启关机**有时会报错**，重新操作后可正常关机（TASS-11）；
4. 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。

### 性能情况

1. **云加密机单VSM签名速度为SJJ1507实体机的一半**（TASS-10）；
2. **集群VSM总体性能不如单个VSM性能好**；
3. 利用我司工具进行1500并发以及时间戳应用进行3000并发测试，集群性能与单个VSM性能基本**相同**；但利用时间戳应用进行1w并发测试，集群性能比单个VSM性能**差**（TASS-11）；我司工具及loadrunner最大连接数的限制条件，详见[第3.2章](#_工具限制_1)。
4. 长期压测后，集群VSM性能会下降（TASS-8）；

说明：时间戳进行3000等并发各10min后，重启集群VSM，400并发成功率在99%以上，平均响应时间约0.3s。不重启VSM执行400并发，成功率在99%以下，平均响应时间约3.1s，时长为重启VSM后的10倍。

1. **使用我司内部工具验证厂家提供的参数，大部分无法达到厂家的速度水平。**

说明：只有RSA产生密钥对速度高于厂家水平，其余参数均低于厂家水平。（我司测试环境与厂家测试环境详见[第3.3章节](#_测试环境_1)）。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | **RSA1024** | | | **RSA2048** | | | **SM2** | | |
| 我司工具 | 厂家参数 | 我司：厂家 | 我司工具 | 厂家参数 | 我司：厂家 | 我司工具 | 厂家参数 | 我司：厂家 |
| 产生密钥对速度(对/s) | 85 | 5 | 快1600% | 12 | 1 | 快1100% | 1666 | 7000 | 慢76% |
| 签名(次/s) | 876 | 2000 | 慢56% | 281 | 400 | 慢30% | 1504 | 3000 | 慢50% |
| 非对称解密(次/s) | 858 | 2000 | 慢57% | 277 | 400 | 慢31% | 833 | 1100 | 慢24% |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | **SM1-ECB加密（Mbps）** | | | **SM1-ECB解密（Mbps）** | | | **SM1-CBC加密（Mbps）** | **SM1-CBC解密（Mbps）** |
| 我司  工具 | 厂家参数 | 我司：厂家 | 我司  工具 | 厂家参数 | 我司：厂家 | 我司工具 | 我司工具 |
| 100K | 3.68 | 15 | 慢75% | 3.56 | 15 | 慢76% | 3.46 | 3.48 |
| 50K | 3.66 | 15 | 慢76% | 3.45 | 15 | 慢77% | 3.34 | 3.66 |
| 10K | 3.22 | 15 | 慢79% | 3.32 | 15 | 慢78% | 3.52 | 3.75 |

1. **除180VSM（说明见下，**TASS-9**），不同VSM同一密钥算法的签名速度基本一致,同一VSM同一算法不同密钥对的签名速度基本一致；**

说明：180VSM是由江南天安实体机SJJ1507执行密钥备份到云加密机的VSM，191VSM是在云加密机中直接创建密钥的VSM中的其中一个代表。180VSM执行密钥备份后未经过重启直接测签名速度，其速度是191VSM的2倍, 未重启前一直重现；180VSM重启后，速度与191VSM基本一致，目前多次重启，180VSM速度均与191等VSM速度基本一致，没有重现重启前的速度。 （厂家初步确定VSM的算法芯片可能有问题，一台云加密机32台VSM使用了一样的算法芯片。）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **算法** | **签名(次/s)** | | | | |
|  |  |  |  | ①：②：③：④ |
| SJJ1507 | 180VSM首测速度未重启前 | 180VSM重启后 | 191VSM |
| **RSA1024** | 1871 | 1612 | 874 | 883 | 1：0.9：0.5：0.5 |
| **RSA2048** | 607 | 614 | 275 | 281 | 1：1：0.5：0.5 |
| **SM2** | 2698 | 2372 | 1594 | 1504 | 1：0.9：0.6：0.6：0.6 |

## 测试数据

### 图表

一、下图图1-3分别表示利用时间戳应用在单VSM及集群VSM的情况下压测的成功率，测试结果显示：

1，单个VSM以及集群VSM情况下，随着并发量增多，成功率会逐渐降低。

2，集群VSM与单个VSM在3000并发下的性能情况基本相同，但在1w并发下，集群VSM的成功率比单个VSM低。

图1：

图2： 图3：

二、下图图4-6分别表示利用时间戳应用在单VSM及集群VSM的情况下压测的平均响应时间，测试结果显示：

1，单个VSM，随着并发量增多，平均响应时间逐渐增加。

2，集群VSM，随着并发量增多，平均响应时间呈现不稳定现象。

3，集群VSM与单个VSM在3000并发下的平均响应时长情况基本相同，但在1w并发下，集群VSM的响应时长比单个VSM更长（图4列出执行400并发前重启VSM前后的2种情况）。

图4：

图5： 图6：

### 数据

本地一台加密机中，单个VSM与集群VSM（10台VSM）性能测试结果如下：

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | VSM类别 | VSM开启情况 | 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) | CPU备注说明 |
| 1 | 单个VSM |  | 1\_200users\_10min  （1s进5个用户） | 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 | 单个VSM |  | 2\_300users\_8h  （1s进5个用户） | 7416097 | 523 | 99.99% | 1.874 | 79.385 | 0.016 | 1132808.266 |  |
| 4 | 单个VSM |  | 3\_400users\_10min  （1s进5个用户） | 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 | 集群  VSM | 10台集群VSM及  22台没用到的VSM全开 | 161316 | 1850 | 98.87% | 3.111 | 63.09 | 0.006 | 654011.875 |  |
| 7 | 集群VSM | 10台集群VSM（执行前全部重启）及  22台没用到的VSM全开 | 373054 | 917 | 99.75% | 0.285 | 2.748 | 0.039 | 2262445.187 |  |
| 8 | 集群  VSM | 10台集群VSM及  22台没用到的VSM全开 | 4\_500users\_10min  （1s进5个用户） | 213439 | 3063 | 98.59% | 1.646 | 25.603 | 0.03 | 908328.5 |  |
| 9 | 集群  VS | 10台集群VSM及  22台没用到的VSM全开 | 5\_760users\_10min  （1s进5个用户） | 230720 | 7334 | 96.92% | 1.892 | 41.922 | 0.117 | 1650515.812 |  |
| 12 | 单个VSM | 单个VSM及  除10台集群外的22台没用到的VSM全开 | 6\_3000users\_10min  （1s进20个用户） | 336993 | 51258 | 86.80% | 1.527 | 20.321 | 0.085 | 1075771.656 | 1台VSMcpu占用约40%  其他VSMCPU为1% |
| 11 | 集群  VSM | 10台集群VSM及  22台没用到的VSM全开 | 292995 | 51914 | 84.95% | 1.342 | 36.662 | 0.045 | 1425446.531 | 每台VSMcpu占用约15%  其他VSMCPU为1% |
| 13 | 单个VSM | 单个VSM及  除10台集群外的22台没用到的VSM全开 | 7\_5000users\_10min  （1s进20个用户） | 262189 | 45631 | 85.18% | 1.705 | 27.579 | 0.115 | 1381686.813 | 1台VSMcpu占用约40%  其他VSMCPU可升至1% |
| 14 | 单个VSM | 单个VSM（执行前重启）及  除10台集群外的22台没用到的VSM全开 | 8\_10000users\_3min  （1s进20个用户） | 412967 | 166421 | 71.28% | 1.986 | 45.984 | 0.025 | 612582.438 | 1台VSMcpu占用约70%  其他VSMCPU可升至1% |
| 15 | 集群VSM | 10台集群VSM（执行前全部重启）及  22台没用到的VSM全开 | 158526 | 214681 | 42.48% | 11.619 | 110.154 | 0.077 | 541318.594 | 每台VSMcpu占用约5%  其他VSMCPU可升至2% |

# 问题列表

发现8个bug，缺陷率为23.5%，厂家未修复bug，故最终缺陷率仍为23.5%。

