修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 日期 | 修订版本 | 修改描述 | 作者 |
| 2023-11-7 | V1.0 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1. 概述 4](#_Toc22350)

[1.1. 编写目的 4](#_Toc31108)

[1.2. 项目背景 4](#_Toc22900)

[1.3. 参考资料 4](#_Toc15130)

[2. 测试概要 4](#_Toc21048)

[2.1. 测试环境 4](#_Toc22367)

[2.2. 测试步骤 4](#_Toc11353)

[3. 测试方法 7](#_Toc29771)

[3.1. 接口基本功能测试 7](#_Toc11071)

[3.2. ShareMemory测试 7](#_Toc28599)

[3.3. 多Session测试 8](#_Toc25928)

[3.4. 基本异常情况测试 8](#_Toc32479)

[3.5. Client挂掉测试 9](#_Toc14759)

[3.6. 单接口性能测试 10](#_Toc20306)

[3.7. RSA签名测试 10](#_Toc26173)

[3.8. 基本功能长稳测试 10](#_Toc23531)

[3.9. VM功能测试用例 10](#_Toc17666)

[3.10. VM性能测试用例 11](#_Toc32520)

[3.11. Sec驱动用例 11](#_Toc13825)

[3.12. 零拷贝 11](#_Toc21286)

[3.13. 安全存储demo 13](#_Toc8695)

[3.14. switchless可靠性测试 13](#_Toc15736)

[4. 测试结果 14](#_Toc8970)

[4.1. 接口基本功能测试结果 14](#_Toc6722)

[4.2. ShareMemory测试结果 14](#_Toc3137)

[4.3. 多session测试 15](#_Toc251)

[4.4. 基本异常情况测试 15](#_Toc3484)

[4.5. Client挂掉测试结果 15](#_Toc1661)

[4.6. 单接口性能测试结果 16](#_Toc25082)

[4.7. RSA签名测试结果 16](#_Toc21974)

[4.8. 基本长稳测试结果 16](#_Toc7477)

[4.9. VM功能测试用例 16](#_Toc31859)

[4.10. VM性能测试用例 17](#_Toc9242)

[4.11. 零拷贝 18](#_Toc27828)

[4.12. Sec驱动用例 19](#_Toc25896)

[4.13. 安全存储demo 20](#_Toc4662)

[4.14. switchless可靠性测试 20](#_Toc24635)

TrustZone感知的机密虚拟机众智项目-一期系统自测报告

# 概述

本文档介绍了TrustZone感知的机密虚拟机众智项目-一期的测试结果

## 编写目的

本测试报告为TrustZone机密计算资源池化系统的自测试报告，目的在于总结测试阶段的测试以及分析测试结果，描述系统是否符合需求。

## 项目背景

本项目为机密计算资源池化技术的实现，满足虚拟化或docker场景下更便利地使用TrustZone特性的安全需求。

## 参考资料

TrustZone感知的机密虚拟机众智项目一期项目测试验收策略。

# 测试概要

本次测试主要包括接口基本功能测试、ShareMemory测试、多Session测试、基本异常情况测试、Client挂掉测试、单接口性能测试、RSA 签名测试、单客户端多session并发测试、多客户端多session并发测试、基本功能长稳测试、VM功能测试、安全存储demo测试。

## 测试环境

Host端：Kunpeng服务器（openEuler 22.03、20.03）

**VM** 端：Kunpeng服务器虚拟机（openEuler22.03、20.03）

## 测试步骤

根据部署手册分别部署好上述测试环境

Host运行vtz\_proxy与teecd

sudo /usr/bin/vtz\_proxy

sudo /usr/bin/teecd

基本功能测试

1. 进入VM测试环境
2. 根据《Kunpeng BoostKit 23.0.RC2 机密计算TrustZone套件 特性指南 01》签名cofig并编译测试用例testcase1、rsa\_demo、secstorage\_demo、secgear\_switchless
3. 执行sudo /vendor/bin/testcase1 1
4. 打印数据、日志文件即为测试结果

ShareMemory测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 2
3. 打印数据、日志文件即为测试结果

多session测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 3
3. 打印数据、日志文件即为测试结果

基本异常情况测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 4
3. 打印数据、日志文件即为测试结果

Client 挂掉测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 5
3. 打印数据、日志文件即为测试结果

单接口性能测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 6
3. 执行sudo /vendor/bin/testcase1 7
4. 执行sudo /vendor/bin/testcase1 8
5. 分别记录打印出的单接口平均运行时间,与host单接口性能进行对比

RSA 签名测试

1. 进入VM测试环境
2. 执行sudo /vendor/bin/testcase1 9
3. 打印数据、日志文件即为测试结果

基本功能长稳测试

1. 进入VM测试环境
2. 进入文件 testcase1/testcase.h中
   * + 1. 将testcase.h中的THREAD\_COUNT设置为10
       2. 将testcase.h中的TEST\_TIME设置为60 \* 60 \* 24
       3. 重新编译testcase
3. 执行sudo /vendor/bin/testcase1 3
4. 打印数据、日志文件即为测试结果

VM功能测试用例

1. 进入VM测试环境
2. 在VM1,VM2中同时运行testcase

VM性能测试用例

1. 进入VM测试环境
2. 基于itrust\_sdk, 编写TA/CA测试程序调用RSA-4096加解密函数
3. 分别在host侧和VM内运行TA/CA测试程序记录接口函数调用时间t1,t2
4. 基于switchless, 编写TA/CA测试程序调用RSA-4096加解密函数
5. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2

SEC驱动用例

1. 进入VM测试环境
2. CA发起salt长度分别为1、32、255、1023，密钥长度64的huk密钥派生请求；
3. CA发起salt长度64，密钥长度16、32、255、4096、4097的huk密钥派生。
4. TA内开启多个线程，每个线程发起100次盐1023和密钥512长度的GP接口调用，线程数128。

安全存储demo

1. 进入VM测试环境
2. 在VM中运行 /vendor/bin/secstorage\_demo
3. 打印数据、日志文件即为测试结果

switchless可靠性测试

1. 进入VM测试环境
2. 在VM中运行 /vendor/bin/secgear\_switchless，连续24h调用
3. 打印数据、日志文件即为测试结果

# 测试方法

## 接口基本功能测试

|  |  |  |
| --- | --- | --- |
| 测试编号 | 测试名 | 测试方法 |
| Interface\_Function-001 | TEEC\_InitializeContext功能测试 | 调用TEECC\_InitializeContex判断返回值是否为true |
| Interface\_Function-002 | TEEC\_OpenSession功能测试 | 调用TEECC\_OpenSession判断返回值是否为true |
| Interface\_Function-003 | TEEC\_InvokeCommand功能测试 | 调用TEECC\_InvokeCommand分别采用 1、不传递参数 2、参数传递采用值传递 3、参数传递采用tmp\_buf的方法进行测试判断返回值是否为true |
| Interface\_Function-004 | TEEC\_CloseSession功能测试 | 调用TEECC\_CloseSession |
| Interface\_Function-005 | TEEC\_FinalizeContext功能测试 | 调用TEECC\_FinalizeContext |

## ShareMemory测试

|  |  |  |
| --- | --- | --- |
| Interface\_Function-006 | TEEC\_AllocateSharedMemory功能测试 | 调用TEECC\_AllocateSharedMemory接口判断返回值是否为true |
| Interface\_Function-011 | TEEC\_InvokeCommand功能测试2 | 调用share\_mem\_test函数进行测试 |
| Interface\_Function-008 | TEEC\_ReleaseSharedMemory功能测试 | 调用TEECC\_ReleaseSharedMemory接口 |
| Interface\_Function-007 | TEEC\_RegisterSharedMemory功能测试 | 调用TEECC\_RegisterSharedMemory接口判断返回值是否为true |
| Interface\_Function-012 | TEEC\_InvokeCommand功能测试3 | 1. 调用share\_mem\_test函数 2、调用TEECC\_ReleaseSharedMemory |

## 多Session测试

|  |  |  |
| --- | --- | --- |
| Interface\_Function-010 | 接口并发调用测试 -- 多Session | 创建多个线程，调用thread\_function |

## 基本异常情况测试

|  |  |  |
| --- | --- | --- |
| Interface\_Exception\_001 | TEEC\_InitializeContext异常测试 | TEECC\_InitializeContext接口传入context指针为空 |
| Interface\_Exception\_002\_1 | TEEC\_OpenSession异常测试 | TEECC\_OpenSession 接口传入context指针为空 |
| Interface\_Exception\_002\_2 | 调用TEECC\_OpenSession 接口，传入 session 指针为空 |
| Interface\_Exception\_002\_3 | 调用TEECC\_OpenSession 接口， 传入TEST\_CASE\_UID 指针为空， |
| Interface\_Exception\_002\_4 | 调用TEECC\_OpenSession 接口，ta\_path指向TA2（ta\_path=TEST\_CASE\_TA\_PATH），其中TA2 没有测试CA执行权限 |
| Interface\_Exception\_002\_5 | 调用 TEECC\_OpenSession 接口，传入TEST\_CASE\_U UID 指向 不存在的TA路径（ta\_path = not\_found.sec） |
| Interface\_Exception\_003\_1 | TEEC\_InvokeCommand 异常测试 | 调用TEECC\_InvokeCommand 接口传入 session 指针为空 |
| Interface\_Exception\_003\_2 | 调用TEECC\_InvokeCommand， 构造非法session（使session\_id++） |
| Interface\_Exception\_003\_3 | 调用TEECC\_InvokeCommand， 传入 operation指针为空 |
| Interface\_Exception\_003\_4 | 调用TEECC\_InvokeCommand， operation 参数带一个未初始化的TEEC\_SharedMemory |
| Interface\_Exception\_003\_5 | 调用TEECC\_InvokeCommand， 要求传入 returnOrigin 指针为空 |
| Interface\_Exception\_004 | TEEC\_CloseSession 异常测试 | 调用TEECC\_CloseSession 接口传入的session 指针为空 |
| Interface\_Exception\_005 | TEEC\_FinalizeContext 异常测试 | 调用TEECC\_FinalizeContext 接口传入的session 指针为空 |

## Client挂掉测试

|  |  |  |
| --- | --- | --- |
| CA\_KILL\_Test\_001 | Client挂掉测试 | 调用TEECC\_InitializeContext与TEECC\_OpenSession后退出CA程序 |

## 单接口性能测试

|  |  |  |
| --- | --- | --- |
| Perfermance\_001 | 单接口性能测试 | 将CA部署在VM测试环境中，分别测试CA调用以下接口1000次后获得响应的时间平均值：  TEEC\_InitializeContext  TEEC\_OpenSession  TEEC\_InvokeCommand  对比性能数据 |

## RSA签名测试

|  |  |  |
| --- | --- | --- |
| RsaSign\_001 | RSA签名测试 | 调用接口进行RSA签名 |

## 基本功能长稳测试

|  |  |  |
| --- | --- | --- |
| Interface\_Stability-001 | 基本功能长稳测试 | 两个客户端，每个客户端内部署1个CA/TA，每个CA开10个session（10个thread）。单个session内循环进行签名任务，测试时间不低于24小时。 |

## VM功能测试用例

|  |  |  |
| --- | --- | --- |
| Function-Vm-005 | 验证不同VM内，同个uuid的TA同时加载 | 1. 创建VM1，VM2  3.在VM1,VM2中同时运行testcase、rsa\_demo 、switchless |
| Function-Vm-006 | 验证VM部署下的安全存储存储于该VM下的目录 | 1. 创建VM,启动VM中的rsa\_demo   2. 通过rsa\_demo调用接口secstorage\_create\_file去调用TA侧，传入正确的参数  3. 查看输出结果，查看/var/itrustee/sec\_storage\_data日志信息 |
| Function-Vm-007 | 验证VM部署下的TA日志存储于该VM下的目录 | 1. 创建VM,启动VM中的CA/TA  2. 查看输出结果，VM内和host侧启动tlogcat -f日志信息 |
| Function-Vm-008 | 验证host侧与VM内可同时运行CA/TA应用 | 1. 同时启动VM和host侧中的testcase、rsa\_demo应用 |
| Function-Vm-011 | Switchless功能测试 | 1. VM 运行secGear 测试用例switchless或switchless\_performance |

|  |  |  |
| --- | --- | --- |
| Function-Vm-015 | 验证VM内TA远程证明场景测试 | 1. REE侧虚机被拉起，虚机内radaemon启动，radaemon向raserver进行注册socket通道，raserver与radaemon建立连接；  2. raclient向raserver发起TA证明，携带TA uuid/nonce、虚机名、虚机type等；  3. raserver根据虚机名和虚机type，通过虚机管理命令行获取vmid和虚机名信息，向QTA注册：<vmid,vm-name>;  4. radaemon通过虚机名，找到连接的radaemon,发送: type+虚机名+TA uuid;  5. radaemon ->QTA-report: 用户证明参数+tzdriver获取的vmid;  6. 报告返回：tcmgr -> QTA-report -> radaemon -> raserver |

## **VM性能测试用例**

|  |  |  |
| --- | --- | --- |
| Performance-Vm-001 | 基于itrust\_sdk,使用RSA-4096签名验签性能测试 | 1. 基于itrust\_sdk, 编写TA/CA测试程序rsa\_demo调用RSA-4096加解密函数  2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2 |
| Performance-Vm-002 | 基于switchless,使用RSA-4096签名验签性能测试 | 1. 基于switchless, 编写TA/CA测试程序调用RSA-4096加解密函数  2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2，预期结果1  3. CA发起线程数为：4，TA发起多线程：8 |

## Sec驱动用例

|  |  |  |
| --- | --- | --- |
| functional\_test\_006 | huk密钥派生，salt不同长度测试 | 1、CA发起salt长度分别为1、32、255、1023，密钥长度64的huk密钥派生请求。（TA内申请内存即可）  2、CA发起salt长度64，密钥长度16、32、255、4096、4097的huk密钥派生  3、两次发送相同salt，返回的密钥一致 |
| functional\_test\_009 | huk密钥派生，TA内多线程调用 | 1、TA内开启多个线程，每个线程发起100次盐1023和密钥512长度的GP接口调用，  2、线程测试范围：128 |

## **零拷贝**

|  |  |  |
| --- | --- | --- |
| ZeroCopy\_function\_001 | CA创建Share Memory测试(内存页4K) | 1. REE侧创建share memory 256M |
| ZeroCopy\_function\_002 | CA创建Share Memory测试(内存页64K) | 1. REE侧创建share memory 256M |
| ZeroCopy\_function\_003 | 零拷贝功能测试(内存页64K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2 |
| ZeroCopy\_function\_004 | 零拷贝功能测试(内存页4K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2 |
| ZeroCopy\_function\_005 | 多个CA/TA调用(内存页64K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写2个测试CA/TA, 预期结果2 |
| ZeroCopy\_function\_006 | 多个CA/TA调用(内存页4K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写2个CA/TA, 预期结果2 |
| ZeroCopy\_function\_007 | 多个CA与唯一TA进行通信(内存页4K) | 1、使传参方式为零拷贝模式编写TA/CA测试程序，CA能够fork出多个进程  2、通过系统OS工具绑定多个CA进程至不同核心上 3、观察TA、多个CA测试程序运行情况 |
| ZeroCopy\_function\_008 | 多个CA与唯一TA进行通信(内存页64K) | 1、使传参方式为零拷贝模式编写TA/CA测试程序，CA能够fork出多个进程  2、通过系统OS工具绑定多个CA进程至不同核心上 3、观察TA、多个CA测试程序运行情况 |
| ZeroCopy\_function\_009 | CA多线程调用(内存页4K) | 1、CA开启多线程，每个线程开一个session，发送100次1M（基于支持的最大值）长度的请求  2、线程数测试范围：20.  3、获取支持的最大线程数 |
| ZeroCopy\_function\_010 | CA多线程调用(内存页64K) | 1、CA开启多线程，每个线程开一个session，发送100次1M（基于支持的最大值）长度的请求  2、线程数测试范围：20.  3、获取支持的最大线程数 |

## **安全存储demo**

|  |  |  |
| --- | --- | --- |
| Function-Vm-001 | 验证CMD\_SECSTORAGE\_CREATE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageCreateFile去调用TA侧，传入正确的参数 |
| Function-Vm-002 | 验证CMD\_SECSTORAGE\_DELETE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageDeleteFile去调用TA侧，传入正确的参数 |
| Function-Vm-003 | 验证CMD\_SECSTORAGE\_READ\_FILE接口功能是否正常 | 通过CA调用接口SecstorageReadFile去调用TA侧，传入正确的参数 |
| Function-Vm-004 | 验证CMD\_SECSTORAGE\_RENAME\_FILE接口功能是否正常 | 通过CA调用接口SecstorageRenameFile去调用TA侧，传入正确的参数 |
| Function-Vm-005 | 验证CMD\_SECSTORAGE\_SEEK\_FILE接口功能是否正常 | 通过CA调用接口SecstorageSeekFile去调用TA侧，传入正确的参数 |
| Function-Vm-006 | 验证CMD\_SECSTORAGE\_TRANSIENT\_AES\_KEY接口功能是否正常 | 通过CA调用接口SecstorageTransientAESkey去调用TA侧，传入正确的参数 |
| Function-Vm-007 | 验证CMD\_SECSTORAGE\_TRUNCATE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageTruncateFile去调用TA侧，传入正确的参数 |
| Function-Vm-008 | 验证CMD\_SECSTORAGE\_WRITE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageWriteFile去调用TA侧，传入正确的参数 |

## **switchless可靠性测试**

|  |  |  |
| --- | --- | --- |
| Stability\_vm\_01 | 验证switchless接口功能可靠性 | 运行 /vendor/bin/secgear\_switchless，连续调用24h |

# 测试结果

## 接口基本功能测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| 测试编号 | 测试名 | 测试期望 | 测试结果 |
| Interface\_Function-001 | TEEC\_InitializeContext功能测试 | Host侧接口正常， 返回 TEEC\_SUCCESSClient接口功能正常，返回 TEEC\_SUCCESS | 运行通过打印  interface\_testcase  pass |
| Interface\_Function-002 | TEEC\_OpenSession功能测试 | Host侧接口正常， 返回 TEEC\_SUCCESSClient接口功能正常，返回 TEEC\_SUCCESS |
| Interface\_Function-003 | TEEC\_InvokeCommand功能测试1 | 1、Host侧接口正常， 返回 TEEC\_SUCCESSClient接口功能正常，返回 TEEC\_SUCCESS 2、Host侧接口正常，返回TEEC\_SUCCESS, 且HOST TEE侧能够获取、打印Client侧值结果 3、Host侧接口正常，返回TEEC\_SUCCESS, 且HOST TEE侧能够获取、打印Client侧tmp\_buf内容 |
| Interface\_Function-004 | TEEC\_CloseSession功能测试 | 1、Host侧接口正常， 释放session资源 Client接口功能正常，无返回。 |
| Interface\_Function-005 | TEEC\_FinalizeContext功能测试 | 1、Host侧接口正常， 释放context资源 Client接口功能正常，无返回 |

## ShareMemory测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| Interface\_Function-006 | TEEC\_AllocateSharedMemory功能测试 | 1、Host侧接口正常，返回TEEC\_SUCCESS，Host共享内存开辟  VM侧接口功能正常，返回TEEC\_SUCCESS,Client动态内存开辟 | 运行通过打印  Sharemem\_interface\_testcase pass |
| Interface\_Function-011 | TEEC\_InvokeCommand功能测试2 | 1、Host侧接口正常，返回TEEC\_SUCCESS, 且HOST TEE侧能够获取、打印VM侧值结果；VM侧能够获取、打印HOST TEE修改后内容，且与HOST TEE写入值保持一致。 |
| Interface\_Function-008 | TEEC\_ReleaseSharedMemory功能测试 | 1、Host侧接口正常，Host共享内存资源释放  VM侧接口功能正常, 如果是 TEEC\_AllocateSharedMemory 接口开辟的内存资源需释放， TEEC\_RegisterSharedMemory 接口注册的内存资源无需释放。 |
| Interface\_Function-007 | TEEC\_RegisterSharedMemory功能测试 | 1、Host侧接口正常，返回TEEC\_SUCCESS,Host共享内存开辟VM侧接口功能正常，返回TEEC\_SUCCESS。 |
| Interface\_Function-012 | TEEC\_InvokeCommand功能测试3 | 1、Host侧接口正常，返回TEEC\_SUCCESS, 且HOST TEE侧能够获取、打印VM侧值结果；VM侧能够获取、打印HOST TEE修改后内容，且与HOST TEE写入值保持一致。 |

## 多session测试

|  |  |  |  |
| --- | --- | --- | --- |
| Interface\_Function-010 | 接口并发调用测试 -- 多Session | 将testcase.h THREAD\_COUNT设置为30创建30线程，调用thread\_function | multi\_thread\_testcase pass |

## 基本异常情况测试

|  |  |  |  |
| --- | --- | --- | --- |
| Interface\_Exception | TEEC\_InitializeContext异常测试 | 在host与VM分别运行 /vendor/bin/testcase1 4，观察输出结果 | Host与VM行为一致 |
| Interface\_Exception | TEEC\_InvokeCommand 异常测试 | 在host与VM分别运行 /vendor/bin/testcase1 4，观察输出结果 | Host与VM行为一致 |
| Interface\_Exception | TEEC\_CloseSession 异常测试 | 在host与VM分别运行 /vendor/bin/testcase1 4，观察输出结果 | Host与VM行为一致 |
| Interface\_Exception | TEEC\_FinalizeContext 异常测试 | 在host与VM分别运行 /vendor/bin/testcase1 4，观察输出结果 | Host与VM行为一致 |

## Client挂掉测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| CA\_KILL\_Test\_001 | Client挂掉测试 | 1、Host侧相关context资源释放关闭  2、Host侧相关session资源释放关闭  3、Host侧共享内存资源释放关闭、VM侧共享内存随进程关闭自动释放 | Client侧共享内存随进程关闭自动释放,打印CA Killed Test begin!, process exit! |

## 单接口性能测试结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试编号 | 测试名 | 测试方法 | Host平均时间 | VM平均时间 | 性能损耗% |
| Perfermance\_001  （TEEC\_InitializeContext） | 单接口性能测试 | 将CA部署在VM测试环境中，分别测试CA调用以下接口1000次后获得响应的时间平均值：  TEEC\_InitializeContext  TEEC\_OpenSession  TEEC\_InvokeCommand  对比性能数据 | 40.848 us | 229.650 us | 462.20 |
| Perfermance\_001  （TEEC\_OpenSession） | 49426.372 us | 49986.193 us | 1.13 |
| Perfermance\_001  （TEEC\_InvokeCommand） | 342.787 us | 484.94 us | 41.46 |

## RSA签名测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| RsaSign\_001 | RSA签名测试 | 调用接口进行RSA签名 | 运行通过打印TEEC RSA Sign  success |

## 基本长稳测试结果

|  |  |  |  |
| --- | --- | --- | --- |
| Interface\_Stability-001 | 基本功能长稳测试 | VM、Host侧基本接口功能均符合预期， 无异常。 | VM、Host侧基本接口功能均符合预期， 无异常。 |

## VM功能测试用例

|  |  |  |  |
| --- | --- | --- | --- |
| Function-Vm-005 | 验证不同VM内，同个uuid的TA同时加载 | 1. 创建VM1，VM2  3.在VM1,VM2中同时运行testcase 、rsa\_demo 、switchless | VM1和VM2中的TA均加载成功 |
| Function-Vm-006 | 验证VM部署下的安全存储存储于该VM下的目录 | 1. 创建VM,启动VM中的rsa\_demo   2. 通过rsa\_demo调用接口secstorage\_create\_file去调用TA侧，传入正确的参数  3. 查看输出结果，查看/var/itrustee/sec\_storage\_data日志信息 | CA运行成功，在VM /var/itrustee/sec\_storage\_data目录下，生成目标文件。 |
| Function-Vm-007 | 验证VM部署下的TA日志存储于该VM下的目录 | 1. 创建VM,启动VM中的CA/TA  2. 查看输出结果，VM内和host侧启动tlogcat -f日志信息 | CA/TA运行成功，日志可在VM查看，host上不存在该TA日志 |
| Function-Vm-008 | 验证host侧与VM内可同时运行CA/TA应用 | 1. 同时启动VM和host侧中的testcase、rsa\_demo应用 | CA/TA运行成功 |
| Function-Vm-011 | Switchless功能测试 | 1. VM 运行secGear 测试用例switchless\_performance | CA/TA运行成功 |
| Function-Vm-015 | 验证VM内TA远程证明场景测试 | 1. REE侧虚机被拉起，虚机内qca\_guest启动，qca\_guest向qca\_host进行注册vsocket通道，qca\_guest与qca\_host建立连接；  2. qca\_client向qca\_host发起TA证明，携带TA uuid、虚拟机pid/nsid等；  3. raserver根据虚机名和虚机type，通过虚机管理命令行获取vmid和虚机名信息，向QTA注册：<vmid,vm-name>;  4. qca\_host通过虚机pid/nsid，找到连接的qca\_guest,发送: type+TA uuid;  5. qca\_guest->QTA-report: 用户证明参数;  6. 报告返回：tcmgr -> QTA-report -> qca\_guest-> qca\_host | client接收到Report并打印 |

## VM性能测试用例

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Performance-Vm-001 | 基于itrust\_sdk,使用RSA-4096签名验签性能测试 | 1. 基于itrust\_sdk, 编写TA/CA测试程序rsa\_demo调用RSA-4096加解密函数  2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2， | Host总耗时  213619.38 us  加解密耗时  6590.10 us | VM总耗时  224084.21 us  加解密耗时  7230.57 us | 性能损耗4.8%  性能损耗  9.7% |
| Performance-Vm-002 | 基于switchless,使用RSA-4096签名验签性能测试 | 1. 基于switchless, 编写TA/CA测试程序调用RSA-4096加解密函数  2. 分别在host侧和VM内运行TA/CA测试程序，记录接口函数调用时间t1,t2，预期结果1  3. CA发起线程数为：4，TA发起多线程：8 | Host  加解密耗时  4945.04us | VM  加解密耗时  4960.06us | 性能损耗  0.30% |

VM与Host分别运行rsa\_demo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | VM | Host | 性能损耗% | VM | Host | 性能损耗% |
| TeecInit cost | 59775.50 us | 50026.70 us | 19.48 | 38685.60us | 41457.90us | -6.68 |
| GenerateRandomCmd cost | 3639.10us | 3558.90 us | 2.25 | 3216.40us | 3152.0 us | 2.04 |
| RsaGenerateKeypairCmd cost | 78481.10 us | 78387.50 us | 0.11 | 81061.50us | 71933.60us | 12.68 |
| RsaSaveKeypairCmd cost | 59556.10us | 57803.00 us | 3.03 | 47155.10us | 42644.80us | 10.57 |
| RsaReadKeypairCmd cost | 27259.30us | 24665.40 us | 10.51 | 25354.40us | 21946.50us | 15.5 |
| RsaEncryptCmd cost | 1470.100us | 1038.00 us | 41.62 | 1175.00us | 965.60 us | 21.68 |
| RsaDecryptCmd cost | 6469.60 us | 6031.00 us | 7.27 | 5785.80us | 5588.10us | 3.53 |
| RsaSignCmd cost | 6050.90 us | 5603.60us | 7.98 | 5806.90us | 5560.30us | 4.43 |
| RsaVerifyCmd cost | 1180.40us | 737.90 us | 59.96 | 907.00 us | 658.10 us | 37.82 |
| Total cost | 249667.60 us | 233124.70us | 7.09 | 214050.10us | 198583.90 us | 7.78 |

VM1与VM2同时运行rsa\_demo

|  |  |  |
| --- | --- | --- |
|  | VM1 | VM2 |
| Total cost | 328537.90us | 322087.10u |

## 零拷贝

|  |  |  |  |
| --- | --- | --- | --- |
| ZeroCopy\_function\_001 | CA创建Share Memory测试(内存页4K) | 1. REE侧创建share memory 256M | 内存创建成功 |
| ZeroCopy\_function\_002 | CA创建Share Memory测试(内存页64K) | 1. REE侧创建share memory 256M | 内存创建成功 |
| ZeroCopy\_function\_003 | 零拷贝功能测试(内存页64K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2 | 结果1：内存创建成功  结果2：测试CA/TA均成功运行 |
| ZeroCopy\_function\_004 | 零拷贝功能测试(内存页4K) | 1. REE侧创建share memory 256M，预期结果1；  2. 使传参方式为零拷贝模式编写CA/TA, 预期结果2 | 结果1：内存创建成功  结果2：测试CA/TA均成功运行 |

## Sec驱动用例

|  |  |  |  |
| --- | --- | --- | --- |
| functional\_test\_006 | huk密钥派生，salt不同长度测试 | 1、CA发起salt长度分别为1、32、255、1023，密钥长度64的huk密钥派生请求。（TA内申请内存即可）  2、CA发起salt长度64，密钥长度16、32、255、4096、4097的huk密钥派生  3、两次发送相同salt，返回的密钥一致 | 1、获取密钥最大长度4096，  2、在支持的最大长度内，所列长度调用都成功返回，  3、相同salt密钥一致 |
| functional\_test\_009 | huk密钥派生，TA内多线程调用 | 1、TA内开启多个线程，每个线程发起100次盐1023和密钥512长度的GP接口调用，  2、线程测试范围：128 | 1、所有接口调用正常  2、结果一致 |

## 安全存储demo

|  |  |  |  |
| --- | --- | --- | --- |
| Function-Vm-001 | 验证CMD\_SECSTORAGE\_CREATE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageCreateFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage create file success: fd=1 |
| Function-Vm-002 | 验证CMD\_SECSTORAGE\_DELETE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageDeleteFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage delete file success. |
| Function-Vm-003 | 验证CMD\_SECSTORAGE\_READ\_FILE接口功能是否正常 | 通过CA调用接口SecstorageReadFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage read file success: fd=1, read count=16. |
| Function-Vm-004 | 验证CMD\_SECSTORAGE\_RENAME\_FILE接口功能是否正常 | 通过CA调用接口SecstorageRenameFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage rename file success: fd=1. |
| Function-Vm-005 | 验证CMD\_SECSTORAGE\_SEEK\_FILE接口功能是否正常 | 通过CA调用接口SecstorageSeekFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage seek file success: fd=0. |
| Function-Vm-006 | 验证CMD\_SECSTORAGE\_TRANSIENT\_AES\_KEY接口功能是否正常 | 通过CA调用接口SecstorageTransientAESkey去调用TA侧，传入正确的参数 | 运行通过打印secstorage transient aes key success. |
| Function-Vm-007 | 验证CMD\_SECSTORAGE\_TRUNCATE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageTruncateFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage truncate file success: fd=1. |
| Function-Vm-008 | 验证CMD\_SECSTORAGE\_WRITE\_FILE接口功能是否正常 | 通过CA调用接口SecstorageWriteFile去调用TA侧，传入正确的参数 | 运行通过打印secstorage write file success: fd=1. |

## switchless可靠性测试

|  |  |  |  |
| --- | --- | --- | --- |
| Stability\_vm\_01 | 验证switchless接口功能可靠性 | 运行 /vendor/bin/secgear\_switchless，连续调用24h | 程序调用正常 |