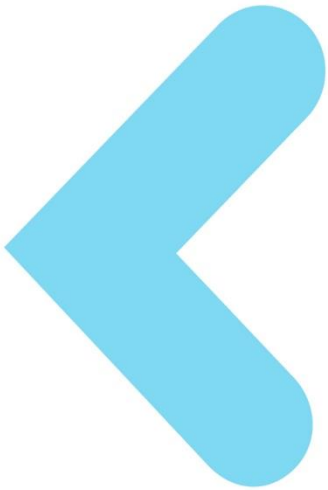
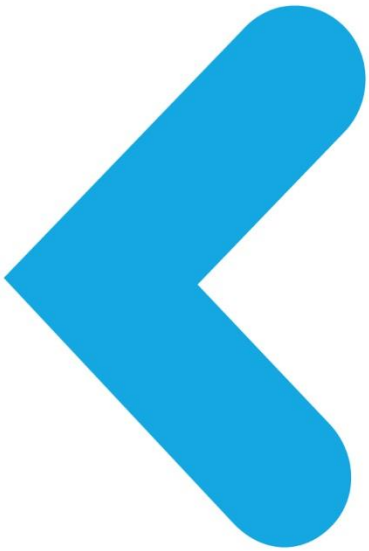
TRUSTONIC

TESTING MANUAL



Trustonic Test Suite (APK)
User's Manual



PREFACE

VERSION HISTORY

Version	Date	Modification
1.0	12/15/2015	Released
1.1	02/24/2015	Additions for RootPA status and automatic Online mode detection in section 1. Additions for user contact information in section 2.2.1. Correction command line instructions in section 1.3. Section 2.5: TA signature script signature command updated with correct key.

TABLE OF CONTENTS

1 QUICKSTART GUIDE

1.1 PURPOSE

The **T**rustonic **T**est **S**uite (TTS) Android application provides a simple way for verifying the Trustonic TEE feature is functional on a device.

It can be installed and used as any other Android applications on supported Android versions.

This manual will guide you through the different options available for testing the Trustonic TEE on your device.

1.2 INSTALLING THE TTS APK

The TTS package is delivered to you as a stand-alone zip file or as part of the Trustonic OEM package.

Once the package is extracted, the TTS application can be found in the folder TTS/bin.

To install the application on the device, use the adb install command as follows:

```
adb install TTS.apk
```

1.3 USING THE TTS APK

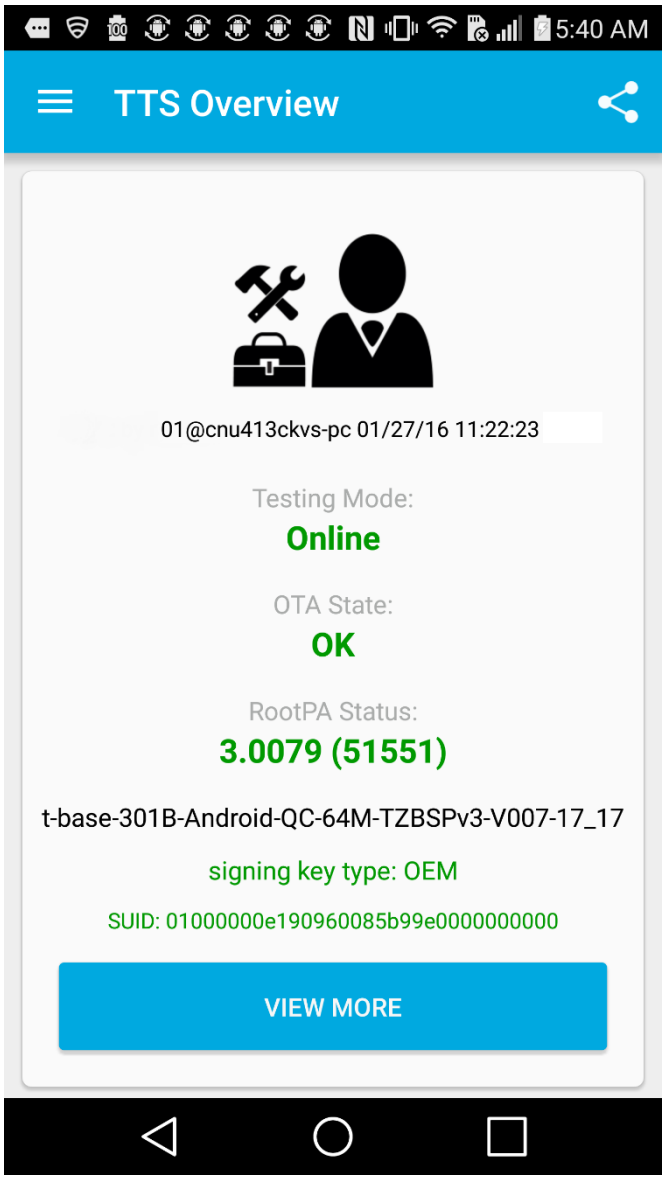
The TTS APK can be used via its Graphical Interface by pressing the TTS icon.

The TTS application can also be started from the adb command line interface as described below:

```
# Start the application
adb shell am start -n com.trustonic.tbase.tests.runner/.SplashscreenActivity
--ez tui_enabled false

# Optional command line parameters:
# --ez tui_enabled "true" will activate the TrustedUI tests (and enable the
Manual TUI Test Menu)


# Start the tests
adb shell am broadcast -a com.trustonic.tbase.tests.runner.START_TEST -e
params "-l /sdcard/trustonic_tests/ -b /sdcard/trustonic_tests/ -f
<TestMode>"

#-f Can take Quick/Basic/Extended/Final_Device
```

1.3.1 The Overview Screen

Once loaded, the application will display the “TTS Overview” screen on which are brought together the basic Trustonic TEE information that the application has collected at startup, which displays the basic Trustonic TEE version, RootPA status, signing key and SUID.



If the RootPA status displays “**NOK**”, please ensure you have installed the mandatory RootPA components on your devices.

The “View More” button will unveil additional information such as the device baseband and Android version as well as some TEE configuration information and SE Linux configuration.

1.3.2 Offline vs. Online testing

Offline testing can be used in the early stages of the Trustonic TEE integration, it doesn't require a network connection to execute the tests.

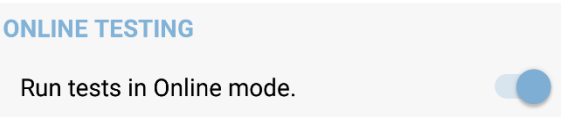
If "**signing key type: Trustonic**" is displayed (meaning the Trustonic TEE binary has been injected with the Trustonic Test vendor key) there are no specific actions to take to run the tests. The binaries required are embedded in the APK and shall be copied to the device when the tests are launched.

If "**signing key type: OEM**" is displayed (meaning the Trustonic TEE binary has been injected with the final OEM vendor key) it is still possible to test Offline. For doing so the OEM will have to convert the test TAs included in the TTS package (TTS/TrustedApplications/*.axf) and manually install them on the device. Section 2.5 provides the details for this operation.

Conversely to Offline testing, Online testing is using the **O**ver **T**he **A**ir (OTA) feature for provisioning test SPTAs into the device. For Online testing the device must have been key injected and had its receipt imported to the Trustonic backend.

It is mandatory to pass Online – Final Device Tests before the device can go to production.

For turning on and off the Online mode manually, press on the menu button and select "Settings.



In the "Settings" screen, turn on the ONLINE TESTING switch. Testing mode on the TTS Overview screen will turn to **Online**.

In Online testing mode, the device must have network access as the application will try to contacts the Trustonic Test Back-End to determine if the device has been registered for Online testing and for downloading the test SPTAs.

The device must be de facto be registered with our Back-End server prior to perform Online testing.

Registration is part of the device binding process described in the KPH document [1].

If the device is known to the Test Back-End, the OTA State will display "**OK**". If the device is not known to the Test Back-End, "**NOK**" will be displayed.

If "NOK" is displayed Online testing using OTA provisioned SPTAs is not possible.

If the device is known the Trustonic Production Back-End but is unknown to the Test Back-End, an SUID forwarding request is automatically sent to Trustonic. You may alternatively ask your Trustonic contact support to forward the SUID of the device onto the Trustonic test Back-End.

Once the device has been registered on the test Back-End, the application can be restarted, the OTA state should have changed from "**NOK**" to "**OK**".

Before launching the Basic and Extensive tests, make sure the SE Linux policies set to permissive mode or some of the tests will fail.

1.3.3 SE Linux considerations

Most of the test included in the TTA application require permissive SE Linux policies. This is required for checking some system folder content and permissions amongst other things.

Only the "Final_Device" tests can be executed with SE Linux policies enforced.

```
# Switch SE Linux policies to permissive
su 0 setenforce 0

# Switch SE Linux policies to enforced
su 0 setenforce 1
```

Figure 1. SE Linux activation adb commands

1.3.4 Executing the first tests

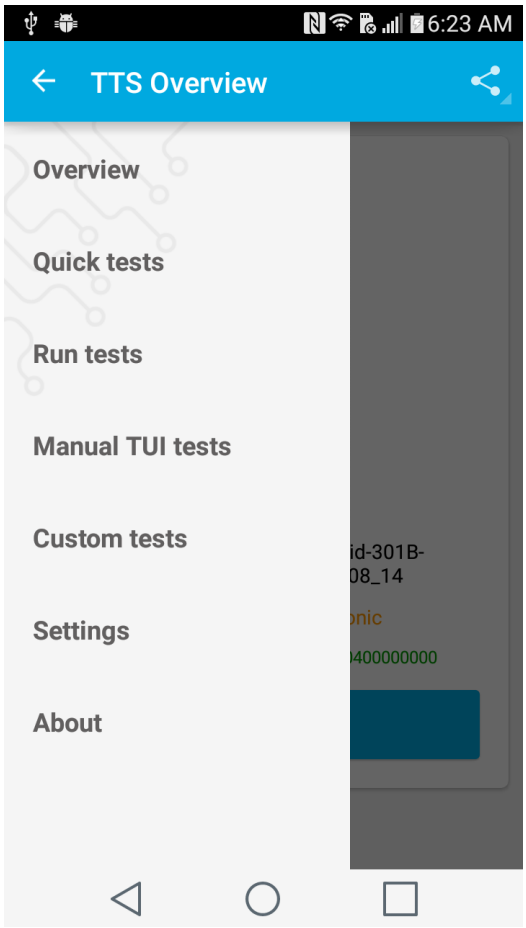
First thing we recommend you do is to execute the "Quick" tests which purpose are to ensure the Trustonic TEE is correctly configured and functional.

The "Quick" tests should last less than 1 minute and perform a brief verification the Trustonic TEE integration guide has been followed:

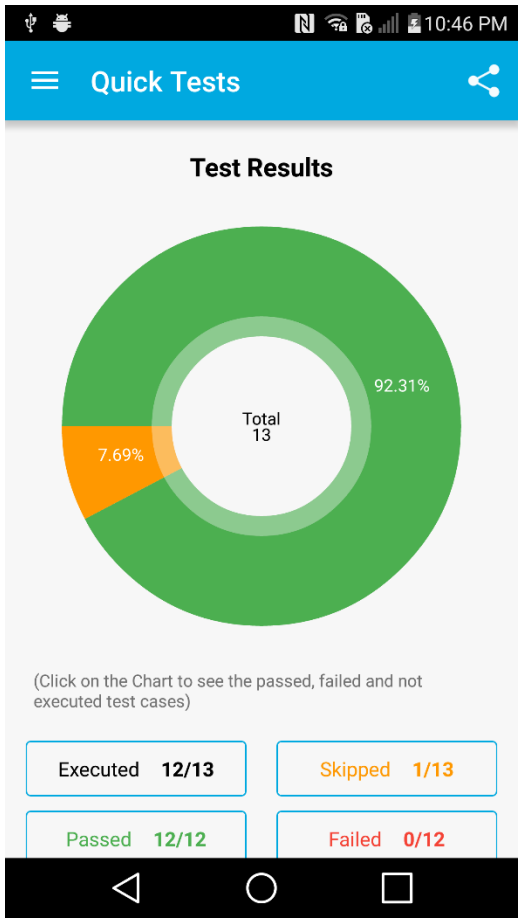
- The Trustonic TEE can be contacted by a client application.
- All components (daemon, RootPA, CMTA etc.) are present on the device (and with the good permissions and build tags).

For launching the tests, select 'Quick tests" from the main menu of the application.

Before starting the tests, Trustonic recommend the User automatically shares the tests results with Trustonic. Activating the automatic sharing email option is described in section 2.2.1.



The application displays the list of tests to be executed press “RUN ALL” at the bottom of the screen. The test will execute and a Test results screen will display the outcome of the tests as depicted hereunder.



For the Quick test to pass it should be 0 failed test meaning the mandatory Trustonic TEE components are present on the device. Pressing the pie chart will disclose the details of the test results. The user can also directly review the Executed / Skipped / Passed / Failed test list by pressing the associated button.

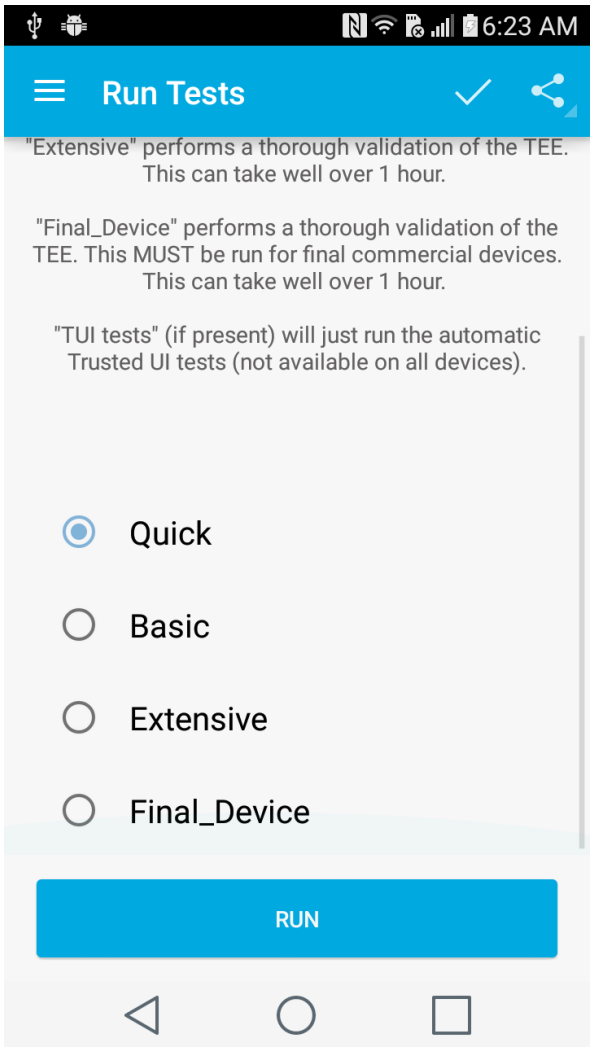
Depending on the version of the Trustonic TEE being tested, some tests might be skipped, users can ignore those tests that are not relevant in the test context.

2 ADVANCED TESTING

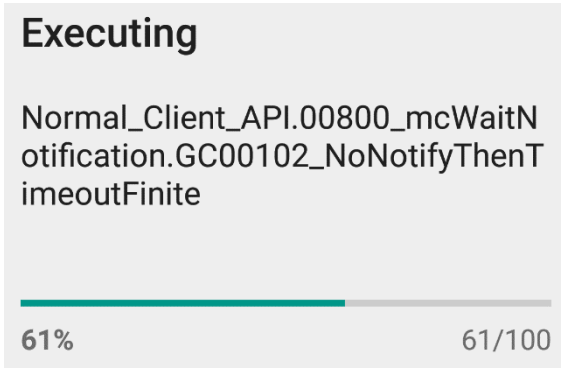
This section introduces the various tests options that can be used to verify a device.

2.1 RUN TESTS

We'll start with the automated tests available in the menu under the "Run tests" item:



There are several automatic tests scenarios available. To launch the tests, select the test scenario to be executed and press "RUN".



During the execution of the tests the application will update a pop-up indicating the test being executed as well as the progression of the overall test group.

2.1.1 Quick tests

There are the same as the quick tests in the main menu. Not using any test TAs doesn't require OTA, checks component presences.

2.1.2 Basic tests

The intent of basic tests is to perform more extensive verifications such as:

- Memory Management,
- TA Loading,
- Secure Object Wrap/Unwrap,
- RNG Quality.

Basic tests should last more than 5 min to execute.

2.1.3 Extensive tests

Trustonic insist the users to execute the extensive tests in Online mode before a device goes to production.

Same as Basic test plus extensive tests of TEE features such as:

- GP,
- Crypto operations and algorithms
- Etc…
- Checks that Trustonic Authorization Key has not been modified / corrupted.

Please allow some time when launching Extensive tests as they might take quite some time to execute, depending on the device the test scenario tests can last more than 1 hour.

2.1.4 Final_Device

To be used if you are executing the test suite on a production device, the “Final_Device” test scenario is mandatory once the SE Linux policies are enforced.

The test will verify that the OEM signing key has been changed i.e. that the image is not using the debug SYS TA / Driver signing key.

Please allow some time when launching Extensive tests as they might take quite some time to execute, depending on the device the test scenario tests can last more than 1 hour.

2.2 TEST RESULTS

The TTS application keeps records of all test execution.

Test results can be reviewed directly from the TTS Overview screen in the “Test Results” pane underneath the “Overview pane”.

Press the pie chart to review the last test results, the “VIEW MORE” button brings you to the “Test History” screen where can be found all test results executed so far.

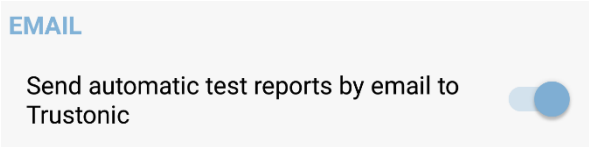
Pressing a Test result line in the “Test History” screen will unveil the test details.

The test history can be erased in the “Settings” screen.

2.2.1 Sharing the test results

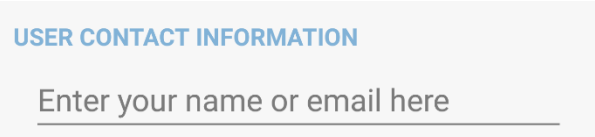
The tests results can be shared with Trustonic in two ways: via email or by manually extracting the test results from the */sdcard/trustonic_tests* folder. Just use the adb pull command for extracting the *result_archive.zip.rename* file.

If the automatic email sharing option is set in the Settings, the application automatically sends out the tests result on a Trustonic email address.



Upon reception of the test report our teams will review your tests reports and come back to you with comments and recommendations.

Before sharing your tests, make sure you fill-in your contact information in the application settings.

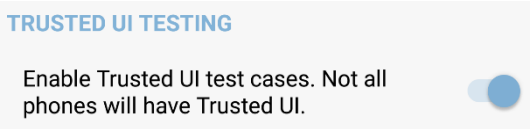


Additionally, if you want a specific Trustonic support contact to receive the test reports, you can use the share button in the top bar.

2.3 MANUAL TUI TESTS

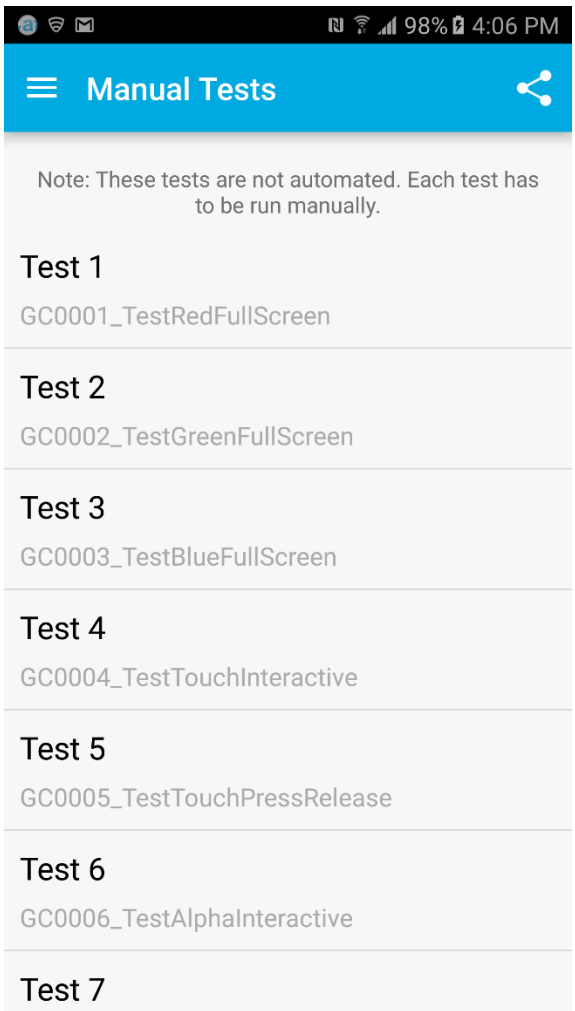
Trusted **U**ser **I**nterface (TUI) tests can only be executed on devices that have implemented this feature. The device must have the TUI secure driver, kernel module and service already integrated.

Before TUI tests can be executed, they have to be activated in the “Settings” screen.



Testing TUI requires user interactions as both display and touchscreen events can only be verified by an operator. These tests validate touch co-ordinates across the full screen, persistent touch “drag-and-drop”, alpha channel images amongst other things.

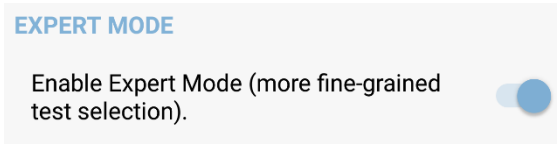
Select the test to run and follow the instructions.

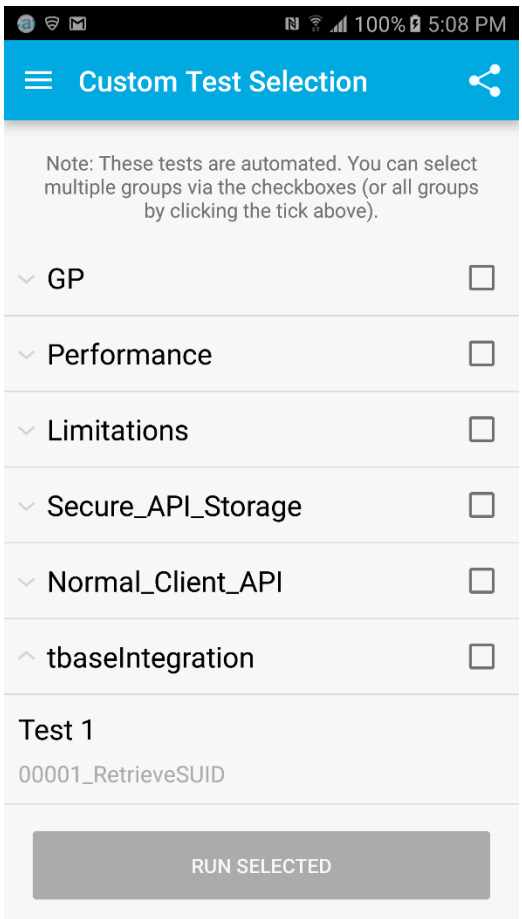


2.4 CUSTOMS TESTS

Using Custom tests is a way to execute a specific test or specific group(s) of tests. This option is usually used for diagnostic and debug purpose.

For the Custom Test Selection to be accessible, the expert mode has to be activated in the “Settings” screen.





A test group or multiple test groups can be selected by checking the group checkboxes. Once the test group selection done, it can then be executed by pressing the “RUN SELECTED” button.

Pressing a test group line will unfold the list of tests that are part of a group, each test can then be individually executed by selecting the test.

2.5 TESTING OFFLINE WITH USERS'S SIGNED TEE

Pre-requisites:
- The device provides a functional adb access.
- The user must have access to its signing key.

It is possible to test the Trustonic TEE feature without the need for OTA and SPTAs. This capability is typically used on devices for which the network connection is not yet available in the early stages of the development.

In this mode of operation, it is supposed the Trustonic TEE has been injected with the *PuK.Vendor.TltSig* key the secure test binaries must be replaced by *User-signed secure test binaries.*

Prior those binaries can be used for testing, they must be first signed by the User with its *PuK.Vendor.TltSig* key, then pushed into the device in the */sdcard/trustonic_tests/mcRegistry/* folder.

Included in the package in the tools folder is a python tool "SignTestTAs.py" (in the tools folder) that will take care of signing all the test TAs included in the "trusted_applications" folder.

The script signs all the "axf" files present in the trusted_applications folder and converts them in TA binaries (.tlbin and .tabin).

```
./SignTestTAs.py –k PrK.Vendor.TltSig -c <path_to_MobiConvert.jar> -i
<input_directory> -o <output_directory> -k <path_to_keyfile>
```

Please note the dependency with the <t-sdk package as signing the TAs uses the ***MobiConvert.java*** tool.

The resulting test binaries are stored in the newly created "Output" folder in the TrustedApplications folder.

The next step is to copy the content of the "Output" folder onto the device in the ***/sdcard/trustonic_tests/mcRegistry/*** folder. For doing this, connect your device to your computer through adb and use the loadTAs.sh bash script (in tools folder).

```
.loadTAs <Output folder>
```

3 TEST PLAN

The TTS package includes an HTML version of the TTS application test plan that can be browsed with any web browser starting from *TTS/test_plan/index.html*.

Browsing through the test plan tree view will provide you with the very details of each test executed by the TTS application.

4 TROUBLESHOOTING AND SUPPORT

If you are having issues using the TTS application, you can check our trouble shooting page at:

https://trustonic.zendesk.com/hc/en-us/categories/200517982-Troubleshooting

You can alternatively send support requests at: https://trustonic.zendesk.com

5 REFERENCES

1. Trustonic-KPHV2-Manual.pdf
2. Kinibi_Integration_Guide.pdf