



Android 10

CTS Verifier 测试操作指南

1.0
2020.02.26

文档履历

版本号	日期	制/修订人	内容描述
1.0	2020.02.26		Android 10 CTS Verifier 测试操作指南

目录

1. 测试方法	1
2. 测试环境要求	2
3. 测试前平板配置	3
4. 各测试项详细测试方法	4
4.1 测试顺序	4
4.2 测试需要的工具	4
4.3 各项测试方法	11
4.3.1 AUDIO	11
4.3.1.1 Audio Frequency Line Test	12
4.3.1.2 Audio Acoustic Echo Cancellation (AEC)Test	12
4.3.1.3 Audio Frequency Microphone Test	13
4.3.1.4 Audio Frequency Speaker Test	17
4.3.1.5 Audio Frequency Unprocessed Test	18
4.3.1.6 Audio Frequency Voice Recognition Test	21
4.3.1.7 Audio Input Devices Notification Test	21
4.3.1.8 Audio Input Routing Notification Test	21
4.3.1.9 Audio Loopback Latency Test	21
4.3.1.10 Audio Output Devices Notification Test	22
4.3.1.11 Audio Output Routing Notification Test	22
4.3.1.12 Hifi Ultrasound Microphone Test	22

4.3.1.13 Hifi Ultrasound Speaker Test	27
4.3.1.14 MIDI Test	30
4.3.1.15 Nation MIDI API Test	30
4.3.1.16 Pro Audio Test	31
4.3.1.17 Ringer Mode Tests	31
4.3.1.18 USB Audio Peripheral Attributes Test	31
4.3.1.19 USB Audio Peripheral Buttons Test	31
4.3.1.20 USB Audio Peripheral Play Test	31
4.3.1.21 USB Audio Peripheral Record Test	32
4.3.2 CAMERA	36
4.3.2.1 Camera FOV Calibration	36
4.3.2.2 Camera Formats	37
4.3.2.3 Camera ITS Test	39
4.3.2.4 Camera Intents	39
4.3.2.5 Camera Orientation	40
4.3.2.6 Camera Performance	40
4.3.2.7 Camera Video	41
4.3.3 CAR	41
4.3.3.1 Car Dock Test	41
4.3.4 CLOCK	41
4.3.4.1 Alarms and Timers Tests	41
4.3.5 DEVICE ADMINISTRATION	47

4.3.5.1 Device Admin Tapjacking Test	47
4.3.5.2 Device Admin Uninstall Test	48
4.3.5.3 Keyguard Disabled Features Test	48
4.3.5.4 Policy Serialization Test	48
4.3.5.5 Redacted Notification Keyguard Disabled Features Test	49
4.3.5.6 Screen Lock Test	49
4.3.5.7 Usb Debugging Dialog Tapjacking Test	49
4.3.6 FEATURES	49
4.3.6.1 Companion Device Test	49
4.3.7 HARDWARE	50
4.3.7.1 MTP Host Test	50
4.3.7.2 USB Accessory Test	50
4.3.7.3 USB Devices Test	50
4.3.8 INSTANT APPS	51
4.3.8.1 Instant Apps Notification Test	51
4.3.8.2 Instant Apps Rescent Test	51
4.3.8.3 View/Delete Instant apps Test	51
4.3.9 OB SCHEDULER	51
4.3.9.1 Charging Constraints	51
4.3.9.2 Connectivity Constraints	52
4.3.10 LOCATION	52
4.3.10.1 Battery Saving Mode Test	52

4.3.10.2 Location Mode Off Test	52
4.3.11 MANAGED PROVISIONING	53
4.3.11.1 BYOD Managed Provisioning	53
4.3.11.2 BYOD Provisioning tests	60
4.3.11.3 Device Owner Requesting Bugreport Tests	60
4.3.11.4 Device Owner Tests	62
4.3.11.5 No Devices Owner Tests	75
4.3.12 NETWORKING	75
4.3.12.1 Bluetooth Test	75
4.3.12.2 Wi-fi Direct Test	77
4.3.12.3 Wi-Fi Test	78
4.3.13 NOTIFICATIONS	79
4.3.13.1 Bubble Notification Tests	79
4.3.13.2 CA Cert Notification Test	79
4.3.13.3 CA Cert Notification on Boot Test	80
4.3.13.4 Condition Provider test	80
4.3.13.5 Notification Attention Management Test	80
4.3.13.6 Notification Listener Test	81
4.3.13.7 Notification Package Priority Test	81
4.3.13.8 Shortcut Reset Rate-limiting Test	82
4.3.14 OTHER	82
4.3.14.1 Recent Task Removal Test	82

4.3.14.2 Screen Pinning Test	82
4.3.14.3 Widget Framework Test	82
4.3.15 PROJECTION TESTS	85
4.3.15.1 Projection Cube Test	85
4.3.15.2 Projection Multitouch Test	86
4.3.15.3 Projection Offscreen Activity	86
4.3.15.4 Projection Scrolling List Test	86
4.3.15.5 Projection Video Playback Test	86
4.3.15.6 Projection Widget Test	86
4.3.16 SECURITY	87
4.3.16.1 Biometric Prompt Bound Keys Test	87
4.3.16.2 Biometric test	87
4.3.16.3 KeyChain Storage Test	87
4.3.16.4 Keyguard PASSword Verification	87
4.3.16.5 Lock Bound Keys Test	88
4.3.16.6 Set New PASSword Complexity Test	88
4.3.17 SENSORS	88
4.3.17.1 6DoF Test	88
4.3.17.2 Accelerometer Measurement Tests	89
4.3.17.3 CTS Sensor Batching Tests	96
4.3.17.4 CTS Sensor Integration Tests	96
4.3.17.5 CTS Sensor Test	96

4.3.17.6 CTS Single Sensor Tests	97
4.3.17.7 Devices Suspend Tests	97
4.3.17.8 Dynamic Sensor Discovery Test	97
4.3.17.9 Event sanitization for idle UID test	97
4.3.17.10 Off Body Sensor Test	98
4.3.17.11 Sensor Batching Manual Test	98
4.3.17.12 Significant Motion Tests	98
4.3.18 STREAMING	98
4.3.18.1 Steaming Video Quality Verifier	98
4.3.18.2 Tile Service Test	98
5. 搜集测试结果	99
6. Declaration	100

1. 测试方法

根据提示，让每个项目的绿色钩钩可以点击，绿色的小勾按钮是 **PASS**，红色的感叹号是 **Fail**。



2. 测试环境要求

CTS Verifier 需要的测试环境如下：

1. 测试平板 2 台。
2. 能够通过 adb 连接平板。电脑用于通过 adb 安装测试需要的 apk 和发送一些指令。
3. 连接能够上国外网络、ipv6 的 Wifi。
4. 在 linux 终端用 unzip 解压 verifier 测试套件。用 cd 命令到达下载解压后的 android-cts-verifier 目录下，通过 adb 命令安装 CtsVerifier.apk、NotificationBot.apk 和 CtsPermissionApp.apk 等应用。

3. 测试前平板配置

平板固件烧录完成后需要进行相关配置才能测试 **cts-verifier**。主要的配置如下：

1. 恢复出厂设置。这一项在有必要的情况下进行。刚烧好固件运行起来的可跳过此步骤。烧写 **GMS** 最新固件 (**User** 固件)。如果烧录好固件后被用作其它用途再进行 **CTS** 测试，则需先恢复出厂设置。
2. 在设置向导中选择语言为 **English(United States)**。
3. **Settings > Display > Sleep** 设置休眠时间为 **never**。
4. 去掉勾选 **Settings > Developer options > Verify apps over USB**。(如果系统中 **Developer options** 是不显示的，需要进入 **About tablet**，然后迅速连续敲击 **Build number**)。
5. 连接能够上国外网络的 **Wifi**。
6. 使用 **Google** 账号登陆过的平板，在测试之后，需清除 **Google** 账号，以免以后烧写固件失败。

4. 各测试项详细测试方法

4.1 测试顺序

Verifier 中有几十个测试项，并不是从上置下一一测试最好。根据以往的经验，测试的顺序应该如下：

1. 测试其它项。
2. 最后才测试 Device Owner Tests (MANAGED PROVISIONING)、Policy Serialization Test (DEVICE ADMINISTRATION)。
3. 每个测试项均有操作提示，各项测试中的 Info 按钮（蓝色的）可以弹出提示框，可以按照提示来进行测试操作，绿色的小勾按钮是 PASS，红色的感叹号是 Fail。

注意：每版测试前，需跟开发确认测试方法无修改。如果有修改需按最新方法测试，实时更新。

4.2 测试需要的工具

1. OTG 转换线



图 1: OTG 转换线

2. 耳机转换 USB 线



图 2: 耳机转换 USB 线

3. USB 数据线



图 3: USB 数据线

4. 回环塞

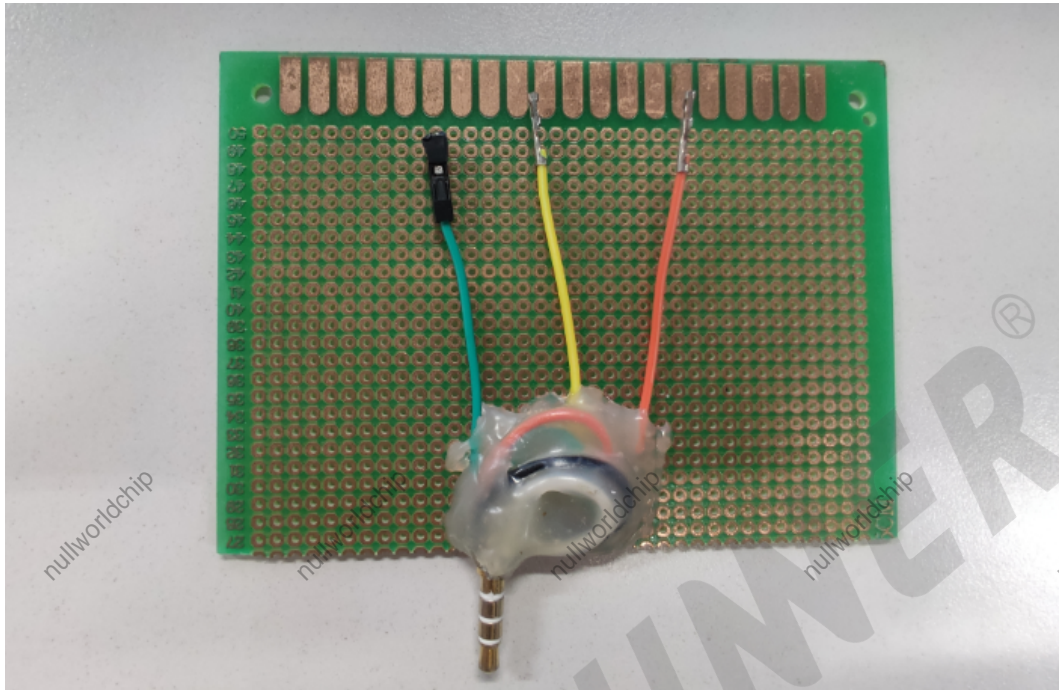


图 4: 回环塞

5. 入耳式含音量键耳机



图 5: 入耳式含音量键耳机

6. 麦克风耳机



图 6: 麦克风耳机

7. 麦克风



图 7: 麦克风

8. AudioBox 音频设备



图 8: AudioBox 音频设备

9. AUDIOBOX USB 音频设备



图 9: AUDIOBOX USB 音频设备

4.3 各项测试方法

本文档更新于 2020 年 02 月 26 日，根据 CTS Verifier 10.0_r1 更新

4.3.1 AUDIO

本项测试需要用到外部设备是：Sony SRS-X5 音箱、USB 麦克风、回环塞头。如果测试设备没有 3.5mm 的耳机插孔，测试者可以跳过该项测试且点击 PASS。

4.3.1.1 Audio Frequency Line Test

本项通过使用麦克风（通过回环塞连接）测量左右声道输出频率响应。需要准备回环塞和麦克风，把回环塞插在耳机插口，连接麦克风，根据提示开始测试，点击 YES 开始。

1. 点击 YES 确认设备具有耳机插口。如果没有，点击 NO，然后点击 PASS 来结束测试。2. 把回环塞插进耳机插口，点击 LOOP BACK PLUG READY。3. 点击 TEST 开始测试。4. 等待频率测试进行，测试结束后，如果结果全 OK 则点击 PASS。



图 10: Audio Frequency Line Test 测试

4.3.1.2 Audio Acoustic Echo Cancellation (AEC) Test

目前没有 AEC, 点击 NO, 然后点击 test 自动测试。

4.3.1.3 Audio Frequency Microphone Test

本项操作需要更仔细。它需要额外的 USB 接口麦克风和额外的扬声器。通过耳机接口连接扬声器。扬声器与测试样机间距离 40cm。系统会测试麦克风的频率响应。



图 11: Audio Frequency Microphone Test 测试

1. 将测试设备置于安静的房间，垂直放置扬声器，离设备中心相距 40cm，通过耳机或音频输出接头连接音箱，打开扬声器，点击第一个框里面的 PLAY 按钮。

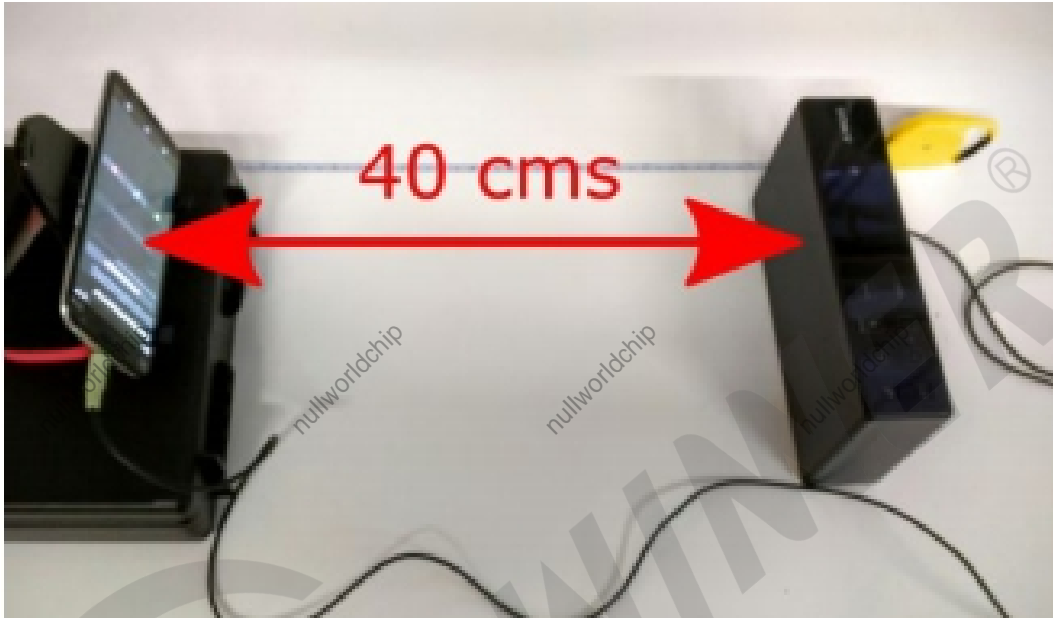


图 12: 测试设备放置

2. 点击 TEST 开始测试。当测试结束后，测试结果会显示在屏幕上。3. 连接 Microphone 或者有 Microphone 的耳机，点击第二个框里面的 TEST 按钮，完成测试后屏幕会出现结果。4. 不要拔掉 Microphone，点击第三个框里面的 PLAY 按钮，再点击 TEST 按钮，测试完会出现结果 PASS 按钮变绿色，即可 PASS。5. 通过这一项测试。



图 13: Audio Frequency Microphone Test 测试结果

4.3.1.4 Audio Frequency Speaker Test

本项测量扬声器的左右声道或单声道频率响应，需要额外的 USB 接口麦克风，系统会测试麦克风的频率。

1. 点连接 USB 麦克风，击 USB REFERENCE MICROPHONE READY。
2. 在安静的房间搭建测试，且 USB 麦克风垂直离屏幕中心约 20cm，点击 TEST。

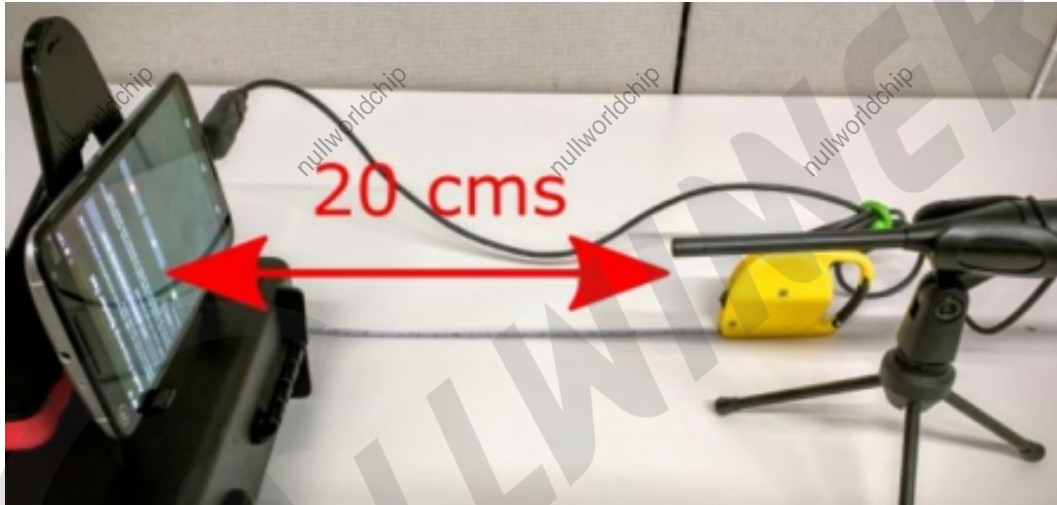


图 14: Audio Frequency Speaker Test 环境搭建

3. 等待几秒，根据测试结果点击 PASS 或 FAIL。

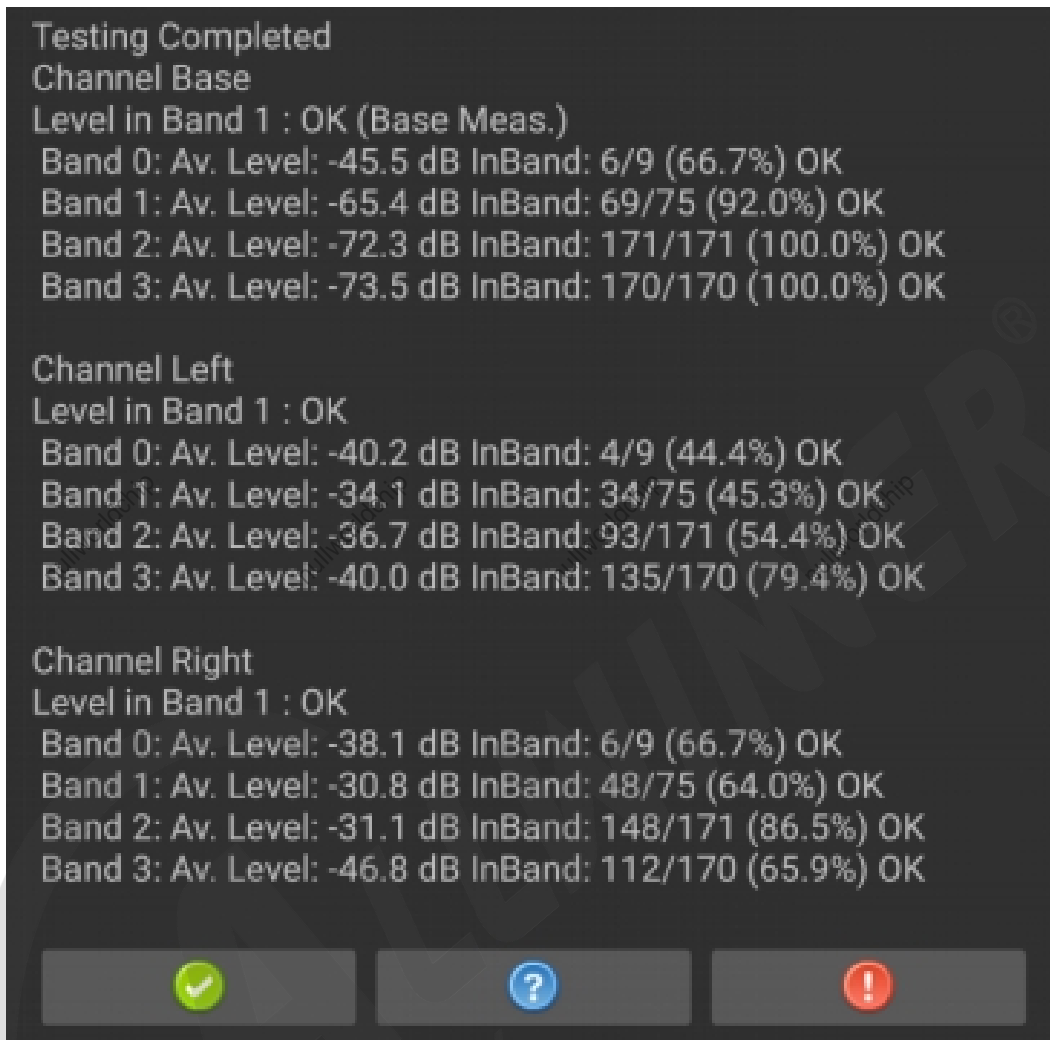


图 15: Audio Frequency Speaker Test 测试结果

4.3.1.5 Audio Frequency Unprocessed Test

1. 拔掉麦克风，点击第一个框里面的 PLAY 按钮，再点击 TEST 按钮，结果会显示 TEST 按钮下面。

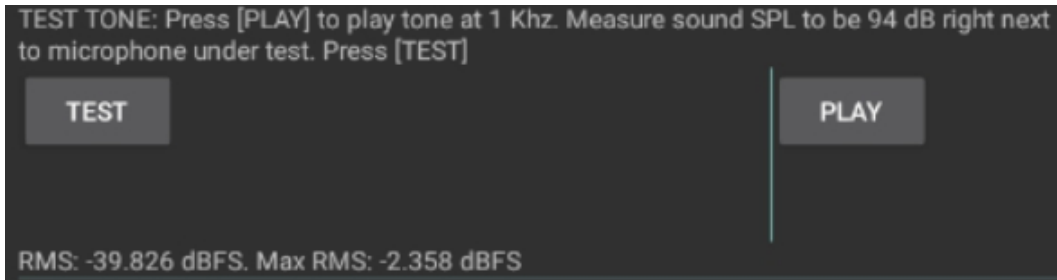


图 16: 测试项 1 操作说明

2. 点击第二个框里面的 PLAY 按钮，再点击 TEST 按钮，结果会显示 TEST 按钮下面。

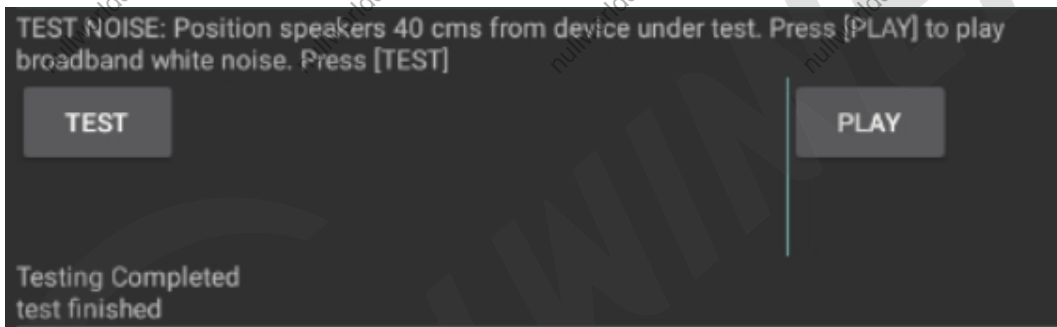


图 17: 测试项 2 操作说明

3. 插上 USB Microphone，点击 TEST 按钮，结果会出现在 TEST 按钮下面。

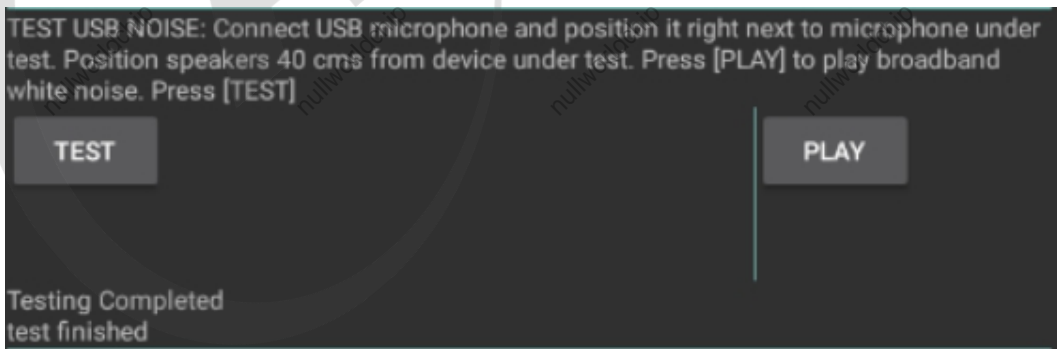


图 18: 测试项 3 操作说明

4. 插上 USB Microphone，点击 PLAY 按钮，再点击 TEST 按钮，结果会出现在 TEST 按钮下面。

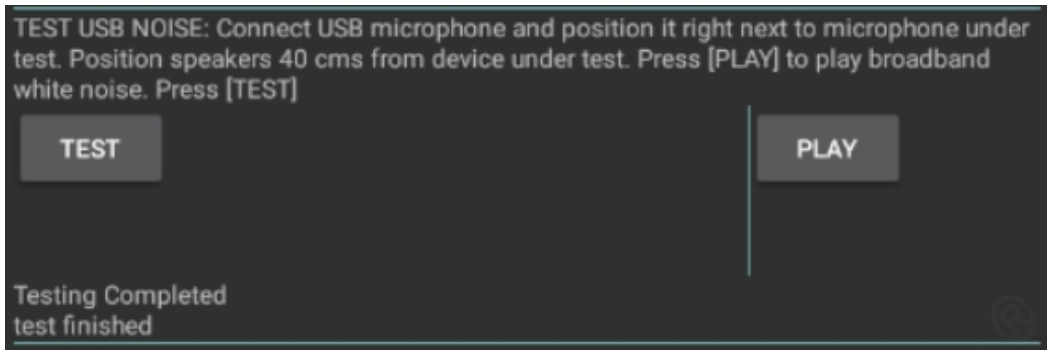


图 19: 测试项 4 操作说明

- 最后结果会显示在屏幕上，最终结果 PASS，则按 PASS。



图 20: Audio Frequency Unprocessed Test 测试结果提示

4.3.1.6 Audio Frequency Voice Recognition Test

1. 拔掉麦克风，点击第一个框里面的 PLAY 按钮，再点击 TEST 按钮，结果会显示 TEST 按钮下面。第二个 RMS 显示值 23 dBFS 左右，且两值相差不大。

注意，外放音量不能太大，控制在百分之 30 左右，第二项依赖于第一项，要保持音量不变。

2. 点击第二个框里面的 PLAY 按钮，再点击 TEST 按钮，结果会显示 TEST 按钮下面。

3. 插上 USB Microphone，点击 TEST 按钮，结果会出现在 TEST 按钮下面。

4. 最后结果会显示在屏幕上，最终结果 PASS，则按 PASS。

注意：一定要在安静的环境下测试这项！

4.3.1.7 Audio Input Devices Notification Test

本项测试插入设备的通知提示是否正常。

1. 点击 YES 确认设备具有耳机插口。如果没有，点击 NO，然后点击 PASS 来结束测试。

2. 点击 CLEAR MESSAGES 然后拔插一下麦克风或有线耳机。如果有正确的通知信息显示在 CLEAR MESSAGES 按钮下，则 PASS，否则 FAIL。

4.3.1.8 Audio Input Routing Notification Test

本项测试需要 4 节耳机进行测试。插入 4 节耳机，点击 YES，点击 RECORD，拔出耳机，观察到 AudioRecord Routing Notifications 下面的信息有变化即 PASS，点击 STOP 结束测试。

4.3.1.9 Audio Loopback Latency Test

本项测试音频输入输出延时。测试前将回环塞插入耳机插孔，根据提示进行测试，置信水平 ≥ 0.6 则为 PASS。

1. 点击 YES 确认设备具有耳机插口。如果没有，点击 NO，然后点击 PASS 来结束测试。

2. 把回环塞插进耳机插口，点击 LOOP BACK PLUG READY。
3. 把音量调节至 60% 以上，点击 TEST 开始测试。
4. 测试结束后，结果显示在屏幕上，当置信值 ≥ 0.6 时，点击 PASS 否则，FAIL。

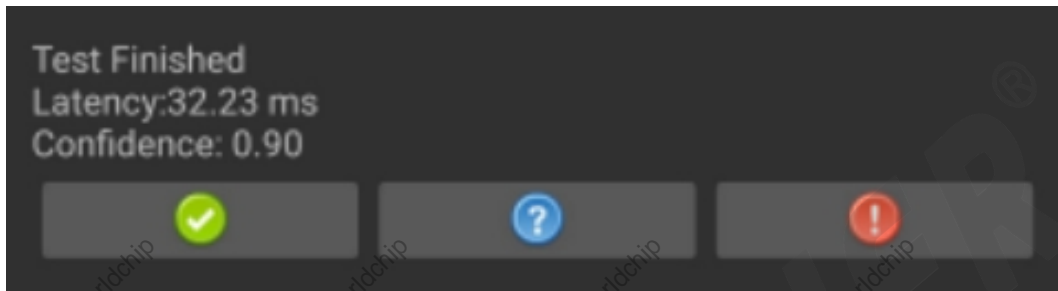


图 21: Audio Loopback Latency Test 测试结果

4.3.1.10 Audio Output Devices Notification Test

本项测试拔出设备的通知提示是否正常。

1. 点击 YES 确认设备具有耳机插口。
2. 点击 CLEAR MESSAGES 然后拔插一下有线耳机。如果有正确的通知信息显示在 CLEAR MESSAGES 按钮下，则 PASS，否则 FAIL。

4.3.1.11 Audio Output Routing Notification Test

本项测试需要 4 节耳机进行测试。插入 4 节耳机，点击 YES，点击 PLAY，拔出耳机，观察到 AudioRecord Routing Notifications 下面的信息有变化即 PASS，点击 STOP 结束测试。

4.3.1.12 Hifi Ultrasound Microphone Test

本项测试需要准备 2 台设备，一台的是待测设备，一台是对比设备，可以是 Nexus6、Nexus5 或者任何可以产生超声波的设备。

1. 在两台设备上安装 CTS Verifier 并进入 Hifi Ultrasound Microphone Test。

2. 在待测设备上点击 RECORD，然后迅速在对比设备上点击 PLAY。
3. 等待测试结束，等待的过程中，设备屏幕显示情况如下图。

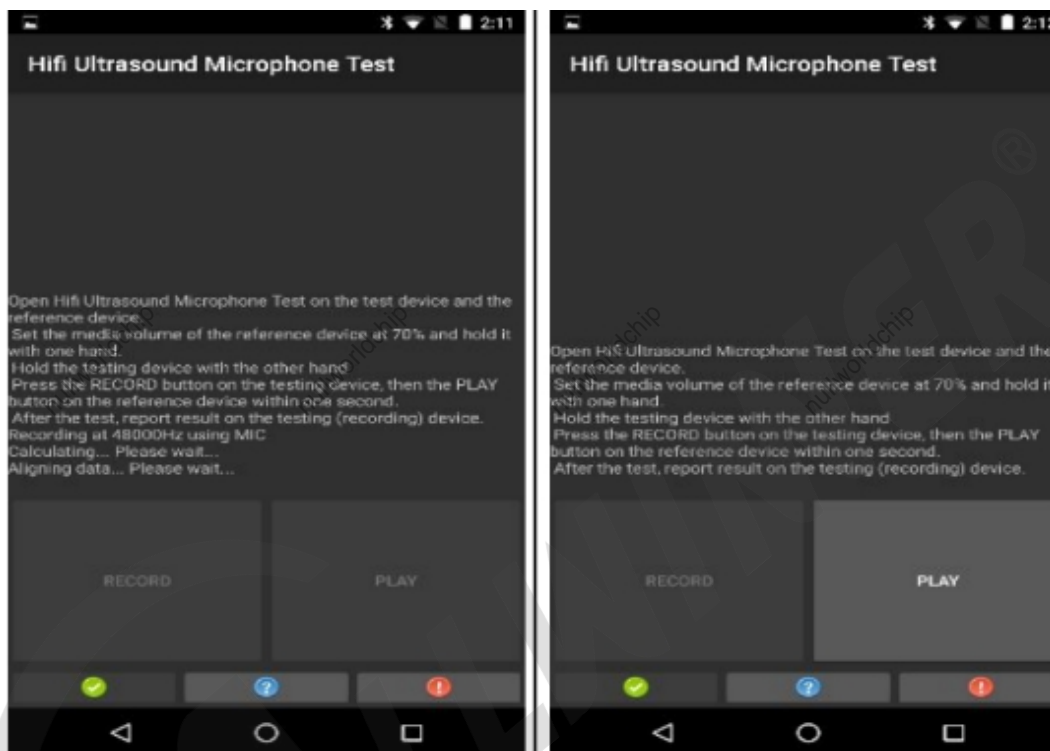


图 22: Hifi Ultrasound Microphone Test 测试界面

4. 在此过程不要做任何操作直到你看见屏幕显示如下面两图。如果待测设备上显示 PASS，则最终结果是 PASS；如果待测设备上显示 FAIL，则最终结果是 FAIL。

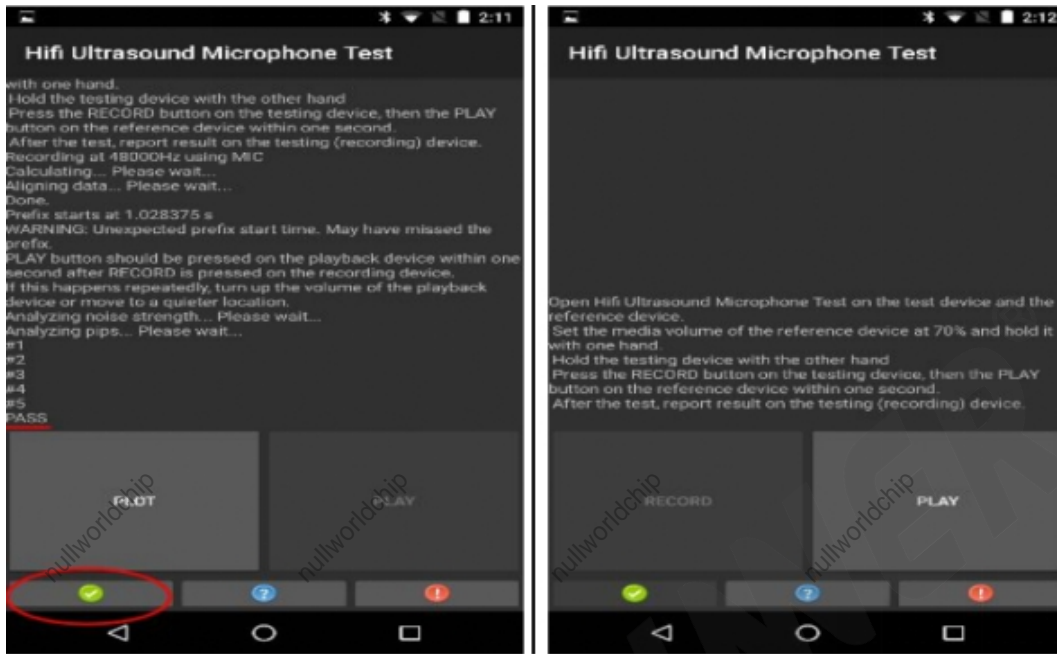


图 23: Hifi Ultrasound Microphone Test 测试过程

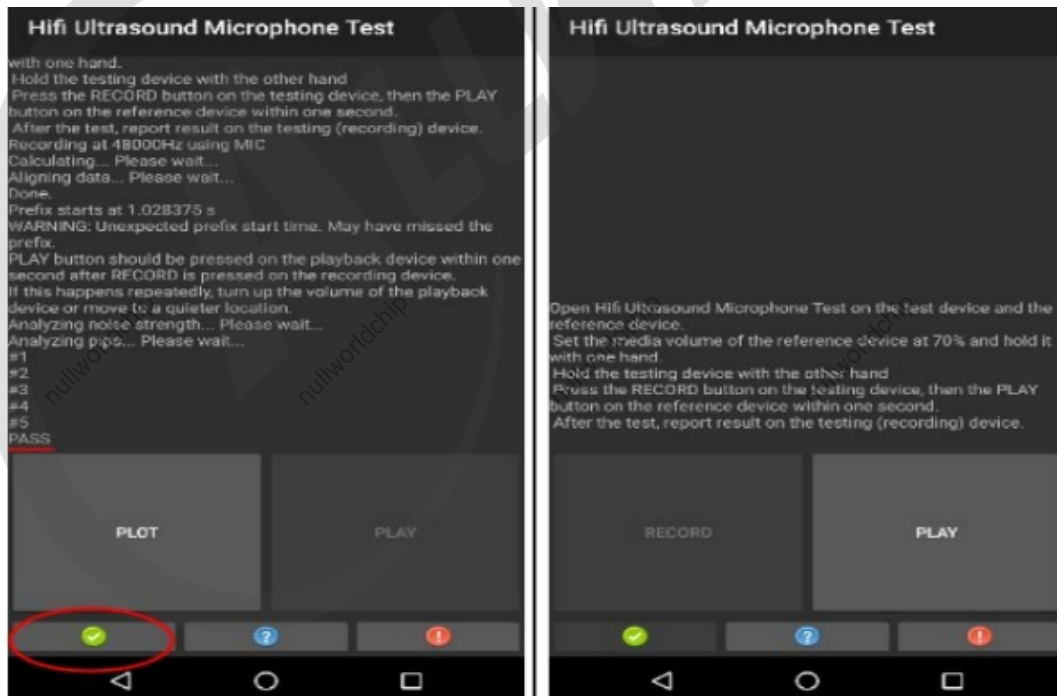


图 24: Hifi Ultrasound Microphone Test 测试结果

以下是非必要步骤，你可以画出计算得到的响应通过 PLOT 按钮。在待测设备上点击 PLOT

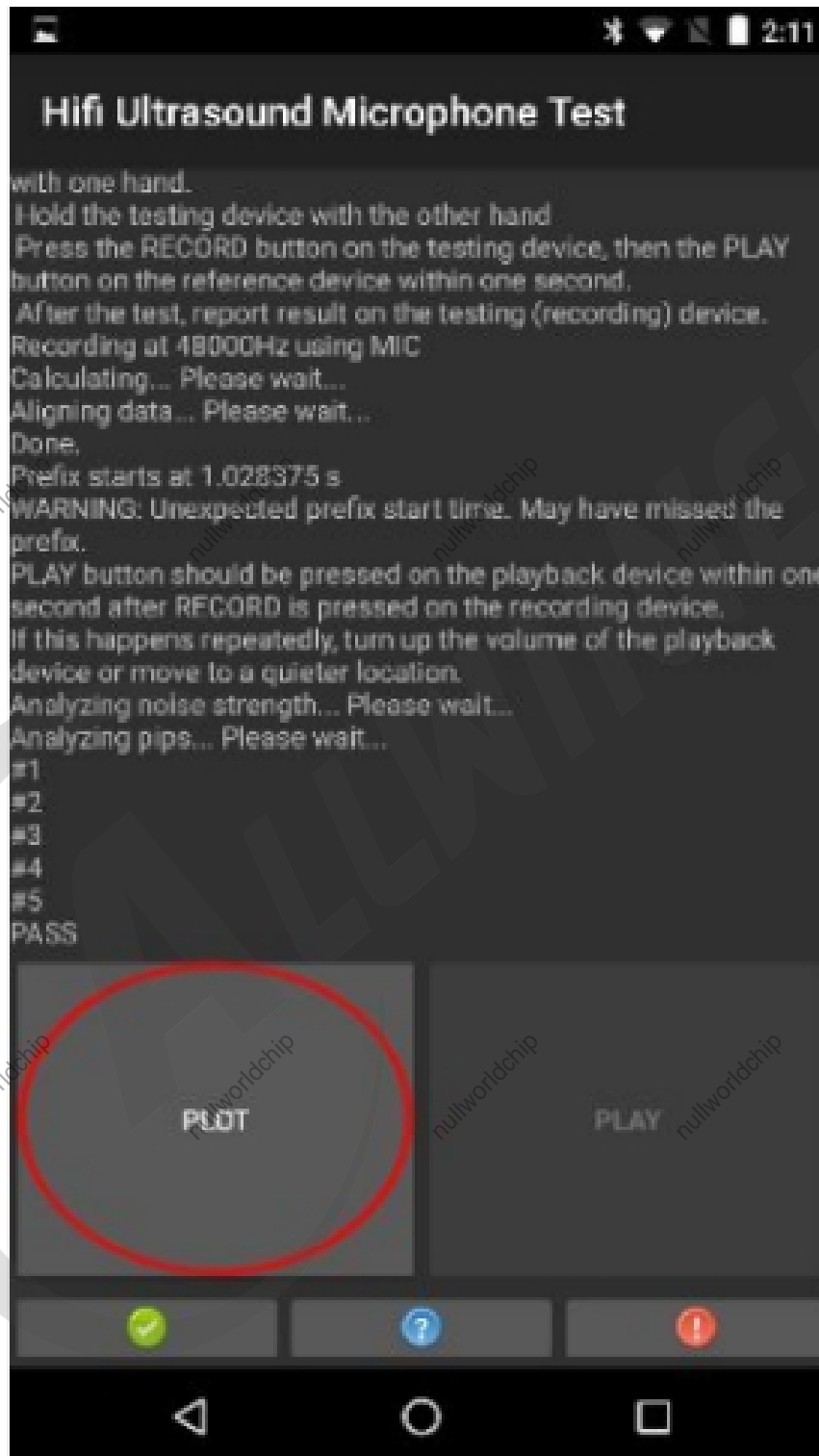


图 25: PLOT 按钮

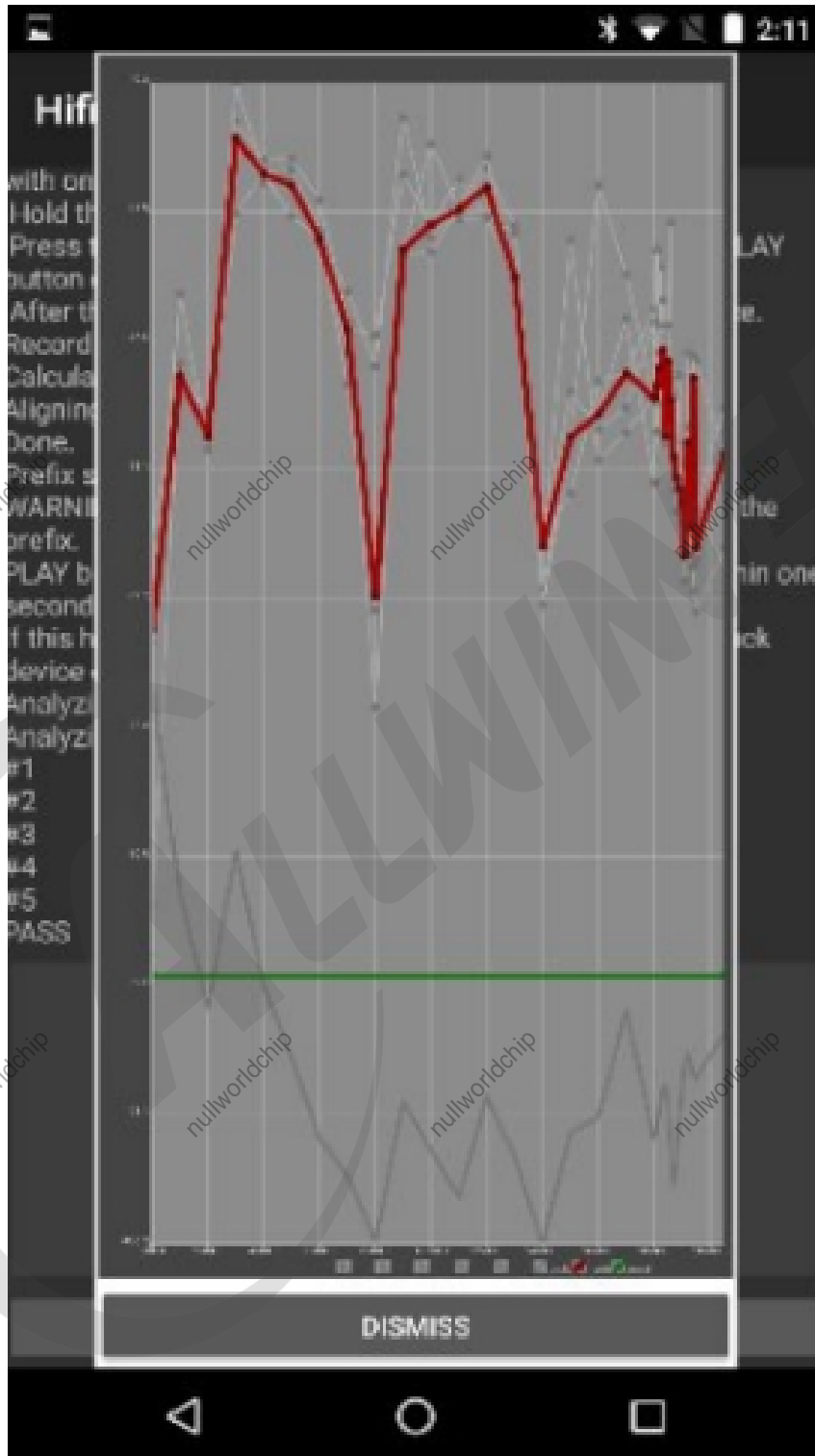


图 26: PLOT 结果

4.3.1.13 Hifi Ultrasound Speaker Test

本项测试需要准备 2 台设备，一台的是待测设备，一台是对比设备，可以是 Nexus6、Nexus5 或者任何可以产生超声波的设备。

1. 在两台设备上安装 CTS Verifier 并进入 Hifi Ultrasound Speaker Test。
2. 在待测设备上点击 PLAY，然后迅速在对比设备上点击 RECOED。

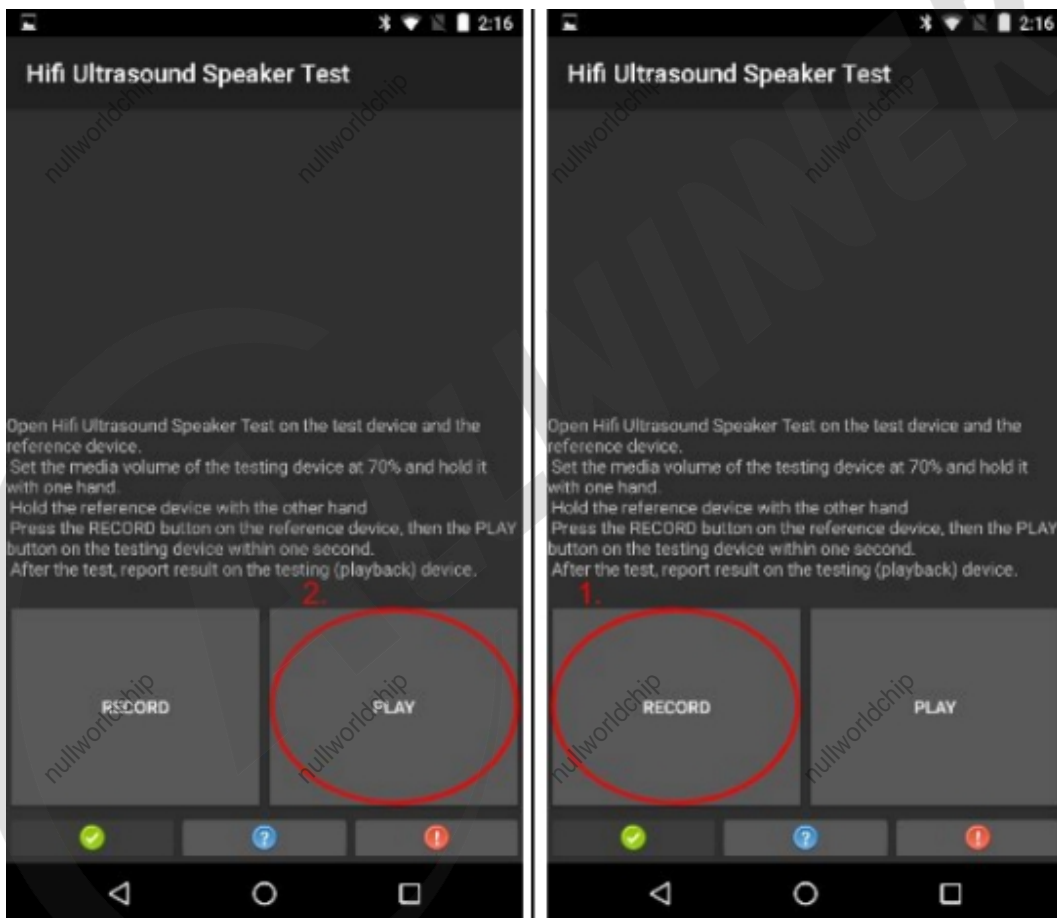


图 27: Hifi Ultrasound Speaker Test 操作

3. 测试开始，等待的过程中，屏幕显示如下，这个过程中不要做任何操作。

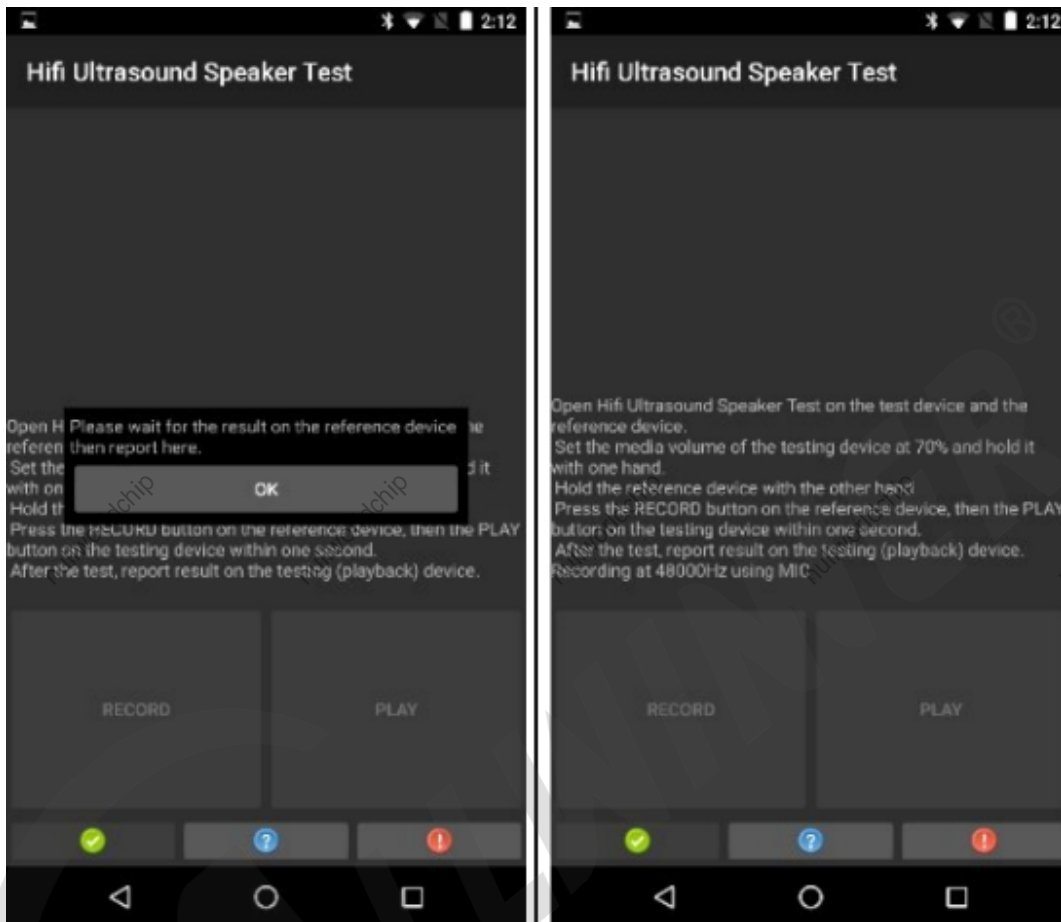


图 28: Hifi Ultrasound Speaker Test 测试过程

4. 当对比设备出现弹出对话框时，在待测设备上点击OK。

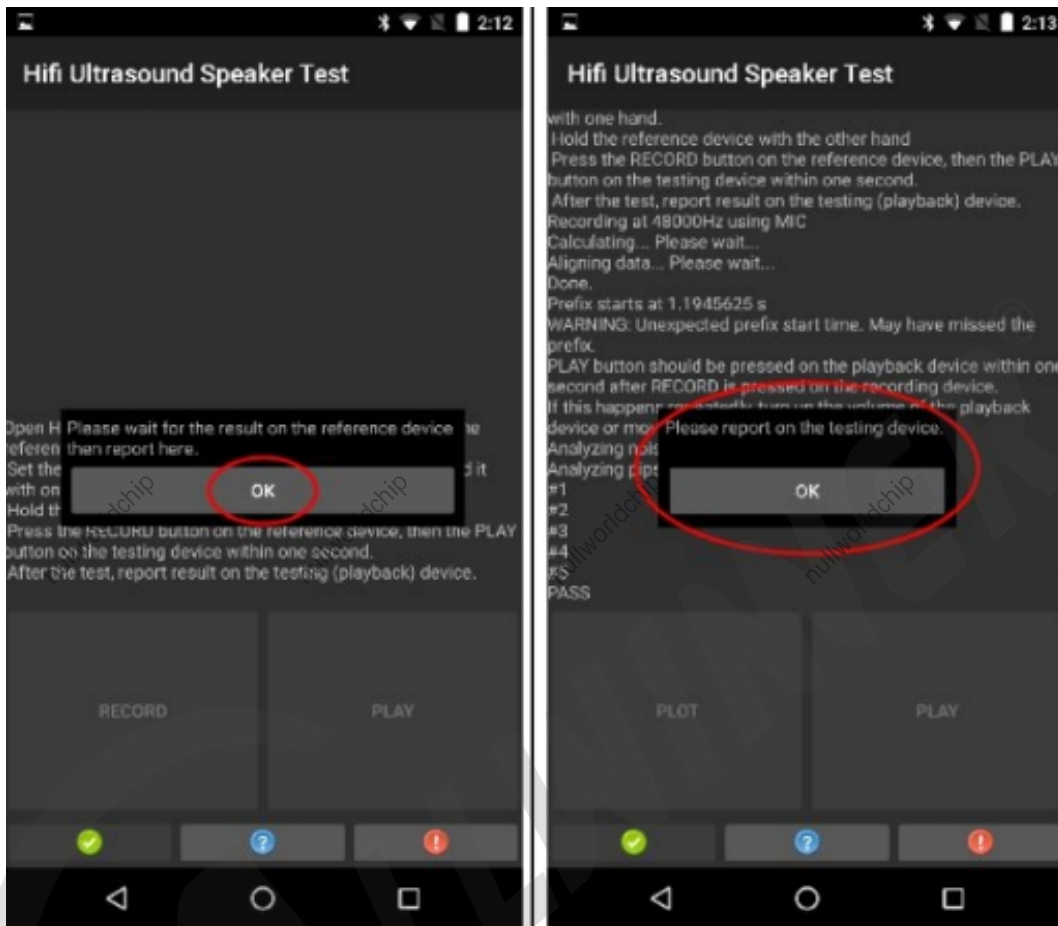


图 29: Hifi Ultrasound Speaker Test 测试结果

5. 在对比设备上，如图测试结果显示 FAIL，则在待测设备上点击 FAIL，否则 PASS。

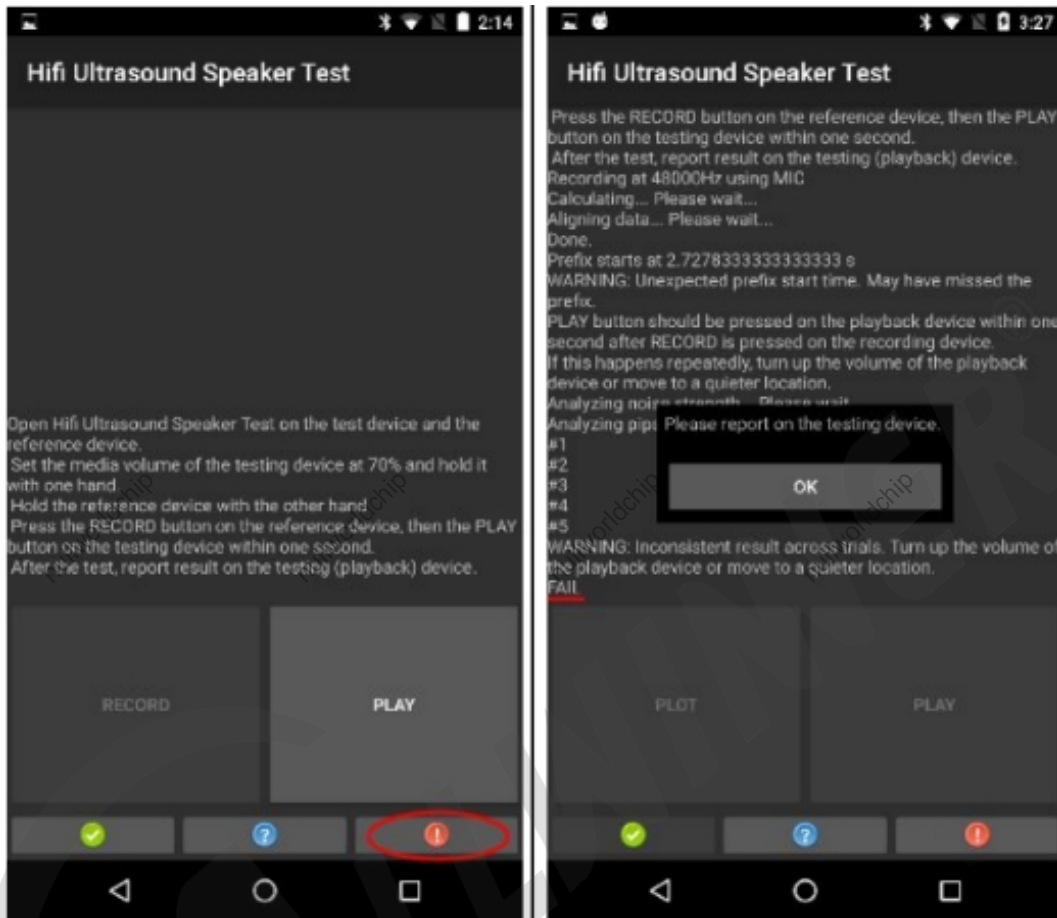


图 30: 对比样机测试过程

以下是非必要步骤，你可以画出计算得到的响应通过 PLOT 按钮。在对比设备上点击 PLOT 即可。

4.3.1.14 MIDI Test

暂时没有这个硬件条件，可直接 PASS。

4.3.1.15 Nation MIDI API Test

暂时没有这个硬件条件，可直接 PASS。

4.3.1.16 Pro Audio Test

连接 HDMI 外围设备 (非耳机), 并且该外围设备的音频输出连接音频输入, (另外对于具有模拟音频插孔或 USB-c 数字到模拟加密狗的设备, 可以使用环回插头。此外, 如果外围设备上有输入级控件, 则必须将设备设置为非零值。) 开始测试时, 打勾 Has HDMI Support, 点击 ROUND-TRIPTEST 按钮,

注意, 为了获得足够置信值, 可能需要多次运行延迟测试。

4.3.1.17 Ringer Mode Tests

1. 关闭勿扰模式, 点击 I'M DONE 按钮。
2. 打开勿扰模式, 选择 Alarms only 模式。
3. 等到下一个 I'M DONE 时, 关闭勿扰模式, 点击 I'M DONE 按钮。
4. 打开声音设置, 打开声音效果, 非静音状态, 点击 I'M DONE 按钮。
5. 测试通过则 PASS。

4.3.1.18 USB Audio Peripheral Attributes Test

1. USB 音频外设已通过外设数据线和 OTG 适配器连接到 Android 设备。

4.3.1.19 USB Audio Peripheral Buttons Test

1. 插上外部有音量控制和播放暂停的耳机, 按顺序按下耳机的播放暂停, 音量+, 音量-按钮。PASS 按钮变绿, 即可点击 PASS 通过。

4.3.1.20 USB Audio Peripheral Play Test

1. 将 USB 音频外设连接到 Android 设备, 耳机已连接到 Android 设备。

4.3.1.21 USB Audio Peripheral Record Test

1. USB 音频接口已通过回环连接到 Android 设备。



图 31: USB 音频接口

2. USB 音频接口背面的连接。



图 32: SB 音频接口背面的连接

3. USB 音频接口正面的连接。



图 33: USB 音频接口正面的连接

4. 建立连接后的屏幕，正在运行录制测试.

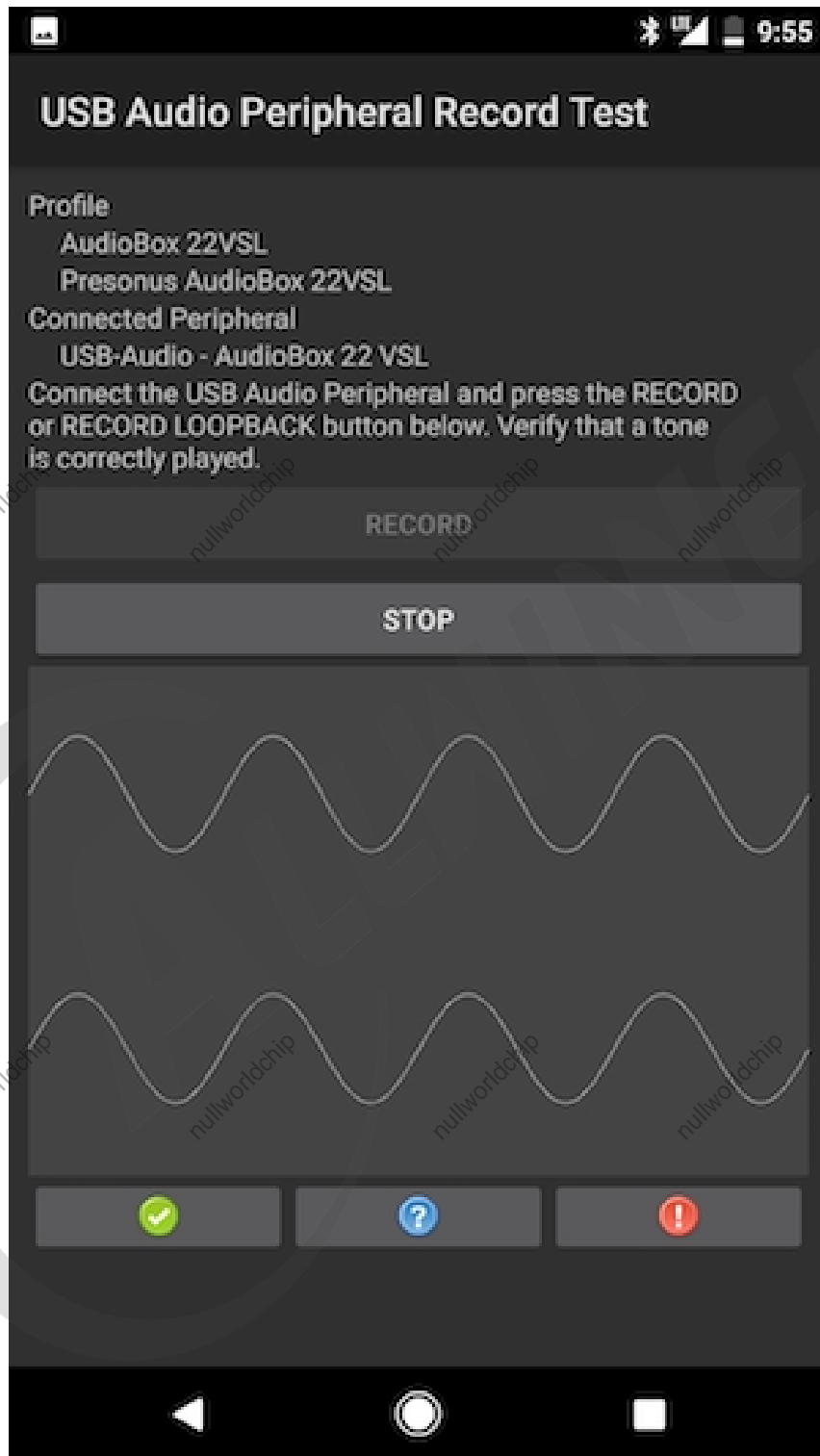


图 34: 运行录制测试

4.3.2 CAMERA

4.3.2.1 Camera FOV Calibration

本测试用例用于检测上报的 Camera 取景角度。测试环境如图 35 所示：

1. 需要一张 A4 测试纸。纸上画有中线和边线。中线位于纸正中央。两条边线位于中线的两边，且据中线的距离相等。两条边线之间的距离为“Marker Distance”

2. 测试平板垂直放在桌面上与测试纸平行。摄像头对准测试纸的中线。平板与测试纸之间的距离为“Target distance”。

上述准备工作完成后，可以进入测试：

1. 进入 Camera FOV Calibration 测试项，点击左上角的“Setup”按钮。将实际的 Marker distance 与 Target distance 写入设置。注意单位为厘米。
2. 返回测试界面。调整平板电脑，让平板测试界面的中线与测试纸的中线重合，并且测试界面中测试纸的两条边线分别与平板左右两端的距离相等。
3. 点击屏幕会产生一副图像。要求生成图像的正中央与测试纸的中线重合。拖动界面下方的可调整进度条使两条绿线与测试纸的边线重合。这时屏幕上方显示的“Displayed FOV”值为实际测量的取景角度，“Reported FOV”是平板上报的取景角度。点击 Done 按钮完成这一小项测试。
4. 一次测试中会对前/后摄像头以及不同的分辨率进行测试，所以需要多次重复步骤 3。测试过程中会自动变更分辨率和摄像头。当所有情况下测量得到的取景角度与上报取景角度的差值均小于 2，则测试通过。

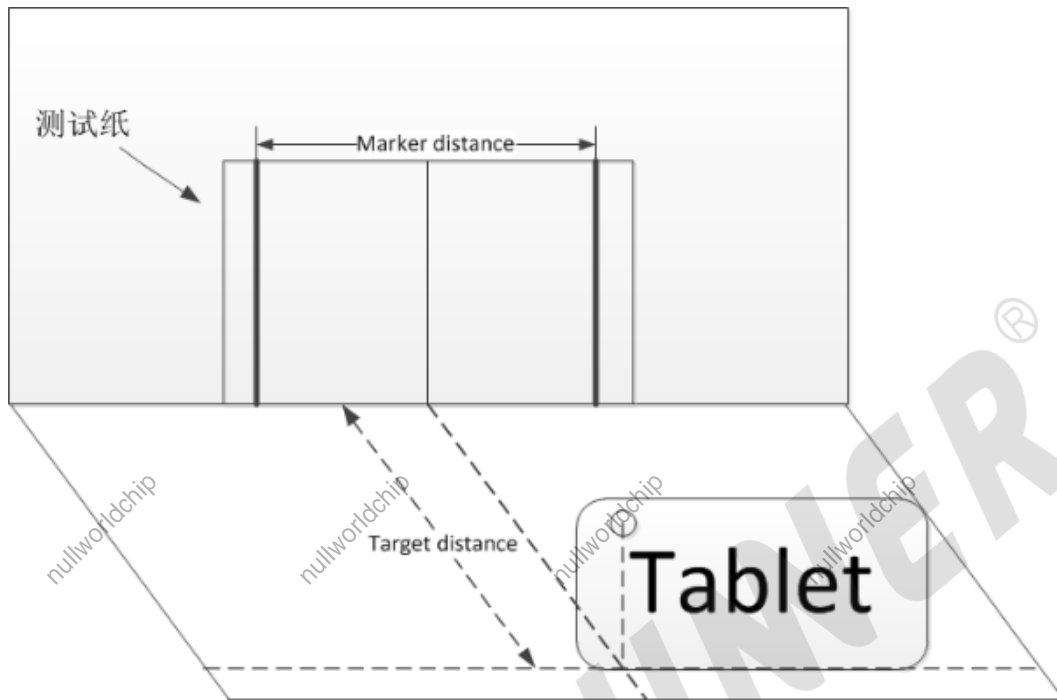


图 35: Camera FOV 测试环境图

4.3.2.2 Camera Formats

本测试用例用于检测 Camera 的回调处理是否正常和 mandatory formats are available。测试界面中有 2 个画面，测试后置设想头时要求 2 者画面一致（如图 36 所示），测试前置摄像头时要求画面水平镜像（如图 37 所示）。对比左右画面不能有失真，变形。

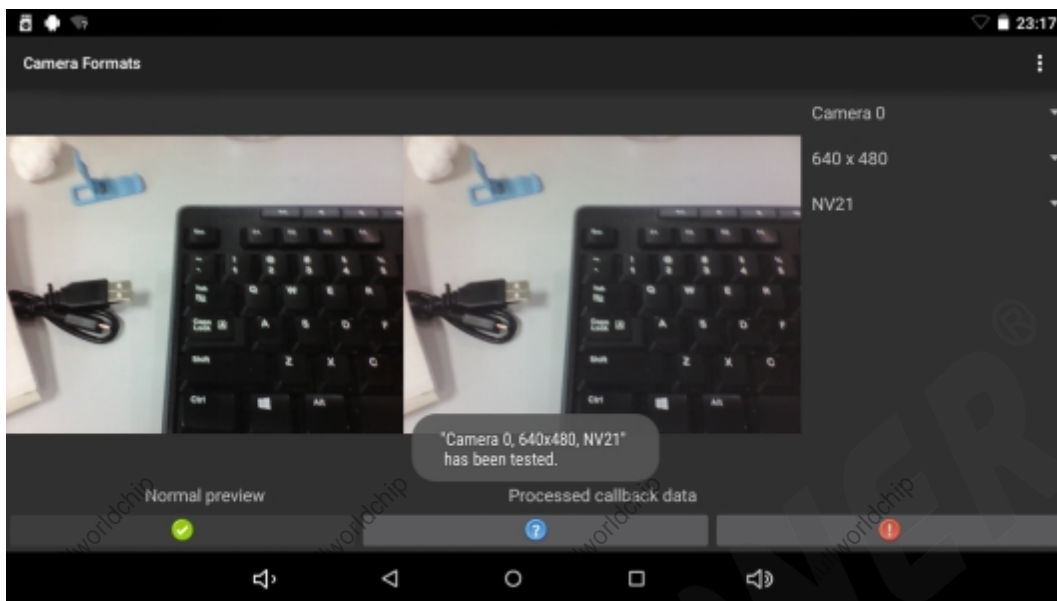


图 36: 后置摄像头 Camera Formats 测试

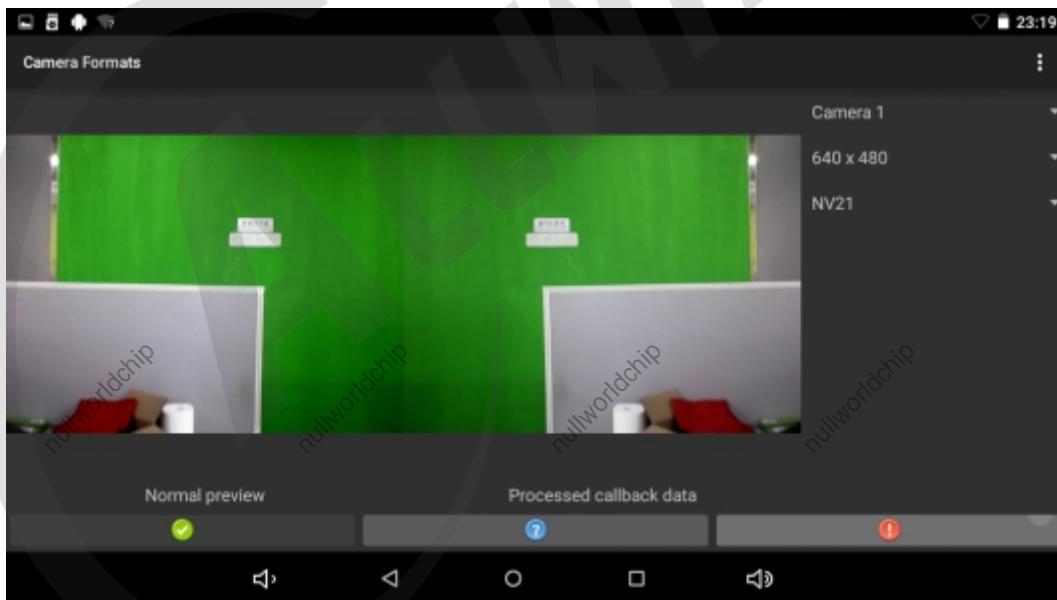


图 37: 前置摄像头 Camera Formats 测试

调节右侧的选择框，遍历所有摄像头，分辨率和格式的组合。当每一种组合均符合要求则测试通过，点击 PASS；否则测试失败，点击 fail。

4.3.2.3 Camera ITS Test

测试目标:

验证图像的正确性。补充 CTS 未覆盖的情景（可验证 HAL 3.2 测试计划的重要组成部分），ITS 是 CTS 验证程序的子程序。ITS 主要测试 camera 的 API，并不是成像质量。

测试方法:

Python 脚本通过 USB 连接 Android 设备的工作站上运行测试（包括 6 个测试场景）。在运行 Python 脚本之前启动 CTS 验证程序和 ITS 子测试，以便这些脚本具有可与之通信的进程。

平板设置:

1. 设置 > 显示 > 休眠 > 无操作 30 分钟后, 自动调节亮度 > 关闭
2. 测试方法: 找到一台已经安装好环境的 linux 系统的电脑, 进入测试包根目录（在 verifier 测试包里面有一个 ITS 的测试包）, 然后运行 `source build/envsetup.sh` 检测环境, 然后运行 `python tools/run_all_test.py device=序列号`, 然后跟着电脑提示操作便可以, 测试时长大概 15 分钟。

4.3.2.4 Camera Intents

进入测试界面后, 测试步骤如下:

1. 点击 START TEST 按钮。
2. 点击 HOME 按键回到 Launcher 主界面, 找到 Camera 应用并且点击进入, 拍一张照片。
3. 通过最近应用按键选择返回 Verifier 测试界面。这时 PASS 按钮应变成可点击。点击 PASS 按钮进入下一小项测试。
4. 点击 START TEST 按钮。
5. 通过最近应用按键选择返回 Camera 应用。调整为摄像模式, 拍摄一段录像。
6. 通过最近应用按键选择返回 Verifier 测试界面。这时 PASS 按钮应变成可点击。点击 PASS 按钮进入下一小项测试。
7. 点击 START TEST 按钮, 这时会进入照相预览。点击照会生成一副图像, 点击此时测试换面

的勾型（打钩）按钮返回测试。时 PASS 按钮应变成可点击。点击 PASS 按钮进入下一小项测试。

8. 点击 START TEST 按钮，这时会进入摄相预览。点击摄像拍摄一小段时间后停止，这时会生成一段视频，点击此时测试换面的勾型按钮返回测试。时 PASS 按钮应变成可点击。点击 PASS 按钮完成此项测试。

上述步骤必须全部通过才能通过此项测试。

4.3.2.5 Camera Orientation

此项测试预览与拍照的图像翻转功能。测试界面中有 2 个图像。左侧是预览图，右侧是拍摄的照片。前后置摄像头均参与此项测试，每个摄像头会测试 0 度，90 度，180 度和 270 度这 4 个旋转角度，所以有 8 个测试小项。在每一个小项中点击“TAKE PHOTO”按钮，预览图像和拍照后的图像均需要符合右上角给出的旋转角度，测试正常时点击 PASS 按钮进入下一小项测试，否则点击 FAIL 按钮。

4.3.2.6 Camera Performance

1. testSingleCapture 点击按键，自动测试，等待结果。
2. testReprocessingLatency 点击按键，自动测试，等待结果。
3. testReprocessingCaptureStall 点击按键，自动测试，等待结果。
4. testLegacyApiPerformance 点击按键，自动测试，等待结果。
5. testHighQualityReprocessingLatency 点击按键，自动测试，等待结果。
6. testReprocessingThroughput 点击按键，自动测试，等待结果。
7. testHighQualityReprocessingThroughput 点击按键，自动测试，等待结果。
8. testMultipleCapture 点击按键，自动测试，等待结果。
9. testCameraLaunch 点击按键，自动测试，等待结果。

4.3.2.7 Camera Video

此项测试 Camera 的摄像功能。在右侧的选择框中便利所有摄像头和摄像质量的组合。在每一种组合中，点击 TEST 按钮，录制 3 秒钟的视频，该视频会自动回放。如果摄像正常则点击 PASS 按钮，否则点击 FAIL 按钮。

4.3.3 CAR

4.3.3.1 Car Dock Test

此项测试 car mode 可以正常打开与 car dock 相关的 APP 当平板进入 car mode 时。点击 Enable Car Mode 开始测试，点击 home 按钮会激活 PASS 按钮。

4.3.4 CLOCK

4.3.4.1 Alarms and Timers Tests

此项测试验证 Clock APP implements the AlarmClock API 正确性。

Show Alarms Test

1. 点击 Show Alarms Test 能够进入如下界面则 PASS。

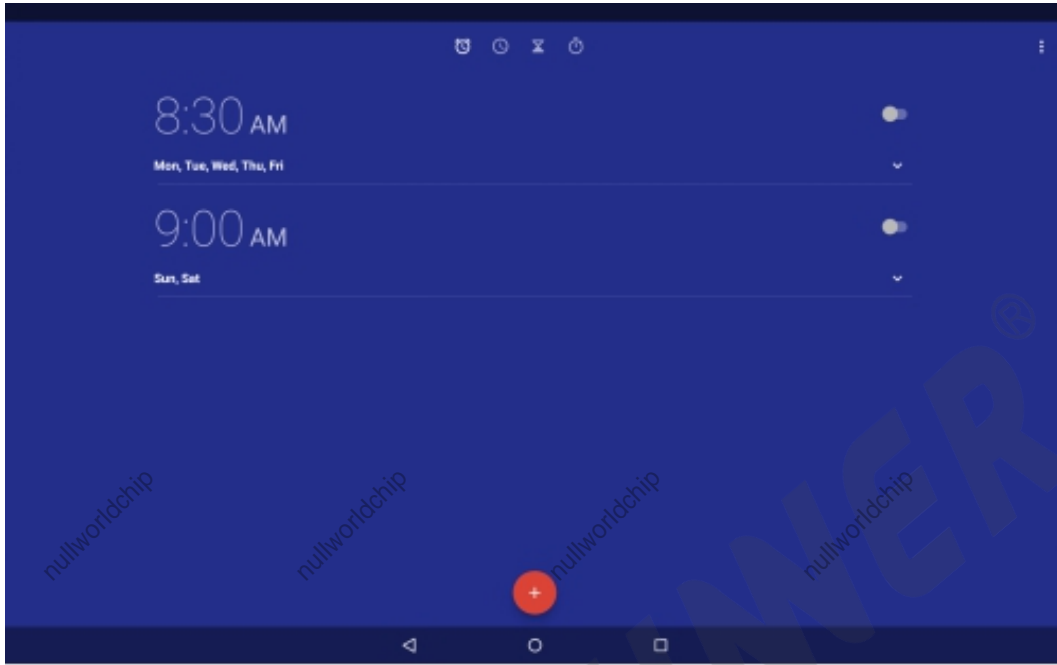


图 38: Show Alarms Test

Set Alarm Test

1. 点击 Set Alarm 按钮后能够进入到如下的闹钟设置界面则可以 PASS，否则 fail。

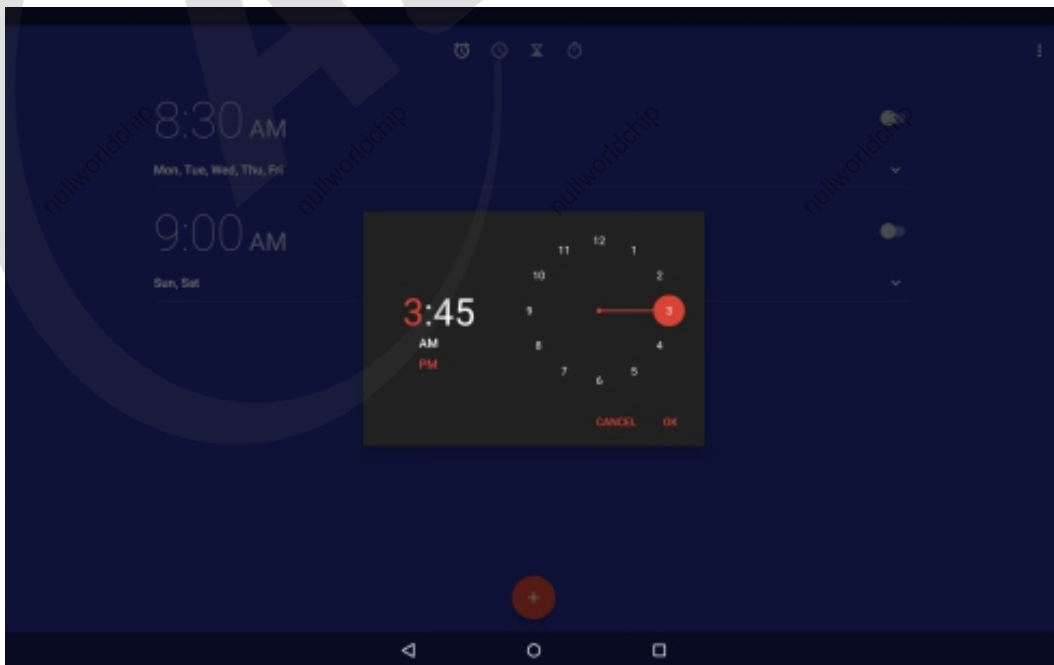


图 39: Set Alarm Test

Start Alarm Test

下述 6 个操作均通过则 PASS，否则 fail。

1. 点击 Set Alarm 按钮，会提示 "Alarm set for 2 minutes"
2. 确认闹钟的 UI 有没有弹出
3. 等待闹钟到点启动（大概 1-2 分钟），启动后的界面如下图所示：



图 40: Start Alarm Test 测试结果

4. 确认启动的闹钟的标题为 Start Alarm Test。
5. 点击取消消除掉此闹钟。
6. 点击 Verify 按钮，确认刚才的闹钟时间不在闹钟列表中，PASS。

Full Alarm Test

1. 点击 Create Alarm 按钮，弹出如下的闹钟设置界面：

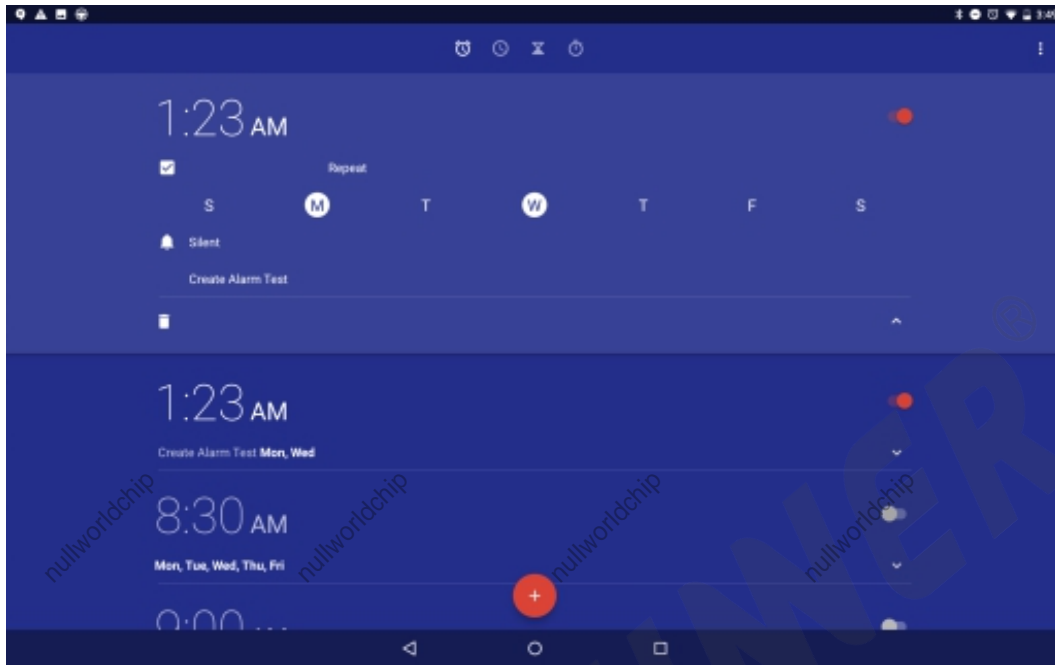


图 41: Full Alarm Test

2. 确认闹钟设置界面中的以下内容:

- 1) 闹钟名称: Create Alarm Test。
- 2) 如果有震动传感器, 需要显示 Vibrate: on。
- 3) 铃声为: Silent。
- 4) 时间为 01:23。
- 5) 重复时间为: Monday 和 Wednesday。

3. 确认无误后点击 PASS。

Set Timer Test

点击 Set Timer 按钮, 能够弹出如下图所示的定时管理界面即 PASS:



图 42: Set Timer Test 测试

Start Timer Test

1. 点击 **Start Timer** 按钮。
2. 确认一个定时器已经启动（左上角的通知栏有计时器的图标），并且没有任何计时器 UI 弹出。
3. 确认 30 秒后定时器响铃，并消除此定时器。
4. 确认定时器被消除。

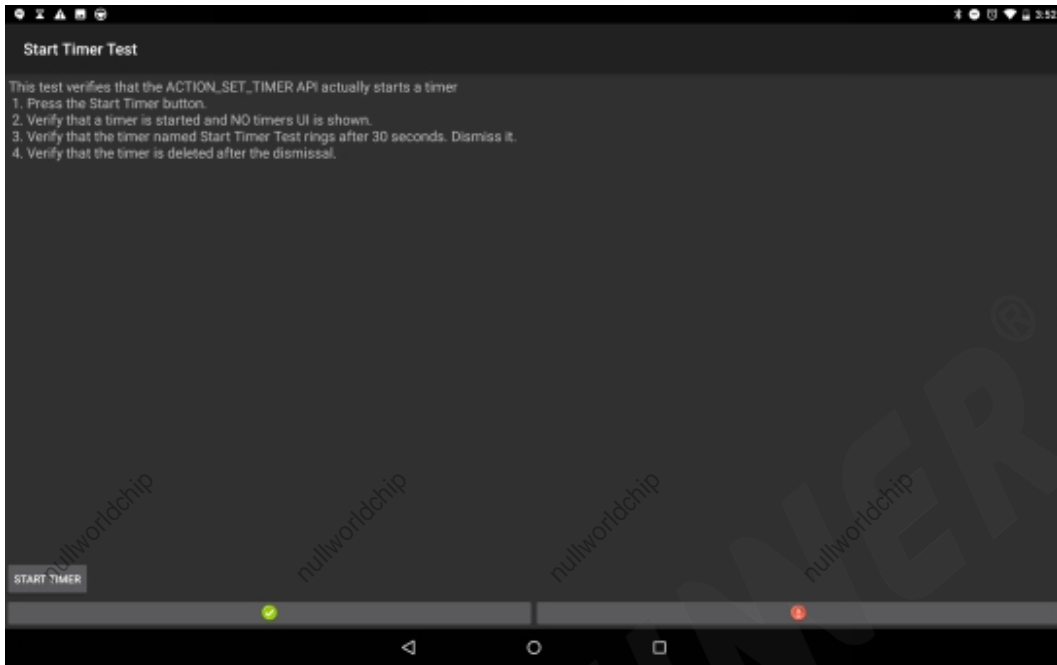


图 43: Set Timer Test 测试结果

5. 点击 PASS

Start Timer With UI Test

1. 点击 **Start Timer** 按钮。
2. 确认出现如下的倒数计时界面，计时器的名字为 **Start Timer Test**。

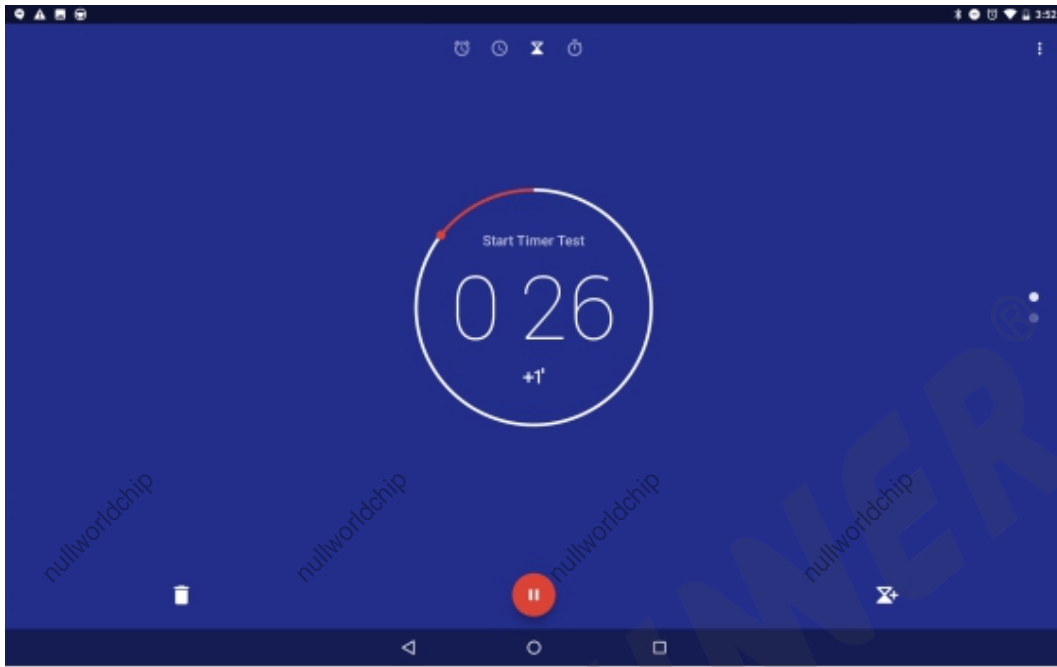


图 44: Start Timer With UI Test 测试

3. 确认 30 秒后铃声响起。
4. 点击 PASS。

4.3.5 DEVICE ADMINISTRATION

4.3.5.1 Device Admin Tapjacking Test

本项测试通过隐藏设备管理细节来检查活动是否不能记录，同时提示用户激活管理员。

1. 通过点击 ENABLE DEVICE ADMIN 按钮来运行设备管理。
2. 等到出现一个透明提示框时，点击返回。
3. 再次点击返回到 verifier 界面，点击 PASS 通过。

4.3.5.2 Device Admin Uninstall Test

1. 安装 ``Test Device Admin" app, 即在 verifier 套件里面的 CtsEmptyDeviceAdmin.apk, 将这个 apk 安装至设备。
2. 点击下面的按钮 ``ENABLE ADMIN" 按钮, 进入活跃管理者设置界面。
3. 将该 app 设置为活跃管理者, 返回到 verifier 界面, 点击 LAUNCH SETTINGS。
4. 点击 UNINSTALL, 卸载 apk, 回到 verifier 界面, 点击 PASS 通过。

4.3.5.3 Keyguard Disabled Features Test

本项测试禁用键盘守卫。进入 Settings->Security->Device administrators 中设置勾选 CTS Verifier 的对话框, 点击 Activate this device administrator 设置 CTS Verifier 为活跃管理员。需要进入 Settings->Security->Screen lock 设置锁屏密码为 ``testPASSWORD", 返回 CTS Verifier, 点击 PREPARE TEST:

1. 点击 Disable trust agents, 会弹出一个对话框, 上面也描述如何操作, 点击 GO 会跳转到 Settings->Security, 然后找到 Trust agents, 如果 agents 是灰色的 (disabled), 返回然后 CTS Verifier, 选择 PASS。
2. 点击 Disable camera, 然后屏幕会锁定, 点亮屏幕, 试着从锁屏界面启动相机, 但是会发现在屏幕的右下角已经没有了相机的图标, 无法在锁屏界面启动屏幕, 则返回 CTS Verifier, 选择 PASS。
3. 点击 Disable notifications, 屏幕会黑屏锁定, 然后观察在锁屏界面有没有通知, 如果没通知消息, 在解锁后进入系统可以看到在通知栏看到有一个通知 -This is a notifications, 则返回 CTS Verifier, 选择 PASS。离开该项测试后需要去 Settings->Security->Screen lock 去掉锁屏密码, 否则后面的 Redacted Notification Keyguard Disabled Features Test 测试会不成功。

4.3.5.4 Policy Serialization Test

本项应该放置在倒数第二项进行测试。

1. 点击 ``GENERATE POLICY" 按钮, 然后点击 ``APPLY POLICY" 按钮。
2. 重新启动平板再次进入该项测试。如果测试成功 PASS 按钮变成可点击。点击此按钮通过测试。

4.3.5.5 Redacted Notification Keyguard Disabled Features Test

本项测试禁用键盘守卫。进入 Settings->Security->Device administrators 中设置勾选 CTS Verifier 的对话框，点击 Activate this device administrator 设置 CTS Verifier 为活跃管理员。需要设置锁屏密码，为 "testPASSWORD"，一般会弹出 Notifications 的选项，选择 Show all notification content。返回 CTS Verifier，点击 PREPARE TEST，点击 Disable unredacted notifications，弹出对话框，选择 GO，屏幕会锁上，然后点亮屏幕，在锁屏界面会看到有通知的消息，那么就 PASS，离开该项测试后活跃管理员状态会被清空，需要手动清除设备密码。

4.3.5.6 Screen Lock Test

该项测试 DevicePolicyManager's lockNow 方法可以马上锁屏（需要设置有锁屏密码以及设置 cts-verifier 为活跃管理员）。点击 Force Lock 可以看到屏幕马上被锁定即为 PASS。

4.3.5.7 Usb Debugging Dialog Tapjacking Test

1. 用 usb 线连接样机和电脑。
2. 点击 SHOW OVERLAY 按钮，在显示的页面中将 CTS---Verifier，display app 权限设置为允许。
3. 打开 cmd 命令输入 "adb shell am start -e fingerprints placeholder -e key placeholder com.android.systemui/.UsbDebuggingActivityAlias"，随后样机会显示一个对话框，点击 OK 键进入 USB debug 模式。连接成功后点击 PASS 通过测试。

4.3.6 FEATURES

4.3.6.1 Companion Device Test

1. 打开蓝牙。
2. 点击 GO 按钮，随后会弹出蓝牙设备搜寻界面，点中任意一个设备，则该项 PASS 按钮变为可点击，则该项通过。

4.3.7 HARDWARE

4.3.7.1 MTP Host Test

这项测试需要两台设备和一条 OTG 线，把 OTG 线插上的设备叫主机，另一台是从机，通过 USB 线连接插在主机的 OTG 线。把两台机器连接之后，在从机上的通知栏会有两个消息（和插在电脑上一样的现象）。

1. 点击从机上的消息栏，选择 Transfer files, 主机会出现从机的文件管理器。
2. 点击第二小项的 PASS。
3. 然后第三小项会提示 usb 连接，点击 ok 即可。
4. 第四小项打开从机拍一张照片，该小项就可以通过了。
5. 点击 PASS 通过该项测试。

4.3.7.2 USB Accessory Test

测试需要两台设备，一台待测设备，一台帮助设备。测试操作步骤如下：

1. 安装 Cts Verifier USB Companion app 在辅助设备上。
2. 使用 OTG 线连接两台设备，OTG 线的一端必须插在辅助设备上。打开辅助设备上安装的 Cts Verifier USB Companion，点击 START ACCESSORY TEST COMPANION，等待两台设备弹出对话框，点击 ok。
3. 等待测试通过，如果没有反应则拔插一下 otg 线。
4. 该项自动会 PASS 或 fail。

4.3.7.3 USB Devices Test

测试需要两台设备，一台待测设备，一台帮助设备。测试操作步骤如下：

1. 安装 Cts Verifier USB Companion app 在辅助设备上。
2. 使用 OTG 线连接两台设备，OTG 线的一端必须插在待测设备上。打开辅助设备上安装的 Cts Verifier USB Companion，点击 START ACCESSORY TEST COMPANION，等待两台设备弹出对话框，点击 ok。
3. 等待测试通过，如果没有反应则拔插一下 otg 线。

4.3.8 INSTANT APPS

4.3.8.1 Instant Apps Notification Test

测试前安装 instant app, 点击 START TEST, 看到 ``hello,world" 返回 PASS。

4.3.8.2 Instant Apps Rescent Test

点击 START TEST, 看到 ``hello,world", 返回 PASS。

4.3.8.3 View/Delete Instant apps Test

点击 START TEST, 看到 ``hello,world", 返回 PASS。

4.3.9 OB SCHEDULER

4.3.9.1 Charging Constraints

进入测试界面后，操作步骤如下：

1. 一开始 ``START TEST" 按钮是灰色的，插入 USB 线使平板进入充电状态。
2. 这时 ``START TEST" 按钮应变成可点击。

3. 等待第二项变绿，断开充电，该项就可以通过了。

4.3.9.2 Connectivity Constraints

进入测试界面后，操作步骤如下：

1. 关闭 wifi 和手机信号。（在通知蓝下拉菜单中启动飞行模式即可）。这时“START TEST”按钮变为可点击。
2. 点击“START TEST”按钮。正常情况下 10 多秒即可完成测试，所有小项均能测试通过。
3. 所有小项测试通过则点击 PASS 按钮。

4.3.10 LOCATION

4.3.10.1 Battery Saving Mode Test

进入测试界面后的操作如下：

1. 在 Settings 中启用 Location 功能。
2. 在 Settings 中选择 Location Mode 为 Battery Saving。
3. 回到测试界面。
4. 正常情况下测试界面中显示的所有测试步骤会用绿色标记，表示测试通过。

4.3.10.2 Location Mode Off Test

进入测试界面后的操作如下：

1. 点击 Launch Settings，弹出设置界面。
2. 在设置界面中关闭 Location。
3. 回到测试界面。

4. 正常情况下测试界面中显示的所有测试步骤会用绿色标记，表示测试通过。

4.3.11 MANAGED PROVISIONING

4.3.11.1 BYOD Managed Provisioning

进入此项目，会看到有“START BYOD PROVISIONING FLOW”按钮，如果设备之前没有加密，那么会提示进行加密，加密的过程会关机，整个过程需要几分钟。

(注意：加密需要设备的电量充足，需要电量在 **90%** 以上才能进行，否则他会提示充电并且无法进行)

Profile owner installed

加密重启之后，会在通知栏有个消息显示“Encryption complete”，则证明加密成功。回到此测试，看到 Profile owner installed 栏还是红色的，再点击“START BYOD PROVISIONING FLOW”按钮设置一下，一直确认 ok 就好，然后 Profile owner installed 就变绿色了。

Full disk encryption enable

需要设置屏幕锁，并且是 PIN 码锁，PIN 码设置为 1111（其它也可以，能记住就可以），设置好之后该项测试就通过了。测试通过之后会提示把锁屏密码去掉，屏幕不设置密码。

Badged work apps visible in Launcher

点击 Badged work apps visible in Launcher，弹出一个对话框，点击 GO 按钮，会打开 Launcher，并且在 Launcher 上会生成名为 Work 的 APP 文件夹，里面有几个图标带有标志的 APP，其中包括 CTS Verifier。返回 CTS Verifier 测试项，如果有上述现象，则 PASS。

Work notification is badge

进入此项之后点击 GO 按钮，下拉通知栏，如果看到有一个新的通知，上面的内容是“This is a notification”，并且在该消息栏右边有个标记（类似一个书包），则 PASS

Work status icon is displayed

进入此项之后点击 GO 按钮，会跳转到一个新的界面，观察屏幕上方的状态栏（电池电量、Wifi 那里），如果有一个白色的小书包标志出现，点击 Finish 则 PASS。

Work status toast is displayed

进入此项之后点击 GO 按钮，会跳转到一个新的界面，然后把屏幕黑屏，过几秒钟之后点亮屏幕，会出现一个 toast 消息，需要留意这个消息上有没有一个白色的小书包标志，（如果没看清楚，可以继续黑屏和亮屏操作，仔细观察）如果有，点击 FINISH 返回，并且 PASS

Profile-aware accounts

进入此项之后点击 GO 按钮，会跳转到 Setting 的页面，进入 Accounts 设置项，看到有 Personal 和 Work 分类，Remove work profile 在 Work 栏。接着连续点击屏幕右上角的“更多”按钮（三个点），看到里面有两个选项，一个是 Auto-sync personal data，另一个是 Auto-sync work data，然后随便去掉人一个勾选，会出现一个警告对话框，那么返回测试界面，PASS。

Profile-aware devices administrator setting

进入此项之后点击 GO 按钮，会跳转到 Setting->Security 页面，找到 Devices administrator，点入，可以看到里面的东西都是成对出现，其中一个是有红色小书包标志，另一个是没有的。在列表中存在 CTS Verifier，尝试去把有红色小书包标志的 CTS Verifier 的勾去掉，会弹出一个页面，在这个页面上有 Remove work profile 选项。返回测试软件，PASS。

Profile-aware trusted credential settings

进入此项之后点击 GO 按钮，会跳转到 Setting->Security 页面，找到 Trusted credential，点入，在列表中分别有 Personal 类的证书和 Work 类的证书，返回测试软件，PASS。

Profile-aware app settings

进入此项之后点击 GO 按钮，会跳转到 Setting 的 APPs 页面，在 APP 列表里面有一些红色小书包标志的应用，点击随便一个这样的 APP，会进入到 APP 的 APP info 页面，PASS。

Profile-aware Location settings

进入此项之后点击 GO 按钮，会跳转到 Setting 的 Location 页面，在页面有一个 Location for work profile，后面的开关能够点击。点击 Location 的开关（屏幕的右上角，最上面的一个）使其为 OFF 状态，则 Location for work profile 的开关状态也随着到 OFF 状态。继续点击 Location 的开关（屏幕的右上角，最上面的一个）使其为 ON 状态，则 Location for work profile 的开关状态也随着到 ON 状态。返回测试软件，PASS。

Profile-aware printing settings

进入此项之后点击 GO 按钮，会跳转到 Setting 的 printing 页面，在 printing 页面的左上角显示

Personal, 这是 Personal 的 printing 的设置页面。点击可以展开内容, 会看到有个 Work, 点击 Work, 页面会切换一下, 看到 Work 在左上角, 现在就是 Work 的 printing 的设置页面。返回测试软件, PASS。

Open app cross profiles from the personal side

进入此项之后点击 GO 按钮, 会弹出一个对话框, 点击 CTS Verifier, 会弹出一个新的界面, 提示 You selected the ctsverifier option, 点击 FINISH, 返回测试软件, PASS。

Open app cross profiles from the work side

进入此项之后点击 GO 按钮, 会弹出一个对话框, 点击 CTS Verifier (有红色小书包标志), 会弹出一个新的界面, 提示 You selected the ctsverifier option, 点击 FINISH, 返回测试软件, PASS。

Disable non-market apps

进入此项之后点击 GO 按钮, 会弹出一个软件安装的界面, 并提示该软件不允许安装, 点击 OK, 返回, PASS。

Enable non-market apps

进入此项之后点击 GO 按钮, 会弹出一个软件安装的界面, 点击 INSTALL, 返回, PASS。

Cross profile intent filters are set

点一下就变绿 PASS 了。

Permissions lockdown

在测试之前先去 Setting->APPS, 看是否有 CtsPermissionAPP, 如果没有, 需要通过 adb 安装。本测试指南的开始介绍有。返回测试的页面, 点击 GO 按钮 (注意, 如果你在 APPS 里看见有 CtsPermissionAPP, 但是点击 GO 之后提示没有安装, 那么需要把 CtsPermissionAPP 卸载后重装), 会跳转到一个叫 Permissions lockdown 的界面。屏幕左下角有三个选项, 在屏幕下端的中间有一个按钮 "OPEN APPLICATION SETTINGS"。先选择 Grant, 然后点击 OPEN APPLICATION SETTINGS, 跳转到一个设置页面, 找到 Permissions, 点击去无法设置。选择 Let user decide, 然后点击 OPEN APPLICATION SETTINGS, 跳转到一个设置页面, 找到 Permissions, 点击去可以设置开关。选择 Deny, 然后点击 OPEN APPLICATION SETTINGS, 跳转到一个设置页面, 找到 Permissions, 在 Permissions 下面有一小行 -NO Permissions granted。完成上面的操作, 点击 FINISH 返回, PASS。

Keyguard disabled features

在测试之前先到 Setting->Security->Devices administrator 勾选 CTS Verifier, 设置 CTS Verifier 为

active admin。然后去 Setting->Security->Screen lock 设置锁屏密码为 ``testPASSword"。然后回到测试，先点击 ``PREPARE TEST"，接着点击 Disable trust agents，弹出一个对话框，点击 GO，跳转到 Setting->Security 页面，找到 Trust agents 点入，显示 Disabled by administrator，返回，PASS。接着点击 Unredacted notifications disabled on keyguard，点击 GO，屏幕会灭，等几秒钟（太久可能会卡死）点亮屏幕，看到通知栏 ``contents hidden by policy" 的通知，通知上有红色小书包标志，解锁后进入系统，下拉通知栏，会看到一个通知消息 -This is a notification，通知上有红色小书包标志，则 PASS。测试完之后把锁屏密码去掉。

Authentication-bound keys

先点击 SET UP 按键，会跳转到 Setting->Security，然后设置锁屏密码，设置一个密码（比如 1234），然后返回，点击 Lockscreen-bound keys，过几秒钟会弹出一个页面确认刚才设置的密码，输入正确，会返回看到 Lockscreen-bound keys 变绿了，PASS。

Check VPN

这一项可以直接 PASS。

Always-on VPN Settings

1. 测试前确保没有安装 CtsVpnFirewallAppApi23.apk，否则卸载从新安装。然后点击 PREPARE VPN，进入第一个测试，点击 go 进入 VNP，点击设置标志，确保 always-on VNP 和 block connections without VNP 属于禁止状态，返回 PASS。

2. 安装 CtsVpnFirewallAppApi24.apk，点击第二个测试，确保 always-on VNP 属于关闭状态，block connections without VNP 属于禁止状态，返回 PASS。

3. 安装 CtsVpnFirewallAppNotAlwaysOn.apk 点击第三个测试，go，确保 always-on VNP 和 block connections without VNP 属于禁止状态。

Turn off work profile

1. 点击第一个测试，go，通知栏出现 this is a notification 通知，PASS；

2. 点击第二个测试前点击 open settings to toggle work profile 去关闭 work profile，返回点击 go，弹出打开它的对话框，点击 OK，自动 PASS。

3. 第三个跟第五个也随着 PASS。

4. 点击第四个测试项，点击 go，打开发射器 Launcher，发现工作应用程序是灰色的，打开 verify 验证没有启动，PASS。

5. 点击第六个，go，下拉状态栏发现状态栏图标不再可见。

6. 点击最后一个测试，go，此时 work profile 已经打开，验证 verify 可以启动。

Select work lock test

点击 go，创建一个新 work lock 区别于之前设置的密码，PASS

Confirm work lock test

完成之前的测试才能进行这一步，点击 go，按下电源键，重新打开并滑动解锁，进入发射器，随便点击一个 work app，出现包含一个手提箱的蓝色背景的解锁页面，验证文本是否显示 cts verifier。且 work app 可以被启动 PASS。

Recents redaction test

点击第一个测试，go，设置一个 work PASSwork，关闭屏幕再打开，转到主屏幕，打开 recent 确认 cts verifier 显示在最近活动中；点击第二个测试，go，remove 掉 work PASSwork，打开最近，确认 cts verifier 显示在最近活动中，确认活动内容没有被隐藏，PASS。

Turn off work mode

点击 Prepare a work notification，看通知栏是否有消息通知，有则 PASS。点击第二行的 Please turn off work mode，会提示点击 OPEN SETTINGS TO TOGGLE WORK MODE 按钮，点击后跳转至 Account 的设置页面，点击 Work profile setting->work mode，去勾选。返回会看到 Please turn off work mode 这行已经变绿。看一下通知栏的是否还有 CTS Verifier 的消息，如果没有，则 PASS。点击 Status bar icon when work mode is off，会跳转至 Setting，在 Setting 页面的顶部显示有 Work profile is off，并且状态栏有个被切开的白色小书包标志，则 PASS。点击 Starting work apps when work mode is off，会弹出一个对话框，点击 GO，会跳转到 Launcher，左右滑动桌面找到一个叫 Work 的 APP 文件夹，如果里面的 APP 是灰色的，而且也无法打开，则 PASS。点击 Please turn work mode back on，会提示去点击 OPEN SETTINGS TO TOGGLE WORK MODE 按钮，去把刚才关闭的 work mode 打开。点击 Status bar icon when work mode is on，会跳转至 Setting，在 Setting 页面的顶部显示有 Work profile is off 已经消失了，PASS。点击 Starting work apps when work mode is on，会弹出一个对话框，点击 GO，会跳转到 Launcher，左右滑动桌面找到一个叫 Work 的 APP 文件夹，如果里面的 APP 恢复正常，则 PASS。

Organization Info

点击屏幕底部的 SETTINGS 按键，跳转到 Setting，设置一个屏幕锁（如果之前已经有，就不需要再设置了），然后把 Security 页面下的 Use one lock 取消勾选，需要设置一个 Work profile 的锁屏密码，设置一个 PIN 密码（其他也可以，能和上一步的屏幕锁有区别就可以）返回 CTS Verifier，在屏幕下

端的 Name 输入:AW, 颜色输入 #FFFF00, 输入好之后点击 SET 按键, 然后去 Setting-Security 把刚才设置的密码去掉, 再次返回 CTS Verifier, 点击 GO 按键, 会跳转到 Work profile 的锁屏界面, 显示有设置的 Name:AW, 整体的界面是黄色, 输入前面设置 Work profile 的锁屏密码, PASS。

Personal PASSword test

点击 GO, 设置一个密码, 然后黑屏锁定屏幕, 然后再亮屏, 输入设置的密码, 如果通过, PASS。

Policy transparency test Disallow controlling apps:

在屏幕的右下角有一个 Disallow controlling apps 的开关, 打开开关, 点击 OPEN SETTINGS, 进入 Setting->APPs, 只需要关注除了 Ctsverifier 之外其他带有小红书包标志的应用 (即工作区的应用), 选择一个应用, 比如 Contacts, 点击去, 尝试去点击 DISABLE 和 FORCE STOP 两个按键, 会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息, PASS。

Disallow modify accounts:

在屏幕的右下角有一个 Disallow modify accounts 的开关, 打开开关, 点击 OPEN SETTINGS, 会进入 Setting->Accounts, 在 Work 栏下添加一个账号, 会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息, PASS。

Disallow share location:

在屏幕的右下角有一个 Disallow share location 的开关, 打开开关, 点击 OPEN SETTINGS, 会进入 Setting->location, 会看到有一行 Location work profile, 点击会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息, PASS。

Disallow uninstall apps:

屏幕的右下角有一个 Disallow uninstall apps 的开关, 打开开关, 点击 OPEN SETTINGS, 会进入 Setting->APPs, 找到工作模式下的 CtsPermissionAPP (带标志的), 点入, 再点 uninstall 按键, 会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息, PASS。

Set permitted accessibility services:

屏幕的右下角有一个 Allow only system accessibility services 的开关, 打开开关, 点击 OPEN SETTINGS, 会进入 Setting->Accessibility, 点击 Dummy accessibility service, 会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信

息，PASS。

Set permitted input methods:

屏幕的右下角有一个 Allow only system input methods 的开关，打开开关，点击 OPEN SETTINGS，会进入一个页面，点击 Dummy input method，会弹出一个对话框，提示 Action not allowed，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息，PASS。

Profile-aware data usage settings (Wi-Fi)

测试此项需要连接 wifi。点击此项目后会弹出一个对话框，点击 GO，跳转到 Setting，找到 Data usage 并进入，再点击 ``Wi-Fi data usage"，再进入 ``All work apps"，里面有一些处于工作模式的 APP 的数据记录，PASS。

Profile-aware data usage settings (Cellular)

对支持 SIM 的设备进行测试，不支持的设备请忽略，PASS。

Disallow apps control

先点击 PREPARE TEST 按钮，然后继续进行，点击 Disabled uninstall button，会跳转到 Setting 的 APPs 页面，在 APP 列表里面有一些红色小书包标志的应用，点击随便一个这样的 APP，会进入到 APP 的 APP info 页面，点击 DISABLE，会弹出一个对话框，提示 Action not allowed，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息，PASS。再点击 Disabled force stop button，会跳转到 Setting 的 APPs 页面，在 APP 列表里面有一些红色小书包标志的应用，点击随便一个这样的 APP，会进入到 APP 的 APP info 页面，点击 FORCE STOP，会弹出一个对话框，提示 Action not allowed，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息，PASS。再点击 Disabled app storage buttons，会跳转到 Setting 的 APPs 页面，在 APP 列表里面有一些红色小书包标志的应用，可以去找到 Google Play Store（其它的也可以，只是可能没有 CLEAR CACHE 选项）点进去，再点开 Storage，里面有 CLEAR DATA 和 CLEAR CACHE 选项，点击会弹出一个对话框，提示 Action not allowed，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息，PASS。

Camera support cross profile image capture

点击 go 进入拍照，验证所捕获的照片是否显示，打钩，点击 close 返回 PASS。

Camera support cross profile video capture(with extra output path)

点击 go 进入录制视屏，验证所捕获的视屏是否显示，打钩，play 可以回放，点击 close 返回 PASS。

Camera support cross profile video capture(without extra output path)

点击 go 进入录制视屏，验证所捕获的视屏是否显示，打钩，play 可以回放，点击 close 返回 PASS。

Sound recorder support cross profile audio capture

点击 GO，会跳转到录音机的界面，点击 play，确认录音机正在工作，然后停止 ->DONE->CLOSE，返回 PASS。

Work profile widget

点击 home，长按主频屏幕，点击 widgets，把 cts verifier 添加到主屏幕，如果可以，PASS。

4.3.11.2 BYOD Provisioning tests

Custom provisioning color

点击 GO，会跳转到 Set up work profile 界面，如果背景色是绿色的，返回，PASS。

Custom provisioning image

点击 GO，会跳转到 Set up work profile 界面，如果界面最顶部的 logo 是 CtsVerifier 的图标，则返回 PASS。

Custom terms

点击 GO，点击 view terms，打开 company ABC，点击两次停止供应，返回 PASS

4.3.11.3 Device Owner Requesting Bugreport Tests

1. 点开 PRECONDITION CHEECKS 按钮，会弹出一个对话框。
2. 然后安装一个 CtsEmptyDeviceOwner.apk。(adb install -t + 文件)
3. 再输入 adb shell dpm set-device-owner com.android.cts.emptydeviceowner/.EmptyDeviceAdmin
4. 点击对话框的 ok。
5. 点击 SET UP DEVICE OWNER 按钮，输入 adb shell dpm set-device-owner

``com.android.cts.verifier/com.android.cts.verifier.managedprovisioning.DeviceAdminTestReceiver" 按要求执行列表的其他测试小项。

(安卓 Q: 如果过程中遇到设置了 Devices owner 后无法测试, 可以移除掉所有者: adb shell dpm remove-active-admin com.android.cts.emptydeviceowner/.EmptyDeviceAdmin 在进行重新设置所有者测试)



图 45: android Q 测试说明

Check device owner

检查设备所有者, 点击该项, 自动变绿则 PASS, 变红则 fail

Sharing of requested bugreport declined while being taken

进入此项测试之后, 点击 REQUEST BUGREPORT 按键, 在通知栏会显示 ``Taking bug report...'', 再按一次 REQUEST BUGREPORT 按键, 会出现一个消息在通知栏, 提示 bugreport is already being collectde on this device. 点击 Taking bug report... 这条消息, 会跳出一个对话框, 点击 DECLINE, ``Taking bug report...'' 这条消息已经不在通知栏, 在通知栏会显示 Bugreport Share declined, 则 PASS, 手动把通知栏清理。

Sharing of requested bugreport accepted while being taken

进入此项测试之后，点击 REQUEST BUGREPORT 按钮，在通知栏会显示“Taking bug report...”，再按一次 REQUEST BUGREPORT 按钮，会出现一个消息在通知栏，提示 bugreport is already being collectde on this device。点击 Taking bug report...这条消息，会跳出一个对话框，点击 SHARE, 等待 bugreport 生成完，“Taking bug report...”这条消息已经不在通知栏，在通知栏会显示 Bugreport Share successful, 则 PASS, 手动把通知栏清理。

Sharing of requested bugreport declined after have being taken

进入此项测试之后，点击 REQUEST BUGREPORT 按钮，在通知栏会显示“Taking bug report...”的消息。再按一次 REQUEST BUGREPORT 按钮，会出现一个消息在通知栏，提示 bugreport is already being collectde on this device。等待 bugreport 生成完毕，“Taking bug report...”这条消息已变成“Share bug report? ”，点击“Share bug report”, 会跳出一个对话框，点击 DECLIN, 在通知栏会显示 Bugreport Share declined, 则 PASS, 手动把通知栏清理。

Sharing of requested bugreport accepted after have being taken

进入此项测试之后，点击 REQUEST BUGREPORT 按钮，在通知栏会显示“Taking bug report...”的消息。再按一次 REQUEST BUGREPORT 按钮，会出现一个消息在通知栏，提示 bugreport is already being collectde on this device。等待 bugreport 生成完毕，“Taking bug report...”这条消息已变成“Share bug report”, 点击“Share bug report”, 会跳出一个对话框，点击 SHARE, 在通知栏会显示 Bugreport Share successful, 则 PASS, 手动把通知栏清理。

Remove devices owner

按下该按钮之后，去 Setting->Security->Devices administrator, 看 CTS Verifier 是否被勾选，如果没有被勾选，则 PASS。

4.3.11.4 Device Owner Tests

(注意: 不要跳出这个测试页面，否则出现错误时点击第一个 **check device owner** 会变红色，就重新执行第二条命令)

理想状态下，该项测试应该是倒数第二项测试。测试前，清除设备已有账号，进入 Settings->Accounts, 点击已有账号进行清除。进入该项测试，点击 SET UP DEVICE OWNER, 打开 USB 调试，在 adb 窗口中输入：

```
adb install -t 文件 CtsEmptyDeviceOwner.apk 和 adb shell dpm set-device-owner ``com.android.cts.verifier/com.android.cts.verifier.managedprovisioning.DeviceAdminTestReceiver``。
```

当结果返回 success 的时候，说明设置成功。

Check device owner

点击 Check device owner，若前面设置成功，该项自动 PASS。

Device administrator settings

进入 Settings->Security->Device administrators，确认 CTS Verifier 存在且激活，CTS Verifier 无法去掉勾选。确认后按返回键返回该测试项，点击 PASS。

WiFi configuration lockdown

(先去掉 wifi) 输入一个可用的 WiFi 的名字和选择 WiFi 的加密方式 (一般是 WAP)，点击 CREATE WIFI CONFIGURATION，然后进入下面的测试项。Aw-Test-Psw1-HK。

Unlocked config is modifiable in Settings:

点击 WIFI CONFIG LOCKDOWN OFF 确保 WiFi 配置可以修改，点击 GO TO WIFI SETTINGS，确认之前输入的 WiFi 的状态是尝试连接或者已经连接的状态，点击屏幕右上角的设置图标 -> 看到 Saved networks 并点击，确认存在 Saved by CTS Verifier 的网络名称且和刚才输入的一致，点击该网络，可选择 FORGET 或 CANCEL 该网络则 PASS。通过返回键返回 CTS Verifier 测试，可点击 PASS。

Locked config is not modifiable in Settings:

点击 WIFI CONFIG LOCKDOWN ON 确保 WiFi 配置无法修改，点击 GO TO WIFI SETTINGS，确认之前输入的 WiFi 的状态尝试连接的状态，点击屏幕右上角的设置图标 -> 看到 Saved networks 并点击，确认存在 Saved by CTS Verifier 的网络名称且和刚才输入的一致，点击该网络，可选择 CANCEL 该网络，无法删除该网络则 PASS。通过返回键返回 CTS Verifier 测试，可点击 PASS。

Locked config can be connected to:

点击 WIFI CONFIG LOCKDOWN ON 确保 WiFi 配置无法修改，点击 GO TO WIFI SETTINGS，点击该网络，看看是否可以手动连接，则 PASS。

Unlocked config ican be forgotten in Settings:

点击 WIFI CONFIG LOCKDOWN OFF 确保 WiFi 配置可以修改，点击 GO TO WIFI SETTINGS，点击之前输入的 WiFi 名字，可忘记该网络则 PASS。

Disallow configuring VPN

点击 SET VPN RESTRICTION 确保 VPN 被限制，再点击 GO，会跳转到 VPN 界面，这个界面显示 This action is disabled，并且无法进行任何操作。然后再返回测试页面，点击 CHECK VPN，会跳转到 Check VPN 的页面，提示 Cannot establish a VPN connection，则 PASS。

Disallow configuring WiFi

点击 SET RESTRICTION，再点击 GO，会跳转到 Wi-Fi 界面，但是没有显示一个 Wi-Fi，并显示 This action is disabled，则 PASS。

Disallow ambient display

点击 SET RESTRICTION，点击 GO，来到 Display 界面，点击 advanced，看到 Lock screen display 为灰色，且点击会显示 This action is disabled。PASS。

Disallow factory reset

点击 SET RESTRICTION 按键，进入 Settings->System->Reset options，进去会看到 Erase all data (factory reset) 变成灰色，为 locked 状态，点击会弹出 Action not allowed 的对话框，并且无法进行任何操作。然后再去 Settings->Developer options，找到 OEM unlocking，点击会提示 Action not allowed。则返回，PASS。

Disallow configuring Bluetooth

点击 SET RESTRICTION 按键，点击 GO，去到 Settings->Bluetooth，并显示 This action is disabled，则 PASS。

Disallow USB file transfer

点击 SET RESTRICTION 限制 USB，把设备通过 USB 线连接，点击通知栏的 USB Charging this device，弹出的界面的 Transfer file(MTP) 和 Transfer photos(PTP) 不存在或是灰色的，点击会弹出提示信息，与电脑无法进行数据的传输，则 PASS。

Disallow status bar

点击 DISABLE STATUS BAR，然后尝试去从屏幕上方拉下状态栏，会没有反应，点击 REENABLE STATUS BAR，再次去下拉，则可以，PASS。

Disable keyguard

然后点击 DISABLE KEYGUARD，然后按电源键黑屏，然后再亮屏，不会看到锁屏的界面，再点击 REENABLE KEYGUARD，则再次操作就会出现锁屏页面。PASS。

Lock Task UI

点击 START LOCKTASK MODE:

Default LockTask UI:

点击下面按钮，发现状态栏不能用，home 按键隐藏，长按关机按键不显示电源按钮菜单，关闭屏幕，再打开，没有解锁界面，PASS

Enable system info :

点击下面按钮以启动系统信息，状态栏信息已经启用，包括时间，连接信息，电量等，home 隐藏，overview 不工作，长按关机按键不显示电源按钮菜单，关闭屏幕，再打开，没有解锁界面，PASS。

Enable notifications :

点击下面按钮，观察状态栏已经开启，但是所有进入 setting 的链接都不可用，按住 home 键右边不会弹出其他任务，长按关机按键不显示电源按钮菜单，关闭屏幕，再打开，没有解锁界面，PASS。

Enable Home button:

点击下面按钮以启动 home 键，按住 home 键右边不会弹出其他任务，观察状态栏已经禁用，长按关机按键不显示电源按钮菜单，关闭屏幕，再打开，没有解锁界面，PASS。

Enable Overview button :

点击下面按钮，home 已启动，确定 overview 视图可以打开，状态栏无法展开，长按关机按键不显示电源按钮菜单，关闭屏幕，再打开，没有解锁界面，PASS。

Enable global action :

点击下面按钮以启用全局，长按电源键显示电源显示菜单，状态栏不显示内容，home 隐藏，关闭屏幕，再打开，没有解锁界面，PASS。

Enable keyguard :

点击下面按钮启用 keyguard 关闭屏幕，长按关机按键不显示电源按钮菜单，再打开有解锁界面，状态栏无法展开，home 隐藏，PASS。

Stop LockTack mode:

点击下面按钮停止锁定模式，状态栏返回正常模式，不再受 LockTask 的限制，PASS。

Setting the user icon:

点击 SET USER ICON 1, 再点击 GO, 看 Settings 里面是否有 Users 选项, 没有则可以 PASS。否则进入 Users, 如果 owner 的图标不是 1, 则 fail, 然后点击 disallow set user icon 和 SET USER ICON 2, 再点击 GO 进入 settings, 确认图标不能手动更改, 而且 Owner 的图标为 2, PASS。

Permissions lockdown:

需要安装 CtsPermissionApp.apk, 先选择 Grant, 然后点击 OPEN APPLICATION SETTINGS, 会跳转到 APP info, 找到 Permissions 点击进去, Contacts 是灰色的, 点击会弹出一个对话框, 提示 Action not allowed, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息。再返回选择 Let user decide, 去到同样的位置, 可以设置 Contacts 的开关。再返回选择 Dney, 去到 Permissions, 会显示 No permissions granted, PASS。

Policy transparency test:

进入后看到一个 SET SHORT SUPPORT MESSAGE 和 SET LONG SUPPORT MESSAGE, 分别点进去设置一个短消息 ``Aw -short message" 和一个长消息 ``Aw-long message"。

Disallow add user:

屏幕的右下角有一个 Disallow add user 的开关, 打开开关, 点击 OPEN SETTINGS, 进入 Setting->USER, 尝试去添加一个 USER, 会弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Disallow adjust volume:

屏幕的右下角有一个 Disallow adjust volume 的开关, 打开开关, 点击 OPEN SETTINGS, 进入 Setting->Sound, 尝试调整音量, 会弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Disallow controlling apps:

屏幕的右下角有一个 Disallow controlling apps 的开关, 打开开关, 点击 OPEN SETTINGS, 进入 Setting->APPS, 随便选择一个应用, 比如 Contacts, 点击去, 尝试去点击 DISABLE 和 FORCE STOP 两个按键, 会弹出一个对话框, 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会提示刚才设置的长消息, PASS。

Disallow config credentials:

屏幕的右下角有一个 Disallow config credentials 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->security，找到 Encryption & credentials 并且点击进入 User credentials，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config tethering:

屏幕的右下角有一个 Disallow config tethering 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Network&internet，点击 Hotspot&tethering，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config Wi-Fi:

屏幕的右下角有一个 Disallow config Wi-Fi 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Wi-Fi，页面显示 This action is disabled，PASS。

Disallow debugging features:

屏幕的右下角有一个 Disallow debugging features 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->About tablet，点击 Build number 去开启开发者选项，但是会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow factory reset:

屏幕的右下角有一个 Disallow debugging features 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->System>Reset options，点击 Factory data reset，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow fun:

屏幕的右下角有一个 Disallow fun 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->TAbout tablet，连续点击 Android version 几次，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow install unknown sources:

屏幕的右下角有一个 Disallow install unknown sources 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->security，点击 Unknown sources，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow modify accounts:

屏幕的右下角有一个 Disallow modify accounts 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Accounts，点击 Add account，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow network reset:

屏幕的右下角有一个 Disallow network reset 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->System>Reset options，去重置网络，点击 Reset Wi-Fi, mobile & Bluetooth，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow remove user:

屏幕的右下角有一个 Disallow remove user 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->User，先添加一个 user，不需要配置这个 user，然后删除这个 user 的时候，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow share location:

屏幕的右下角有一个 Disallow share location 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Location，而且状态是 OFF，点击一下看看能否打开，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow uninstall apps:

屏幕的右下角有一个 Disallow uninstall apps 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->APPS，随便找个 APP（除了 CTS Verifier），然后去去卸载，需要点击 DISABLE 和 FORCE STOP，会看到弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的

LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config date time:

屏幕的右下角有一个 Disallow config date time 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Date & time，点击随意一个设置时间和日期的按键，会看到弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config location:

屏幕的右下角有一个 Disallow config location 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Location，而且状态是 OFF，点击一下看看能否打开，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow airplane mode:

屏幕的右下角有一个 Disallow airplane mode 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Network & internet，点击 Airplane mode，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config screen timeout:

屏幕的右下角有一个 Disallow config screen timeout 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Display，点击 Screen timeout，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Disallow config brightness:

屏幕的右下角有一个 Disallow config brightness 的开关，打开开关，点击 OPEN SETTINGS，进入 Setting->Display，点击 Brightness level，会弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

set auto (network) time required:

屏幕的右下角有一个 set auto (network) time required 的开关，打开开关，点击 OPEN SETTINGS，

进入 Setting->Date&time, 点击 Automatic, 会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Disallow lockscreen unredacted notification:

屏幕的右下角有一个 Disallow lockscreen unredacted notification 的开关, 打开开关, 点击 OPEN SETTINGS, 进入 Setting->Security, 设置锁屏密码, 如果之前设置有了, 需要先去掉锁屏密码, 再去设置一个新的密码, 在设置新的屏幕锁的过程会有一个 Notifications, 去点击 Show all notification content, 会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Set lock screen info:

屏幕的右下角有一个输入框和一个 UPDATA 按键, 输入 AW 点击 UPDATA, 再点击 OPEN SETTINGS, 进入 Setting->Display。点击 Lock screen display, 看到 Lock Screen message 显示刚才设置的 AW, 点击会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Set maximum time to lock:

屏幕的右下角有一个输入框和一个 UPDATA 按键, 输入 30 再点击 UPDATA, 再点击 OPEN SETTINGS, 进入 Setting->Display, 点击 Sleep, 选项只有低于等于 30 秒的, 点击 LEARN MORE, 会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Set password quality:

屏幕的右下角有一个选项框, 可以选择锁屏的质量, 比如选择 Smoothing 类型, 会再点击 OPEN SETTINGS, 进入锁屏类型的选择, 此时的 None 和 Swipe 是灰色的, 如果点击选择, 会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Set permitted accessibility services:

屏幕的右下角有一个开关, 打开, 再点击 OPEN SETTINGS, 进入 Setting->Accessibility, 找到 Dummy accessibility service 并点击, 会看到弹出一个对话框, 提示 Action not allowed 并显示刚才设置的短消息, 点击对话框的 LEARN MORE 会跳转到 Device administrator, 并且有一些提示的信息包括刚才设置的长消息, PASS。

Set permitted input methods:

屏幕的右下角有一个开关，打开，再点击 OPEN SETTINGS，进入 Available virtual keyboard，看到灰色的 Dummy input method，点击会看到弹出一个对话框，提示 Action not allowed 并显示刚才设置的短消息，点击对话框的 LEARN MORE 会跳转到 Device administrator，并且有一些提示的信息包括刚才设置的长消息，PASS。

Managed device info tests

Managed device info page:

进入 Setting->Security->Managed device info，进去之后你可以更改设置，能够看见 data associated with your work account ,list of all apps ,each app ,可以锁设备，改变 Password，清除设备。

Retrieve traffic logs :

TRAFFIC LOGS 按钮，记住你按下的时间，等待一分钟，按下 OPEN SETTINGS 按钮，在打开的页面可以看到 Traffic Logs 的日期为按下按钮的时间。

Request bug report:

点击 REQUEST BUG REPORT 按钮，记住你按下的时间，等待一分钟，按下 OPEN SETTINGS 按钮，在打开的页面可以看到 bug report 的日期为按下按钮的时间。

Retrieve security logs:

点击 RETRIEVE SECURITY LOGS 按钮，记住你按下的时间，等待一分钟，按下 OPEN SETTINGS 按钮，在打开的页面可以看到 Security logs 的日期为按下按钮的时间。

Enterprise-installed apps:

把 NotificationBot.APK 推入/sdcard 路径里面，(命令: adb push 文件/sdcard) 按下 Uninstall 按钮，打开 Open Setting 按钮，在打开的页面可以看到你的用户没有安装任何 app，点击返回到测试页面，点击 INSTALL 按钮，打开设置页面看到有一个已经被安装，点开确认是否为 CTS Robot，是则返回测试界面，点击 UNINSTALL 按钮，在打开设置界面，看到没有 app 安装，返回界面，PASS，否则，fai。

Location access permission:

按下 Reset 按钮，打开设置界面，不能看 location permission 的 app，返回到测试界面，点击 GRANT 按钮，打开设置界面，可以看到有一个 location permission 的 app 至少有一个，而且有一个是 CTS verifier，返回到测试界面，按下 Reset 按钮，再打开设置界面，没有看到该 Location permissions，返回

PASS, 否则 fail。

Microphone access permission:

按下 Reset 按钮, 打开设置界面, 不能看 Microphone permission 的 app, 返回到测试界面, 点击 GRANT 按钮, 打开设置界面, 可以看到有一个 Microphone permission 的 app 至少有一个, 而且有一个是 CTS verifier, 返回到测试界面, 按下 Reset 按钮, 再打开设置界面, 没有看到该 Microphone permissions, 返回 PASS, 否则 fail。

Camera access permission:

按下 Reset 按钮, 打开设置界面, 不能看 Camera permission 的 app, 返回到测试界面, 点击 GRANT 按钮, 打开设置界面, 可以看到有一个 Camera permission 的 app 至少有一个, 而且有一个是 CTS verifier, 返回到测试界面, 按下 Reset 按钮, 再打开设置界面, 没有看到该 Camera permissions, 返回 PASS, 否则 fail。

Default apps:

打开 Setting->App¬ifications->Default apps->Browser app, 设置 CTS verifier 为默认浏览器, 点击 Reset 按钮, 打开设置界面, 在界面上看不到 default app, 返回到测试界面, 点击 SET DEFAULT APPS 按钮, 打开设置界面, 可以看到 default apps 有六个 apps, 点开可以看到 Browser app。点击返回到界面, PASS, 否则 fail。

Default keyboard:

打开设置界面, 可以看到 default keyboard 还没有被设置, 返回到测试界面, 按下 SET KEYBOARD 将默认键盘设置为 CTS Verifier, 打开设置界面, 可以看到 default keyboard 被设置为 cts verifier, 返回测试界面, PASS, 否则 fail。

Always-on VPN:

打开设置界面, 可以看到 always-on VPN 还没有被设置, 返回到测试界面, 点击 SET VPN 设置, 在打开设置界面可以看到 Always-on VPN turned on 返回到测试界面, 点击 FINISH 界面清除掉 always-on VPN, 点击设置界面可以看到 Always-on VPN turned on 已经被清除, 返回测试界面点击 PASS, 否则点击 fail。

Global HTTP Proxy:

打开设置界面, 可以看到 global HTTP proxy 还没有被设置, 返回到测试界面, 点击 SET PROXY 设置, 在打开设置界面可以看到 Global HTTP proxy set 返回到测试界面, 点击 CLEAR PROXY 界面清

除掉 Global HTTP proxy set，点击设置界面可以看到 Global HTTP proxy set 已经被清除，返回测试界面点击 PASS，否则点击 fail。

Trusted CA certs:

打开设置界面，不能看到 Trusted credentials，返回到设置界面，点击 INSTALL CERT，再打开设置界面，可以看到 Trusted credentials。返回到设置界面，点击 FINISH 按钮，打开设置界面确认 Trusted credentials 已经消失，回到测试界面点击 PASS，否则 fail。

Wipe on authentication failure:

打开设置界面，不能看到 password attempts，返回到设置界面，点击 SET LIMIT，再打开设置界面，可以看到 Failed password attempts before deleting all device data 100 attempts。返回到设置界面，点击 FINISH 按钮，打开设置界面确认 password attempts 已经消失，回到测试界面点击 PASS，否则 fail。

Quick settings disclosure:

点击 CLEAR ORG 按钮，完全打开快捷设置栏，可以看到 Device is managed by your organization。点击 SET ORG 按钮，再完全打开快捷设置栏，可以看到 Device is managed by Foo, Inc。点击该信息，看到 Device management 信息，点击 VIEW POLICIES，可以跳转到 Managed devices info 界面。返回到测试界面，点击 PASS，否则 fail。

Keyguard disclosure:

点击 OPEN SETTINGS，设置锁屏方式为滑动解锁，返回测试界面，点击 CLEAR ORG 按钮，锁上设备，解锁设备，在解锁界面可以看到 This device is managed by your organization。进入测试界面，点击 SET ORG 按钮，再关上设备，唤醒设备，可以看到锁屏界面显示 This device is managed by Foo, Inc.。重复 1 到 11 步骤，遍历除了 None 以外的所有解锁方式。

Add account disclosure:

点击 CLEAR ORG，打开设置界面，可以看到 This device is managed by your organization，返回到测试界面，点击 SET ORG，打开设置界面，可以看到 This device is managed by Foo, Inc。打开 Learn more 可以跳转到 Managed device info 界面。返回测试界面，PASS，否则 fail。

Managed User

点击 GO 进入到 Managed User，关闭密钥：

1. 点击 check affiliated profile owner 验证。

2. 点击 device administrator settings, 点击 go, 点击的 device admin apps CTS Verifier 存在并被激活, CTS Verifier 不能禁用。

3. 点击 disable status bar, 点击下面第一个按钮禁用状态栏, 确认不再提供快速设置, 通知和辅助手势, 点击第二个按钮重新启动状态栏, 验证状态栏是否出现。

4. 点击 disable keyguard, 确保没有设置屏幕密码, 按下面第一个按钮禁用 keyguard, 电源锁屏, 然后开屏, 确认没有 keyguard 保护, 点击第二个按钮重新启用 keyguard 并重复上述步骤, 这一次验证显示了 keyguard。

5. 点击 disallow remove user, 点击 SET RESTRICTION 设置用户权限, 点击 GO 进入 setting, 手动查找并打开 System > Multiple users, 发现 Remove user 选项被禁用, 单击触发一个支持对话框, 无法找到该选项。

6. 点击 Policy transparency test, 设置长信息、短信息, 重复上面 Policy transparency test 的步骤

Corporate Owned Managed Profile

点击 OK, 创建一个 work profile, 然后设置一个长信息, 一个短信息, 点击 set default message, set message, 返回, 进入 disallow remove managed profile, 打开下面开关, 点击 open setting 点击 APPS notifications, special app access, install unknown apps, 点击带有标志的 CTS Verifier, 点击 allow from this source, 弹出 action not allowed 对话框点击 learn more, 点击 remove work profile, 弹出长信息, 点击了 learn more 弹出长信息。

Logout

点击 GO 已启动 logout, 将会切换到一个创建新用户, 通过不解锁屏的情况下注销当前用户, 长电源键出现电源按钮菜单, 选择第三个注销当前用户, 成功登出并且回主用户时, 再次确认电源按钮菜单没有了刚才的登出控件。

Disallow user switch

点击 CREATE UNINITIALIZED USER 创建未设置的用户, 按 SET RESTRICTION 设置用户限制, 点击 GO, settingAdvanced > Lock screen display), 返回点击 go, 设置屏幕锁定为 none, PASS。

User switcher message

点击 WITH USER SWITCHER MESSAGE, 等待自动切换到辅助页面出现 star user session, 再等待自动切回主页面出现对话框 en

d user session, 点击 WITHOUT USER SWITCHER MESSAGE 等待自动切换到辅助页面出现 star

user session, 再等待自动切回主页面出现对话框 end user session。

Remove devices owner

按下该按键之后, 去 Setting->Security->Devices administrator, 看 CTS Verifier 是否被勾选, 如果没有被勾选, 则 PASS。

4.3.11.5 No Devices Owner Tests

Device owner provisioning

点击 START PROVISIONING 弹出对话框, 显示 Device is already set up, 点击 ok。

Quick setting disclosure

打开并完全展开快速设置, 确认在快速设置的底部, 你没有被告知该设备已被管理, 关闭快速设置, 点击 PASS。按下 Go 按钮打开设置, 设置锁屏方式为滑动方式, 返回到测试界面, 锁屏, 打开锁屏界面, 你没有被告知该设备已被管理, 解锁设备, 重复 1 到 6 步骤, 遍历所有锁屏方式除了 none。

Keyguard disclosure

按下 Go 按钮打开设置, 设置锁屏方式为滑动方式, 返回到测试界面, 锁屏, 打开锁屏界面, 你没有被告知该设备已被管理, 解锁设备, 重复 1 到 6 步骤, 遍历所有锁屏方式除了 none。

Add account disclosure

按下 Go 按钮打开设置界面, 在该界面你没有被告知该设备已被管理, 关闭快速设置, 点击 PASS。

4.3.12 NETWORKING

4.3.12.1 Bluetooth Test

蓝牙测试需要 2 台平板配合测试。(确保 location 打开)

Toggle Bluetooth 点击按钮 Enable Bluetooth 和 Disable Bluetooth。确认蓝牙可以正常打开和关闭即可通过测试。注意: 最后需要打开蓝牙用来继续后续的测试。

Bluetooth HID Device 与 Bluetooth HID Host

测试需要 2 个平板，一个当作服务端，另一个当作客户端。客户端打开 Bluetooth HID Host 界面，服务端打开 Bluetooth HID Device 界面。在服务端点击 REGISTER APP, MAKE DISCOVERABLE, 在客户端点击 SELECT DEVICE, 连接该设备，等待对话框出现打勾配对两设备，点击服务端的 TEST SEND_REPORT, 随后点击 TEST REPLY_REPORT, TEST REPORT_ERROR, 如果这三个按钮都按成功，则点击 UNREGISTERAPP 按钮，再 PASS。

Bluetooth LE insecure Client Test 与 Bluetooth LE secure Client Test

拿专用手机来当服务端，先匹配上蓝牙，然后点击客户端的测试项，在弹出的对话框做对应的 pair 或 connect；每测一个都要 forget 掉历史记录，重新连接配对连接。注意到 03bluetooth le encrypted client test 时需要一个个依次点击蓝色问号项，显示 test running 中，不要动，自己测试（在第一个的测试项配对成功的前提下，不要 forget，再测 03）

Insecure Client 与 Insecure Server

测试需要 2 个平板，一个当作服务端，另一个当作客户端。客户端打开 Insecure Client 界面，服务端打开 Insecure Server 界面。

1. 在服务端点击 Make Discoverable 按钮。让自己可以被附近的客户端寻找到。
2. 在客户端点击 Scan for Devices 按钮，寻找服务端。当 New Devices 栏中出现服务器的信息（可以根据平板设备名称和蓝牙地址来判断），点击该服务器则会自动开始传输测试。
3. 测试成功时 PASS 按钮变成可点击。

Secure Client 与 Secure Server

测试需要 2 个平板，一个当作服务端，另一个当作客户端。客户端打开 Insecure Client 界面，服务端打开 Insecure Server 界面。

在服务端点击 Make Discoverable 按钮。让自己可以被附近的客户端寻找到。

在客户端点击 Scan for Devices 按钮，寻找服务端。当 New Devices 栏中出现服务器的信息（可以根据平板设备名称和蓝牙地址来判断），点击该服务器则会自动开始传输测试。

测试过程中会提示需要配对，在客户端和服务端均点击 pair 让彼此配对。

测试成功时 PASS 按钮变成可点击。

注意：当平板在 **Secure Client** 与 **Secure Server** 之间切换测试时，需要先解除蓝牙配对，然后进行测试。

Network Background Connectivity Test

本项测试 IPv6 网络在关屏的情况下的连接性能, 测试步骤:

1. 连接一个有 IPv6 网络接入的 WiFi 网络。
2. 断开设备的电源连接。
3. 关屏。
4. 等待屏亮起(至少需要 2min), wcap
5. 根据结果状态判断 PASS 还是 FAIL。

4.3.12.2 Wi-fi Direct Test

注意:WiFi 必须忘记所有 Wifi 的密码, 需要自己手动去清除。同时得打开 Location

GROUP FORMATION

GO Negotiation Responder Test 主要是为 GO Negotiation Requester Test 设计的, 作为 Responder 测试, 这个很容易过, 就不多说了。

GO Negotiation Requester Test 中有两个测试项, Go negotiation test(push button) 和 Go negotiation test(PIN), 进行这两个测试之前, 要有一台对等机, wifi 地址和测试机的地址不一致(如果两台机器 wifi 的 Mac 地址一样, 需要找相关同事烧写不一样的 wifi Mac 地址), 打开对等机的 wifi。在打开了对等机的 wifi direct 之后, 进入 CTS Verifier, 将对等机的 GO Negotiation Responder Test 打开, 对等机的准备工作到此为止, 接下来开始测试机的操作。测试机同样也打开 wifi, 然后进入 CTS Verifier 里测试 GO Negotiation Requester Test 里面的两个测试项。两个测试项的测试都是先搜索设备, 查找服务, 连接。push button 在查找到服务后, 需要在对等机确认是否连接, 点击接受后, 测试机进行连接; PIN 测试在查找到服务后, 需要在对等机输入测试机产生的 PIN 码, 如果 PIN 码输入正确, 并且没有超时(PIN 码输入时间是有时间的, 太久时间没有输入完成, 后续连接会失败), 连接成功, 测试 PASS。

测试完一个测试项之后, 测试机和对等机都退出 CTS, 去 settings 菜单重启下 wifi, 然后再做下面的测试。当然重启完之后, 双方交换位置, 对等机进 CTS 处于 Requester 界面, 测试机进行后面的测试。

GROUP JOIN

Group Owner Test 是为 Group Client Test 做准备，里面的两个测试项 Join p2p group test(push button) 和 Join p2p group test(PIN) 测试跟第一项测试大体一致，对等机处于 Group Owner Test 界面，测试机进行测试，测试完一项重启下 wifi direct.

GROUP JOIN WITH CONFIG

Group OwnerWith Config Test, Group client With Config Test, 两个测试项的测试都是先搜索设备，查找服务，连接，跟第一项测试大体一致，测试机会出现 Test PASSEd successfully.

GROUP JOIN WITH CONFIG 2G BAND

Group owner with config 2g band test, Group client with config 2g band test, 两个测试项的测试都是先搜索设备，查找服务，连接，跟第一项测试大体一致，测试机会出现 Test PASSEd successfully.

GROUP JOIN WITH CONFIG FIXED FREQUENCY

Group owner with config fixed frequency test, Group client with config fixed frequency test, 两个测试项的测试都是先搜索设备，查找服务，连接，跟第一项测试大体一致，测试机会出现 Test PASSEd successfully.

SERVICE DISCOVERY

Service Discovery Responder Test 是为 Services Discovery Requester Test 做准备的，对等机打开 Service Discovery Responder Test，测试机进行 Services Discovery Requester Test 测试，每测试完一个项，对等机退出 CTS，重启下 wifi direct. 其中 Multiple clients test 01 02 03 的测试需要至少两台对等机，测试搜索到两台设备之后，点击任意一个设备即可。

如果测试时，在搜索到设备按确定之后，弹出 test failed，这时候按返回键先退出失败界面，再按测试项如 Request all services test 01 继续测试。

如果测试时，点击测试项之后没去搜索设备直接显示 services discovery...，这个也是错误的状态，直接按返回键重新测试，requester 的所有测试都是先搜索设备的。

4.3.12.3 Wi-Fi Test

NETWORK SUGGESTION TESTS

Bubble Notification Tests, 重置 WiFi, 打开对等机的热点, 密码 none, 依次点击各项搜索, 注意查看通知栏信息, 点击 yes 或 conect, 出现 Test PASSEd successfully;

4.3.13 NOTIFICATIONS

4.3.13.1 Bubble Notification Tests

单击下面按钮, 启用气泡, PASS。

Step1: 再单击下面按钮, 发送一个带有通知的气泡, 气泡出现在屏幕上且通知阴影中有一个通知, PASS

Step2: 单击下面按钮, 验证气泡仍然在屏幕上, 但是通知隐藏在通知阴影中, PASS

Step3: 单击下面按钮, 验证气泡仍然在屏幕上, 但是通知在通知阴影中, PASS

Step4: 单击下面按钮, 确认气泡已从屏幕上移除, 并且通知在通知阴影中, PASS

Step5: 单击下面按钮, 验证气泡是否出现在屏幕上, 但是通知在通知阴影中仍可见, PASS

Step6: 轻击气泡使其打开, 然后再次点轻击气泡使其折叠并返回到此屏幕, 验证打开气泡后, 在通知阴影中不再有可见通知。

Step7: 单击下面按钮, 验证气泡仍然在屏幕上, 并且通知在通知阴影中可见。拖动气泡将显示 UI 启示: 拖放 UI 可视性上的气泡会将其从屏幕上移除, 通知应该保持在通知阴影中, PASS

Step8: 单击下面按钮, 验证气泡是否出现在屏幕上, 但是通知在通知阴影中仍可见, 取消通知, 验证气泡是否仍在屏幕上, PASS

Step9: 单击下面按钮, 确认屏幕上出现一个气泡, 自动展开, PASS

以上都 PASS, 则 PASS

4.3.13.2 CA Cert Notification Test

1. 点击第一条信息, 点击 GO, 在 (左上角三条横线) 管理器里面点击本机选择 myCA.cer, 点击安装, 随便输入名字点击 ok, 返回点击对话框的 PASS。

2. 点击第条信息，点击 GO，弹出的界面可以看到 Internet Widgits Pty Ltd，返回点击 PASS。
3. 去把设置的锁屏密码（remove）去掉。

4. 检查以下内容。下拉通知栏，可以看到“Certificate authority installed”这栏通知。点击此通知，出现更详细的信息，和一个显示为“Check Certificate”的按钮。点击此按钮可以看到安装的证书。如果以上检测都正确，那边则点击第三栏的 Done 按钮。

5. 在下拉通知栏中，向左或者右滑动“Certificate authority installed”栏，去除此条通知。如果能够成功去除则点击第四栏的 Done 按钮。

以上 5 步均通过测 PASS，否则 fail。

4.3.13.3 CA Cert Notification on Boot Test

1. 点击 Check Credentials 按钮确认是否已经安装证书。如果没有安装证书，则点击 Install credential 进行安装（如果之前测试了 CA Cert Notification Test 都会已经安装证书，就不用继续安装证书，总之，测试本项需要去除锁屏密码）。

2. 重启平板。重新启动后检查通知栏出现“Network may be monitored”这栏通知，并且点击进入后可以查看到详细信息。

以上操作正常则 PASS。

4.3.13.4 Condition Provider test

提示比较简单，按照 CTS Verifier 里面的提示步骤操作即可。

1. 设置 do not disturb, 点击下键打开 cts verifier, 直到下一个 launch settings 建时 2. 点击 launch settings, 关闭 cts verifier,

4.3.13.5 Notification Attention Management Test

1. 点击 Launch Settings。在弹出窗口中勾选 Notification Listener for CTS Verifier，然后返回测试界面。正常情况下测试界面中的栏目会一行行标绿直到第一个 I'M DONE 按钮。

2. 下拉通知栏，开启 Do not disturb，弹出的对话框点击 Total silence，点击 DONE，然后点击第一个 I'M DONE 按钮。正常情况下测试界面中的栏目会一行行标绿直到第二个 I'M DONE 按钮。

3. 下拉通知栏，关闭 Do not disturb，然后点击第二个 I'M DONE 按钮。正常情况下测试界面中的栏目会一行行标绿直到第三个 I'M DONE 按钮。

4. 下拉通知栏，开启 Do not disturb，弹出的对话框点击 Priority only，点击 MORE SETTINGS，弹出一个 DO not disturb 设置界面，点击 Priority only allows->Messages->From starred contacts only，设置好后返回，然后点击第三个 I'M DONE。正常情况下测试界面中的栏目会一行行标绿直到第四个 I'M DONE 按钮。

5. 下拉通知栏，关闭 Do not disturb，然后点击第四个 I'M DONE 按钮。正常情况下测试界面中的栏目会一行行标绿直到结束。

4.3.13.6 Notification Listener Test

进行此项测试前首先要清空左上角的通知栏，所以平板不能连电脑（否者会有 USB 连接的通知无法消除）。

1. 点击 Launch Settings。在弹出窗口中勾选 Notification Listener for CTS Verifier，然后返回测试界面。正常情况下测试界面中的栏目会一行行标绿直到下一个 Launch Settings 按钮。

2. 点击第二个 Launch Settings 按钮。在弹出窗口中取消勾选 Notification Listener for CTS Verifier，然后返回测试界面。正常情况下测试界面中剩下的栏目会标绿。

3. 所有栏目标绿后可以通过测试。

4.3.13.7 Notification Package Priority Test

1. 点击 Launch Settings，在弹出窗口中勾选 Notification Listener for CTS Verifier，然后返回测试界面。

2. 在 Settings->Notifications->All apps 找到 CTS Verifier，点击进入，取消勾选 Override Do Not Disturb，然后点击第一个 I'M DONE。正常情况下测试界面中的栏目会一行行标绿直到第三个 I'M DONE 按钮。

3. 在 Settings->Notifications->All apps 找到 CTS Verifier，点击进入，勾选 Override Do

4.3.13.8 Shortcut Reset Rate-limiting Test

测试前安装 NotificationBot.apk，点击进入该项目会自动进行测试，找到通知，点开通知，随便输入一些东西。（记得关掉 Do not disturb）

4.3.14 OTHER

4.3.14.1 Recent Task Removal Test

安装 Stophelper app，第一个 PASS，点击下面按钮，第二个 PASS，在最近应用中 remove 该活动，PASS

4.3.14.2 Screen Pinning Test

1. 点击 NEXT，弹出的提示框点击 GOT IT，屏幕会提示 Screen pinned。
2. 点击 NEXT 来验证 CTS Verifier 界面被固定在屏幕。
3. 点击任意按键确定屏幕已经被锁定，点击 NEXT。
4. 同时点击 hold back 键（返回键，三角形）和 overview（正方形）键来解锁屏幕，点击 CTS Verifier 返回测试，点击 NEXT。
5. 点击 NEXT 来再次锁定屏幕，弹出的提示框点击 GOT IT。
6. 点击 NEXT。
7. 弹出提示 All tests completed successfully 可点击 PASS。

4.3.14.3 Widget Framework Test

此项测试需要在使用到 Verifier 的 Widget 插件进行测试。

1. 在主界面长按，点击 WIDGET。在平板的 Widgets 或者（安卓为箭头标志）中找到 CTS Verifier。

如下图所示：

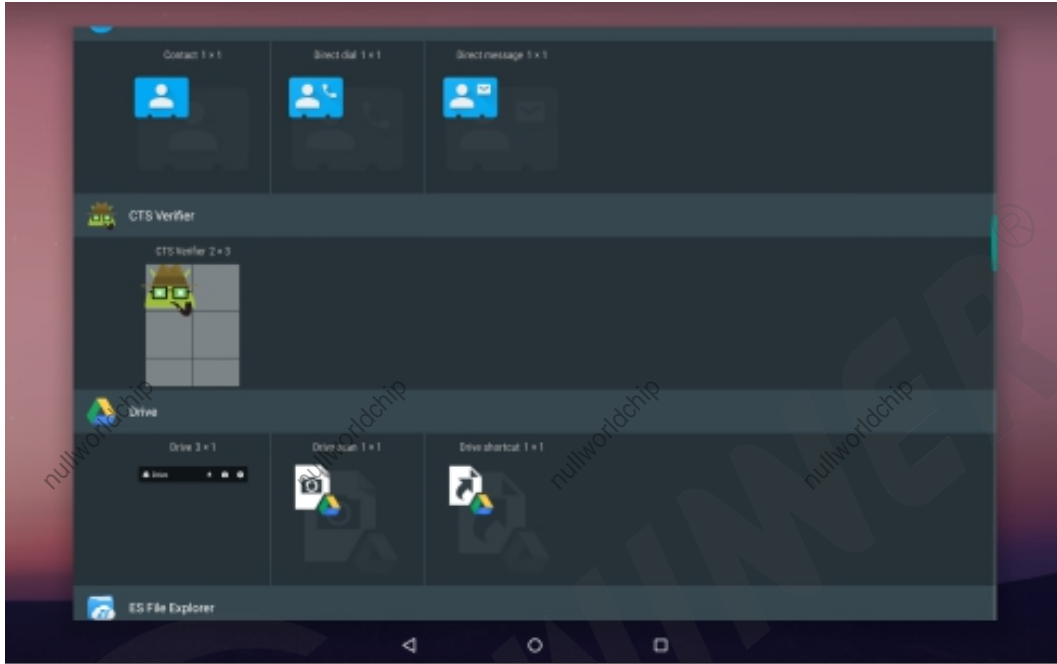


图 46: Widget Framework Test

2. 将 CTS Verifier Widget 拖放到桌面，点击 Start Test 进行测试

Step1: Verify dimensions。界面中会显示宽度（Width:xxx）和高度（Height:yyy）。这些值的单位均为 dp，这个值是与屏幕密度无关的。160dp 即为 1 英寸。所以先计算出 widget 应有的宽、高值。

3. 例如：测试的 widget 提示 Width: 367 Height: 366

则 widget 的实际大小需要为：

$$\text{宽度} = 367\text{dp} * (1/160)\text{inch/dp} * 2.54 \text{ cm/inch} = 5.82 \text{ cm}$$

$$\text{高度} = 366\text{dp} * (1/160)\text{inch/dp} * 2.54 \text{ cm/inch} = 5.81 \text{ cm}$$

所以测量 widget 的宽度是否接近 5.82 cm 高度是否接近 5.81cm 即可，注意不是测量整个屏幕。

这一项不需要精确，Verifer 中也提示了：reasonable approximations of the widget's actual size。

有时一些误差是可以接受的，正常误差的产生原因如下：在产品的 makefile 中有屏幕像素密度的设置：ro.sf.lcd_density。这个值的配置有几个固定的值可以选取（参见 frameworks/base/core/java/android/util/DisplayMetrics.java）：

- (1) `public static final int DENSITY_LOW = 120;`
- (2) `public static final int DENSITY_MEDIUM = 160;`
- (3) `public static final int DENSITY_TV = 213;`
- (4) `public static final int DENSITY_HIGH = 240;`
- (5) `public static final int DENSITY_XHIGH = 320;`
- (6) `public static final int DENSITY_400 = 400;`
- (7) `public static final int DENSITY_XXHIGH = 480;`
- (8) `public static final int DENSITY_XXXHIGH = 640;`

屏幕实际的像素密度肯能和上面几个值并不相符，所以需要选取一个与实际情况相近的值。这样就会在测试 `Widget Framework Test` 时就会产生误差。例如 Nexus10 的实际像素密度为 299DPI，它设置 `ro.sf.lcd_density` 时选取 320。所以 Nexus10 在测试 `Widget Framework Test` 也会有比较大的误差。Nexus7 的实际像素密度为 213。在取值范围中有刚好有一个值与它相等，它设置 `ro.sf.lcd_density` 时选取 213。所以 Nexus7 在测试 `Widget Framework Test` 时非常精确。

屏幕像素密度实际值与设置的 `ro.sf.lcd_density` 差别越大，在测试 `Widget Framework Test` 的误差也就越大，这种误差关系成正比。

4. **Step 2:Verify resizeability.** 长按 Verifier 桌面控件然后释放，可以看到控件的 4 条边出现变化如下图所示，可以拖拽 4 条边来改变控件的大小。



图 47: Verify resizeability

5. Step 3: Verify collections。确认控件中有编号为 1-50 的 50 个可滑动条目。

6. Step 4: Verify category。确认当前控件的位置, 应该显示 "Widget is reportedly on: HOME SCREEN"。

7. 此小空间同样可以在解锁界面中测试, 解锁界面中不要求改变控件的大小。在解锁界面中添加控件需要先勾选 Settings->Security->Enable Widgets, 然后再解锁界面中可以滑动时钟控件, 出现添加控件的页面, 点击添加即可。解锁界面测试 Step 4: Verify category 时, 需要显示 "Widget is reportedly on: KEYGUARD"。上述所有操作均通过时, 可以返回测试界面, 点击 PASS。否则 Fail。

4.3.15 PROJECTION TESTS

4.3.15.1 Projection Cube Test

测试界面中应该出现两个翻转的方块。点击屏幕方块分裂。如果观察到的现象一致则测试通过。

4.3.15.2 Projection Multitouch Test

测试界面中使用手指点击屏幕屏幕，屏幕对应的位置应该出现彩色的圆点。多个手指同时按在屏幕上，应该出现多个彩色圆点。拖动手指圆点应跟随移动。我们的屏一般都具有 5 点触摸的能力，可以用 5 个手指同时进行测试观察。符合上述要求则点击 PASS 按钮。

4.3.15.3 Projection Offscreen Activity

进入测试界面后，操作步骤如下：

1. 按电源键，使屏幕关闭。这时已经启动测试。
2. 等待测试完成。需要等待 5 秒钟左右，测试完成后平板会发出提示音。这时再次按下电源键，点亮屏幕。
3. 如果测试成功，PASS 按钮变成可点击，点击此按钮通过测试。

注意：测试时避免让平板处于充电状态。

4.3.15.4 Projection Scrolling List Test

测试界面中应该出现一个滚动栏，总共有 50 个项目，滑动屏幕可以上下滚动。符合上述要求即可点击 PASS 按钮通过测试。

4.3.15.5 Projection Video Playback Test

测试界面中应该出现闪动的白色方块，并且有“BEEP”声响与其闪烁的频率一致。符合上述要求即可点击 PASS 按钮通过测试。

4.3.15.6 Projection Widget Test

通过点击屏幕上方的 UP，DOWN 按钮，可以高亮屏幕下方的 4 个按键。点击高亮的按键后其色彩恢复正常。符合上述要求即可点击 PASS 按钮通过测试。

4.3.16 SECURITY

4.3.16.1 Biometric Prompt Bound Keys Test

Setting>security 设置密码, 点击 STARTTEST, PASS

4.3.16.2 Biometric test

点击 START TEST 1, PASS

4.3.16.3 KeyChain Storage Test

本项测试检查安装到系统的证书可以被授权、恢复和创建有效的 HTTPS 连接。测试前为设备设置开屏 PIN 密码或图案密码。

1. 点击 NEXT 来生成证书。
2. 点击 NEXT 安装证书到系统密钥, 弹出解压证书密码输入框直接点 OK, 弹出证书命名框直接点 OK。
3. 提示证书安装成功, 点击 NEXT。
4. 点击 NEXT 测试 HTTPS 连接。
5. 弹出提示框选择证书, 直接点击 ALLOW。
6. 提示 Connection succeed 后点击 NEXT, 找到 Clear credentials, 点击 OK 去除所有内容。找到 Screen Lock, 去除屏锁密码, 设置开屏方式为无。
7. 返回 CTS Verifier 测试, 提示 All tests completed 后点击 PASS。

4.3.16.4 Keyguard PASSword Verification

本项测试检查能否修改密码。

1. 如果设备尚未设置密码，则点击 SET PASSWORD。否则点击 CHANGE PASSWORD。
2. 点击 CHANGE PASSWORD 后，应该首先看到提示现有密码，否则该测试项 FAIL。成功修改密码则该测试项 PASS。

4.3.16.5 Lock Bound Keys Test

1. 设置屏幕锁屏：Settings->Security->Screen Lock，设置屏幕锁屏为 PIN 密码方式或图案方式或密码方式。
2. 点击 START TEST。
3. 弹出解锁界面，成功解锁进入则为 PASS。

4.3.16.6 Set New PASSword Complexity Test

1. 点击 HIGH, 设置 PIN 密码没有重复数字和有序性，长度至少为 8；
2. 点击 MEDIUM, 设置 PIN 密码没有重复数字和有序性，长度至少为 4；
3. 点击 LOW, 设置 PASSword 或者 PIN；
4. 点击 DONE, 设置为 NONE；

4.3.17 SENSORS

4.3.17.1 6DoF Test

点击，自动 PASS

4.3.17.2 Accelerometer Measurement Tests

注意：做测试前需要了解设备的屏幕方向怎么摆放才是正向，比如 **A63 t1** 平板的横向才是正向，与下图的刚好相反！

进入测试界面后按照如下的顺序操作：

1. 按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 **Stay Awake** 选项，关闭位置服务。所有需要关闭的 **sensor** 均关闭后，点击 **NEXT** 按钮开始测试。
2. 将平板垂直立在它的底边框，点击 **Next** 按钮。测试成功后会显示 **PASS**。

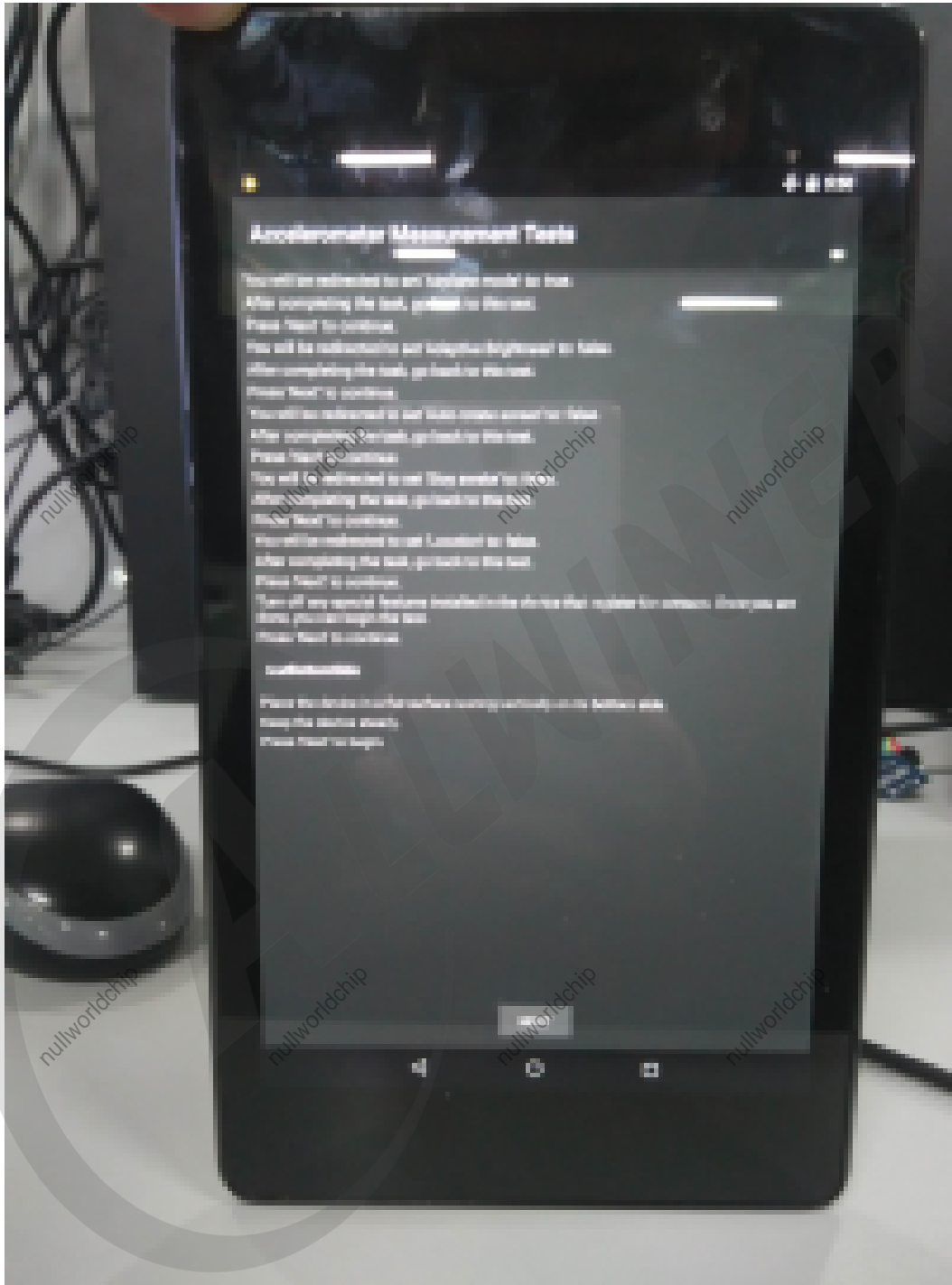


图 48: 平板垂直

3. 点击 Next 按钮，然后迅速将屏幕面向桌面，平放在桌面上，等待测试完毕。这时测试员看不到屏幕，平板会通过一声铃响来通知测试完毕。听到声音后，翻转屏幕，插件测试结果。测试成功后

会显示 PASS。



图 49: 平放在桌面

4. 将平板水平放在桌面，屏幕面向天花板，点击 Next 按钮。测试成功后会显示 PASS。



图 50: 平放面朝上

5. 将平板垂直立在它的左边框，点击 Next 按钮。测试成功后会显示 PASS。

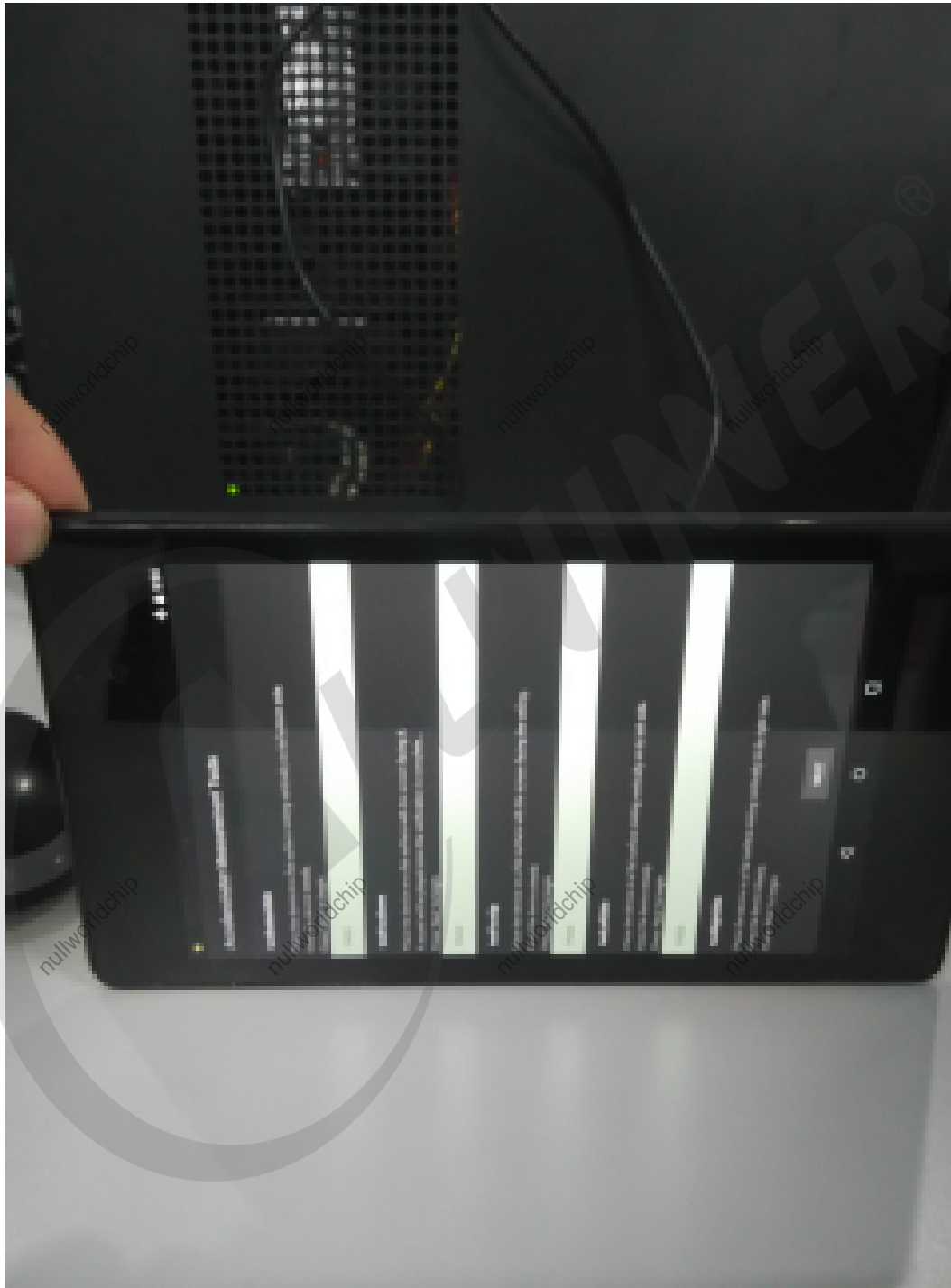


图 51: 垂直在左边

6. 将平板垂直立在它的右边框，点击 Next 按钮。测试成功后会显示 PASS。



图 52: 垂直在右边

7. 将平板垂直立在它的顶边框，点击 Next 按钮。测试成功后会显示 PASS。

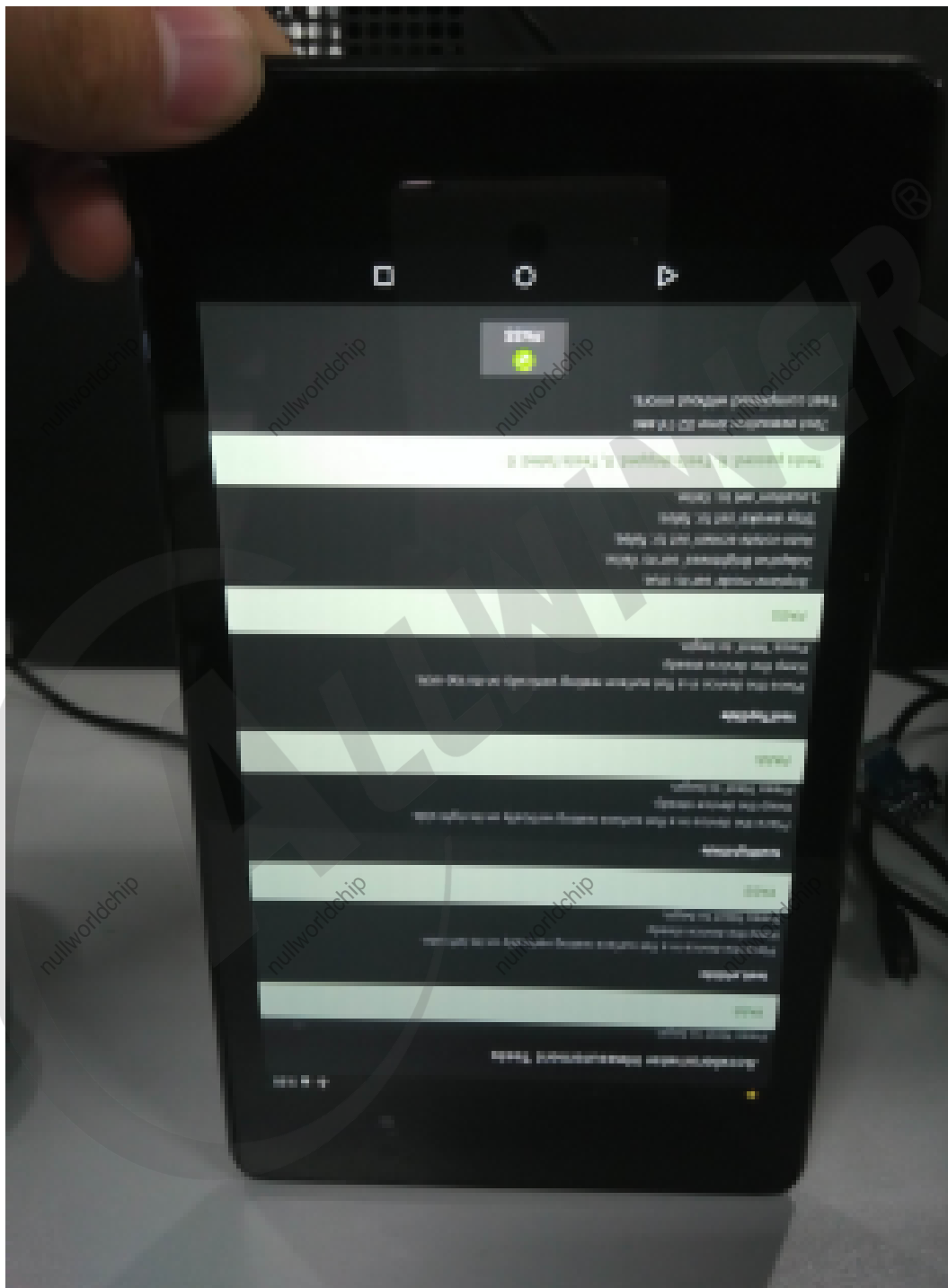


图 53: 垂直倒立

8. 最后恢复测试前的设置（自动亮度，关闭飞行模式等）。上述所有项均通过后可以点击最后的 Next 按钮通过测试。

只要有一项 fail 就会无法继续测试。

4.3.17.3 CTS Sensor Batching Tests

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将平板水平放置在桌面，点击 NEXT 按钮开始测试。这时屏幕会关闭，等待平板测试完毕（测试完毕后平板会发出提示音并自动亮屏）。

亮屏后观察测试结果，一般来说没有特殊说明，所有小项均需要通过测试。如果测试中出现了出错的项目，确认此错误可以忽略，还可以点击 PASS ANYWAY 按钮通过测试。目前我们使用的传感器均不具备 batch 功能，所以不会测试此项。

4.3.17.4 CTS Sensor Integration Tests

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将平板水平放置在桌面，点击 NEXT 按钮开始测试。这时屏幕会关闭，等待平板测试完毕（测试完毕后平板会发出提示音并自动亮屏）。亮屏后观察测试结果，一般来说没有特殊说明，所有小项均需要通过测试。如果测试中出现了出错的项目，确认此错误可以忽略，还可以点击 PASS ANYWAY 按钮通过测试。

4.3.17.5 CTS Sensor Test

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将平板水平放置在桌面，点击 NEXT 按钮开始测试。这时屏幕会关闭，等待平板测试完毕（测试完毕后平板会发出提示音并自动亮屏）。亮屏后观察测试结果，一般来说没有特殊说明，所有小项均需要通过测试。如果测试中出现了出错的项目，确认此错误可以忽略，还可以点击 PASS ANYWAY 按钮通过测试。

4.3.17.6 CTS Single Sensor Tests

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将平板水平放置在桌面，点击 NEXT 按钮开始测试。这时屏幕会关闭，等待平板测试完毕（测试完毕后平板会发出提示音并自动亮屏）。亮屏后观察测试结果，一般来说没有特殊说明，所有小项均需要通过测试。如果测试中出现了出错的项目，确认此错误可以忽略，还可以点击 PASS ANYWAY 按钮通过测试。

4.3.17.7 Devices Suspend Tests

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将点击 NEXT 按钮开始测试。拔掉 USB 连接，关屏进入延迟模式，等待平板测试完毕（测试完毕后平板会发出提示音并自动亮屏）。亮屏后观察测试结果，一般来说没有特殊说明，所有小项均需要通过测试。如果测试中出现了出错的项目，确认此错误可以忽略，还可以点击 PASS ANYWAY 按钮通过测试。

4.3.17.8 Dynamic Sensor Discovery Test

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务，点击 NEXT，就直接出结果了，可能会提示传感器不支持，具体看设备有没有传感器，没有，直接 PASS。

4.3.17.9 Event sanitization for idle UID test

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将点击 NEXT 按钮开始测试。执行 Shell 命令 `adb shell cmd sensorservice set-uid-state com.android.cts.verifier idle` 来模拟被闲置的 ctsverizer UID，点击 NEXT 按钮继续，等到听到声音之后，执行 Shell 命令 `adb shell cmd sensorservice set-uid-state com.android.cts.verifier` 来停止模拟被闲置的 ctsverizer UID，点击 NEXT 按钮恢复设置，点击 PASS。

4.3.17.10 Off Body Sensor Test

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将点击 NEXT 按钮开始测试。当屏幕提示测试无错误的完成即可点击 PASS。

4.3.17.11 Sensor Batching Manual Test

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将点击 NEXT 按钮开始测试，根据提示，在机器面前挥动你的手。然后，点击 NEXT 按钮，拿着设备走路。点击 NEXT 按钮恢复设置，点击 PASS。

4.3.17.12 Significant Motion Tests

进入测试界面后按照提示启动飞行模式，关闭屏幕自动调节亮度，关闭屏幕自动翻转，去掉 Stay Awake 选项，关闭位置服务。所有需要关闭的 sensor 均关闭后，将点击 NEXT 按钮开始测试。当屏幕提示测试无错误的完成即可点击 PASS。

4.3.18 STREAMING

4.3.18.1 Steaming Video Quality Verifier

该项测试需要连接 WiFi，并且是香港网络，然后点击里面的每一个小项，就会加载视频和播放视频，如果网络不好，视频加载时间比较长，需要耐心等待。如果能播放，则 PASS。

4.3.18.2 Tile Service Test

第一个自动 PASS, 打开快速设置 setting>Accessibility 确 Dummy accessibility service 为 off, 返回第二个 PASS; 打开快速设置并单击自定义设置，检查是否可以添加 CTS Verifier 的 service, PASS。

5. 搜集测试结果

测试完毕后，Verifier 测试软件可以生成测试报告。

软件生成的测试报告查看麻烦，如果需要自己出测试结果报告，请手动记下各项 FAIL 项统计结果。

点击右上角的眼睛图案可以浏览目前的测试结果。

点击右上角的存盘图案可以将当前测试报告保存到 `sdcard` 中。路径为 `/sdcard/ctsVerifierReports/`。通过 MTP 一般看不到测试报告，可以通过 `adb pull` 命令取出测试报告。androidQ 之后的版本，可能需要输入 `adb shell appops set com.android.cts.verifier android:read_device_identifiers allow`

测试报告的文件名较长，可以先进入 `/sdcard/ctsVerifierReports/` 目录，通过 `ls` 命令取得文件名，然后取出对应的测试报告，当然也可一次将 `/sdcard/ctsVerifierReports/` 中的所有文件取出。命令：`adb pull /storage/emulated/0/verifierReports/2020.02.13_13.37.38-CTS_VERIFIER-Allwinner-ceres_b3-ceres-b3-QP1A.191105.004.zip D:\verifier_report`

6. Declaration

This document is the original work and copyrighted property of Allwinner Technology (“Allwinner”). Reproduction in whole or in part must obtain the written approval of Allwinner and give clear acknowledgement to the copyright owner. The information furnished by Allwinner is believed to be accurate and reliable. Allwinner reserves the right to make changes in circuit design and/or specifications at any time without notice. Allwinner does not assume any responsibility and liability for its use. Nor for any infringements of patents or other rights of the third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Allwinner. This document neither states nor implies warranty of any kind, including fitness for any particular application.