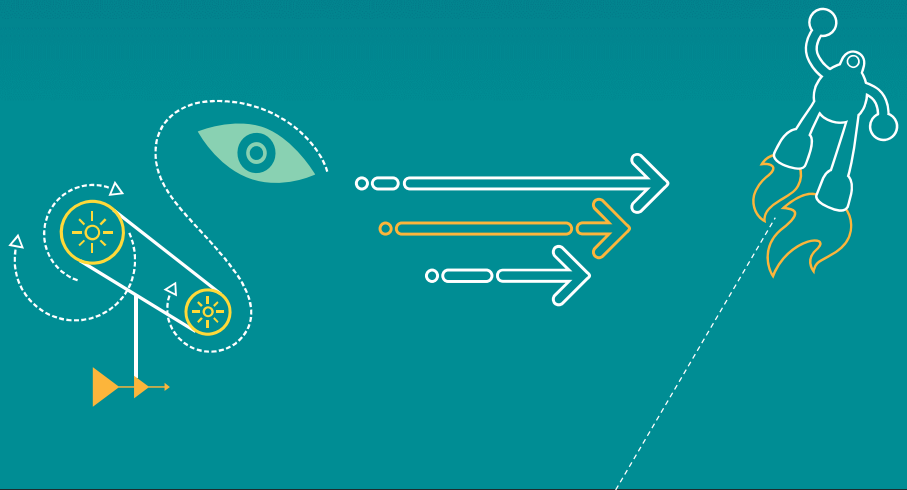
高通Lab Test技术期刊 – 201603

Qualcomm Technologies, Inc.



Confidential and Proprietary – Qualcomm Technologies, Inc.

Qualcomm Technologies, Inc. 5775 Morehouse Drive San Diego, CA 92121 U.S.A.
高通技术股份有限公司，美国加利福尼亚州圣地亚哥市莫豪斯路 **5775** 号，邮编 **92121**

Revision History

Revision	Date	Description
A	Mar 2016	Initial release

Note: There is no Rev. I, O, Q, S, X, or Z per Mil. standards.

Contents

CMCC: How to Test NS-IoT Case TC5.1.21

- Background
  - Spam messages sent by malicious base station brought lots of trouble to people's daily life. It also brought side effect to the carrier.
  - To evaluate UE's behavior under malicious base station, TC7.1.21 "Integrity protection of AS signaling" and TC5.1.22 "Integrity protection of NAS signaling" was required by CMCC during the NS-IoT test.
  - More specifically, TC5.1.21 is designed to verify that the UE supports AS integrity algorithm eia1~eia2. But for eia0(reserved) or spare1~spare5, UE will refuse the integrity procedure. UE receives an Security Mode Command message by eia0(reserved) or spare1~spare5, UE will transmit a Security Mode Failure message.
  - For EIA0, it is only allowed for unauthenticated emergency calls according to 3GPP TS33.401. If such unauthenticated emergency call is not a regulatory requirement, EIA0 should be disabled in MME and eNB.
- Issue Description
  - At step9, SS transmits a SecurityModeCommand message with EIA0 to activate AS security, and expects UE replies security mode failure. But it's observed some UE replied security mode complete as eia0_allowed was configured.

CMCC: How to Test NS-IoT Case TC5.1.21

- Log Analysis

//Step 9: TE sends Security Mode Command with integrity protection algorithm EIA0

16:23:37.149 EVENT_LTE_RRC_DL_MSG DL Channel Type = DL DCCH, Message Type = Security Mode Command

2010 Apr 15 16:23:37.149 [CE] 0xB0C0 LTE RRC OTA Packet -- DL_DCCH / SecurityModeCommand

```
…
        {
          cipheringAlgorithm eea0,
          integrityProtAlgorithm eia0-v920
        }
…
```

//EIA0 is allowed by UE via EFS

16:23:37.149 lte_rrc_sec.c 3536 H RRC SEC: Received RRC Security Mode Command DLM
16:23:37.149 lte_rrc_sec.c 2345 H RRC SEC:**EIA0 is allowed from EFS**
16:23:37.149 lte_rrc_sec.c 2401 H RRC SEC:Null integrity is valid: Integrity algo = 0, Ciphering algo = 0

//As a result, security mode complete msg is sent by UE

16:23:37.150 lte_rrc_sec.c 3190 H RRC SEC: Sent RRC Security Mode Complete message
16:23:37.150 EVENT_LTE_RRC_UL_MSG UL Channel Type = UL DCCH, Message Type = Security Mode Complete
16:23:37.150 EVENT_LTE_RRC_SECURITY_CONFIG Status = Success

- Solution:
  - Delete EFS /nv/item_files/modem/lte/rrc/sec/eia0_allowed.

CMCC: Common Issues for TDSCDMA RRM Case TC4.3.8.8

- Issue Description
  - For TDS RRM test case 4.3.8.8, GSM and TD-SCDMA cells are active simultaneously when UE is switched on. If UE camped on GSM network first, this case will become inconclusive.
- Issue analysis:
  - Issue #1: GSM has higher priority than TD-SCDMA in EFS /sd/rat_acq_order

// sys_mode 3 (GSM) with highest priority in RAT priority list

```
05:28:13.306  reg_state.c  9174  H  DS: SUB 1 =REG= CM_SERVICE_REQ
05:28:13.306  reg_state.c  1928  H  DS: SUB 1 =REG= Rat priority list num_items = 3

05:28:13.306  reg_state.c  1933  H  DS: SUB 1 =REG= sys_mode = 3 bst_rat_acq_required = 1
05:28:13.306  reg_state.c  1951  H  DS: SUB 1 XXX rat list contain GSM
05:28:13.306  reg_state.c  2000  H  DS: SUB 1 =REG= band_cap = 82313600
05:28:13.306  reg_state.c  2003  H  DS: SUB 1 =REG= bst_band_cap = 2621824
```

// sys_mode = 5 represents UMTS

```
05:28:13.306  reg_state.c  1933  H  DS: SUB 1 =REG= sys_mode = 5 bst_rat_acq_required = 1
05:28:13.306  reg_state.c  1946  H  DS: SUB 1 XXX rat list contain UMTS
05:28:13.306  reg_state.c  2000  H  DS: SUB 1 =REG= band_cap = 82313600
05:28:13.306  reg_state.c  2003  H  DS: SUB 1 =REG= bst_band_cap = 79691776
```

// sys_mode = 11 represents TD-SCDMA

```
05:28:13.306  reg_state.c  1933  H  DS: SUB 1 =REG= sys_mode = 11 bst_rat_acq_required = 1
```

// UE send registration request on highest priority network GSM, test case fail

```
05:28:13.310  reg_sim.c    4284  H  DS: SUB 2 =REG= LAST RPLMN RAT UNDEFINED
05:28:13.310  reg_send.c   1668  H  DS: SUB 2 =REG= MMR_REG_REQ PLMN(466-2) RAT(GSM)
```

CMCC: Common Issues for TDSCDMA RRM Case TC4.3.8.8

- Issue #2: PLMN(466-02) is not added into EFS tdscdma_op_plmn_list

//After power on, UE searches TDSCDMA firstly according to rat_acq_order setting

```
00:08:21.597  dsatcmdp.c   1542   H   ATCoP Operating mode = 0, Present mode = 3, Qcsimapp = 0
00:08:21.597  dsatcmdp.c   1624   H   Command Name +cfun Op = 0xb
00:08:21.597  dsatcmdp.c   1628   H   arg[0] = 1

00:08:21.598  cmph.c       44022  H   =CM= TOT: num_rat : 4
00:08:21.598  cmph.c       44026  H   =CM= TOT: acq_sys_mode[0] = 9
00:08:21.598  cmph.c       44026  H   =CM= TOT: acq_sys_mode[1] = 11
00:08:21.598  cmph.c       44026  H   =CM= TOT: acq_sys_mode[2] = 3
00:08:21.598  cmph.c       44026  H   =CM= TOT: acq_sys_mode[3] = 5


00:08:21.622  reg_send.c   1566   H   ds1=REG= MMR_REG_REQ PLMN(0-0) RAT(TDSCDMA)
00:08:21.624  mmrrcconn.c  1291   H   ds1MM sent TDSRRC_SERVICE_REQ
```

//tdscdma_lab_op_plmn_list is not configured, UE stay in limited service state

```
00:08:22.541  tdsrrccsp.c  32917  H   Reporting Freq: 10062, CPID: 0, PLMN: 466-2, LAC: 0x79,0x1a to
registered call back functions.

00:08:22.542  reg_nv.c     962    H   ds1=REG= Read RPLMN  ff ff ff from cache
00:08:22.542  reg_send.c   667    H   ds1=REG= CM_SERVICE_CNF
00:08:22.542  reg_state.c  8623   H   ds1=REG= LIMITED_SERVICE on VPLMN(466-2)

00:08:28.721  reg_sim.c    3590   H   ds1=REG= CS RPLMN(466-2)
00:08:28.721  reg_sim.c    3645   H   ds1=REG= Stored RPLMN(466-2)
```

//Later UE search RPLMN with RAT GSM, leading to test case fail

```
00:08:28.723  reg_send.c   1560   H   ds1=REG= MMR_REG_REQ PLMN(466-2) RAT(GSM)
00:08:33.878  EVENT_SMGMM_REQUEST_SENT  Request Message ID = Attach Request, Request Type = 3
```

CMCC: Common Issues for TDSCDMA RRM Case TC4.3.8.8

- Issue #3: Network mode is changed to GSM only after at+cfun=0

// AT + CFUN = 0, mode_pref of subscription 1 is 62, which contains TDS and GSM

```
06:40:49.278  dsatcmdp.c  1306   H   Command Name +cfun Op = 0xb
06:40:49.278  dsatcmdp.c  1310   H   arg[0] = 0
06:40:49.278  cm.c        7797   H   =CM= cm_ph_cmd_oprt_mode(), mode=6
06:40:49.686  dsatrsp.c   310    H   Command output OK

06:40:49.730  cmph.c      16013  H   =CM= DSDX: ds1 mode_pref=62
06:40:49.730  cmph.c      16013  H   =CM= DSDX: ds2 mode_pref=13
```

//Then AP set mode_pref to GSM only(13) for subscription 1 after at+cfun=0

2015 Dec 27 06:40:50.562 [FF] 0x1390 QMI Link 2 RX PDU

```
IFType = 1
QmiLength = 17
QmiCtlFlags = 0
QmiType = NAS
Service_Nas {
ClientId = 2
SduCtlFlags = REQ
MsgType = QMI_NAS_SET_SYSTEM_SELECTION_PREFERENCE
MsgLength = 5
QmiNasSetSystemSelectionPreference {
QmiNasSetSystemSelectionPreferenceReqTlvs[0] {
Type = 17
Length = 2
Mode Preference tlv {
mode_pref = GSM
}

06:40:50.567  cmph.c      16013  H   =CM= DSDX: ds1 mode_pref=13
06:40:50.567  cmph.c      16013  H   =CM= DSDX: ds2 mode_pref=13
```

CMCC: Common Issues for TDSCDMA RRM Case TC4.3.8.8

// AT + CFUN = 1

```
06:41:12.779  dsatcmdp.c   1306   H   Command Name +cfun Op = 0xb
06:41:12.779  dsatcmdp.c   1310   H   arg[0] = 1
06:41:12.779  cm.c         7797   H   =CM= cm_ph_cmd_oprt_mode(), mode=5
06:41:12.780  cmph.c       17327  H   =CM= go online cdma 0, gwl 0
06:41:12.780  cmph.c       17331  H   =CM= go online hybr_gw 0, hybr_gw3 0
06:41:12.780  cmph.c       17514  H   =CM= LPM to ONLINE. ph_ptr PLMN and CSG ID reset
```

// UE request the GSM only service because mode pref is 13 GSM only

```
06:41:12.788  sdcmd.c      5199   H   =SD= srv_req_type-2
06:41:12.788  sdss.c       19259  H   =SD= ACQ_GWL: sys_mode = 3 band_cap = 0x0 0x280180
06:41:12:788,sdss.c        19272  H   =SD= ACQ_GWL, sel_type=2 domain=2 srv_req_type=2
```

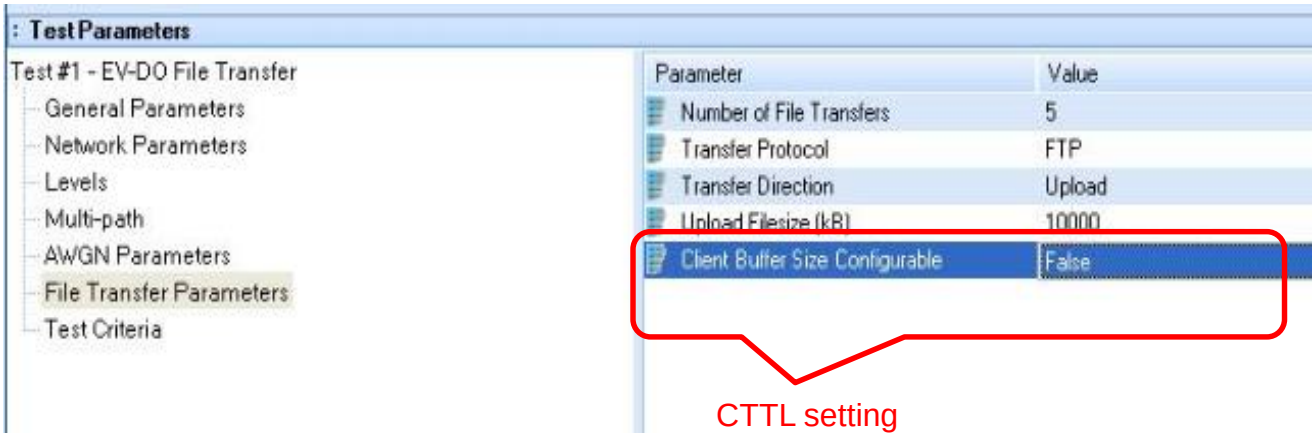
//UE register with GSM before AP change the mode_pref back , test case fail

```
06:41:12.823  reg_send.c   1560   H   ds1=REG= MMR_REG_REQ PLMN(466-2) RAT(GSM)
06:41:13.078  EVENT_SMGMM_REQUEST_SENT   Request Message ID = Attach Request, Request Type = 3
```

- Summary:
  - To avoid the network selection issue for TDS RRM test case TC4.3.8.8, please make sure below UE configuration is correct:
    - TDSCDMA is higher than GSM in EFS /sd/rat_acq_order.
    - PLMN(466-02) is added into EFS /nv/item_file/modem/nas/tdscdma_op_plmn_list.
    - AP will not change network selection preference during the test, especially after at+cfun=0.

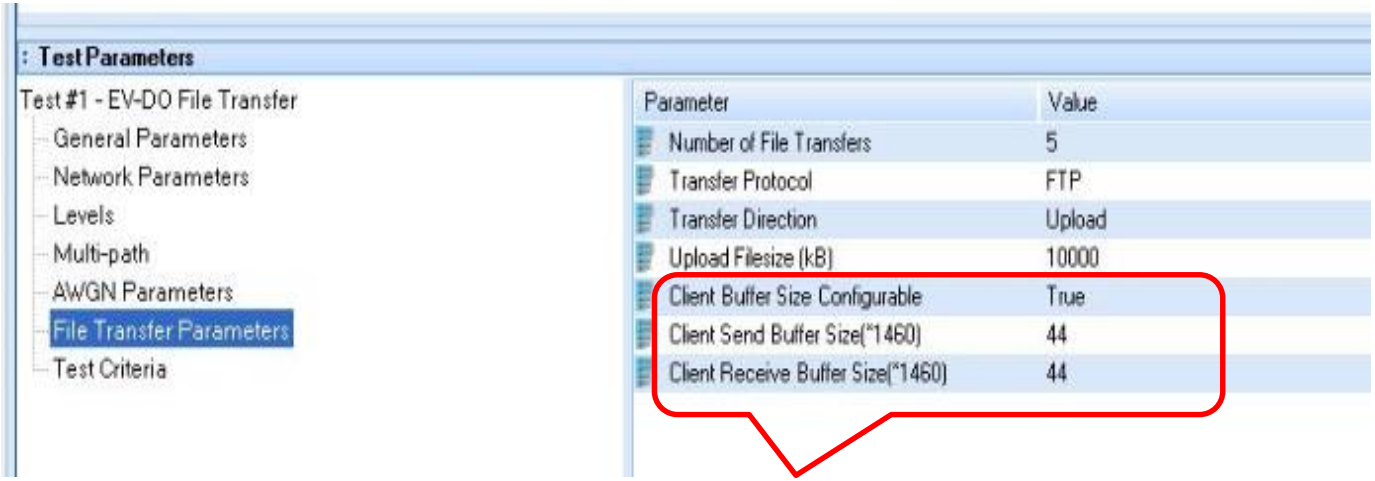
CT: EVDO Throughput Case TC-DORA-01006 Failed in CTTL Lab

- Issue Description
  - Some OEMs report EVDO throughput case TC-DORA-01006 failure in CTTL, but the same device can pass the case in QC lab. We found the throughput test suite CTTL used is too old, QC and CT had update the test suite from 2012 to fix the issue.
- Solution
  - Need modify the ***client send buffer size*** **configuration** on Spirent TE side to pass this case, please refer to below for detail:
    - The default setting in CTTL, which is incorrect



CT: EVDO Throughput Case TC-DORA-01006 Failed in CTTL Lab

- The correct setting used in QC lab



QC lab setting

CT: Inter-RAT/eHRPD Test – Data Call isn't Initiated on HRPD

- Issue Description
  - During recent CT inert-RAT, eHRPD test, while UE doing inter-RAT from LTE or eHRPD to HRPD on Android M device, it is always observed that UE not initiates data call on HRPD.
  - some CT inter-RAT cases (such as TC05002, TC05005, TC05006, TC11001) and CT eHRPD test cases (TC35001 and TC01002 etc) may fail owing to this.
- Log Analysis:

//CT inter-RAT case TC05002. QXDM log, PS iface is down

MSG DS 3GPP/High 07:52:06.639 ds_3gpp_bearer_context.c 09326 Posting CLR_PENDING_REDIAL_CMD to DS task
MSG Data Services/Medium 07:52:07.300 ds_dsd_pref_sys.c 00767 Pref sys changed. Notify

EVENT EVENT_DS_EPC_PDN 07:52:10.023 EPC IFace Instance = 0, PDN IP Type = V4 Only, Call Type = V4, PDN State = Down, Data Serving System = HRPD, SRAT IFace Name = Invalid, SRAT IFace Instance = 0, TRAT IFace Name = Invalid, TRAT IFace Instance = 0, APN = ctnet

MSG Data Services/Medium 07:52:10.002 ds_dsd_pref_sys.c 00767 Pref sys changed. Notify
MSG DS 3GPP/High 07:52:10.006 ds_3gpp_pdn_context.c 04209 **Tearing down PDN context**

MSG DS 3G Manager/High 07:52:10.014 ds3gcmif.c 04115 Rx'ed CM_CALL_END_CMD
MSG DS 3GPP/High 07:52:10.016 ds_3gpp_auth_mgr.c 01013 ds_3gpp_auth_mgr_call_failure: Not an auth fallback scenario. APN: ctnet, requested_auth_type: 0, cause_code: 197636
MSG DS 3GPP/High 07:52:10.016 ds_3gpp_pdn_redial_hdlr.c 00410 Read auth_type 0 from profile
MSG DS 3GPP/High 07:52:10.016 ds_3gpp_auth_mgr.c 00763 ds_3gpp_auth_mgr_need_redial: No redial. APN: ctnet, requested_auth_type: 0, cause_code: 197636
MSG DS EPC/High 07:52:10.020 ds_epc_pdn_meta.c 00661 EPC DOWN hdlr: EPC_IFACE 0x8880:0

CT: Inter-RAT/eHRPD Test – Data Call isn't Initiated on HRPD

//ADB log

//PS attached on LTE, data call setup

12-18 07:50:26.807 4569 4691 D RILJ : [3897]< DATA_REGISTRATION_STATE {1, null, 00000001, 14, null, 20, 1, 0, 1, null, null} [SUB0]
12-18 07:50:27.119 4569 4728 D RILJ : [3905]> SETUP_DATA_CALL 16 0 ctnet 0 IPV4V6 [SUB0]
12-18 15:50:27.450 4569 4691 D RILJ : [3905]< SETUP_DATA_CALL DataCallResponse: {version=11 status=0 retry=-1 cid=0 active=2 type=IPV4V6 ifname=rmnet_data0 mtu=1500 addresses=[192.168.9.1/30] dnses=[] gateways=[192.168.9.2] pcscf=[]} [SUB0]

//PS switched to DO, data calls reset

12-18 07:52:09.979 4569 4691 D RILJ : [3964]< DATA_REGISTRATION_STATE {1, null, null, 8, null, 20, null, null, null, null, null} [SUB0]
12-18 07:52:10.035 4569 4569 D QtiCdmaDCT: [0]onUpdateIcc: tryRestartDataConnections nwTypeChanged
12-18 07:52:10.065 4569 4728 D RILJ : [3966]> DEACTIVATE_DATA_CALL 0 0 [SUB0]

//Dun call request, dun data call is blocked as there is no matching dun apn found

12-18 07:52:11.301 4569 4569 D QtiDctController: [TNF 1]Cellular needs Network for NetworkRequest [id=7, legacyType=4, [Transports: CELLULAR Capabilities: DUN&TRUSTED&NOT_VPN]]
12-18 07:52:11.330 4569 4569 D QtiCdmaDCT: [0]trySetupData for type:dun due to dataEnabled apnContext={mApnType=dun mState=IDLE mWaitingApns={null} mWaitingApnsPermanentFailureCountDown=0 mApnSetting={null} mReason=dataEnabled mDataEnabled=true mDependencyMet=true}

12-18 07:52:11.363 4569 4569 D QtiCdmaDCT: [0]trySetupData: X No APN found retValue=false

//Default data call request blocked as dun call request is higher priority

12-18 07:52:13.055 4569 4569 D QtiCdmaDCT: [0]**trySetupData for type:default** due to nwTypeChanged apnContext={mApnType=default mState=IDLE mWaitingApns={[[ApnSettingV3] China Telecom, 1147, 46003, ctnet, , , , , , 3, default | hipri | ia, IPV4V6, IPV4V6, true, 0, 0, 0, false, 0, 0, 0, 0, ,]} mWaitingApnsPermanentFailureCountDown=1 mApnSetting={[ApnSettingV3] China Telecom, 1148, 46011, ctnet, , , , , , -1, default | hipri | ia, IPV4V6, IPV4V6, true, 0, 0, 0, false, 0, 0, 0, 0, , } mReason=nwTypeChanged mDataEnabled=true mDependencyMet=true}

12-18 07:52:13.065 4569 4569 D QtiCdmaDCT: [0]setupData: **Higher priority ApnContext active. Ignoring call**

CT: Inter-RAT/eHRPD Test – Data Call isn't Initiated on HRPD

- From the above log, default data call was setup on LTE initially. Later when PS got switched to DO, there are two data call requests, one for dun (tethering enbled, which is required by CT test), and the other for default.
- As single pdn arbitration is enabled for HRPD (**only one data call allowed at a time**), and dun data call has higher priority, default data call is not setup. And dun data call is not setup as there is no matching APN found.

- Solution
  - For **Android L** release, settings.db is used to disable DUN tethering:

```
adb shell ->
cd /data/data/com.android.providers.settings/databases
sqlite3 settings.db
select * from secure;
insert into secure (name,value) values ('tether_dun_required', '0');
select * from global;
insert into global (name,value) values ('tether_dun_required', '0');
```

  - For **Android M** release, the setting is changed, please use below command:

```
adb shell settings put global tether_dun_required 0
```

80-P5399-1: Lab Conformance Test Guide

- Document 80-P5399-1 “Lab Conformance Test Configuration and Execution Guide” is released in QC CreatePoint system.
- This document is to guide OEMs to check the UE and PICS/Pixit setting for certification test, such as GCF, PTCRB. We also list test cases which are often failed because of wrong configuaration or operation.
- OEMs can do self-checking once meet such failures and try the recommended solution as debugging purpose.

CTA: Solution #00030145 - "How to Enable MIIT Security Feature?"

- MIIT Security feature is mandatory for China Market. To enable this feature, please follow below command:

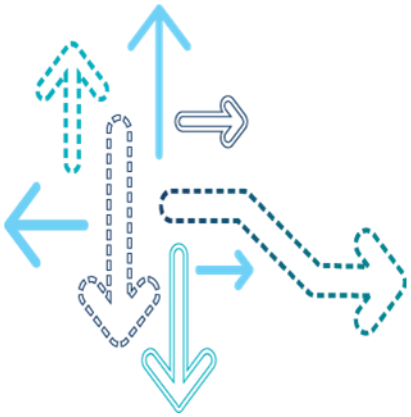
  setprop persist.sys.strict_op_enable true

- Please check if OEM can find the below path from the build. If it can be found, then the build supports **MIIT Security Level 5**. If not, it only supports **MIIT Security Level 3**.

  \vendor/qcom/proprietary/SecProtect

References

Documents	
Qualcomm Technologies, Inc.	
Title	DCN
Lab Conformance Test Configuration and Execution Guide	80-P5399-1 A
高通Lab Test技术期刊--201509	/
高通Lab Test技术期刊--201510	/
高通Lab Test技术期刊--201511	/
高通Lab Test技术期刊--201512	/
高通Lab Test技术期刊--201601	/
高通Lab Test技术期刊--201602	/



Questions?

https://support.cdmatech.com