Test Toolkit Events for eSIM / iSIM

June 2021

Qualcomm

Confidential and Proprietary - Qualcomm Technologies, Inc.

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

Content

- Initial LS from GSMA eSIMTEST to CT6 and the reply LS
- 3GPP CT WG6 Work Item for devices with eSIM or iSIM
- Why do we need Test Events?
- Limitations in TC modifications (implicit verification)
- Test Events for 3GPP 31.121 test cases
- Security aspects of Test Events
- Can Test Event support exist in Commercial cards?
- Current status of Test Events verification
- Development of Test Systems for devices with eSIM or iSIM
- Why do we still need Test modification (implicit verification)?
- Next step
- Backup slides

Initial LS from GSMA eSIMTEST to CT6 and the reply LS

- Initial LS from GSMA to CT6 (TSG LS to 3GPP and ETSI regarding 3GPP 31 130 v2.docx)
  - eSIMTEST requested additional three EVENTs be defined in 3GPP 31.130 to enable Conformance testing on devices with eSIM using TS.48 Generic Test Profile.
- Reply LS from CT6 (C6-200618_Reply LS to GSMA regarding 3GPP TS 31.130 specification final.docx)
  - For a non-removable solution, a black box approach seems to be more appropriate
  - 3GPP CT WG6 is investigating the possibility to modify the test specifications, introducing different versions of test cases.

3GPP CT WG6 Work Item for devices with eSIM or iSIM

- WI (C6-210062) was created to develop a new test specification to include new test methods required for devices with eSIM or iSIM.
  - Exiting device conformance test systems are limited to devices with removable SIMs only.
- New test methods shall enable
  - an implicit verification of 3GPP requirements at Network simulator end and
  - alternative verification methods using the Test Toolkit Events at eSIM or iSIM end when specified and available in ETSI Java API specifications.

- Refer to back up slides for the details of two Test Toolkit Events.

Why do we need Test Events?

- New CT6 WI will focus on implicit verification of test requirements by modifying the TCs in the new specification. However,
  - All the GCF/PTCRB test requirements will not be able to verify even if TCs are modified.
    > Some of the GCF/PTCRB test requirements will be removed when implicit verification is not possible for certain requirements.
  - Correctness of ADPUs send by the Terminal that is essential for UICC testing but it will never be verified.
  - Unable to assure if data is read from the device memory (from a copy of the files in eSIM) or from the eSIM
- MNOs may face field issues on GCF/PTCRB certified devices due to lack of original test requirements in the new specifications.
- Without an entity owned by test system loaded on to the eSIM, verification of the interface between Terminal and eSIM can’t be trusted.
- Above points will raise concerns on the test methods used for devices with eSIM.
- The alternative test method with proposed Test Toolkit Events can be used to verify all the GCF/PTCRB USIM requirements without removing any existing Conformance Requirements.

Limitations in TC modifications (implicit verification)

- Unable to verify correctness of the content and the format of the APDUs sent by the ME.
- Verification of APDU content has been an important requirement for USIM / USAT testing. That is the main difference between 3GPP USIM / USAT testing and 3GPP Protocol testing (RAN).
- Most of the 3GPP NW interface requirements are tested in 3GPP Protocol testing. 3GPP USIM TCs verify similar core requirements but focus on SIM interface verification. If APDU verification is removed from 3GPP USIM test cases it will verify only the NW interface as tested in 3GPP Protocol TCs.
- READ BINARY of EF-UST can't be verified using implicit verification methods for many TCs.
  - Only the SUCI calculation related bits can be verified by the test system implicitly.
  - SUCI calculation may have to be verified in many TCs (non-SUCI TCs) unnecessarily.
  - Read of this EF can't be verified for SUCI TCs.
- EF-SQN is not a standard elementary file and it may not be available in all the SIMs. Also, EF-SQN verification shall be disabled for RAN5 TCs while EF-SQN update is enabled for USIM Tests (implicit verification).
  - EF-SQN can't be used for verifying AUTHENTICATE APDUs implicitly.

Test Events for 3GPP 31.121 test cases

- Test Toolkit Events can be used to verify all the GCF/PTCRB USIM requirements in 3GPP 31.121 without removing any existing Conformance Requirements.
- However, Toolkit Events and Handlers already defined in ETSI 102.241 would be sufficient for verifying Toolkit (USAT) requirements in 3GPP 31.124 specifications. A very minimum modification is required for 5G test cases in 3GPP 31.124.
  - SETUP EVENT LIST proactive command should be considered as an initial condition in test procedure (to verify ENVELOP commands).
- Proposed Test Events for 3GPP 31.121 can prove device has really read the data from eSIM and not from the device's own memory.
- Test Toolkit Applets will be owned by the Test System, and it shall be compliant with ETSI 102.241 / 3GPP 31.130.
  - Implicit verification or Test Toolkit Events based verification is required for 3GPP 31.121 test cases only.
  - Standard Toolkit Events and Handlers shall be used for 3GPP 31.124 test cases with eSIM.
  - Hence new test systems supporting eSIM or iSIM shall include Toolkit Test Applet based solutions irrespective of the choice for 3GPP 31.121.
- Irrespective of the new Toolkit Test Events requirements for test cases in 3GPP 31.121, Test Applet Based solution will be required for USAT test cases in 3GPP 31.124. Hence it is appropriate for Test Systems to use same Test Applet with new Test Events for the test cases in 3GPP 31.121.
- Reference .java Test Applet code and reference uicc.toolkit.test libraries are already available for Test Applet based Test System implementation.

Security aspects of Test Events

- As per Qualcomm proposal in **SCPREQ(21)000002r2**,
  - Event registration for both events will be successful only if the active profile is a test profile. JCRE shall block event registration if the active profile is a commercial profile.
  - Event triggering for both events will be successful only if the active profile is a test profile. JCRE shall block event triggering if the active profile is a commercial profile.
  - Determination of Test Profile is associated with Authentication Keys , Authentication algorithm and IMSI being used.
  - Test Applet installation on commercial cards is protected with Data Encryption Key and other Security Parameters (RC/CC/DS). This is already available in commercial networks.
  - Specifications do not define any response method for applets to trigger a response to an Event it received. Events are for monitoring purpose only.

  Note: A 'Profile' is a combination of a file structure, data and applications on an eSIM. It is referred to the same meaning as the profile referred in REFRESH mode 'eUICC Profile State Change' in section 6.4.7 of ETSI TS 102.223.

- A malicious applet must be installed and then change the Authentication Key (to have a Test Key), Authentication algorithm to Test algorithm or change the IMSI (to have a test IMSI) to receive any of the test specific events.
- Installation of a malicious applet and modifying the authentication parameters is well protected in commercial cards today.
- If those actions are protected and JCRE strictly follows the rules to expose the Test events, new events should not have any impact to commercial cards or commercial applications.

Can Test Event support exist in Commercial cards?

- Since the Test Events registration and triggering will not be successful at JCRE level with Commercial Profiles Test Events support can be enabled in commercial cards if choose to.
- However, card OS vendor can choose other options as well.
- Do not include Test Events support in commercial cards.
  - If tester needs to test a commercial device, then OS Update procedure can be used to have the Test Event support in the commercial device for testing only. Qualcomm verified this method already.
  - If tester knows the device is a test sample, can load the OS with Test events directly.
- If the card OS vendor prefers to have one OS, Test Event support can be disabled in the commercial devices and enable it using the proprietary commands when required.

Current status of Test Events verification

- Proof of Concept for Test Events was completed recently using a removable eSIM with TS.48 profile loaded.
- Proprietary event numbers were used by the card OS for implementing the proposed events.
- Triggering of EVENT_TEST_EXTERNAL_FILE_READ upon receiving READ BINARY command for EF-UST file read from the terminal was verified successfully.
- Triggering of EVENT_TEST_RX_APDU event upon receiving GET IDENITY command and AUTHENTICATE command from the terminal were tested successful as well.
- OS Update procedure was used to update an existing card OS to support the new Test Events.

- **Results from Test Applet during SUCI Calculation by USIM at power up and AUTHENTICATION during 5G REGISTRATION:**

01 51 ---------- *Offsets of TCin and TCout*
00 4D ---------- *Total length of data*

02 02 81 82 ---------- *Destination identity*
12 07 01 3F 00 7F FF 6F 38 ----- *File List (EF-UST)*
22 05 00 B0 00 00 11 ---------- *C-APDU (**READ BINARY** '00 B0 00 00 11')*

02 02 81 82 ---------- *Destination identity*
22 05 80 78 00 01 00 ---------- *C-APDU (**GET IDENTITY** '80 78 00 01 00)*

02 02 81 82 ---------- *Destination identity*
22 28 00 88 08 81 22---------- *C-APDU (**AUTHENTICATE** '00 88 08 81 22 <data> Le')*
10 D5 77 0C 6D 36 3E 30 C3 64 A4 07 8F 1B F8 ED 3A
10 6E 32 24 D6 BF 7B D5 55 D5 76 11 8E 49 2C E3 91
3D

- **Above data verifies the READ BINARY command for EF-UST, GET IDENTITY command and AUTHENTICATE command sent by the Terminal.**

Development of Test Systems for Devices with eSIM

- A reference GCF Test Applet that supports most of the conformance requirements was tested recently. This reference Test Applet is based on GSMA TS.48 guidelines and compliant with ETSI 102.241 and 3GPP 31.130.
- New Test Events with proprietary Event numbers were integrated the same GCF Test Applet and verified those events with a removable eSIM.
- If Test Events are standardized same reference Test Applets can be used with the new uicc.toolkit.test library.

Why do we still need Test modification (implicit verification)?

- All the existing USIM/USAT test requirements in the current specification can be verified if the proposed Toolkit Test Events are standardized.
- However, in some cases support of Test Events may not be possible due to limitations in the device or in the eSIMs.
  - Mobile handsets may not face such limitations as such devices have SIM Toolkit support.
  - Devices used in IoT market may not have SIM Toolkit support.
  - Some of the eSIMs may have memory limitations and unable to support SIM Toolkit Applets.
  - Unable to enable Toolkit Test Event support in commercial devices (OS Update may not be supported).
- In such cases Device Conformance testing shall be done using implicit verification as in new Test specification.
- Hence Test Systems shall support both Test Toolkit Events based TCs and Implicit verification using modified test cases.

Next step

- SCP REQ took an action item (during SCP REQ #86) to organize a joint conference call with SCP TEC, 3GPP CT6 and SCP REQ to agree on the task distribution among the three groups.
  - Since CT6 has already started the WI for creating a new specification SCP will wait for CT6 to make some progress on the WID.
- During C6 #104e session, CT6 included Test Events in the WID with the condition Test Event method can be used when available in ETSI Java API specifications.
- During C6 #106e session, CT6 discussed to update GSMA with current findings and get GSMA recommendation on this matter.
- Requesting GSMA working groups to review the current status and eSIMTEST to send an LS with GSMA recommendation.
- CT6 can work with ETSI SCP in releasing the updated TS 102.241 with proposed two Test Toolkit Events.

Backup slides

Qualcomm

Test Events details

EVENT_TEST_EXTERNAL_FILE_READ

Toolkit Applet shall use registerTestEventFileRead() method to register for this EVENT and shall use deregisterTestEventFileRead() method to deregister this EVENT.

void registerTestEventFileRead (
short fileEvent, byte[] baFileList, short sOffset1, short sLength1, byte[] baADFAid, short sOffset2, byte bLength2)

The CAT Runtime Environment shall trigger all the Toolkit applets registered to this event with the associated read file,

- Upon successful execution of a READ BINARY or READ RECORD APDU command sent by the Terminal to the UICC (External File Read) as defined in 102.221 and
- if the READ command is executed for a file in the registered File List and
- if the active profile is a Test Profile.

An applet shall only be triggered once per command.

When an applet is triggered by the EVENT_TEST_FILE_READ event, the system EnvelopeHandler shall be made available, and shall contain the following COMPREHENSION TLVs (the order of the TLVs given in the system EnvelopeHandler is not specified):

- Device Identity with source set to terminal and destination set to UICC for External File Read as defined in TS 102 223;
- File List, as defined in TS 102 223. The number of files shall be set to one. If a SFI referencing is used in the APDU Command, it shall be converted to its File Identifier;
- C-APDU object as defined in TS 102 223.

Byte(s)	Description	Length
1	C-APDU Tag	1
2	Length	1 or 2
T	C-APDU	T

EVENT_TEST_RX_APDU

Toolkit Applet shall use registerTestEventRxApdu() method with the command specified in the Instruction Code INS to register for this EVENT and shall use deregisterTestEventRxApdu() to deregister this EVENT.

void registerTestEventRxApdu (
short event,
byte[] baInsCode, # INS, Instruction Code as defined in ETSI 102.221
short sOffset1,
short sLength1)

Upon successful execution of the command specified in INS (sent by the Terminal and received by the UICC) as defined in TS 102 221 and if the active profile is a Test Profile, the CAT Runtime Environment shall trigger all the Toolkit applets registered to this event.

An applet shall only be triggered once per command. This event shall be triggered for at least INS=78 (GET IDENTITY) and INS='88' (AUTHENTICATION) and it shall not be triggered for File Management commands (eg: INS='B0, D6, B2, DC, etc') and Toolkit commands (INS='C2, 14, 12').

When an applet is triggered by the EVENT_TEST_RX_APDU event, the system EnvelopeHandler shall be made available, and shall contain the following COMPREHENSION TLVs (the order of the TLVs given in the system EnvelopeHandler is not specified):

- Device Identity with source set to terminal and destination set to UICC, as defined in TS 102 223;
- C-APDU object as defined in TS 102 223.

Byte(s)	Description	Length
1	C-APDU Tag	1
2	Length	1
T	C-APDU	T

Rules for identifying a Test Profile

- ‘Profile’ is a combination of a file structure, data and applications on an eSIM. It is referred to the same meaning as the profile referred in REFRESH mode ‘eUICC Profile State Change’ in section 6.4.7 of ETSI TS 102.223.
- A Test Profile in an eSIM can be identified by JCRE using rules listed below. If any of the rule matches JCRE shall consider the active profile as a Test Profile.
  - Key(s) for network authentication is '00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F' (default K value of Test USIM as defined in Section 8.2 of 3GPP TS 34.108).
  - Key(s) for network authentication has all bits except the lowest 32 bits set to zero.
  - The network authentication algorithm is the Test Algorithm as defined in Section 8.1.2 of 3GPP TS 34.108.
  - The IMSI value complies with the Test USIM IMSI defined in 3GPP TC 31.121, 3GPP TS 31.124 and in section 8.3.2.2 of 3GPP TS 34.108.

NOTE: A live commercial network would never use a key with so little entropy.